Lesson 1: What is Blockchain?

Module A: Blockchain Foundations

MSc Blockchain & Cryptocurrency

Digital Finance Program

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Define blockchain as a cryptographically-secured distributed ledger
2. Trace the historical evolution from 1991 to 2025
3. Explain the double-spending problem and its consensus-based solution
4. Formalize the hash chain structure: $H(B_n) = H(\text{header}_n || \text{prev_hash}_{n-1})$
5. Compare centralized, decentralized, and distributed architectures

Prerequisites: Cryptographic hash functions, basic probability theory

---

MSc level: Full mathematical rigor expected in subsequent slides

The Problem: How can strangers transact without intermediaries?

The Challenge
In digital systems, any file can be copied infinitely. How do we create digital scarcity for money without a central authority to track ownership?

Why It Matters

- Without a solution, digital cash can be spent multiple times (double-spending)
- Pre-Bitcoin e-cash systems (DigiCash, 1990s) required central trust — defeating decentralization

What We Need

- Trustless verification mechanism
- A way to prevent spending the same coin twice without a central ledger

The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How blockchain addresses the double-spending challenge

Formal Definition of Blockchain

Mathematical Definition
A blockchain $\mathcal{B}$ is an ordered sequence of blocks:

$$\mathcal{B} = (B_0, B_1, \ldots, B_n)$$

Where each block B_i contains:

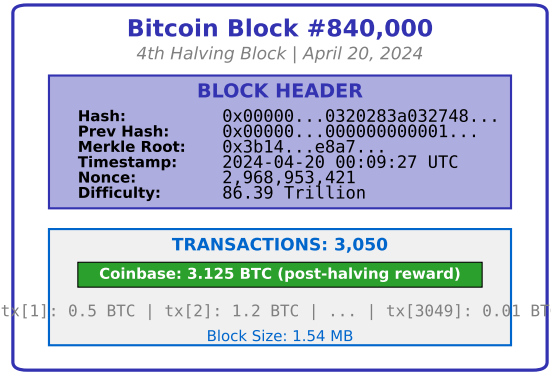
- Header h_i with metadata (version, timestamp, nonce, difficulty)
- Transaction set $T_i = \{tx_1, \ldots, tx_k\}$
- Hash pointer to previous block: $H(B_{i-1})$

Integrity Constraint:

$$\forall i > 0 : B_i.\text{prev} = H(B_{i-1})$$

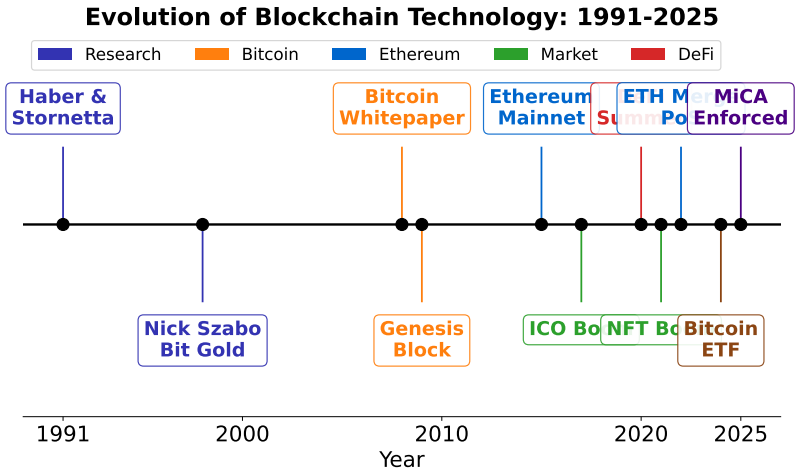
The hash pointer creates a tamper-evident linked data structure

Anatomy of a Blockchain Block



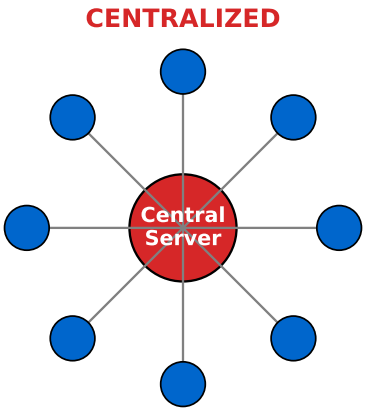
Bitcoin block header: 80 bytes — Block body: 1-2 MB of transactions

Historical Evolution: 1991–2025



Key inflection points: 2008 (Nakamoto), 2015 (Ethereum), 2024 (Bitcoin ETFs)

Centralized Architecture

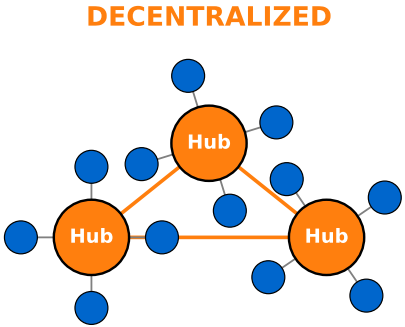


Single point of failure | High throughput | Low latency

Characteristics: Single authority, 10^6 TPS, <10ms latency

Traditional systems: banks, exchanges, cloud services

Decentralized Architecture

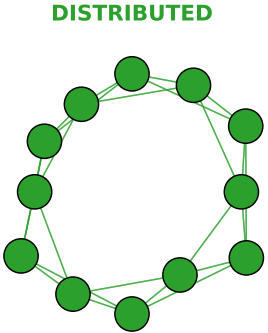


Multiple hubs | Federation trust | Moderate latency

Characteristics: Multiple hubs, federated trust, 10^3 TPS

Examples: Federated exchanges, consortium blockchains

Distributed Architecture (Blockchain)

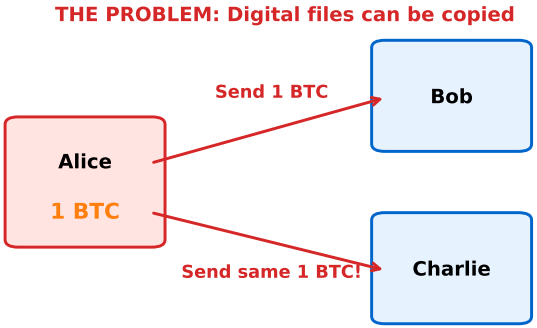


No single point of failure | Cryptographic trust | All nodes equal

Characteristics: No hierarchy, cryptographic trust, 10^1 TPS

Blockchain trades performance for trustlessness

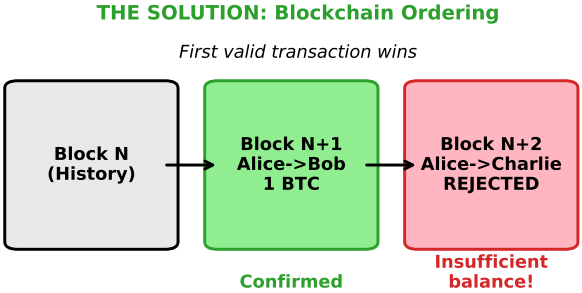
The Double-Spending Problem



Problem: Prevent $\text{Transfer}(a, A \to B) \wedge \text{Transfer}(a, A \to C)$

Digital files can be copied infinitely — no inherent scarcity in bits

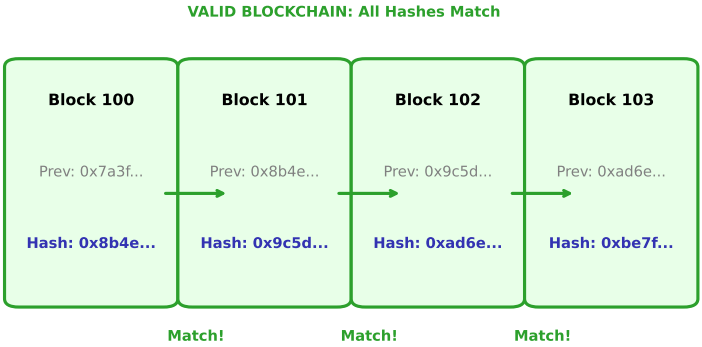
The Blockchain Solution



Solution: Distributed consensus determines transaction ordering

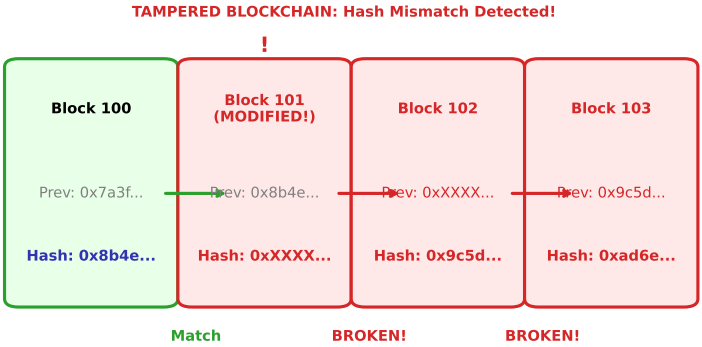
Nakamoto's key insight: Use computational work to achieve probabilistic finality

Valid Blockchain: Hash Chain Integrity



Hash pointers create a tamper-evident linked data structure

Tampered Blockchain: Detection



Modifying any block invalidates ALL subsequent blocks

Modifying B_k requires recomputing all subsequent hashes: $O(n-k) \times 2^{76}$ ops

Merkle Tree: Efficient Transaction Verification

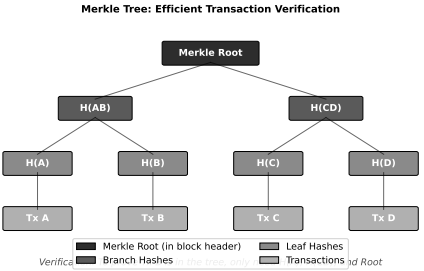
Structure
Binary hash tree over transactions:

$$\text{Root} = H(H(H(tx_1)||H(tx_2))||H(H(tx_3)||H(tx_4)))$$

Verification Complexity:

- Full verification: $O(n)$ hashes
- Merkle proof: $O(\log n)$ hashes
- SPV clients use proofs, not full chain

Bitcoin Block Header:
32-byte Merkle root commits to all transactions



Merkle trees enable lightweight clients: verify transactions without downloading full blocks

Core Properties and Guarantees

Cryptographic Properties

- **Collision Resistance:**
  $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$
- **Preimage Resistance:**
  Given h, infeasible to find $x : H(x) = h$
- **Avalanche Effect:**
  1-bit change $\Rightarrow$ 50% output bits flip

System Properties

- **Liveness:**
  Valid transactions eventually confirmed
- **Safety:**
  No double-spends with $> k$ confirmations
- **Consistency:**
  All honest nodes agree on prefix

Probability of Reversal (after k confirmations, attacker with $q < 0.5$ hashrate):

$$P(\text{reversal}) < \left(\frac{q}{1-q}\right)^k$$

6 confirmations $\Rightarrow$ reversal probability $< 0.1\%$ for $q = 0.3$

Real-World Applications: Finance (1/2)

Cryptocurrency Markets (Jan 2026)

- Bitcoin: $1.8T market cap, $50B daily volume
- Stablecoins: $311B market cap (USDT $175B, USDC $75B)
- DeFi TVL: $120B across protocols

Institutional Adoption

- Bitcoin ETFs: $140B AUM (launched Jan 2024, surpassed gold ETFs Dec 2024)
- JPMorgan Onyx: $1B+ daily settlements

Source: CoinGecko, DefiLlama (Jan 2026) — Institutional adoption accelerating

Real-World Applications: Enterprise & Government (2/2)

Enterprise Blockchain

- IBM Food Trust: 500+ organizations tracking supply chain
- Maersk TradeLens: 1.5B shipping events (shut down Nov 2022 — lesson in adoption challenges)

Government & CBDC

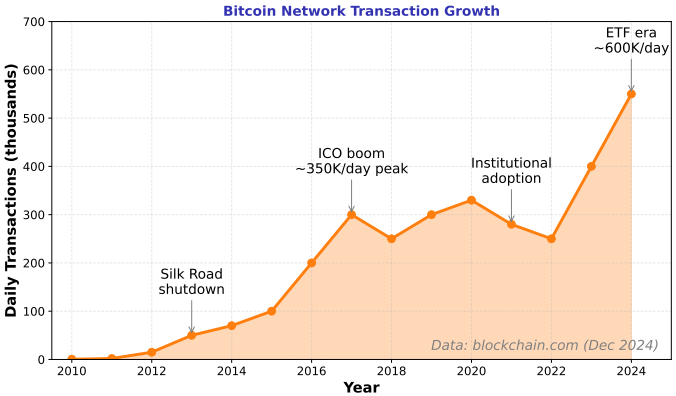
- China e-CNY: 260M+ wallets (largest CBDC deployment)
- EU Digital Euro: Pilot phase ongoing
- 130+ countries exploring CBDCs (Atlantic Council tracker)

Emerging Applications: Real-World Assets (RWA), Decentralized Identity (DID), Carbon credits

---

CBDCs represent central bank adoption of blockchain technology principles

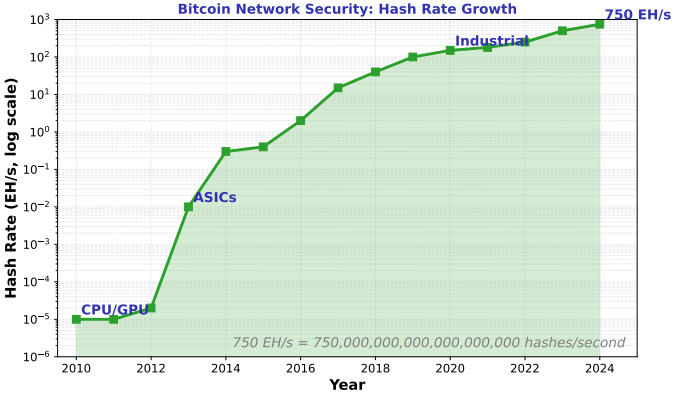
Network Adoption: Bitcoin Transactions



From $<$1K daily transactions (2010) to $>$600K daily (2024)

Transaction volume indicates real economic activity on the network

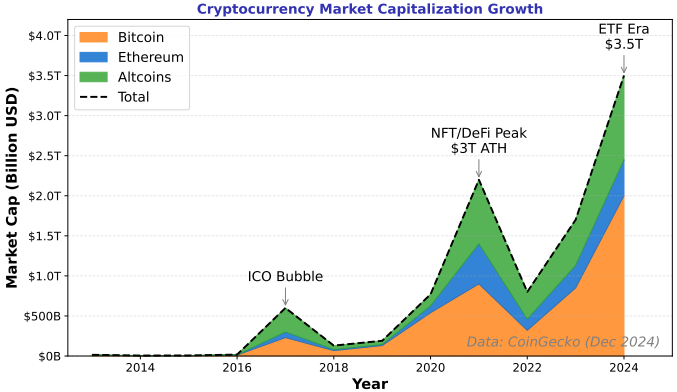
Network Security: Hash Rate Growth



1,000 EH/s (1 ZH/s) = 10^{21} SHA-256 hashes per second (milestone reached Jan 2026)

Higher hash rate = more computational cost to attack the network

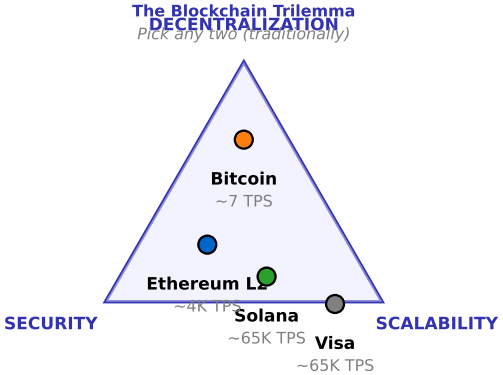
Market Growth: Cryptocurrency Capitalization



Total market cap: $3.1T (Jan 2026); Bitcoin dominance: ∼57%

Market cap growth reflects institutional adoption and mainstream acceptance

The Blockchain Trilemma



Layer 2 solutions attempt to optimize all three dimensions

Decision Framework: When to Use Blockchain

Use Blockchain When:

- ✓ Multiple writers, no trusted party
- ✓ Immutable audit trail required
- ✓ Disintermediation creates value
- ✓ Censorship resistance needed
- ✓ Cross-organizational data sharing

Use Traditional DB When:

- × Single organization controls data
- × High throughput required (>10K TPS)
- × Data deletion/modification needed
- × Strong privacy requirements
- × Existing solutions work well

Decision Heuristic:

$$\text{Blockchain Value} \propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$$

Most enterprise "blockchain" projects could use a replicated database

Problem Solved? The Double-Spend Problem

The Original Problem

How can strangers transact without intermediaries?

How Blockchain Solves It

- Distributed ledger records all transactions with cryptographic proofs
- Cryptographic proof-of-work establishes transaction ordering through consensus
- Hash-chain structure makes tampering computationally intractable

Remaining Limitations

- Energy consumption: Bitcoin network uses $\sim$150 TWh/year (comparable to Argentina)
- Scalability vs decentralization trade-off (blockchain trilemma)

Open Questions

- Can we achieve the same security guarantees without energy waste? (PoS alternatives)
- Risk: 51% attacks, eclipse attacks, long-range attacks

Blockchain partially solves trustless coordination but introduces energy/scalability trade-offs

Key Takeaways

Core Concepts:

1. Blockchain = hash-chained blocks + distributed consensus + cryptographic signatures
2. Double-spending solved via total ordering through consensus mechanism
3. Immutability achieved through computational intractability of hash chain modification
4. Trade-off: Performance $\leftrightarrow$ Trustlessness $\leftrightarrow$ Decentralization

Mathematical Foundations:

- Hash functions: $H : \{0,1\}^* \to \{0,1\}^{256}$ (SHA-256)
- Merkle trees: $O(\log n)$ verification complexity
- Reversal probability: Exponential decay with confirmations

Next Lesson: L02 – Distributed Ledger Technology (DLT) deep dive

---

Blockchain is a tool, not a solution — evaluate against specific requirements

Questions for Reflection

1. Why is the hash pointer critical for blockchain immutability? What would happen if we used regular pointers?
2. How does the double-spending problem differ between physical cash and digital currencies?
3. When would a traditional database be a better choice than blockchain? Give a specific example.
4. Why does Bitcoin prioritize decentralization over transaction throughput?
5. How do Merkle trees enable "light clients" to verify transactions without downloading the full blockchain?

Discussion: Consider a supply chain use case — what trust deficit would justify the performance trade-off of blockchain?

Prepare answers for next session discussion — Reference slides 3, 9-10, 13, 18

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority
Answer: C – Consensus determines transaction ordering, preventing the same coin from being spent twice.

Q3. What is the verification complexity of a Merkle proof?
A) $O(1)$ B) $O(\log n)$ C) $O(n)$ D) $O(n^2)$

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority
Answer: C – Consensus determines transaction ordering, preventing the same coin from being spent twice.

Q3. What is the verification complexity of a Merkle proof?
A) $O(1)$ B) $O(\log n)$ C) $O(n)$ D) $O(n^2)$
Answer: B – Merkle proofs require only $\log n$ hashes, enabling efficient lightweight client verification.

Q4. Bitcoin's hash rate reaching 1 ZH/s means:
A) Transactions are faster B) Network is more secure C) Fees are lower D) Blocks are larger

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority
Answer: C – Consensus determines transaction ordering, preventing the same coin from being spent twice.

Q3. What is the verification complexity of a Merkle proof?
A) $O(1)$ B) $O(\log n)$ C) $O(n)$ D) $O(n^2)$
Answer: B – Merkle proofs require only $\log n$ hashes, enabling efficient lightweight client verification.

Q4. Bitcoin's hash rate reaching 1 ZH/s means:
A) Transactions are faster B) Network is more secure C) Fees are lower D) Blocks are larger
Answer: B – Higher hash rate increases the computational cost required to attack the network.

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation
Answer: B – You cannot maximize all three simultaneously; Layer 2 solutions attempt to optimize this.

Q7. When should you NOT use blockchain?
A) Multiple untrusted parties B) Single organization controls data C) Audit trail needed D) Cross-border payments

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation
Answer: B – You cannot maximize all three simultaneously; Layer 2 solutions attempt to optimize this.

Q7. When should you NOT use blockchain?
A) Multiple untrusted parties B) Single organization controls data C) Audit trail needed D) Cross-border payments
Answer: B – A traditional database is more efficient when a single trusted party controls the data.

Q8. What year did Bitcoin's whitepaper appear?
A) 2006 B) 2008 C) 2010 D) 2015

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation
Answer: B – You cannot maximize all three simultaneously; Layer 2 solutions attempt to optimize this.

Q7. When should you NOT use blockchain?
A) Multiple untrusted parties B) Single organization controls data C) Audit trail needed D) Cross-border payments
Answer: B – A traditional database is more efficient when a single trusted party controls the data.

Q8. What year did Bitcoin's whitepaper appear?
A) 2006 B) 2008 C) 2010 D) 2015
Answer: B – Satoshi Nakamoto published the Bitcoin whitepaper on October 31, 2008.

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation
Answer: B – SPV clients verify transactions using Merkle proofs without downloading full blocks.

Q11. A centralized architecture typically achieves:
A) 10^1 TPS B) 10^3 TPS C) 10^6 TPS D) 10^9 TPS

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation
Answer: B – SPV clients verify transactions using Merkle proofs without downloading full blocks.

Q11. A centralized architecture typically achieves:
A) 10^1 TPS B) 10^3 TPS C) 10^6 TPS D) 10^9 TPS
Answer: C – Centralized systems like Visa can process millions of transactions per second.

Q12. The Merkle root in a Bitcoin block header is:
A) 16 bytes B) 32 bytes C) 64 bytes D) 80 bytes

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation
Answer: B – SPV clients verify transactions using Merkle proofs without downloading full blocks.

Q11. A centralized architecture typically achieves:
A) 10^1 TPS B) 10^3 TPS C) 10^6 TPS D) 10^9 TPS
Answer: C – Centralized systems like Visa can process millions of transactions per second.

Q12. The Merkle root in a Bitcoin block header is:
A) 16 bytes B) 32 bytes C) 64 bytes D) 80 bytes
Answer: B – The 32-byte Merkle root commits to all transactions in the block.

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025
Answer: C – Bitcoin ETFs surpassed gold ETFs in December 2024, less than a year after launch.

Q15. The integrity constraint B_i.prev $= H(B_{i-1})$ ensures:
A) Transaction privacy B) Tamper evidence C) Faster validation D) Lower fees

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025
Answer: C – Bitcoin ETFs surpassed gold ETFs in December 2024, less than a year after launch.

Q15. The integrity constraint B_i.prev $= H(B_{i-1})$ ensures:
A) Transaction privacy B) Tamper evidence C) Faster validation D) Lower fees
Answer: B – This constraint creates a tamper-evident chain; any modification breaks the hash link.

Q16. How many countries are exploring CBDCs according to Atlantic Council?
A) 50+ B) 80+ C) 130+ D) 200+

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025
Answer: C – Bitcoin ETFs surpassed gold ETFs in December 2024, less than a year after launch.

Q15. The integrity constraint B_i.prev $= H(B_{i-1})$ ensures:
A) Transaction privacy B) Tamper evidence C) Faster validation D) Lower fees
Answer: B – This constraint creates a tamper-evident chain; any modification breaks the hash link.

Q16. How many countries are exploring CBDCs according to Atlantic Council?
A) 50+ B) 80+ C) 130+ D) 200+
Answer: C – Over 130 countries are researching or piloting central bank digital currencies.

Lesson 1: What is Blockchain?

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

Digital Finance Program

2025

[Comic] The Trust Problem

- When Alice sends money to Bob online, who guarantees Alice actually has the funds?
- Traditional answer: A trusted third party (bank, PayPal) keeps the ledger — but this creates a single point of failure and control

[COMIC: Insert XKCD or custom illustration showing trust intermediary problems — e.g., two people wanting to transact while a central figure says "I'll hold the money"]

Source: [PLACEHOLDER: XKCD #xxx or custom illustration] — The core problem blockchain solves: trustless coordination

Learning Objectives

By the end of this lesson, you will be able to:

1. Define blockchain as a cryptographically-secured distributed ledger
2. Trace the historical evolution from 1991 to 2025
3. Explain the double-spending problem and its consensus-based solution
4. Formalize the hash chain structure: $H(B_n) = H(\text{header}_n || \text{prev_hash}_{n-1})$ where $||$ denotes concatenation (joining)
5. Compare centralized, decentralized, and distributed architectures

Prerequisites: basic probability theory

BSc level: Full mathematical rigor expected in subsequent slides

Hash Function Primer: What is a Hash?

Intuitive Definition
A hash function is like a **digital fingerprint machine**:

- Takes any input (text, file, image) of any size
- Produces a fixed-size output (e.g., 256 bits for SHA-256)
- The output is called a **hash** or **digest**

Example:

- Input: "Hello World" → Hash: `a591a6d...` (64 hex characters)
- Input: "Hello World!" → Hash: `7f83b16...` (completely different!)

Think of it as a one-way compression that creates a unique ID for any data.

Hash functions are covered in depth in L03 — this primer provides foundation for L01

Hash Function Primer: Key Properties

1. **Deterministic**
   - Same input → always same output
   - No randomness involved
2. **One-Way (Preimage Resistant)**
   - Easy: input → hash
   - Impossible: hash → input
   - Cannot reverse-engineer the original
3. **Collision Resistant**
   - Virtually impossible to find two different inputs with the same hash
   - Like unique fingerprints
4. **Avalanche Effect**
   - Tiny change in input → completely different hash
   - No way to predict output changes

These properties enable tamper detection — any change is immediately visible

Hash Function Primer: Why Hashes Matter for Blockchain

Hash functions enable three critical blockchain features:

1. **Data Integrity**
   - Each block stores hash of previous block
   - Changing any data changes all subsequent hashes
   - Tampering is immediately detectable
2. **Efficient Verification**
   - Verify large datasets with small hashes
   - 1 GB file $\rightarrow$ 32-byte hash
   - Quick comparison
3. **Proof-of-Work**
   - Mining = finding hash below target
   - One-way property makes this a lottery
   - Secures the network

Key Insight: *Without hash functions, blockchain would be impossible — they create the "chain" in blockchain by linking blocks cryptographically.*

Now you're ready to understand how blockchain uses hashes to create tamper-evident ledgers

The Problem: How can strangers transact without intermediaries?

The Challenge
In digital systems, any file can be copied infinitely. How do we create digital scarcity for money without a central authority to track ownership?

Why It Matters

- Without a solution, digital cash can be spent multiple times (double-spending)
- Pre-Bitcoin e-cash systems (DigiCash, 1990s) required central trust — defeating decentralization

What We Need

- Trustless verification mechanism
- A way to prevent spending the same coin twice without a central ledger

The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How blockchain addresses the double-spending challenge

What is the Formal Definition of Blockchain?

Mathematical Definition
A blockchain $\mathcal{B}$ is an ordered sequence of blocks:

$$\mathcal{B} = (B_0, B_1, \ldots, B_n)$$

Where each block B_i contains:

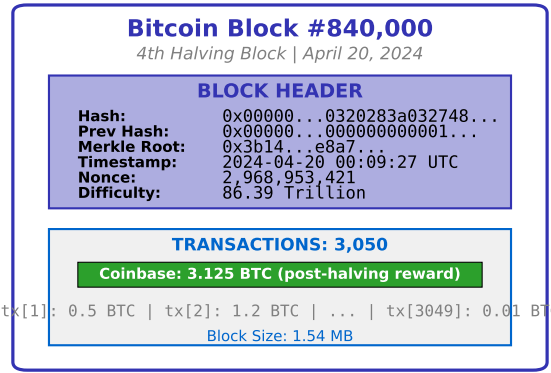
- Header h_i with metadata (version, timestamp, nonce, difficulty)
- Transaction set $T_i = \{tx_1, \ldots, tx_k\}$ (a set of transactions)
- Hash pointer to previous block: $H(B_{i-1})$

Integrity Constraint:

$$\text{For every block } i > 0: \quad B_i.\text{prev} = H(B_{i-1})$$

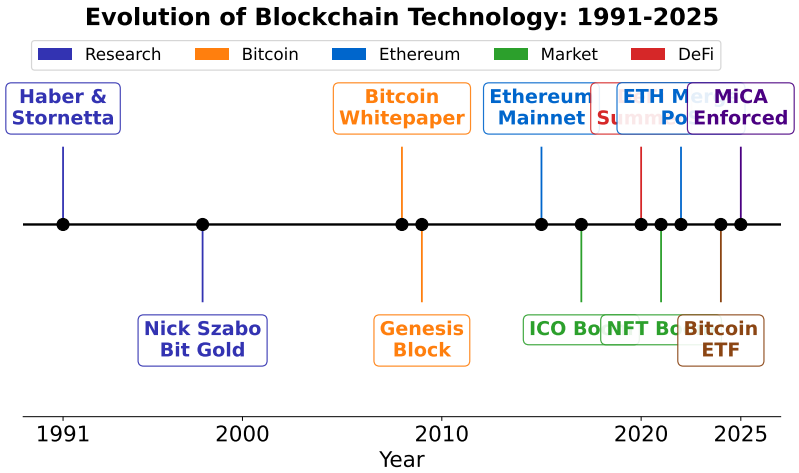
The hash pointer creates a tamper-evident linked data structure

What's Inside a Blockchain Block?



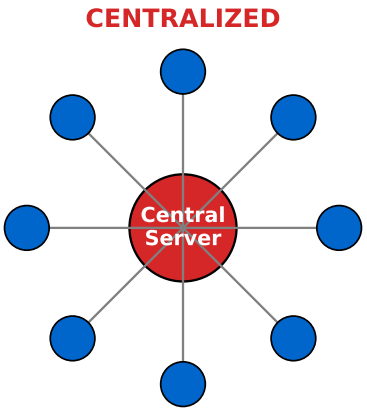
Bitcoin block header: 80 bytes — Block body: 1-2 MB of transactions

How Has Blockchain Evolved Since 1991?



Key inflection points: 2008 (Nakamoto), 2015 (Ethereum), 2024 (Bitcoin ETFs)

How Does Centralized Architecture Work?

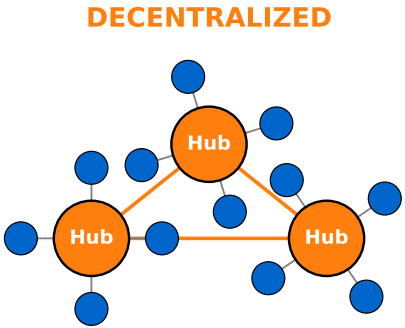


Single point of failure | High throughput | Low latency

Characteristics: Single authority, 10^4–10^5 TPS, $<$10ms latency

Traditional systems: banks, exchanges, cloud services

How Does Decentralized Architecture Work?



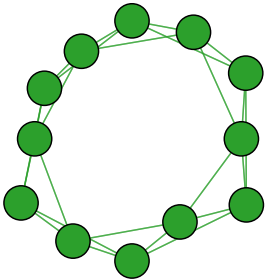
Multiple hubs | Federation trust | Moderate latency

Characteristics: Multiple hubs, federated trust, 10^3 TPS

Examples: Federated exchanges, consortium blockchains

How Does Distributed Architecture Work?

DISTRIBUTED

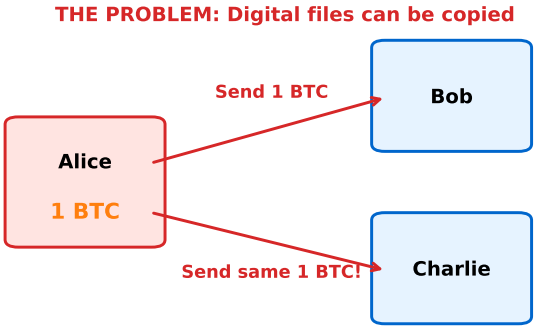


No single point of failure | Cryptographic trust | All nodes equal

Characteristics: No hierarchy, cryptographic trust, 10^1 TPS

Blockchain trades performance for trustlessness

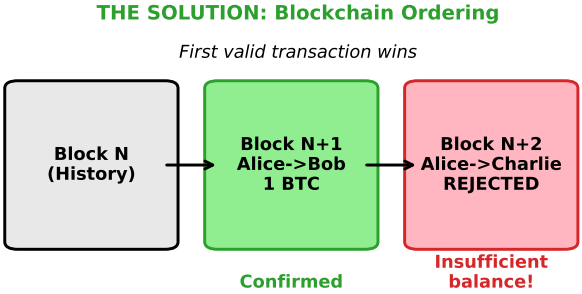
What is the Double-Spending Problem?



Problem: Prevent $\text{Transfer}(a, A \to B) \wedge \text{Transfer}(a, A \to C)$

Digital files can be copied infinitely — no inherent scarcity in bits

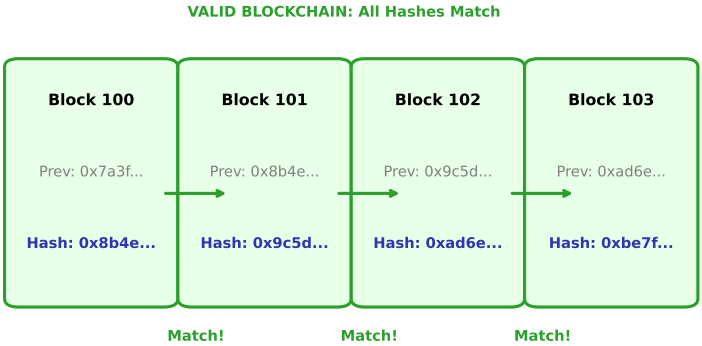
How Does Blockchain Solve Double-Spending?



Solution: Distributed consensus determines transaction ordering

Nakamoto's key insight: Use computational work to achieve probabilistic finality

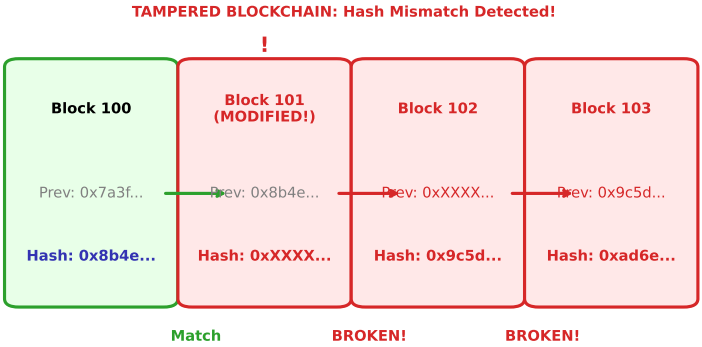
How Does Hash Chaining Ensure Integrity?



Each block references the hash of the previous block

Hash pointers create a tamper-evident linked data structure

How is Tampering Detected?



Modifying any block invalidates ALL subsequent blocks

Modifying B_k requires recomputing all subsequent hashes: $O(n-k) \times 2^{76}$ ops

How Do Merkle Trees Enable Efficient Verification?

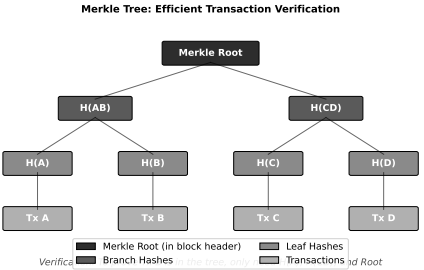
Structure
Binary hash tree over transactions:

$$\text{Root} = H(H(H(tx_1)||H(tx_2))||H(H(tx_3)||H(tx_4)))$$

Verification Complexity:

- Full verification: $O(n)$ hashes
- Merkle proof: $O(\log n)$ hashes
- Simplified Payment Verification (SPV) clients use proofs, not full chain

Bitcoin Block Header:
32-byte Merkle root commits to all transactions



Merkle trees enable lightweight clients: verify transactions without downloading full blocks

What Are the Core Properties and Guarantees?

Cryptographic Properties

- **Collision Resistance:**
  $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$
- **Preimage Resistance:**
  Given h, infeasible to find $x : H(x) = h$
- **Avalanche Effect:**
  1-bit change $\Rightarrow$ 50% output bits flip

System Properties

- **Liveness:**
  Valid transactions eventually confirmed
- **Safety:**
  No double-spends with $> k$ confirmations
- **Consistency:**
  All honest nodes agree on prefix

Probability of Reversal (after k confirmations, attacker with $q < 0.5$ hashrate):

$$P(\text{reversal}) < \left(\frac{q}{1-q}\right)^k$$

6 confirmations $\Rightarrow$ reversal probability $< 0.1\%$ for $q = 0.3$

How is Blockchain Used in Finance?

Cryptocurrency Markets (Jan 2026)

- Bitcoin: $1.8T market cap, $50B daily volume
- Stablecoins: $311B market cap (USDT $175B, USDC $75B)
- DeFi TVL: $120B across protocols

Institutional Adoption

- Bitcoin ETFs: $140B AUM (launched Jan 2024, surpassed gold ETFs Dec 2024)
- JPMorgan Onyx: $1B+ daily settlements

Source: CoinGecko, DefiLlama (Jan 2026) — Institutional adoption accelerating

How is Blockchain Used by Enterprise & Government?

Enterprise Blockchain

- IBM Food Trust: 500+ organizations tracking supply chain
- Maersk TradeLens: 1.5B shipping events (shut down Nov 2022 — lesson in adoption challenges)

Government & CBDC

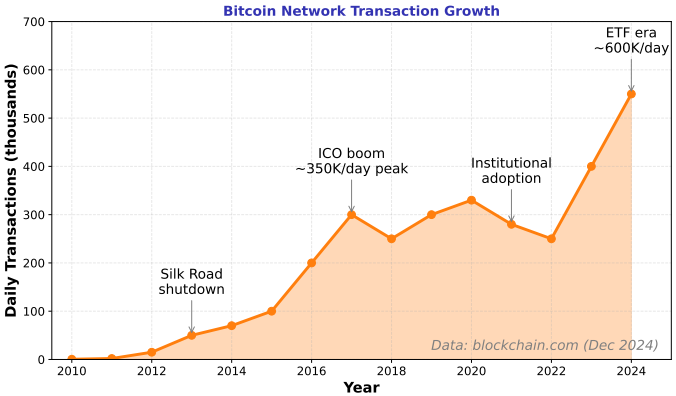
- China e-CNY: 260M+ wallets (largest CBDC deployment)
- EU Digital Euro: Pilot phase ongoing
- 130+ countries exploring CBDCs (Atlantic Council tracker)

Emerging Applications: Real-World Assets (RWA), Decentralized Identity (DID), Carbon credits

---

CBDCs represent central bank adoption of blockchain technology principles

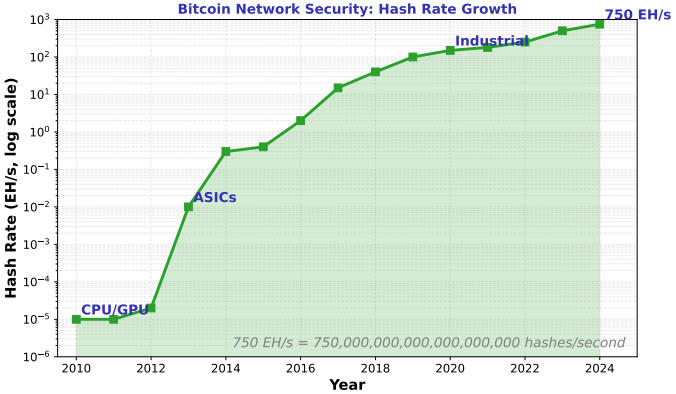
How Has Bitcoin Network Adoption Grown?



From $<$1K daily transactions (2010) to $>$600K daily (2024)

Transaction volume indicates real economic activity on the network

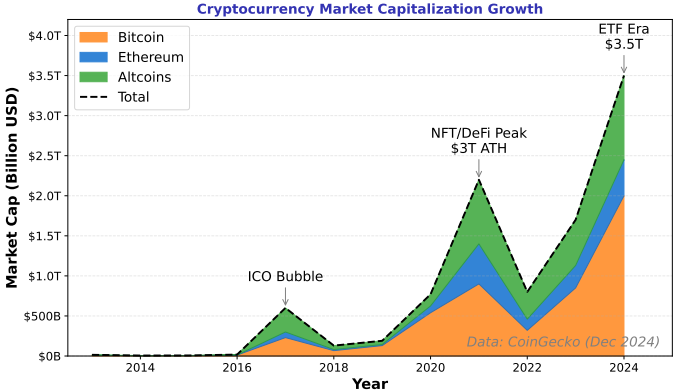
How Has Bitcoin's Hash Rate Grown?



1,000 EH/s (1 ZH/s) = 10^{21} SHA-256 hashes per second (milestone reached Jan 2026)

Higher hash rate = more computational cost to attack the network

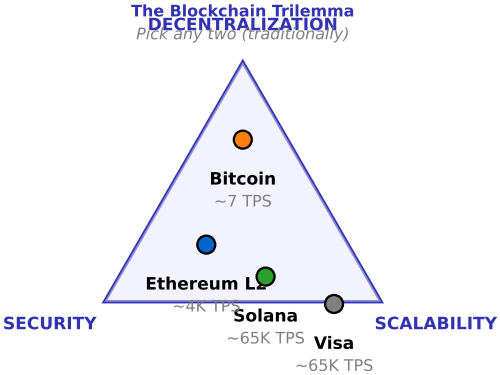
How Has Cryptocurrency Market Cap Grown?



Total market cap: $3.1T (Jan 2026); Bitcoin dominance: ∼57%

Market cap growth reflects institutional adoption and mainstream acceptance

What is the Blockchain Trilemma?



Layer 2 solutions attempt to optimize all three dimensions

When Should You Use Blockchain?

Use Blockchain When:

- ✓ Multiple writers, no trusted party
- ✓ Immutable audit trail required
- ✓ Disintermediation creates value
- ✓ Censorship resistance needed
- ✓ Cross-organizational data sharing

Use Traditional DB When:

- × Single organization controls data
- × High throughput required (>10K TPS)
- × Data deletion/modification needed
- × Strong privacy requirements
- × Existing solutions work well

Decision Heuristic:

$$\text{Blockchain Value} \propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$$

Most enterprise "blockchain" projects could use a replicated database

Problem Solved? The Double-Spend Problem

The Original Problem

How can strangers transact without intermediaries?

How Blockchain Solves It

- Distributed ledger records all transactions with cryptographic proofs
- Cryptographic proof-of-work establishes transaction ordering through consensus
- Hash-chain structure makes tampering computationally intractable

Remaining Limitations

- Energy consumption: Bitcoin network uses $\sim$150 TWh/year (comparable to Argentina)
- Scalability vs decentralization trade-off (blockchain trilemma)

Open Questions

- Can we achieve the same security guarantees without energy waste? (PoS alternatives)
- Risk: 51% attacks, eclipse attacks, long-range attacks

Blockchain partially solves trustless coordination but introduces energy/scalability trade-offs

The Economics of The Double-Spend Problem

Incentive Structure

- **Core Problem:** Preventing double-spending without a trusted third party
- **Why act honestly?** Miners earn block rewards (3.125 BTC $\approx$ \$300K) for valid blocks; invalid blocks are rejected and wasted
- **Value Flow:** Users pay transaction fees (\$1-50); miners invest in hardware and electricity (\$0.05-0.10/kWh)

Economic Security

- Attack cost = energy + hardware
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Miners earn \$300K per block (every 10 min); Users pay \$1-50 per transaction; Network consumes 150 TWh/year

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Bitcoin's cryptoeconomic security: Mining rewards make honest behavior more profitable than double-spending

Design Space: The Double-Spend Problem

Alternatives Considered

1. **Proof of Work (Bitcoin):** Energy-intensive but proven since 2009 – decentralized, censorship-resistant
2. **Proof of Stake:** Lower energy consumption but different security assumptions (nothing-at-stake problem)
3. **Traditional Systems:** Banks/PayPal prevent double-spending via central ledgers – fast but requires trust

Design Questions

- **How much energy cost is acceptable for trustless money?**
- What's optimized? Security, decentralization
- What's sacrificed? Energy efficiency, speed

Key Insight

The Energy Trade-off

Bitcoin chose security over efficiency: 150 TWh/year to secure $1.2 trillion network

Bitcoin's design choice: Maximize security and decentralization at the cost of energy and throughput

Failure Modes: The Double-Spend Problem

Critical Failure Mode

- **What breaks:** 51% attack – attacker controls majority of hash power, can double-spend
- **Why it happens:** Assumption violated: honest majority no longer controls network

Root Cause

- **Assumption:** Honest miners control ¿50% of hash power
- Mining pool concentration
- Coordinated attack by nation-state

Historical Context

- **2014:** GHash.io mining pool reached 51% of Bitcoin hash power – voluntarily reduced; no attack occurred
- **2018-2024:** Multiple 51% attacks on smaller PoW chains (Bitcoin Gold, Ethereum Classic)

Early Warning Signs

- ! Top 3 pools control ¿50% combined
- ! Single pool approaches 40%
- ! Geographic concentration of hash power

Bitcoin's security depends on hash power decentralization – pool concentration is the main systemic risk

[Comic] How Does Blockchain Act as a Digital Notary?

- Each block's hash depends on all previous blocks — changing history requires rewriting everything that follows
- The "chain" in blockchain creates a tamper-evident record: like a notary that timestamps every entry and links them together

[COMIC: Insert illustration of hash chain creating tamper-evident record — e.g., blocks linked by chains with visible fingerprints/hashes, or a notary stamping documents in sequence]

Source: [PLACEHOLDER: Custom illustration] — Hash pointers: the cryptographic glue that makes blockchain immutable

Key Takeaways

Core Concepts:

1. Blockchain = hash-chained blocks + distributed consensus + cryptographic signatures
2. Double-spending solved via total ordering through consensus mechanism
3. Immutability achieved through computational intractability of hash chain modification
4. Trade-off: Performance $\leftrightarrow$ Trustlessness $\leftrightarrow$ Decentralization

Mathematical Foundations:

- Hash functions: $H : \{0,1\}^* \to \{0,1\}^{256}$ (SHA-256)
- Merkle trees: $O(\log n)$ verification complexity
- Reversal probability: Exponential decay with confirmations

Next Lesson: L02 – Distributed Ledger Technology (DLT) deep dive

---

Blockchain is a tool, not a solution — evaluate against specific requirements

Questions for Reflection

1. Why is the hash pointer critical for blockchain immutability? What would happen if we used regular pointers?
2. How does the double-spending problem differ between physical cash and digital currencies?
3. When would a traditional database be a better choice than blockchain? Give a specific example.
4. Why does Bitcoin prioritize decentralization over transaction throughput?
5. How do Merkle trees enable "light clients" to verify transactions without downloading the full blockchain?

Discussion: Consider a supply chain use case — what trust deficit would justify the performance trade-off of blockchain?

Prepare answers for next session discussion — Reference slides 3, 9-10, 13, 18

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority
Answer: C – Consensus determines transaction ordering, preventing the same coin from being spent twice.

Q3. What is the verification complexity of a Merkle proof?
A) $O(1)$ B) $O(\log n)$ C) $O(n)$ D) $O(n^2)$

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority
Answer: C – Consensus determines transaction ordering, preventing the same coin from being spent twice.

Q3. What is the verification complexity of a Merkle proof?
A) $O(1)$ B) $O(\log n)$ C) $O(n)$ D) $O(n^2)$
Answer: B – Merkle proofs require only $\log n$ hashes, enabling efficient lightweight client verification.

Q4. Bitcoin's hash rate reaching 1 ZH/s means:
A) Transactions are faster B) Network is more secure C) Fees are lower D) Blocks are larger

Quiz Questions (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Encrypt transaction data B) Link blocks immutably C) Store wallet addresses D) Calculate fees
Answer: B – Hash pointers create tamper-evident links; changing any block invalidates all subsequent hashes.

Q2. The double-spending problem is solved in blockchain through:
A) Encryption B) Faster networks C) Distributed consensus D) Central authority
Answer: C – Consensus determines transaction ordering, preventing the same coin from being spent twice.

Q3. What is the verification complexity of a Merkle proof?
A) $O(1)$ B) $O(\log n)$ C) $O(n)$ D) $O(n^2)$
Answer: B – Merkle proofs require only $\log n$ hashes, enabling efficient lightweight client verification.

Q4. Bitcoin's hash rate reaching 1 ZH/s means:
A) Transactions are faster B) Network is more secure C) Fees are lower D) Blocks are larger
Answer: B – Higher hash rate increases the computational cost required to attack the network.

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation
Answer: B – You cannot maximize all three simultaneously; Layer 2 solutions attempt to optimize this.

Q7. When should you NOT use blockchain?
A) Multiple untrusted parties B) Single organization controls data C) Audit trail needed D) Cross-border payments

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation
Answer: B – You cannot maximize all three simultaneously; Layer 2 solutions attempt to optimize this.

Q7. When should you NOT use blockchain?
A) Multiple untrusted parties B) Single organization controls data C) Audit trail needed D) Cross-border payments
Answer: B – A traditional database is more efficient when a single trusted party controls the data.

Q8. What year did Bitcoin's whitepaper appear?
A) 2006 B) 2008 C) 2010 D) 2015

Quiz Questions (6–10)

Q5. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Preimage resistance B) Collision resistance C) Avalanche effect D) Determinism
Answer: B – Collision resistance: $\Pr[H(x) = H(y) \wedge x \neq y] \approx 2^{-128}$.

Q6. The blockchain trilemma suggests trade-offs between:
A) Speed, cost, security B) Decentralization, security, scalability C) Privacy, transparency, speed D) Mining, staking, delegation
Answer: B – You cannot maximize all three simultaneously; Layer 2 solutions attempt to optimize this.

Q7. When should you NOT use blockchain?
A) Multiple untrusted parties B) Single organization controls data C) Audit trail needed D) Cross-border payments
Answer: B – A traditional database is more efficient when a single trusted party controls the data.

Q8. What year did Bitcoin's whitepaper appear?
A) 2006 B) 2008 C) 2010 D) 2015
Answer: B – Satoshi Nakamoto published the Bitcoin whitepaper on October 31, 2008.

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation
Answer: B – SPV clients verify transactions using Merkle proofs without downloading full blocks.

Q11. A centralized architecture typically achieves:
A) 10^1 TPS B) 10^3 TPS C) 10^4–10^5 TPS D) 10^9 TPS

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation
Answer: B – SPV clients verify transactions using Merkle proofs without downloading full blocks.

Q11. A centralized architecture typically achieves:
A) 10^1 TPS B) 10^3 TPS C) 10^4–10^5 TPS D) 10^9 TPS
Answer: C – Centralized systems like Visa can process tens of thousands of transactions per second (peak 65,000 TPS).

Q12. The Merkle root in a Bitcoin block header is:
A) 16 bytes B) 32 bytes C) 64 bytes D) 80 bytes

Quiz Questions (11–15)

Q9. The probability of block reversal after k confirmations:
A) Increases linearly B) Decreases exponentially C) Stays constant D) Increases exponentially
Answer: B – $P(\text{reversal}) < (q/(1-q))^k$ decreases exponentially with confirmations.

Q10. What does "SPV client" stand for?
A) Secure Private Vault B) Simplified Payment Verification C) Standard Protocol Version D) Synchronized Peer Validation
Answer: B – SPV clients verify transactions using Merkle proofs without downloading full blocks.

Q11. A centralized architecture typically achieves:
A) 10^1 TPS B) 10^3 TPS C) 10^4–10^5 TPS D) 10^9 TPS
Answer: C – Centralized systems like Visa can process tens of thousands of transactions per second (peak 65,000 TPS).

Q12. The Merkle root in a Bitcoin block header is:
A) 16 bytes B) 32 bytes C) 64 bytes D) 80 bytes
Answer: B – The 32-byte Merkle root commits to all transactions in the block.

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025
Answer: C – Bitcoin ETFs surpassed gold ETFs in December 2024, less than a year after launch.

Q15. The integrity constraint B_i.prev $= H(B_{i-1})$ ensures:
A) Transaction privacy B) Tamper evidence C) Faster validation D) Lower fees

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025
Answer: C – Bitcoin ETFs surpassed gold ETFs in December 2024, less than a year after launch.

Q15. The integrity constraint B_i.prev $= H(B_{i-1})$ ensures:
A) Transaction privacy B) Tamper evidence C) Faster validation D) Lower fees
Answer: B – This constraint creates a tamper-evident chain; any modification breaks the hash link.

Q16. How many countries are exploring CBDCs according to Atlantic Council?
A) 50+ B) 80+ C) 130+ D) 200+

Quiz Questions (16–20)

Q13. Which is NOT a cryptographic property of hash functions?
A) Collision resistance B) Preimage resistance C) Reversibility D) Avalanche effect
Answer: C – Hash functions are one-way; reversibility would break preimage resistance.

Q14. Bitcoin ETFs surpassed gold ETFs in AUM in:
A) January 2024 B) June 2024 C) December 2024 D) January 2025
Answer: C – Bitcoin ETFs surpassed gold ETFs in December 2024, less than a year after launch.

Q15. The integrity constraint B_i.prev $= H(B_{i-1})$ ensures:
A) Transaction privacy B) Tamper evidence C) Faster validation D) Lower fees
Answer: B – This constraint creates a tamper-evident chain; any modification breaks the hash link.

Q16. How many countries are exploring CBDCs according to Atlantic Council?
A) 50+ B) 80+ C) 130+ D) 200+
Answer: C – Over 130 countries are researching or piloting central bank digital currencies.

Lesson 1: What is Blockchain?

Mini-Lecture (30 min) — Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

Digital Finance Program

2025

Learning Objectives: Define blockchain — Understand architecture — Explain double-spending — Identify use cases

What is Blockchain?

Mathematical Definition
A blockchain $\mathcal{B}$ is an ordered sequence of blocks:

$$\mathcal{B} = (B_0, B_1, \ldots, B_n)$$

Where each block B_i contains:

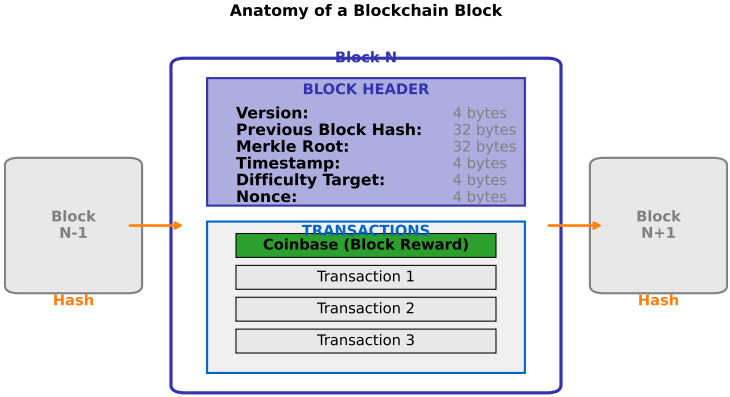
- Header h_i with metadata (version, timestamp, nonce, difficulty)
- Transaction set $T_i = \{tx_1, \ldots, tx_k\}$
- Hash pointer to previous block: $H(B_{i-1})$

Integrity Constraint:

$$\forall i > 0 : B_i.\text{prev} = H(B_{i-1})$$

The hash pointer creates a tamper-evident linked data structure

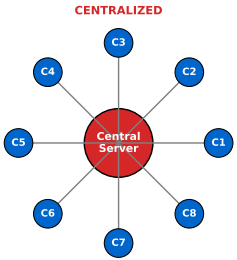
Anatomy of a Blockchain Block



Average Bitcoin block: ~1-2 MB | ~2000-3000 transactions

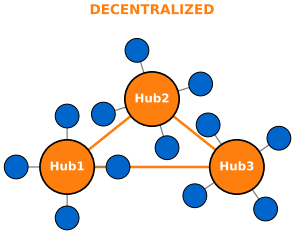
Bitcoin block header: 80 bytes — Block body: 1-2 MB of transactions

Network Architectures: Centralized vs Distributed



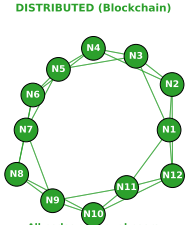
Single point of failure | High throughput (~10^6 TPS) | <10ms latency

Centralized
10^6 TPS, $<$10ms



Multiple hubs | Federation trust | ~10^3 TPS | ~1s latency

Decentralized
10^3 TPS, federated



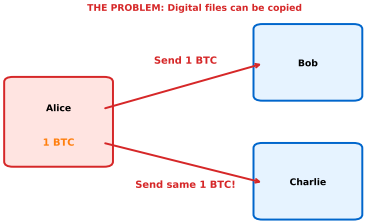
No single point of failure | Cryptographic trust | ~10 TPS | ~10 min finality

Distributed
10^1 TPS, trustless

Blockchain trades performance for trustlessness — no central authority required

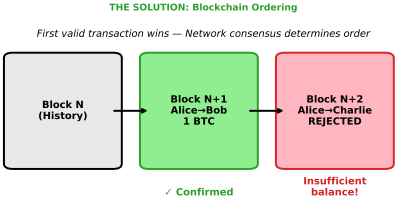
The Double-Spending Problem and Solution

The Problem



Prevent: Transfer$(a, A \to B) \wedge$ Transfer$(a, A \to C)$

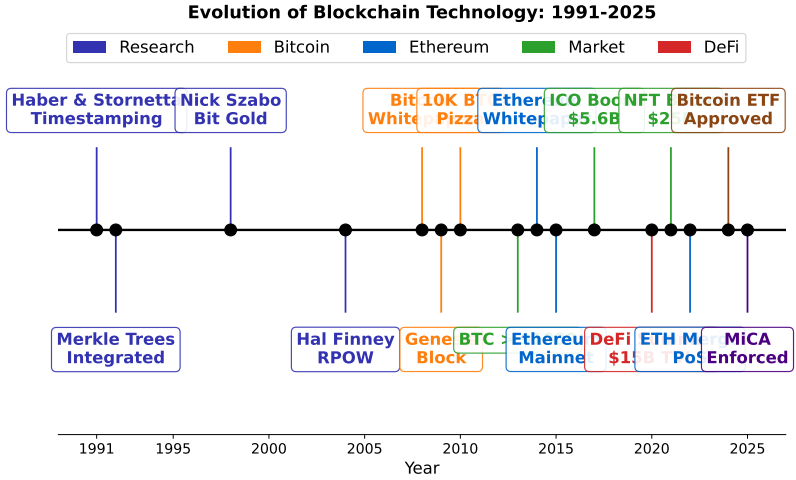
The Solution



Distributed consensus determines transaction ordering

Nakamoto's insight: Use computational work for probabilistic finality

Blockchain Evolution: 1991–2025



Key milestones: 2008 (Nakamoto), 2015 (Ethereum), 2024 (Bitcoin ETFs surpass gold)

Real-World Applications (2025)

Finance & Payments

- Bitcoin: $2T market cap
- DeFi TVL: $134B across protocols
- Bitcoin ETFs: $129B AUM (Dec 2024)
- Stablecoins: $200B+ circulation

Enterprise

- IBM Food Trust: 500+ organizations
- JPMorgan Onyx: $1B+ daily settlements

Government & CBDC

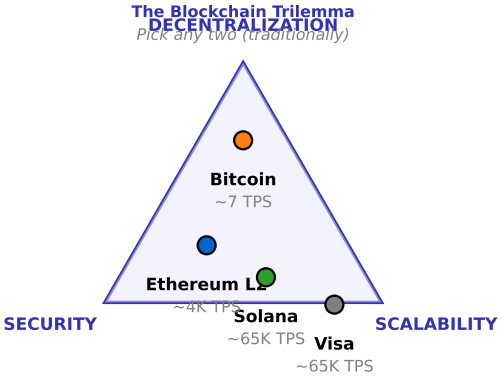
- China e-CNY: 260M+ wallets
- 130+ countries exploring CBDCs

Emerging Applications

- Real-World Assets (RWA): $15B+
- Decentralized Identity (DID)
- Supply chain provenance

Source: DeFi Llama, CoinGecko, Atlantic Council CBDC Tracker (Dec 2024)

The Blockchain Trilemma



The Trade-Off:

- **Security:** Resistance to attacks
- **Decentralization:** No single point of control
- **Scalability:** High transaction throughput

Cannot optimize all three simultaneously.

Layer 2 solutions attempt to optimize all dimensions.

Bitcoin prioritizes security + decentralization; Solana prioritizes scalability + security

Key Takeaways

Core Concepts:

1. Blockchain = hash-chained blocks + distributed consensus + cryptographic signatures
2. Double-spending solved via total ordering through consensus mechanism
3. Immutability achieved through computational intractability of hash chain modification
4. Trade-off: Performance $\leftrightarrow$ Trustlessness $\leftrightarrow$ Decentralization

Decision Heuristic:

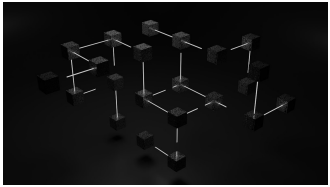
$$\text{Blockchain Value} \propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$$

Next Lesson: L02 – Distributed Ledger Technology (DLT) deep dive

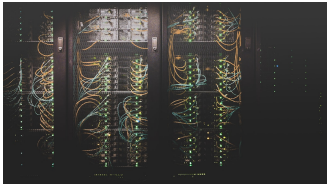
---

Blockchain is a tool, not a solution — evaluate against specific requirements

Blockchain in Visual Perspective



Immutable Chain



Distributed Network

Cryptographic Trust

Blockchain: Linked blocks, distributed globally, secured by cryptography

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015
Answer: C – Satoshi Nakamoto published the Bitcoin whitepaper in October 2008.

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q9. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory DB C) Supply chain D) Decentralized identity

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q9. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory DB C) Supply chain D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary.

Q10. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

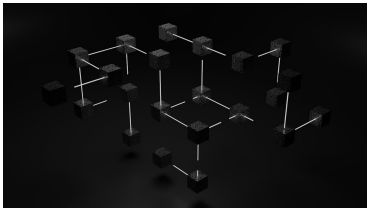
Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

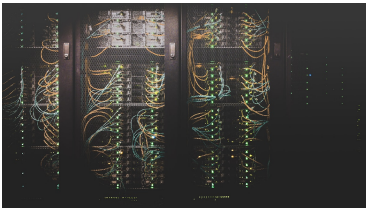
Q9. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory DB C) Supply chain D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary.

Q10. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

What is Blockchain?

Learning Objectives: Define blockchain — Understand architecture — Explain double-spending — Identify use cases





What is Blockchain?

Mathematical Definition
A blockchain $\mathcal{B}$ is an ordered sequence of blocks:

$$\mathcal{B} = (B_0, B_1, \ldots, B_n)$$

Where each block B_i contains:

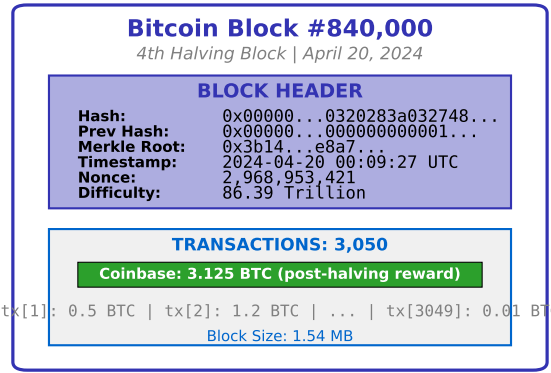
- Header h_i with metadata (version, timestamp, nonce, difficulty)
- Transaction set $T_i = \{tx_1, \ldots, tx_k\}$
- Hash pointer to previous block: $H(B_{i-1})$ (e.g., 0x00000...a032748)

Integrity Constraint:

$$\forall i > 0 : B_i.\text{prev} = H(B_{i-1})$$

The hash pointer creates a tamper-evident linked data structure

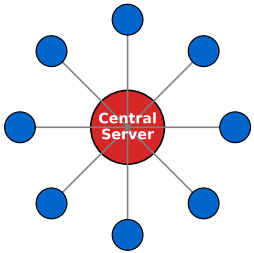
Bitcoin Block #840,000 (Real Example)



4th halving block (April 20, 2024) – Reward reduced from 6.25 to 3.125 BTC

Network Architectures: Centralized vs Distributed

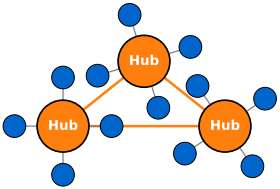
CENTRALIZED



Single point of failure | High throughput | Low latency

Centralized
Visa, Banks

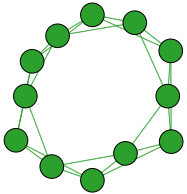
DECENTRALIZED



Multiple hubs | Federation trust | Moderate latency

Decentralized
R3 Corda

DISTRIBUTED



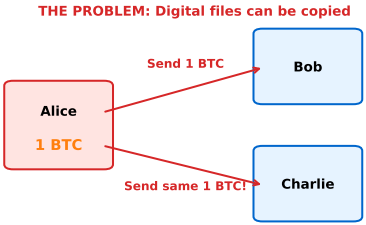
No single point of failure | Cryptographic trust | All nodes equal

Distributed
Bitcoin

Blockchain trades performance for trustlessness — no central authority required

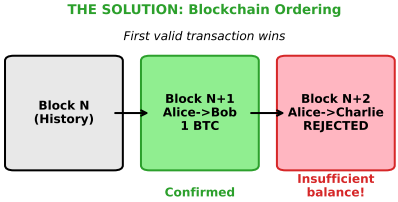
The Double-Spending Problem and Solution

The Problem



Prevent: Transfer$(a, A \to B) \wedge$ Transfer$(a, A \to C)$

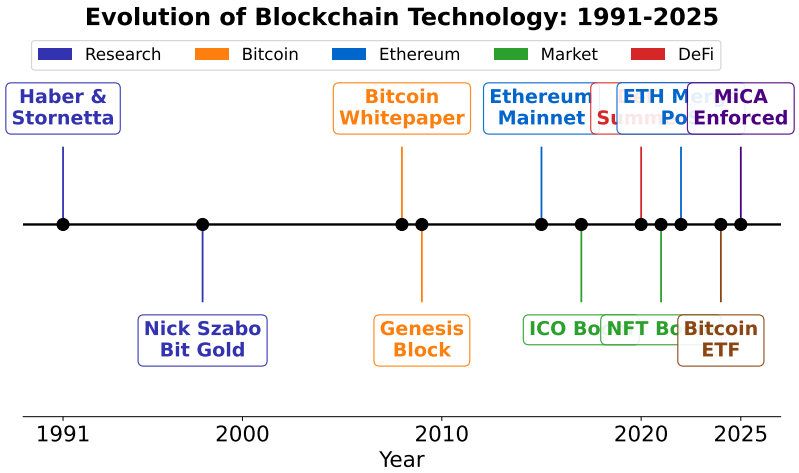
The Solution



Distributed consensus determines transaction ordering

Historical attack: Mt. Gox 2014 ($450M) exploited tx malleability before consensus

Blockchain Evolution: 1991–2025



Key milestones: 2008 (Nakamoto), 2015 (Ethereum), 2024 (Bitcoin ETFs surpass gold)

Real-World Applications (2025)

Finance & Payments

- Bitcoin: $2T market cap
- DeFi TVL: $134B (Lido $25B, Aave $14B)
- Bitcoin ETFs: $129B (BlackRock IBIT $37B)
- Stablecoins: $200B+ (USDT $137B)

Enterprise

- IBM Food Trust: 500+ organizations
- JPMorgan Onyx: $1B+ daily settlements

Government & CBDC

- China e-CNY: 260M+ wallets
- 130+ countries exploring CBDCs

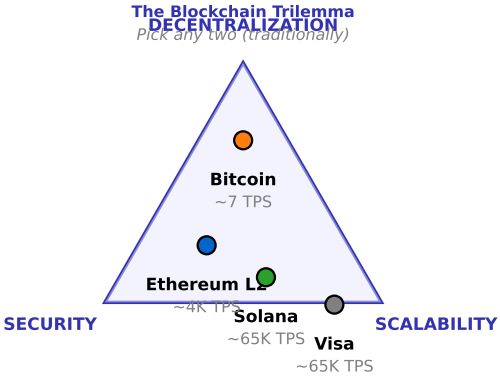
Emerging Applications

- Real-World Assets (RWA): $15B+
- Decentralized Identity (DID)
- Supply chain provenance

Source: DeFi Llama, CoinGecko, Atlantic Council CBDC Tracker (Dec 2025)

(c) Joerg Osterrieder 2025

The Blockchain Trilemma



The Trade-Off:

- **Security:** Resistance to attacks
- **Decentralization:** No single point of control
- **Scalability:** High transaction throughput

Cannot optimize all three simultaneously.

Layer 2 solutions attempt to optimize all dimensions.

Bitcoin: 7 TPS, 50K nodes — Solana: 65K TPS, 1K validators — Lightning L2: instant, 5K+ BTC

Key Takeaways

Core Concepts:

1. Blockchain = hash-chained blocks + distributed consensus + cryptographic signatures
2. Double-spending solved via total ordering through consensus mechanism
3. Immutability achieved through computational intractability of hash chain modification
4. Trade-off: Performance $\leftrightarrow$ Trustlessness $\leftrightarrow$ Decentralization

Decision Heuristic:

$$\text{Blockchain Value} \propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$$

Next Lesson: L02 – Distributed Ledger Technology (DLT) deep dive

---

Blockchain is a tool, not a solution — evaluate against specific requirements

Concrete Examples: Making It Real

Bitcoin Block #840,000 (Halving Block, Apr 20, 2024)

- Hash: `0x00000...0320283a032748...`
- Timestamp: 2024-04-20 00:09:27 UTC
- Nonce: 2,968,953,421
- Transactions: 3,050
- Difficulty: 86.39 trillion

SHA-256 Avalanche Effect

- `SHA256("Hello")` = `185f8db3...`
- `SHA256("hello")` = `2cf24dba...`
- 1 bit change $\Rightarrow$ 50% output bits flip

Network Examples

- Centralized: Visa (65,000 TPS, single DC)
- Decentralized: R3 Corda (bank consortium)
- Distributed: Bitcoin (50,000+ nodes, 7 TPS)

Real Applications (Dec 2025)

- ETF: BlackRock IBIT ($37B AUM)
- DeFi: Lido ($25B staked ETH)
- CBDC: China e-CNY (260M wallets)
- RWA: BlackRock BUIDL ($560M)
- L2: Lightning Network (5,000+ BTC)

All data verified Dec 2025 — Block 840,000 is Bitcoin's 4th halving block (reward: 3.125 BTC)

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015

Quick Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase speed B) Link blocks with tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the fee B) Spending same asset twice C) Mining two blocks D) Wrong address
Answer: B – Blockchain prevents spending same coins twice via consensus ordering.

Q3. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015
Answer: C – Satoshi Nakamoto published the Bitcoin whitepaper in October 2008.

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties

(c) Joerg Osterrieder 2025

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q9. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory DB C) Supply chain D) Decentralized identity

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q9. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory DB C) Supply chain D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary.

Q10. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls

Quick Quiz (6–10)

Q6. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency D) Mining, staking
Answer: B – Trilemma: cannot optimize security, decentralization, and scalability simultaneously.

Q7. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q8. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for finality D) Trusted parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q9. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory DB C) Supply chain D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary.

Q10. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

Quiz: What is Blockchain

Instructions: 23 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal, cryptographic trust.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal, cryptographic trust.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015
Answer: C – Satoshi Nakamoto published the Bitcoin whitepaper in October 2008.

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block header is exactly 80 bytes containing metadata.

Q10. The avalanche effect means:
A) Hash output grows exponentially B) 1-bit input change flips 50% of output bits C) Blocks cascade faster D) Network congestion increases

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block header is exactly 80 bytes containing metadata.

Q10. The avalanche effect means:
A) Hash output grows exponentially B) 1-bit input change flips 50% of output bits C) Blocks cascade faster D) Network congestion increases
Answer: B – Avalanche: small input change causes large, unpredictable output change.

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s
Answer: C – Bitcoin hash rate reached 1,200 EH/s (1.2×10^{21} hashes/sec).

Q15. SPV (Simplified Payment Verification) clients use:
A) Full blockchain B) Merkle proofs C) Trusted servers only D) No verification

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s
Answer: C – Bitcoin hash rate reached 1,200 EH/s (1.2×10^{21} hashes/sec).

Q15. SPV (Simplified Payment Verification) clients use:
A) Full blockchain B) Merkle proofs C) Trusted servers only D) No verification
Answer: B – SPV clients verify transactions using Merkle proofs without full chain.

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) $1B B) $10B C) $129B D) $500B

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus
Answer: B – Modifying B_k requires recomputing all $n - k$ subsequent block hashes.

Q20. The formula Value $\propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$ suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit is high with coordination needs D) Single entity controls data

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus
Answer: B – Modifying B_k requires recomputing all $n - k$ subsequent block hashes.

Q20. The formula Value $\propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$ suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit is high with coordination needs D) Single entity controls data
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q23. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q23. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

Quiz: What is Blockchain

Instructions: 23 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal, cryptographic trust.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015

Quiz (1–5)

Q1. What is the primary purpose of the hash pointer in a blockchain?
A) Increase transaction speed B) Link blocks creating tamper-evidence C) Encrypt data D) Reduce storage
Answer: B – Hash pointers create integrity: changing any block invalidates all subsequent hashes.

Q2. The double-spending problem refers to:
A) Paying twice the transaction fee B) Spending the same digital asset twice C) Mining two blocks D) Sending to wrong address
Answer: B – Digital files can be copied; blockchain prevents spending same coins twice via consensus.

Q3. What is the verification complexity using a Merkle proof?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q4. Which network type does blockchain represent?
A) Centralized B) Decentralized C) Distributed D) Hierarchical
Answer: C – Blockchain is distributed: no central authority, all nodes equal, cryptographic trust.

Q5. The Bitcoin whitepaper was published in:
A) 1991 B) 2001 C) 2008 D) 2015
Answer: C – Satoshi Nakamoto published the Bitcoin whitepaper in October 2008.

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block header is exactly 80 bytes containing metadata.

Q10. The avalanche effect means:
A) Hash output grows exponentially B) 1-bit input change flips 50% of output bits C) Blocks cascade faster D) Network congestion increases

Quiz (6–10)

Q6. What does collision resistance mean for hash functions?
A) Hashes never collide B) Finding two inputs with same hash is computationally infeasible C) Hashes are random D) Hashes can be reversed
Answer: B – Collision resistance: $\Pr[H(x) = H(y), x \neq y] \approx 2^{-128}$.

Q7. The blockchain trilemma involves trade-offs between:
A) Speed, cost, reliability B) Security, decentralization, scalability C) Privacy, transparency, efficiency D) Mining, staking, governance
Answer: B – Trilemma: cannot optimize all three simultaneously.

Q8. How many confirmations typically provide $< 0.1\%$ reversal probability?
A) 1 B) 3 C) 6 D) 100
Answer: C – 6 confirmations give reversal probability $< 0.1\%$ for attacker with $q = 0.3$ hashrate.

Q9. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block header is exactly 80 bytes containing metadata.

Q10. The avalanche effect means:
A) Hash output grows exponentially B) 1-bit input change flips 50% of output bits C) Blocks cascade faster D) Network congestion increases
Answer: B – Avalanche: small input change causes large, unpredictable output change.

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s
Answer: C – Bitcoin hash rate reached 1,200 EH/s (1.2×10^{21} hashes/sec).

Q15. SPV (Simplified Payment Verification) clients use:
A) Full blockchain B) Merkle proofs C) Trusted servers only D) No verification

Quiz (11–15)

Q11. Nakamoto's key innovation for solving double-spending was:
A) Faster databases B) Better encryption C) Computational work for probabilistic finality D) Trusted third parties
Answer: C – Proof of Work creates consensus without trusted intermediaries.

Q12. Which is NOT a valid use case for blockchain?
A) Cross-border payments B) Single-company inventory database C) Supply chain provenance D) Decentralized identity
Answer: B – Single organization control makes blockchain unnecessary; use traditional DB.

Q13. The integrity constraint $B_i.\textbf{prev} = H(B_{i-1})$ ensures:
A) Faster processing B) Each block links to its predecessor cryptographically C) Blocks can be deleted D) Transactions are encrypted
Answer: B – Hash pointer links blocks, making tampering detectable.

Q14. Current Bitcoin network hash rate (2024) is approximately:
A) 1 TH/s B) 100 PH/s C) 1,200 EH/s D) 1 ZH/s
Answer: C – Bitcoin hash rate reached 1,200 EH/s (1.2×10^{21} hashes/sec).

Q15. SPV (Simplified Payment Verification) clients use:
A) Full blockchain B) Merkle proofs C) Trusted servers only D) No verification
Answer: B – SPV clients verify transactions using Merkle proofs without full chain.

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) $1B B) $10B C) $129B D) $500B

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus
Answer: B – Modifying B_k requires recomputing all $n - k$ subsequent block hashes.

Q20. The formula Value $\propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$ suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit is high with coordination needs D) Single entity controls data

Quiz (16–20)

Q16. A distributed network differs from decentralized by:
A) Having more nodes B) No hierarchy at all; all nodes equal C) Being faster D) Using encryption
Answer: B – Distributed: no hubs/hierarchy; Decentralized: multiple hubs but still hierarchy.

Q17. The Merkle root in a Bitcoin block header commits to:
A) Previous block only B) All transactions in the block C) Mining difficulty D) Network nodes
Answer: B – 32-byte Merkle root is cryptographic commitment to all block transactions.

Q18. Bitcoin ETFs reached what AUM by December 2024?
A) \$1B B) \$10B C) \$129B D) \$500B
Answer: C – Bitcoin ETFs reached \$129B AUM, surpassing gold ETFs in Dec 2024.

Q19. To modify block B_k in a chain of n blocks, an attacker must:
A) Change only B_k B) Recompute hashes for all blocks after B_k C) Get permission D) Wait for consensus
Answer: B – Modifying B_k requires recomputing all $n - k$ subsequent block hashes.

Q20. The formula Value $\propto \frac{\text{Trust Deficit} \times \text{Coordination Benefit}}{\text{Performance Requirements}}$ suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit is high with coordination needs D) Single entity controls data
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q23. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls

Quiz (21–23)

Q21. What is Merkle proof verification complexity?
A) $O(1)$ B) $O(n)$ C) $O(\log n)$ D) $O(n^2)$
Answer: C – Merkle proofs require only $\log n$ hashes vs. n for full verification.

Q22. The avalanche effect in hash functions means:
A) Hash grows exponentially B) 1-bit input change flips 50% output C) Blocks cascade D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q23. The value formula suggests blockchain is best when:
A) Performance is critical B) Trust is high C) Trust deficit + coordination needs D) Single entity controls
Answer: C – Blockchain adds value when trust is lacking and coordination benefits are high.

Lesson 2a: DLT Fundamentals

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Define Distributed Ledger Technology (DLT) and distinguish it from blockchain
2. Explain the Byzantine Generals Problem and its relevance to consensus
3. Compare network topologies: centralized, decentralized, and distributed

Prerequisites: L01 - What is Blockchain?

This is Part 1 of 2 on DLT concepts. Part 2 (L02b) covers block structure and node types.

The Problem: How do we reach agreement in unreliable networks?

Part 1/2: Distributed Ledger Technology (Fundamentals)

The Challenge

Financial systems require all nodes to agree on the state of transactions, but some nodes may be offline, compromised, or deliberately malicious. How can we build consensus when we cannot trust every participant?

Why It Matters

- Without Byzantine fault tolerance, a single malicious node can cause payment systems to fail
- Traditional databases rely on trusted administrators; DLT must work in adversarial environments

What We Need

- Trustless verification mechanism
- Consensus protocols that tolerate up to $< 1/3$ malicious actors
- Network architectures that prevent single points of failure

The Cryptoeconomics Question

Coordinating without trusted intermediaries

Today's lesson: How Distributed Ledger Technology addresses this challenge

What is Distributed Ledger Technology?

DLT Definition

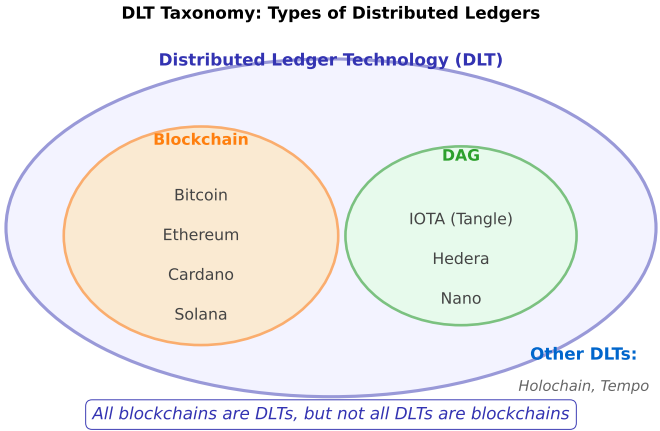
A **Distributed Ledger Technology (DLT)** is a database architecture where data is synchronized, replicated, and shared across multiple nodes in a network, without a central administrator.

Key Characteristics:

- **Distributed**: Data stored across many nodes (no single source of truth)
- **Synchronized**: All nodes maintain consistent state through consensus
- **Replicated**: Each node has a complete or partial copy of the ledger
- **Shared**: Multiple parties can read/write to the ledger
- **Consensus-driven**: Agreement mechanism validates changes

All blockchains are DLTs, but not all DLTs are blockchains

DLT Taxonomy: Types of Distributed Ledgers



Key Insight: Blockchain is a subset of DLT. Other approaches include DAGs (IOTA), Holochain, and Tempo (Radix).

Blockchain vs. Other DLTs

Blockchain

- Data organized in sequential blocks
- Blocks linked via cryptographic hashes
- Linear chain structure
- Append-only (immutable history)
- Examples: Bitcoin, Ethereum

Directed Acyclic Graph (DAG)

- Transactions reference previous transactions
- No blocks, no miners
- Parallel processing
- Examples: IOTA (Tangle), Hedera Hashgraph

Different DLT architectures optimize for different trade-offs

Holochain

- Agent-centric (not data-centric)
- Each agent maintains own chain
- Distributed Hash Table (DHT)
- No global consensus required

Tempo (Radix)

- Sharded state machine
- Logical clocks for ordering
- Scalable to millions of TPS
- Hybrid consensus

Ledger Types: Shared vs. Distributed

Shared Ledger (Traditional)

- Multiple parties access same database
- Central authority controls access
- Single version of truth
- Fast, but trust required

Example: Banking consortium database

Challenges:

- Single point of failure
- Administrator can alter records
- Reconciliation between systems

Distributed Ledger (DLT)

- Each party has own copy
- No central authority
- Consensus creates truth
- Slower, but trustless

Example: Public blockchain

Benefits:

- No single point of failure
- Transparent, auditable history
- No reconciliation needed

The Byzantine Generals Problem (1982)

Historical Context

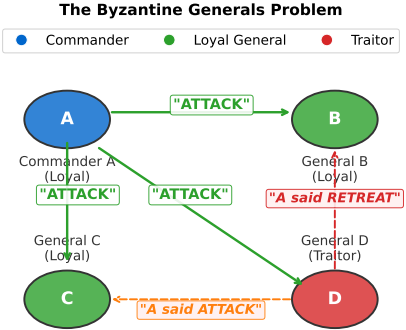
Leslie Lamport, Robert Shostak, and Marshall Pease formulated this thought experiment to describe the challenge of achieving consensus in distributed systems with potentially faulty or malicious actors.

The Scenario:

- Byzantine army surrounds an enemy city
- Army divided into divisions, each led by a general
- Generals must coordinate: **ATTACK** or **RETREAT**
- Communication only via messengers
- Some generals may be traitors (Byzantine faults)

Challenge: How can loyal generals reach consensus when traitors send conflicting messages?

Byzantine Generals: The Communication Challenge



Problem: How can loyal generals reach consensus when traitors send conflicting messages?

Problem: Traitor D sends conflicting messages to B and C, causing coordination failure.

Byzantine Generals: Example Scenario

Setup: 4 Generals (A, B, C, D), 1 is a traitor

Round 1 - Commander A sends orders:

- To General B: "ATTACK"
- To General C: "ATTACK"
- To General D (traitor): "ATTACK"

Round 2 - Traitor D sends conflicting messages:

- To General B: "A said RETREAT" (lie)
- To General C: "A said ATTACK" (truth)

Result Without Byzantine Fault Tolerance:

- General B thinks majority said RETREAT (withdraws alone)
- General C thinks majority said ATTACK (attacks alone)
- Army coordination fails, both divisions defeated

Byzantine Fault Tolerance (BFT)

Formal Result

Consensus is achievable if and only if at least $\frac{2}{3}$ of the actors are honest. Formally: $n \geq 3f + 1$ where n = total nodes, f = faulty nodes.

BFT Solution Requirements:

1. **Agreement**: All honest nodes decide on the same value
2. **Validity**: If all honest nodes propose value v, then v is decided
3. **Termination**: All honest nodes eventually decide

Blockchain Context:

- Bitcoin's Proof-of-Work solves Byzantine Generals Problem
- Nakamoto Consensus: Longest chain = majority decision
- Tolerates up to 49% malicious hash power (in practice, 51% attack possible)
- Practical BFT (PBFT) used in permissioned blockchains (Hyperledger)

Types of Faults in Distributed Systems

Crash Faults (Simpler)

- Node fails and stops responding
- Predictable behavior
- Detectable by timeout
- Example: Server power loss

Handling:

- Majority voting
- Heartbeat monitoring
- Leader election

Example: Apache Zookeeper, etcd (use Paxos/Raft)

Byzantine Faults (Complex)

- Node sends incorrect/conflicting information
- Malicious or software bugs
- Unpredictable behavior
- Example: Hacked node

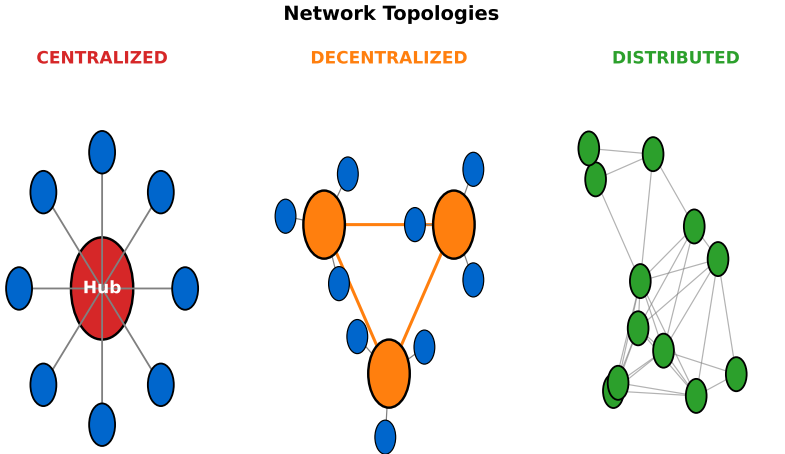
Handling:

- Cryptographic proofs
- Economic incentives
- Supermajority consensus ($> 2/3$)

Example: Bitcoin (PoW), Tendermint (BFT)

Key Insight: Public blockchains assume Byzantine environment; private blockchains may assume only crash faults

Network Topologies Comparison



Key Trade-off: Centralized is fast but fragile; Distributed is resilient but slower.

Centralized Networks

Architecture:

- Single central node (hub)
- All communication flows through hub
- Clients connect to central server
- Hub controls access and data

Advantages:

- Fast and efficient
- Easy to manage and update
- Low coordination overhead

Disadvantages:

- Single point of failure
- Censorship possible
- Privacy concerns (hub sees all data)

Examples: Traditional banking systems, Facebook, Gmail

Decentralized Networks

Architecture:

- Multiple hubs (federated model)
- Each hub serves subset of nodes
- Hubs communicate with each other
- No single central authority

Advantages:

- More resilient than centralized
- Regional autonomy
- Balanced between efficiency and resilience

Disadvantages:

- Hubs still represent points of failure
- Coordination between hubs needed
- Potential for fragmentation

Examples: Email (SMTP), Tor network, Mastodon (federated social media)

Distributed Networks

Architecture:

- Peer-to-peer (P2P) topology
- No hubs or central points
- Every node equal (or nearly equal)
- Direct node-to-node communication

Advantages:

- Maximum resilience (no single point of failure)
- Censorship resistant
- Highly fault-tolerant

Disadvantages:

- Slower coordination (consensus overhead)
- Complex to manage and upgrade
- Higher resource requirements per node

Examples: Bitcoin, Ethereum, BitTorrent, IPFS

Topology Comparison Table

Property	Centralized	Decentralized	Distributed
Control	Single entity	Multiple entities	All participants
Speed	Very fast	Fast	Slower
Resilience	Low (SPOF)	Medium	High
Censorship Resistance	None	Moderate	Strong
Coordination Overhead	Minimal	Moderate	High
Scalability	Easy (vertical)	Moderate	Hard (horizontal)
Trust Required	High	Medium	Low
Examples	Banks, Facebook	Email, Mastodon	Bitcoin, IPFS

Blockchain networks typically use fully distributed topology for maximum trustlessness

Problem Solved? Distributed Ledger Technology

The Original Problem

How do we reach agreement in unreliable networks?

How Distributed Ledger Technology Solves It

- **DLT taxonomy**: Permissioned vs permissionless architectures allow different trust assumptions
- **Byzantine fault tolerance**: Mathematical guarantee that $> 2/3$ honest nodes achieve consensus
- **Distributed topology**: Peer-to-peer networks eliminate single points of failure

Remaining Limitations

- **CAP theorem trade-offs**: Cannot simultaneously maximize consistency, availability, and partition tolerance
- **Coordination overhead**: Distributed consensus is slower than centralized systems

Open Questions

- What is the optimal fault tolerance ratio (f/n) for real-world networks?
- Risk: Sybil attacks, eclipse attacks

DLT partially solves "agreement in unreliable networks" but introduces new trade-offs (speed vs decentralization)

(c) Joerg Osterrieder 2025

Key Takeaways

What You Should Remember:

1. **DLT** is broader than blockchain; includes DAGs, Holochain, etc.
2. **Byzantine Generals Problem**: Achieving consensus with potentially malicious actors requires $> 2/3$ honest nodes
3. **Network Topologies**:
   - Centralized: fast but fragile
   - Decentralized: balanced
   - Distributed: resilient but slower
4. Public blockchains assume Byzantine faults; private may assume only crash faults

Next: L02b covers block structure, Merkle trees, and node types

Discussion Questions

Consider and discuss:

1. **DLT Selection**: When would a DAG (like IOTA) be preferable to a blockchain?
2. **Byzantine Assumptions**: Are public blockchains too conservative in assuming Byzantine faults?
3. **Network Design**: Why do most cryptocurrencies choose distributed over decentralized topologies?

Thank you

Questions?

Continue to L02b: DLT Architecture

Quiz Questions (1/2)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., DAGs like IOTA).

Q2. In the Byzantine Generals Problem, what minimum fraction of nodes must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – The formal requirement is $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed (P2P) networks have no central hubs, maximizing resilience.

Q4. Which fault type is more challenging for distributed systems to handle?
A) Crash faults B) Network partitions C) Byzantine faults D) Timeout errors
Answer: C – Byzantine faults involve malicious/conflicting behavior, harder than simple crashes.

Q5. What is the main advantage of centralized networks over distributed ones?
A) Censorship resistance B) Speed and efficiency C) No single point of failure D) Maximum decentralization
Answer: B – Centralized networks are faster/more efficient but have single point of failure.

Quiz Questions (2/2)

Q6. Which DLT architecture uses a Directed Acyclic Graph instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger Fabric D) Cardano
Answer: B – IOTA uses DAG (Tangle) where transactions reference previous transactions.

Q7. Who formulated the Byzantine Generals Problem in 1982?
A) Satoshi Nakamoto B) Vitalik Buterin C) Lamport, Shostak, and Pease D) Nick Szabo
Answer: C – Lamport, Shostak, and Pease published the foundational paper in 1982.

Q8. What consensus algorithm is commonly used for crash fault tolerance (not Byzantine)?
A) Proof-of-Work B) PBFT C) Paxos/Raft D) Proof-of-Stake
Answer: C – Paxos and Raft handle crash faults; PBFT and PoW handle Byzantine faults.

Q9. Which is an example of a decentralized (not distributed) network?
A) Bitcoin B) Email (SMTP) C) IPFS D) Ethereum
Answer: B – Email uses federated servers (decentralized hubs), not full P2P distribution.

Q10. What is the key difference between shared ledgers and distributed ledgers?
A) Shared ledgers are faster B) Distributed ledgers require no central authority C) Shared ledgers use consensus D) Distributed ledgers need permission
Answer: B – Distributed ledgers achieve consensus without central authority; shared ledgers rely on one.

Lesson 2a: DLT Fundamentals

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

The Coordination Problem

[COMIC: Byzantine generals disagreement]

Placeholder for comic illustration:

Four generals around a city. General A sends "ATTACK"

but traitor D tells B "retreat" and C "attack".

Caption: "When you can't trust the messenger..."

The Setup

- Generals must coordinate attack
- Messages may be lies
- Some generals are traitors

The Question

- How do loyal generals agree?
- How many traitors tolerable?
- Sound familiar? (blockchain nodes)

This 1982 thought experiment defines the core problem that DLT solves

Learning Objectives

By the end of this lesson, you will be able to:

1. Define Distributed Ledger Technology (DLT) and distinguish it from blockchain
2. Explain the Byzantine Generals Problem and its relevance to consensus
3. Compare network topologies: centralized, decentralized, and distributed

Prerequisites: L01 - What is Blockchain?

This is Part 1 of 2 on DLT concepts. Part 2 (L02b) covers block structure and node types.

Building on L01: What is Blockchain?

The Problem: How do we reach agreement in unreliable networks?

Part 1/2: Distributed Ledger Technology (Fundamentals)

The Challenge

Financial systems require all nodes to agree on the state of transactions, but some nodes may be offline, compromised, or deliberately malicious. How can we build consensus when we cannot trust every participant?

Why It Matters

- Without Byzantine fault tolerance (the ability to reach agreement despite some malicious participants), a single malicious node can cause payment systems to fail
- Traditional databases rely on trusted administrators; DLT must work in adversarial environments

What We Need

- Trustless verification mechanism
- Consensus protocols that tolerate up to $< 1/3$ malicious actors
- Network architectures that prevent single points of failure

The Cryptoeconomics Question

Coordinating without trusted intermediaries

Today's lesson: How Distributed Ledger Technology addresses this challenge

What is Distributed Ledger Technology?

DLT Definition

A **Distributed Ledger Technology (DLT)** is a database architecture where data is synchronized, replicated, and shared across multiple nodes in a network, without a central administrator.

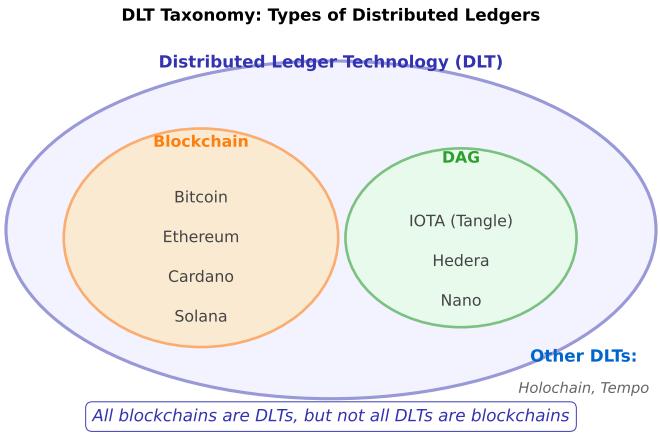
Key Characteristics:

- **Distributed**: Data stored across many nodes (no single source of truth)
- **Synchronized**: All nodes maintain consistent state through consensus
- **Replicated**: Each node has a complete or partial copy of the ledger
- **Shared**: Multiple parties can read/write to the ledger
- **Consensus-driven**: Agreement mechanism validates changes

All blockchains are DLTs, but not all DLTs are blockchains

DLT solves distributed agreement by replicating state across nodes without requiring a trusted coordinator

What Are the Different Types of DLT?



Key Insight: Blockchain is a subset of DLT. Other approaches include DAGs (IOTA), Holochain, and Tempo (Radix).

How Does Blockchain Differ from Other DLTs?

Blockchain

- Data organized in sequential blocks
- Blocks linked via cryptographic hashes
- Linear chain structure
- Append-only (immutable history)
- Examples: Bitcoin, Ethereum

Directed Acyclic Graph (DAG)

- Transactions reference previous transactions
- No blocks, no miners
- Parallel processing
- Examples: IOTA (Tangle), Hedera Hashgraph

Different DLT architectures optimize for different trade-offs

Holochain

- Agent-centric (not data-centric)
- Each agent maintains own chain
- Distributed Hash Table (DHT)
- No global consensus required

Tempo (Radix)

- Sharded state machine
- Logical clocks for ordering
- Scalable to millions of TPS
- Hybrid consensus

What's the Difference Between Shared and Distributed Ledgers?

Shared Ledger (Traditional)

- Multiple parties access same database
- Central authority controls access
- Single version of truth
- Fast, but trust required

Example: Banking consortium database

Challenges:

- Single point of failure
- Administrator can alter records
- Reconciliation between systems

Distributed Ledger (DLT)

- Each party has own copy
- No central authority
- Consensus creates truth
- Slower, but trustless

Example: Public blockchain

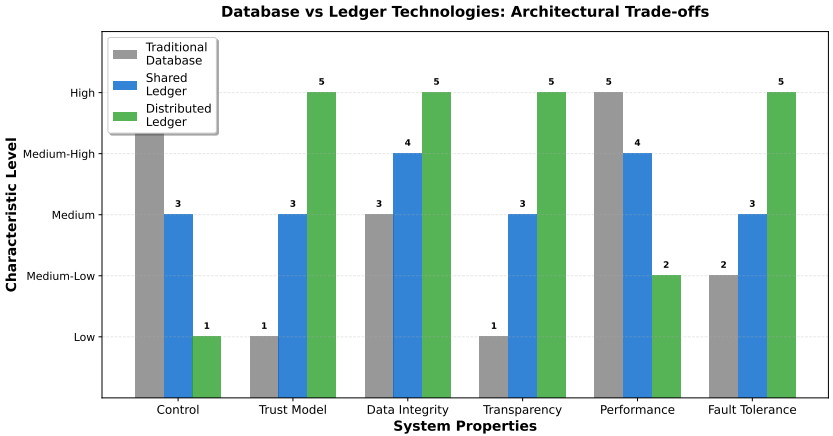
Benefits:

- No single point of failure
- Transparent, auditable history
- No reconciliation needed

Shared ledgers trust administrators; distributed ledgers achieve consensus through Byzantine fault tolerance protocols

(c) Joerg Osterrieder 2025

How Do Databases Differ from Distributed Ledgers?



Interpretation: Traditional DBs optimize for performance and central control. Shared Ledgers balance multiple parties' needs. Distributed Ledgers prioritize trustlessness and fault tolerance over speed.

Key Insight: Traditional databases optimize for performance; DLTs trade speed for trustlessness and fault tolerance.

The Byzantine Generals Problem (1982)

Historical Context

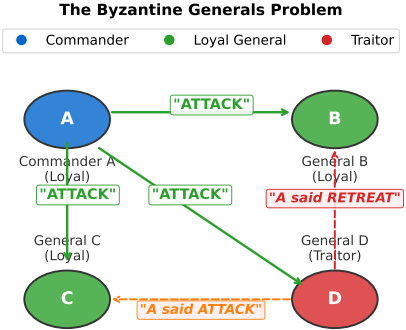
Leslie Lamport, Robert Shostak, and Marshall Pease formulated this thought experiment to describe the challenge of achieving consensus in distributed systems with potentially faulty or malicious actors.

The Scenario:

- Byzantine army surrounds an enemy city
- Army divided into divisions, each led by a general
- Generals must coordinate: **ATTACK** or **RETREAT**
- Communication only via messengers
- Some generals may be traitors (Byzantine faults)

Challenge: How can loyal generals reach consensus when traitors send conflicting messages?

How Do Byzantine Generals Illustrate the Consensus Challenge?



Problem: How can loyal generals reach consensus when traitors send conflicting messages?

Problem: Traitor D sends conflicting messages to B and C, causing coordination failure.

How Does the Byzantine Generals Problem Work?

Setup: 4 Generals (A, B, C, D), 1 is a traitor

Round 1 - Commander A sends orders:

- To General B: "ATTACK"
- To General C: "ATTACK"
- To General D (traitor): "ATTACK"

Round 2 - Traitor D sends conflicting messages:

- To General B: "A said RETREAT" (lie)
- To General C: "A said ATTACK" (truth)

Result Without Byzantine Fault Tolerance:

- General B thinks majority said RETREAT (withdraws alone)
- General C thinks majority said ATTACK (attacks alone)
- Army coordination fails, both divisions defeated

Problem Check-In: Distributed Ledger Technology

Recall Our Problem

How do we reach agreement in unreliable networks?

What We've Learned So Far

- Distributed systems face the Byzantine Generals Problem
- Consensus protocols enable agreement despite faulty nodes
- Both concepts address trust in unreliable networks

Still to Address

- How do we achieve finality? What are the trade-offs?
- Can we tolerate more than 1/3 Byzantine nodes?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we reach agreement in unreliable..."?

How Many Honest Nodes Are Needed for Byzantine Fault Tolerance?

Formal Result

Consensus is achievable if and only if at least $\frac{2}{3}$ of the actors are honest. Formally: $n \geq 3f + 1$ where n = total nodes, f = faulty nodes.

BFT Solution Requirements:

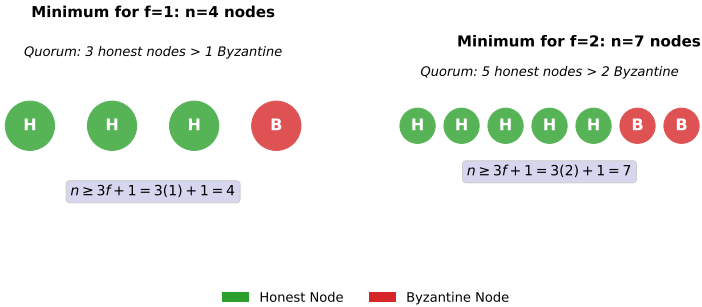
1. **Agreement**: All honest nodes decide on the same value
2. **Validity**: If all honest nodes propose value v, then v is decided
3. **Termination**: All honest nodes eventually decide

Blockchain Context:

- Bitcoin's Proof-of-Work solves Byzantine Generals Problem
- Nakamoto Consensus: Longest chain = majority decision
- Tolerates up to 49% malicious hash power (in practice, 51% attack possible)
- Practical BFT (PBFT) used in permissioned blockchains (Hyperledger)

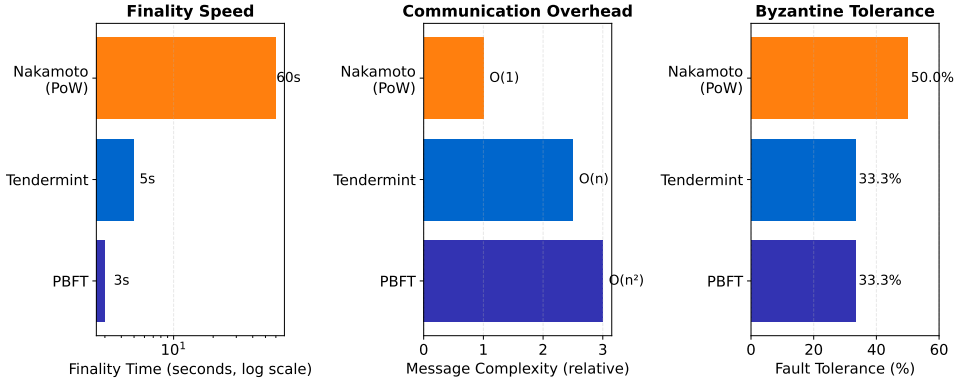
Byzantine fault tolerance provides mathematical guarantee: consensus with $< 1/3$ malicious nodes, critical for trustless agreement

Why Do We Need n $\geq$ 3f+1 Nodes for Byzantine Fault Tolerance?



Key Insight: Need at least 3f+1 total nodes to tolerate f Byzantine failures - quorum of honest nodes must outnumber Byzantine nodes.

How Do Different Consensus Protocols Compare?



Trade-off: PBFT offers fast finality but high message overhead; Nakamoto consensus is simpler but slower.

What Types of Faults Can Occur in Distributed Systems?

Crash Faults (Simpler)

- Node fails and stops responding
- Predictable behavior
- Detectable by timeout
- Example: Server power loss

Handling:

- Majority voting
- Heartbeat monitoring
- Leader election

Example: Apache Zookeeper, etcd (use Paxos/Raft)

Byzantine Faults (Complex)

- Node sends incorrect/conflicting information
- Malicious or software bugs
- Unpredictable behavior
- Example: Hacked node

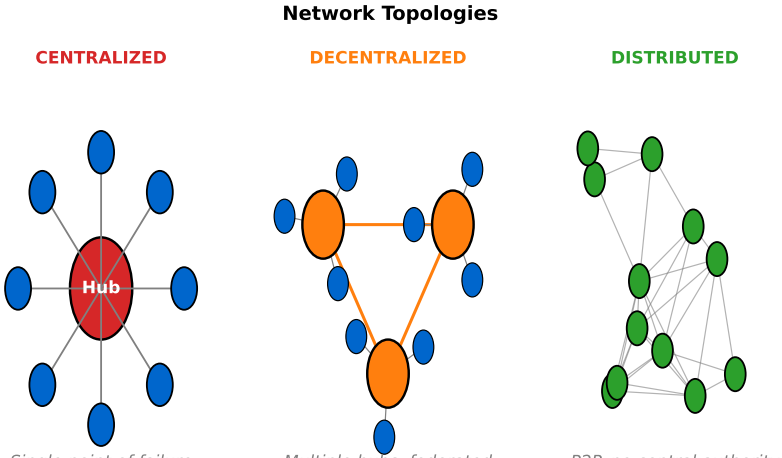
Handling:

- Cryptographic proofs
- Economic incentives
- Supermajority consensus ($> 2/3$)

Example: Bitcoin (PoW), Tendermint (BFT)

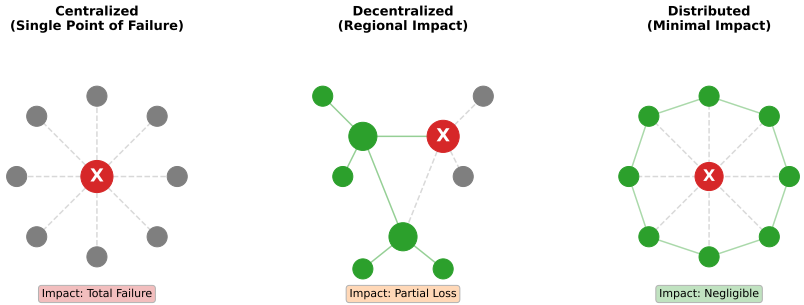
Key Insight: Public blockchains assume Byzantine environment; private blockchains may assume only crash faults

How Do Network Topologies Compare?



Key Trade-off: Centralized is fast but fragile; Distributed is resilient but slower.

How Does Network Topology Affect Resilience to Node Failures?



Key Insight: Single node failure has catastrophic impact in centralized networks, negligible impact in distributed mesh networks.

How Do Centralized Networks Work?

Architecture:

- Single central node (hub)
- All communication flows through hub
- Clients connect to central server
- Hub controls access and data

Advantages:

- Fast and efficient
- Easy to manage and update
- Low coordination overhead

Disadvantages:

- Single point of failure
- Censorship possible
- Privacy concerns (hub sees all data)

Examples: Traditional banking systems, Facebook, Gmail

Centralized networks solve coordination efficiently but cannot provide Byzantine fault tolerance without trusted authority

How Do Decentralized Networks Work?

Architecture:

- Multiple hubs (federated model)
- Each hub serves subset of nodes
- Hubs communicate with each other
- No single central authority

Advantages:

- More resilient than centralized
- Regional autonomy
- Balanced between efficiency and resilience

Disadvantages:

- Hubs still represent points of failure
- Coordination between hubs needed
- Potential for fragmentation

Examples: Email (SMTP), Tor network, Mastodon (federated social media)

(c) Joerg Osterrieder 2025

How Do Distributed Networks Work?

Architecture:

- Peer-to-peer (P2P) topology
- No hubs or central points
- Every node equal (or nearly equal)
- Direct node-to-node communication

Advantages:

- Maximum resilience (no single point of failure)
- Censorship resistant
- Highly fault-tolerant

Disadvantages:

- Slower coordination (consensus overhead)
- Complex to manage and upgrade
- Higher resource requirements per node

Examples: Bitcoin, Ethereum, BitTorrent, IPFS

(c) Joerg Osterrieder 2025

What Are the Key Trade-offs Between Network Topologies?

Property	Centralized	Decentralized	Distributed
Control	Single entity	Multiple entities	All participants
Speed	Very fast	Fast	Slower
Resilience	Low (SPOF)	Medium	High
Censorship Resistance	None	Moderate	Strong
Coordination Overhead	Minimal	Moderate	High
Scalability	Easy (vertical)	Moderate	Hard (horizontal)
Trust Required	High	Medium	Low
Examples	Banks, Facebook	Email, Mastodon	Bitcoin, IPFS

Blockchain networks typically use fully distributed topology for maximum trustlessness

The Solution: Distributed Consensus

[COMIC: Distributed vs centralized control]

Placeholder for comic illustration:

Left: King on throne (Centralized – single point of failure)

Right: Circle of equal nodes holding ledger copies

Caption: "When everyone keeps the books, no one can cheat"

What We Learned

- BFT: $> 2/3$ honest nodes required
- Network topology affects resilience
- DLT = consensus without central authority

The Trade-off

- Centralized: Fast but fragile
- Distributed: Resilient but slower

DLT transforms the Byzantine problem from military metaphor to working technology

Problem Solved? Distributed Ledger Technology

The Original Problem

How do we reach agreement in unreliable networks?

How Distributed Ledger Technology Solves It

- **DLT taxonomy**: Permissioned vs permissionless architectures allow different trust assumptions
- **Byzantine fault tolerance**: Mathematical guarantee that $> 2/3$ honest nodes achieve consensus
- **Distributed topology**: Peer-to-peer networks eliminate single points of failure

Remaining Limitations

- **CAP theorem trade-offs**: Cannot simultaneously maximize consistency, availability, and partition tolerance
- **Coordination overhead**: Distributed consensus is slower than centralized systems

Open Questions

- What is the optimal fault tolerance ratio (f/n) for real-world networks?
- Risk: Sybil attacks, eclipse attacks

DLT partially solves "agreement in unreliable networks" but introduces new trade-offs (speed vs decentralization)

(c) Joerg Osterrieder 2025

The Economics of Byzantine Fault Tolerance

Incentive Structure

- **Core Problem:** Reaching consensus despite Byzantine (arbitrary) failures
- **Why act honestly?** Validators stake assets; misbehavior results in slashing penalties
- **Value Flow:** Honest validators earn rewards; Byzantine actors lose their stake

Economic Security

- Slashing penalties ¿ potential gain from attack
- Staking creates "skin in the game"

Key Economic Question

Who Pays, Who Earns?

Byzantine actors pay slashing penalties; honest validators earn block rewards and fees

Design Principle

$$\text{Slash Amount} > \text{Attack Gain}$$

Byzantine tolerance through economic incentives: Make honesty profitable, misbehavior costly

Design Space: Byzantine Consensus Mechanisms

Alternatives Considered

1. **PBFT:** Tolerates f failures with $3f + 1$ nodes, but $O(n^2)$ messages
2. **Nakamoto Consensus:** Probabilistic finality, but simpler protocol

Trade-offs Made

- Immediate finality vs probabilistic finality
- Communication complexity vs simplicity

Design Questions

- What's acceptable: deterministic or probabilistic finality?
- How many rounds of communication are tolerable?
- Permissioned (known validators) or permissionless?

Key Insight

Consensus Trade-offs

Fast finality requires more communication overhead; simple protocols sacrifice determinism.

Design question: Immediate finality vs probabilistic finality - what's acceptable for your use case?

Failure Modes: Byzantine Fault Tolerance

Critical Assumption

- **What's assumed:** At most 1/3 of nodes are Byzantine ($f < n/3$)
- **What breaks:** More than 1/3 Byzantine nodes violates safety

Root Cause

- Network partitions can violate Byzantine assumptions temporarily
- Coordinated validator takeover
- Economic attack vectors (bribery)

Historical Context

- **2016 The DAO:** Smart contract exploit, not consensus failure, but led to contentious fork
- Consensus held; social layer split

Early Warning Signs

! Validator centralization (geographic, entity)

! Network partition events

! Sustained high confirmation delays

Warning: Network partitions can violate Byzantine assumptions temporarily - monitor validator diversity

Key Takeaways

What You Should Remember:

1. **DLT** is broader than blockchain; includes DAGs, Holochain, etc.
2. **Byzantine Generals Problem**: Achieving consensus with potentially malicious actors requires $> 2/3$ honest nodes
3. **Network Topologies**:
   - Centralized: fast but fragile
   - Decentralized: balanced
   - Distributed: resilient but slower
4. Public blockchains assume Byzantine faults; private may assume only crash faults

Next: L02b covers block structure, Merkle trees, and node types

Next Lesson: L02b – DLT Architecture

Discussion Questions

Consider and discuss:

1. **DLT Selection**: When would a DAG (like IOTA) be preferable to a blockchain?
2. **Byzantine Assumptions**: Are public blockchains too conservative in assuming Byzantine faults?
3. **Network Design**: Why do most cryptocurrencies choose distributed over decentralized topologies?

Thank you

Questions?

Continue to L02b: DLT Architecture

Quiz Questions (1/2)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., DAGs like IOTA).

Q2. In the Byzantine Generals Problem, what minimum fraction of nodes must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – The formal requirement is $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed (P2P) networks have no central hubs, maximizing resilience.

Q4. Which fault type is more challenging for distributed systems to handle?
A) Crash faults B) Network partitions C) Byzantine faults D) Timeout errors
Answer: C – Byzantine faults involve malicious/conflicting behavior, harder than simple crashes.

Q5. What is the main advantage of centralized networks over distributed ones?
A) Censorship resistance B) Speed and efficiency C) No single point of failure D) Maximum decentralization
Answer: B – Centralized networks are faster/more efficient but have single point of failure.

Quiz Questions (2/2)

Q6. Which DLT architecture uses a Directed Acyclic Graph instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger Fabric D) Cardano
Answer: B – IOTA uses DAG (Tangle) where transactions reference previous transactions.

Q7. Who formulated the Byzantine Generals Problem in 1982?
A) Satoshi Nakamoto B) Vitalik Buterin C) Lamport, Shostak, and Pease D) Nick Szabo
Answer: C – Lamport, Shostak, and Pease published the foundational paper in 1982.

Q8. What consensus algorithm is commonly used for crash fault tolerance (not Byzantine)?
A) Proof-of-Work B) PBFT C) Paxos/Raft D) Proof-of-Stake
Answer: C – Paxos and Raft handle crash faults; PBFT and PoW handle Byzantine faults.

Q9. Which is an example of a decentralized (not distributed) network?
A) Bitcoin B) Email (SMTP) C) IPFS D) Ethereum
Answer: B – Email uses federated servers (decentralized hubs), not full P2P distribution.

Q10. What is the key difference between shared ledgers and distributed ledgers?
A) Shared ledgers are faster B) Distributed ledgers require no central authority C) Shared ledgers use consensus D) Distributed ledgers need permission
Answer: B – Distributed ledgers achieve consensus without central authority; shared ledgers rely on one.

Lesson 2b: DLT Architecture

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Describe the structure and components of a blockchain block
2. Explain Merkle trees and their role in transaction verification
3. Differentiate between node types: full nodes, light nodes, miners, validators
4. Contrast permissioned and permissionless blockchain architectures

Prerequisites: L02a - DLT Fundamentals

This is Part 2 of 2 on DLT concepts. Part 1 (L02a) covered DLT definition and Byzantine consensus.

The Problem: How do we structure data for trustless verification?

Part 2/2: DLT Architecture (Integration)

The Challenge
How do we structure blocks and verify transactions efficiently across thousands of nodes without a central database?

Why It Matters

- Block structure determines security properties and performance limits
- Bitcoin's block size debate (2015-2017) led to SegWit upgrade and Lightning Network

What We Need

- Trustless verification mechanism
- Efficient data structures for tamper-evident storage at scale

The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How DLT architecture addresses this challenge through Merkle trees and node design

Anatomy of a Block: Overview

A blockchain block contains two main parts:

1. **Block Header** (80 bytes in Bitcoin)
   - Metadata about the block
   - Links to previous block
   - Proof-of-Work evidence
2. **Block Body** (variable size)
   - Transaction data
   - Can contain hundreds to thousands of transactions

Block Size Limits:

- Bitcoin: 1 MB (base block) to 4 MB (with SegWit)
- Ethereum: Dynamic gas limit ($\approx$ 30M gas, $\approx$ 15 MB)
- Bitcoin Cash: 32 MB

(c) Joerg Osterrieder 2025

Block Header Components

Bitcoin Block Header Fields (80 bytes):

1. **Version** (4 bytes): Block version number (for protocol upgrades)
2. **Previous Block Hash** (32 bytes): Hash of the previous block header
3. **Merkle Root** (32 bytes): Hash of all transactions in this block
4. **Timestamp** (4 bytes): Unix epoch time (seconds since Jan 1, 1970)
5. **Difficulty Target** (4 bytes): Required difficulty for PoW
6. **Nonce** (4 bytes): Counter used for PoW mining

Key Insight:

$$\text{Block Hash} = \text{SHA256}(\text{SHA256}(\text{Header}))$$

The hash must be below the difficulty target for the block to be valid.

Merkle Trees: Efficient Transaction Verification

Merkle Tree Definition

A **Merkle tree** is a binary hash tree where each leaf node is a hash of a transaction, and each non-leaf node is a hash of its two children.

Construction Process:

1. Hash each transaction: $H(Tx_1), H(Tx_2), ..., H(Tx_n)$
2. Pair hashes and hash again: $H(H(Tx_1)||H(Tx_2))$
3. Repeat until single root hash (Merkle Root)

Benefits:

- **Compact Proof**: Verify transaction inclusion with $O(\log n)$ hashes
- **Efficient Storage**: Light clients store only 80-byte headers
- **Integrity**: Any transaction change alters Merkle Root

Example: Prove transaction in block with 1,000 tx requires only 10 hashes ($\log_2 1000 \approx 10$)

Merkle Proof Example

Scenario: Block contains 8 transactions, prove Tx_3 is included

Tree Structure:

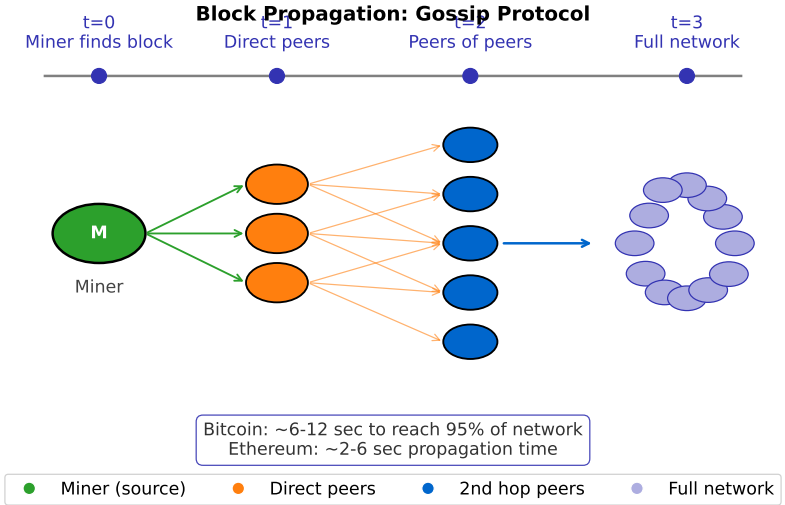
- Level 3 (Root): $R = H(AB||CD)$ where $AB = H(A||B)$, $CD = H(C||D)$
- Level 2: $A = H(Tx_1||Tx_2)$, $B = H(Tx_3||Tx_4)$, etc.
- Level 1: Tx_1, Tx_2, Tx_3, Tx_4, ..., Tx_8

Merkle Proof for Tx_3:

1. Verifier has: Block header with Merkle Root R
2. Prover provides: Tx_3, $H(Tx_4)$, $H(A)$, $H(CD)$
3. Verifier computes: $H(Tx_3)$, then $B = H(H(Tx_3)||H(Tx_4))$
4. Then: $AB = H(H(A)||B)$, finally $R' = H(AB||H(CD))$
5. If $R' = R$, then Tx_3 is proven to be in the block

Only 3 hashes needed instead of downloading all 8 transactions

Block Propagation via Gossip Protocol



Timeline: Miner broadcasts to peers, who propagate to their peers, until full network coverage.

(c) Joerg Osterrieder 2025

Block Propagation Details

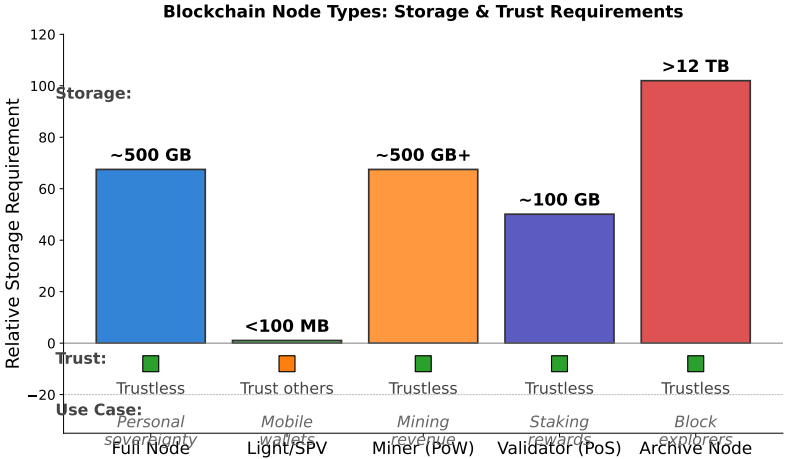
How New Blocks Spread Through Network:

1. Miner finds valid block (solves PoW puzzle)
2. Miner broadcasts block to connected peers ($\approx$ 8-125 peers)
3. Peers validate block:
   - Check block hash meets difficulty target
   - Verify all transactions are valid
   - Ensure no double-spends
4. Valid block propagated to peers' peers (gossip protocol)
5. Process repeats until entire network has the block

Propagation Time:

- Bitcoin: $\approx$ 6-12 seconds to reach 95% of network
- Ethereum (pre-merge): $\approx$ 2-6 seconds
- Faster propagation reduces orphan block rate

Blockchain Node Types: Storage and Trust



Trade-off: Higher storage requirements enable trustless verification; lower requirements require trusting others.

Full Nodes

Full Node Definition

A **full node** downloads and validates the entire blockchain history, enforcing all consensus rules without relying on third parties.

Responsibilities:

- Store complete blockchain (Bitcoin: $\approx$ 600 GB, Ethereum: $\approx$ 2 TB)
- Validate all blocks and transactions independently
- Relay valid transactions and blocks to peers
- Serve blockchain data to light clients

Benefits:

- Maximum security (trust no one)
- Support network decentralization
- Can verify historical transactions

Requirements: $\approx$ 500 GB storage, $\approx$ 5 GB/day bandwidth, moderate CPU

Light Nodes (SPV Nodes)

Simplified Payment Verification (SPV)

Described in Bitcoin whitepaper: Light nodes download only block headers ($\approx$ 80 bytes each) instead of full blocks, relying on Merkle proofs to verify transactions.

Operation:

- Download all block headers ($\approx$ 50 MB for Bitcoin)
- Request Merkle proofs from full nodes for relevant transactions
- Verify transaction inclusion in block
- Assume longest chain is valid

Trade-offs:

+ Low storage ($<$ 100 MB vs. 500 GB)
+ Suitable for mobile devices
- Must trust full nodes for transaction data
- Vulnerable to bloom filter privacy leaks

Miner Nodes (PoW)

Specialized Nodes in Proof-of-Work Blockchains

Functions:

1. Collect unconfirmed transactions from mempool
2. Construct candidate block (select transactions based on fees)
3. Attempt to find valid nonce (compute millions of hashes/second)
4. Broadcast valid block if found
5. Receive block reward + transaction fees

Requirements:

- Specialized hardware (ASICs for Bitcoin, GPUs for some altcoins)
- High electricity consumption (Bitcoin: $\approx$ 150 TWh/year globally)
- Cooling infrastructure
- High-bandwidth internet connection

Economics:

- Bitcoin block reward: 3.125 BTC (post-April 2024 halving)
- Break-even depends on: Hash rate, electricity cost, BTC price

Validator Nodes (PoS)

Specialized Nodes in Proof-of-Stake Blockchains

Functions:

1. Stake cryptocurrency as collateral (Ethereum: 32 ETH minimum)
2. Selected to propose/attest blocks based on stake
3. Earn rewards for honest participation
4. Risk slashing (stake confiscation) for malicious behavior

Ethereum Validator Requirements:

- 32 ETH staked (locked)
- Run validator client 24/7 ($>$ 99% uptime)
- Consumer-grade hardware (4 GB RAM, 100 GB SSD)
- Stable internet (10 Mbps)

Comparison to Mining:

+ 99.95% less energy consumption
+ Lower hardware requirements
- Capital locked (opportunity cost)
- Slashing risk if offline or malicious

Archive Nodes

Full Historical State Storage

- Store every state of the blockchain at every block height
- Enable queries like: "What was Alice's balance at block 1,000,000?"
- Required for block explorers (Etherscan, Blockchain.com)
- Needed for advanced analytics and forensics

Storage Requirements:

- Bitcoin archive node: $\approx$ 500 GB (same as full node, UTXO model)
- Ethereum archive node: $\approx$ 12 TB (account model stores all states)
- Grows continuously (Ethereum: $+1$ TB/year)

Use Cases:

- Block explorers
- Tax reporting services
- Academic research
- Forensic analysis

Node Type Comparison

Node Type	Storage	Validation	Trust Model	Use Case
Full Node	$\approx$ 500 GB	All blocks & txs	Trustless	Personal sovereignty
Light/SPV	$<$ 100 MB	Headers only	Trust full nodes	Mobile wallets
Miner (PoW)	$\approx$ 500 GB +	Full validation	Trustless	Mining revenue
Validator (PoS)	$\approx$ 100 GB	Full validation	Trustless	Staking rewards
Archive Node	$>$ 10 TB	Full + history	Trustless	Analytics, explorers

Decentralization Trade-off:

- More full nodes = more decentralization
- High storage requirements = fewer full nodes
- Blockchain scalability trilemma: Security, Decentralization, Scalability

Permissionless Blockchains (Public)

Definition

Permissionless (public) blockchains allow anyone to join, read, write, and participate in consensus without approval from a central authority.

Characteristics:

- Open participation (anyone can run a node)
- Pseudonymous identities (addresses, not real names)
- Transparent transaction history (all data public)
- Censorship resistant
- Token-based incentives (mining/staking rewards)

Examples: Bitcoin, Ethereum, Cardano, Solana

Best For: Global, trustless applications (DeFi, NFTs), censorship-resistant systems

(c) Joerg Osterrieder 2025

Permissioned Blockchains (Private/Consortium)

Definition

Permissioned blockchains restrict participation to verified entities. Access to read, write, or validate is controlled by administrators.

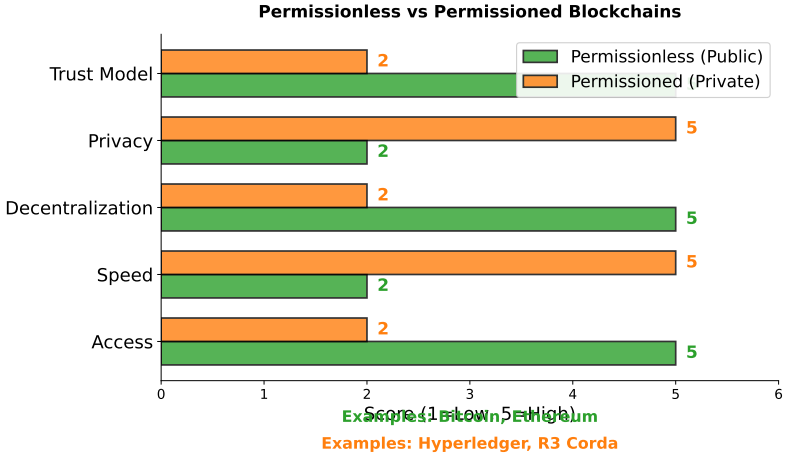
Characteristics:

- Controlled participation (invitation-only)
- Known identities (KYC/AML compliance)
- Selective transparency (private channels possible)
- Efficient consensus (no mining, BFT-based)
- No native cryptocurrency (optional)

Examples: Hyperledger Fabric, R3 Corda, JP Morgan Quorum

Best For: Enterprise consortia (supply chain, trade finance), regulatory compliance

Permissioned vs Permissionless: Key Dimensions



Trade-off: Permissionless maximizes decentralization/trust; Permissioned maximizes speed/privacy.

Comparison: Permissionless vs. Permissioned

Permissionless (Public)

Advantages:

- Maximum decentralization
- Censorship resistant
- Network effects (large user base)
- Innovation without permission

Disadvantages:

- Slower throughput (5-30 TPS)
- Higher costs (gas fees)
- Energy intensive (PoW)
- No privacy by default

Permissioned (Private)

Advantages:

- High throughput (1,000+ TPS)
- Low/no transaction fees
- Energy efficient (BFT)
- Configurable privacy

Disadvantages:

- Central point of control
- Limited network effects
- Potential for censorship
- Requires trust in admins

Hybrid models exist: Public with private sidechains (e.g., Polygon for Ethereum)

(c) Joerg Osterrieder 2025

When to Choose Each Type

Criterion	Permissionless	Permissioned
Trust Model	No trust required	Parties partially trust each other
Participants	Unknown, global	Known, verified entities
Governance	Decentralized (hard forks)	Centralized/consortium voting
Performance	5-30 TPS	1,000-10,000+ TPS
Privacy	Pseudonymous, transparent	Configurable, private channels
Use Cases	DeFi, NFTs, payments	Supply chain, trade finance, CBDCs

Problem Solved? DLT Architecture

The Original Problem

How do we structure data for trustless verification across thousands of nodes?

How DLT Architecture Solves It

- Merkle trees enable O(log n) verification instead of downloading all transactions
- Block headers separate metadata from transaction data (80 bytes vs. MB)
- Full nodes independently validate entire history without trusting anyone

Remaining Limitations

- Block size limits transaction throughput (Bitcoin: 7 TPS, Ethereum: 30 TPS)
- Storage requirements create centralization pressure (600 GB+ for full nodes)

Open Questions

- Optimal balance between full nodes (decentralization) and light clients (accessibility)?
- Risk: As storage grows, fewer users can verify independently

DLT architecture enables trustless verification but introduces scalability-decentralization trade-offs

Key Takeaways

What You Should Remember:

1. **Block Structure**: Header (80 bytes) + Body (transactions), linked via cryptographic hashes
2. **Merkle Trees**: Enable efficient transaction verification ($O(\log n)$ proof size)
3. **Node Types**:
   - Full (trustless), Light (trust others)
   - Miner/Validator (consensus), Archive (historical queries)
4. **Permissioned vs. Permissionless**: Public for trustless apps, private for enterprise consortia

Next: L03 - Cryptographic Hash Functions

Discussion Questions

Consider and discuss:

1. **Decentralization Trade-offs**: At what point does storage cost compromise decentralization?
2. **Node Selection**: When would you run a full node vs. use a light client?
3. **Enterprise Blockchain**: Why do enterprises often prefer permissioned chains?

Thank you

Questions?

Continue to L03: Cryptographic Hash Functions

Quiz Questions (1/2)

Q1. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes (6 fields).

Q2. What is the purpose of the Merkle Root in a block header?
A) Identify previous block B) Prove all transactions included C) Set mining difficulty D) Store timestamp
Answer: B – Merkle Root commits to all transactions, enabling efficient verification.

Q3. How many hashes are needed to verify a transaction in a block with 1,024 transactions using a Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes needed for Merkle proof.

Q4. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of 2025).

Q5. What does SPV stand for in the context of light nodes?
A) Secure Payment Validation B) Simplified Payment Verification C) Shared Proof Verification D) Synchronized Peer Validation
Answer: B – SPV (Simplified Payment Verification) described in Bitcoin whitepaper.

Quiz Questions (2/2)

Q6. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q7. Which node type stores every historical state at every block height?
A) Full node B) Light node C) Archive node D) Miner node
Answer: C – Archive nodes store complete historical state (e.g., 12 TB for Ethereum).

Q8. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public chains B) Permissioned private chains C) Both equal D) Depends only on hardware
Answer: B – Permissioned chains achieve 1,000+ TPS vs. 5-30 TPS for public chains.

Q9. What protocol do Bitcoin nodes use to propagate new blocks?
A) HTTP B) FTP C) Gossip protocol D) TCP handshake
Answer: C – Gossip protocol: nodes relay to peers, who relay to their peers.

Q10. Which field in the Bitcoin block header links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp
Answer: C – Previous Block Hash (32 bytes) creates the cryptographic chain.

Lesson 2b: DLT Architecture

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Building the Blockchain

[COMIC: Block stacking like Tetris]

"Each block must fit perfectly with the one below—
one wrong piece and the whole structure is compromised."

Today's Challenge: How do we structure data so thousands of computers can verify it independently?

Learning Objectives

By the end of this lesson, you will be able to:

1. Describe the structure and components of a blockchain block
2. Explain Merkle trees and their role in transaction verification
3. Differentiate between node types: full nodes, light nodes, miners, validators
4. Contrast permissioned and permissionless blockchain architectures

Prerequisites: L02a - DLT Fundamentals

This is Part 2 of 2 on DLT concepts. Part 1 (L02a) covered DLT definition and Byzantine consensus.

Building on L02a: DLT Fundamentals

The Problem: How do we structure data for trustless verification (no third-party trust required)?

Part 2/2: DLT Architecture (Integration)

The Challenge

How do we structure blocks and verify transactions efficiently across thousands of nodes without a central database?

Why It Matters

- Block structure determines security properties and performance limits
- Bitcoin's block size debate (2015-2017) led to SegWit upgrade and Lightning Network

What We Need

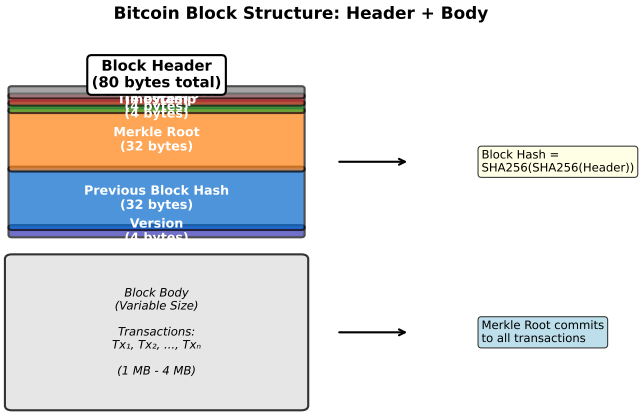
- Trustless verification mechanism
- Efficient data structures for tamper-evident storage at scale

The Cryptoeconomics Question

Coordinating without trusted intermediaries

Today's lesson: How DLT architecture addresses this challenge through Merkle trees and node design

What is Inside a Block?



Block Size Limits: Bitcoin: 1 MB (base block) to 4 MB (with SegWit) — Ethereum: Dynamic gas limit (≈ 30M gas, ≈ 15 MB)

Block structure provides tamper-evident data containers that enable trustless verification without central coordination

What Are the Components of a Block Header?

Bitcoin Block Header Fields (80 bytes):

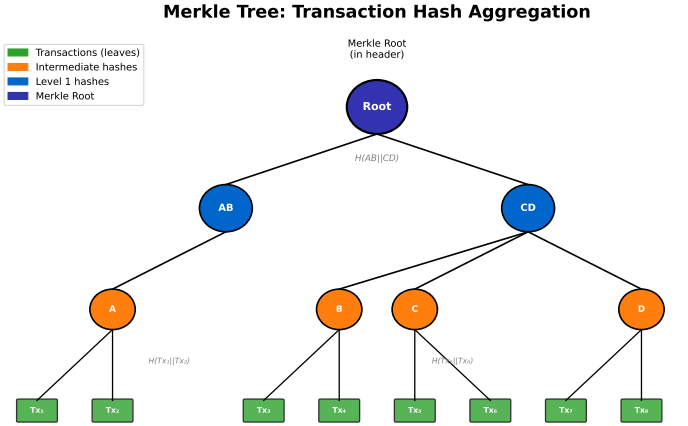
1. **Version** (4 bytes): Block version number (for protocol upgrades)
2. **Previous Block Hash** (32 bytes): Hash of the previous block header
3. **Merkle Root** (32 bytes): Hash of all transactions in this block
4. **Timestamp** (4 bytes): Unix epoch time (seconds since Jan 1, 1970)
5. **Difficulty Target** (4 bytes): Required difficulty for PoW
6. **Nonce** (4 bytes): Counter used for PoW mining

Key Insight:

$$\text{Block Hash} = \text{SHA256}(\text{SHA256}(\text{Header}))$$

The hash must be below the difficulty target for the block to be valid.

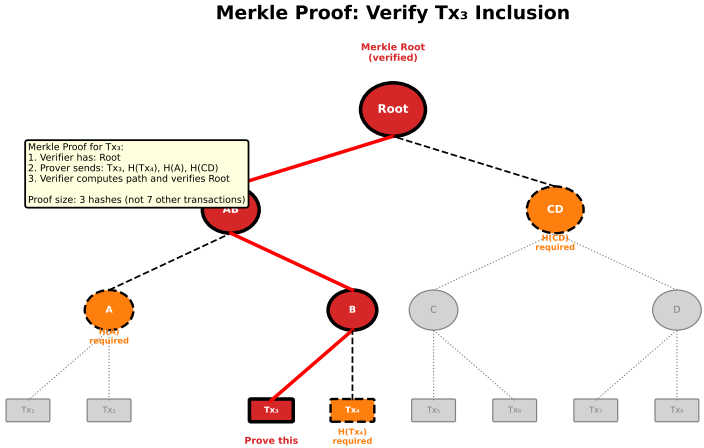
How Do Merkle Trees Enable Efficient Verification?



Benefits: Compact Proof ($O(\log n)$ hashes), Efficient Storage (light clients store only headers), Integrity (any change alters Merkle Root)

Merkle trees enable light clients to verify transaction inclusion without downloading all transactions

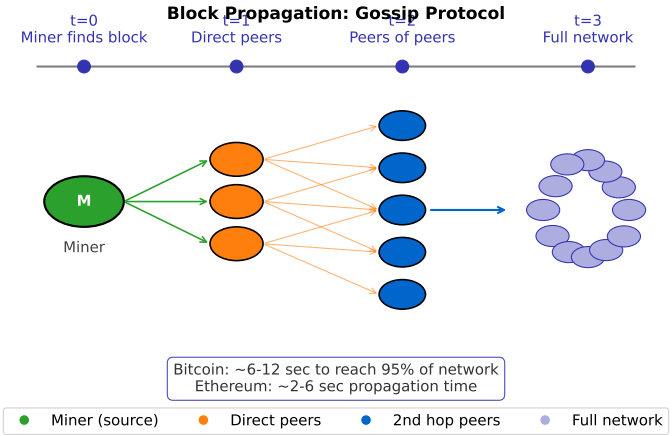
How Do Merkle Proofs Work?



Only 3 hashes needed instead of downloading all 8 transactions

Merkle proofs enable SPV (Simplified Payment Verification) for light clients

How Do Blocks Spread Through the Network?



Timeline: Miner broadcasts to peers, who propagate to their peers, until full network coverage.

Gossip protocol ensures distributed block propagation without central coordination; faster propagation reduces fork probability

How Do Blocks Propagate Through the Network?

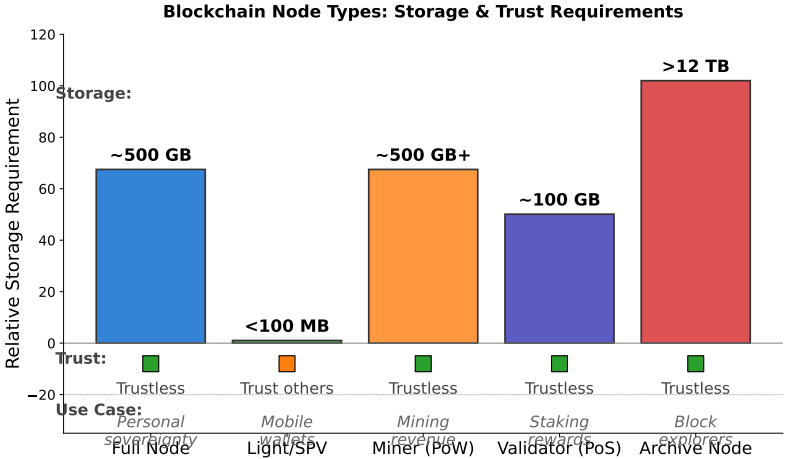
How New Blocks Spread Through Network:

1. Miner finds valid block (solves PoW puzzle)
2. Miner broadcasts block to connected peers ($\approx$ 8-125 peers)
3. Peers validate block:
   - Check block hash meets difficulty target
   - Verify all transactions are valid
   - Ensure no double-spends
4. Valid block propagated to peers' peers (gossip protocol)
5. Process repeats until entire network has the block

Propagation Time:

- Bitcoin: $\approx$ 6-12 seconds to reach 95% of network
- Ethereum (pre-merge): $\approx$ 2-6 seconds
- Faster propagation reduces orphan block rate

What Types of Nodes Exist in Blockchains?



Trade-off: Higher storage requirements enable trustless verification; lower requirements require trusting others.

What Do Full Nodes Do?

Full Node Definition

A **full node** downloads and validates the entire blockchain history, enforcing all consensus rules without relying on third parties.

Responsibilities:

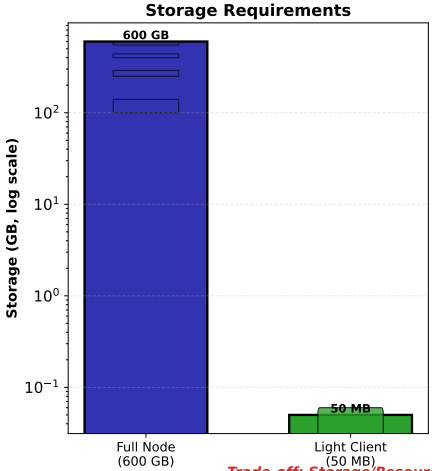
- Store complete blockchain (Bitcoin: $\approx$ 600 GB, Ethereum: $\approx$ 2 TB)
- Validate all blocks and transactions independently
- Relay valid transactions and blocks to peers
- Serve blockchain data to light clients

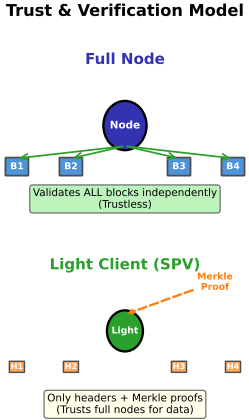
Benefits:

- Maximum security (trust no one)
- Support network decentralization
- Can verify historical transactions

Requirements: $\approx$ 500 GB storage, $\approx$ 5 GB/day bandwidth, moderate CPU

Full Nodes vs. Light Clients: The Trust-Storage Trade-off





Trade-off: Storage/Resources ↔ Trust/Security

12,000x storage difference creates accessibility barrier determining network decentralization

Light clients enable broader participation but introduce trust assumptions

Problem Check-In: DLT Architecture

Recall Our Problem

How do we reach agreement in unreliable networks?

What We've Learned So Far

- Block headers enable efficient verification (80 bytes vs full block)
- Node diversity distributes trust across the network
- Both enable scalable, trustless architecture

Still to Address

- How do permissioned vs permissionless architectures differ?
- What are the storage/bandwidth trade-offs for different node types?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we reach agreement in unreliable..."?

How Do Miner Nodes Work in Proof-of-Work?

Specialized Nodes in Proof-of-Work Blockchains

Functions:

1. Collect unconfirmed transactions from mempool
2. Construct candidate block (select transactions based on fees)
3. Attempt to find valid nonce (compute millions of hashes/second)
4. Broadcast valid block if found
5. Receive block reward + transaction fees

Requirements:

- Specialized hardware (ASICs for Bitcoin, GPUs for some altcoins)
- High electricity consumption (Bitcoin: $\approx$ 150 TWh/year globally)
- Cooling infrastructure
- High-bandwidth internet connection

Economics:

- Bitcoin block reward: 3.125 BTC (post-April 2024 halving)
- Break-even depends on: Hash rate, electricity cost, BTC price

Economic incentives (block rewards + fees) align miner behavior with network security despite unreliable communication

How Do Validator Nodes Work in Proof-of-Stake?

Specialized Nodes in Proof-of-Stake Blockchains

Functions:

1. Stake cryptocurrency as collateral (Ethereum: 32 ETH minimum)
2. Selected to propose/attest blocks based on stake
3. Earn rewards for honest participation
4. Risk slashing (stake confiscation) for malicious behavior

Ethereum Validator Requirements:

- 32 ETH staked (locked)
- Run validator client 24/7 ($>$ 99% uptime)
- Consumer-grade hardware (4 GB RAM, 100 GB SSD)
- Stable internet (10 Mbps)

Comparison to Mining:

+ 99.95% less energy consumption
+ Lower hardware requirements
- Capital locked (opportunity cost)
- Slashing risk if offline or malicious

(c) Joerg Osterrieder 2025

Why Do Archive Nodes Matter?

Full Historical State Storage

- Store every state of the blockchain at every block height
- Enable queries like: "What was Alice's balance at block 1,000,000?"
- Required for block explorers (Etherscan, Blockchain.com)
- Needed for advanced analytics and forensics

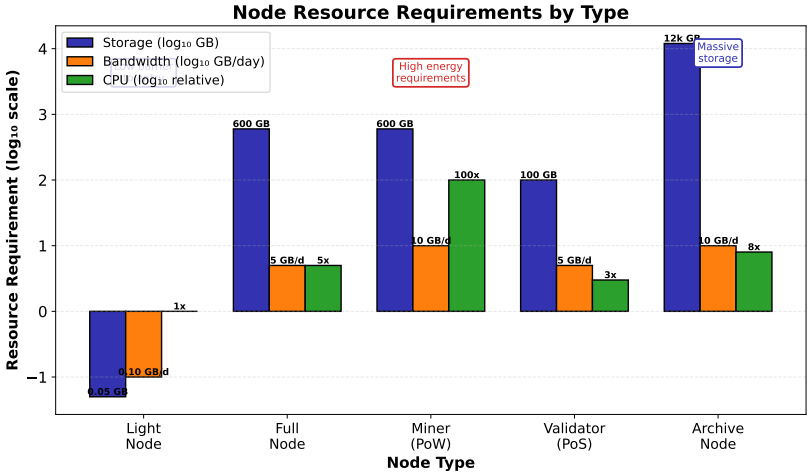
Storage Requirements:

- Bitcoin archive node: $\approx$ 500 GB (same as full node, UTXO model)
- Ethereum archive node: $\approx$ 12 TB (account model stores all states)
- Grows continuously (Ethereum: $+1$ TB/year)

Use Cases:

- Block explorers
- Tax reporting services
- Academic research
- Forensic analysis

How Do Node Requirements Compare?



High storage requirements create barrier to entry, reducing full nodes

Resource requirements determine accessibility and decentralization level

What Makes Permissionless Blockchains Different?

Definition

Permissionless (public) blockchains allow anyone to join, read, write, and participate in consensus without approval from a central authority.

Characteristics:

- Open participation (anyone can run a node)
- Pseudonymous identities (addresses, not real names)
- Transparent transaction history (all data public)
- Censorship resistant
- Token-based incentives (mining/staking rewards)

Examples: Bitcoin, Ethereum, Cardano, Solana

Best For: Global, trustless applications (DeFi, NFTs), censorship-resistant systems

---

Permissionless architecture enables agreement among unknown parties by removing trusted gatekeepers at the cost of efficiency

Why Use Permissioned Blockchains?

Definition

Permissioned blockchains restrict participation to verified entities. Access to read, write, or validate is controlled by administrators.

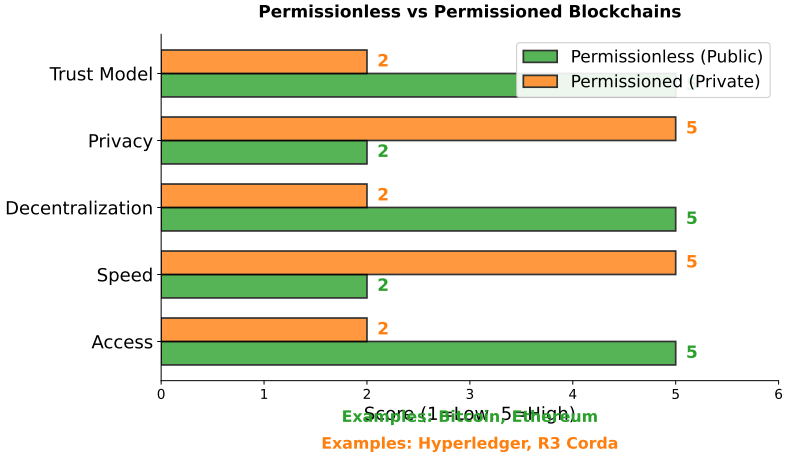
Characteristics:

- Controlled participation (invitation-only)
- Known identities (KYC/AML compliance)
- Selective transparency (private channels possible)
- Efficient consensus (no mining, BFT-based)
- No native cryptocurrency (optional)

Examples: Hyperledger Fabric, R3 Corda, JP Morgan Quorum

Best For: Enterprise consortia (supply chain, trade finance), regulatory compliance

How Do Permissioned and Permissionless Blockchains Compare?



Trade-off: Permissionless maximizes decentralization/trust; Permissioned maximizes speed/privacy.

What Are the Trade-offs Between Permissionless and Permissioned?

Permissionless (Public)

Advantages:

- Maximum decentralization
- Censorship resistant
- Network effects (large user base)
- Innovation without permission

Disadvantages:

- Slower throughput (5-30 TPS)
- Higher costs (gas fees)
- Energy intensive (PoW)
- No privacy by default

Permissioned (Private)

Advantages:

- High throughput (1,000+ TPS)
- Low/no transaction fees
- Energy efficient (BFT)
- Configurable privacy

Disadvantages:

- Central point of control
- Limited network effects
- Potential for censorship
- Requires trust in admins

Hybrid models exist: Public with private sidechains (e.g., Polygon for Ethereum)

(c) Joerg Osterrieder 2025

When Should You Choose Permissioned vs. Permissionless?

Criterion	Permissionless	Permissioned
Trust Model	No trust required	Parties partially trust each other
Participants	Unknown, global	Known, verified entities
Governance	Decentralized (hard forks)	Centralized/consortium voting
Performance	5-30 TPS	1,000-10,000+ TPS
Privacy	Pseudonymous, transparent	Configurable, private channels
Use Cases	DeFi, NFTs, payments	Supply chain, trade finance, CBDCs

Problem Solved? DLT Architecture

The Original Problem

How do we structure data for trustless verification across thousands of nodes?

How DLT Architecture Solves It

- Merkle trees enable O(log n) verification instead of downloading all transactions
- Block headers separate metadata from transaction data (80 bytes vs. MB)
- Full nodes independently validate entire history without trusting anyone

Remaining Limitations

- Block size limits transaction throughput (Bitcoin: 7 TPS, Ethereum: 30 TPS)
- Storage requirements create centralization pressure (600 GB+ for full nodes)

Open Questions

- Optimal balance between full nodes (decentralization) and light clients (accessibility)?
- Risk: As storage grows, fewer users can verify independently

DLT architecture enables trustless verification but introduces scalability-decentralization trade-offs

The Economics of DLT Architecture

Incentive Structure

- **Core Problem:** Maintaining consistent distributed state across unreliable networks
- **Why act honestly?** Full nodes verify independently; light clients trust but verify headers
- **Value Flow:** Node operators pay storage (600GB Bitcoin) and bandwidth costs; gain sovereignty and privacy

Economic Security

- Independent verification ¿ trusted intermediaries
- Storage costs limit full node participation

Key Economic Question

Who Pays, Who Earns?

Node operators pay storage/bandwidth costs; users gain trustless verification and censorship resistance

Design Principle

$$\text{Verification Cost} \ll \text{Trust Risk}$$

Architecture economics: Distributed state requires economic actors to bear verification costs

Design Space: DLT Architecture

Alternatives Considered

1. **Full nodes:** Maximum security, 600GB storage, 2TB for Ethereum
2. **Light clients:** Minimal storage, trust headers via SPV proofs
3. **Archive nodes:** Complete historical state, 12+ TB for Ethereum

Trade-offs Made

- Storage vs. trustlessness
- Accessibility vs. decentralization

Design Questions

- How much should users trust vs verify?
- What's the UX trade-off?
- Can we reduce storage without sacrificing security?

Key Insight

Storage-Trust Spectrum

Users choose between running full nodes (maximum sovereignty) and light clients (lower barrier to entry).

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: DLT Architecture

Critical Failure Mode

- **What breaks:** Block propagation reaches majority before next block is mined
- **Why it happens:** Network partitions, slow propagation, malicious miners

Root Cause

- Assumption: Honest majority sees blocks quickly
- Violators: Eclipse attacks, network latency
- Result: Chain splits, double-spend attempts

Historical Context

- 2015 Bitcoin fork: BIP66 caused chain split due to uneven propagation
- 2013 Bitcoin 0.7/0.8 fork: Database limits caused temporary split

Early Warning Signs

! Eclipse attacks can isolate nodes from honest network view

! Increasing orphan block rate signals propagation issues

! Few full nodes = centralization risk

Prediction: What could cause this to fail? How would you detect it early?

Key Takeaways

What You Should Remember:

1. **Block Structure**: Header (80 bytes) + Body (transactions), linked via cryptographic hashes
2. **Merkle Trees**: Enable efficient transaction verification ($O(\log n)$ proof size)
3. **Node Types**:
   - Full (trustless), Light (trust others)
   - Miner/Validator (consensus), Archive (historical queries)
4. **Permissioned vs. Permissionless**: Public for trustless apps, private for enterprise consortia

Next: L03 - Cryptographic Hash Functions

Next Lesson: L03 – Cryptographic Hash Functions

Discussion Questions

Consider and discuss:

1. **Decentralization Trade-offs**: At what point does storage cost compromise decentralization?
2. **Node Selection**: When would you run a full node vs. use a light client?
3. **Enterprise Blockchain**: Why do enterprises often prefer permissioned chains?

The Family Tree of Transactions

[COMIC: Merkle trees as family genealogy]

"Just like you can prove your ancestry with a few certificates, you can prove a transaction belongs with just a few hashes."

Key Insight: Merkle trees compress thousands of transactions into one fingerprint—change any ancestor, and the entire family tree looks different.

Thank you

Questions?

Continue to L03: Cryptographic Hash Functions

Quiz Questions (1/2)

Q1. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes (6 fields).

Q2. What is the purpose of the Merkle Root in a block header?
A) Identify previous block B) Prove all transactions included C) Set mining difficulty D) Store timestamp
Answer: B – Merkle Root commits to all transactions, enabling efficient verification.

Q3. How many hashes are needed to verify a transaction in a block with 1,024 transactions using a Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes needed for Merkle proof.

Q4. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of 2025).

Q5. What does SPV stand for in the context of light nodes?
A) Secure Payment Validation B) Simplified Payment Verification C) Shared Proof Verification D) Synchronized Peer Validation
Answer: B – SPV (Simplified Payment Verification) described in Bitcoin whitepaper.

Quiz Questions (2/2)

Q6. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q7. Which node type stores every historical state at every block height?
A) Full node B) Light node C) Archive node D) Miner node
Answer: C – Archive nodes store complete historical state (e.g., 12 TB for Ethereum).

Q8. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public chains B) Permissioned private chains C) Both equal D) Depends only on hardware
Answer: B – Permissioned chains achieve 1,000+ TPS vs. 5-30 TPS for public chains.

Q9. What protocol do Bitcoin nodes use to propagate new blocks?
A) HTTP B) FTP C) Gossip protocol D) TCP handshake
Answer: C – Gossip protocol: nodes relay to peers, who relay to their peers.

Q10. Which field in the Bitcoin block header links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp
Answer: C – Previous Block Hash (32 bytes) creates the cryptographic chain.

Lesson 2: Distributed Ledger Technology

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Define Distributed Ledger Technology (DLT) and distinguish it from blockchain
2. Explain the Byzantine Generals Problem and its relevance to consensus
3. Compare network topologies: centralized, decentralized, and distributed
4. Describe the structure and components of a blockchain block
5. Differentiate between node types: full nodes, light nodes, miners, validators
6. Contrast permissioned and permissionless blockchain architectures

Prerequisites: L01 - What is Blockchain?

What is Distributed Ledger Technology?

DLT Definition

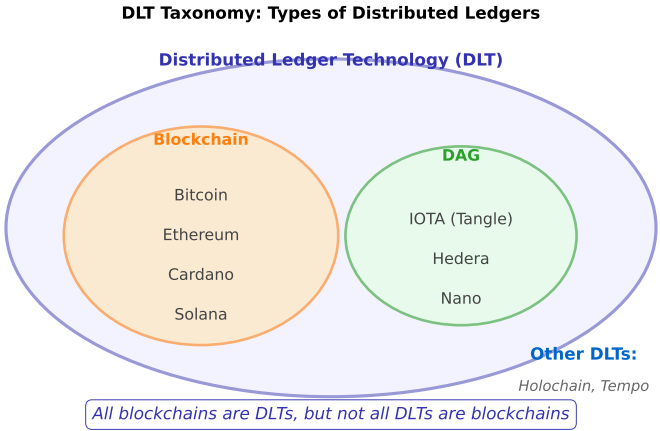
A **Distributed Ledger Technology (DLT)** is a database architecture where data is synchronized, replicated, and shared across multiple nodes in a network, without a central administrator.

Key Characteristics:

- **Distributed**: Data stored across many nodes (no single source of truth)
- **Synchronized**: All nodes maintain consistent state through consensus
- **Replicated**: Each node has a complete or partial copy of the ledger
- **Shared**: Multiple parties can read/write to the ledger
- **Consensus-driven**: Agreement mechanism validates changes

All blockchains are DLTs, but not all DLTs are blockchains

DLT Taxonomy: Types of Distributed Ledgers



Key Insight: Blockchain is a subset of DLT. Other approaches include DAGs (IOTA), Holochain, and Tempo (Radix).

Blockchain vs. Other DLTs

Blockchain

- Data organized in sequential blocks
- Blocks linked via cryptographic hashes
- Linear chain structure
- Append-only (immutable history)
- Examples: Bitcoin, Ethereum

Directed Acyclic Graph (DAG)

- Transactions reference previous transactions
- No blocks, no miners
- Parallel processing
- Examples: IOTA (Tangle), Hedera Hashgraph

Different DLT architectures optimize for different trade-offs

Holochain

- Agent-centric (not data-centric)
- Each agent maintains own chain
- Distributed Hash Table (DHT)
- No global consensus required

Tempo (Radix)

- Sharded state machine
- Logical clocks for ordering
- Scalable to millions of TPS
- Hybrid consensus

Ledger Types: Shared vs. Distributed

Shared Ledger (Traditional)

- Multiple parties access same database
- Central authority controls access
- Single version of truth
- Fast, but trust required

Example: Banking consortium database

Challenges:

- Single point of failure
- Administrator can alter records
- Reconciliation between systems

Distributed Ledger (DLT)

- Each party has own copy
- No central authority
- Consensus creates truth
- Slower, but trustless

Example: Public blockchain

Benefits:

- No single point of failure
- Transparent, auditable history
- No reconciliation needed

The Byzantine Generals Problem (1982)

Historical Context

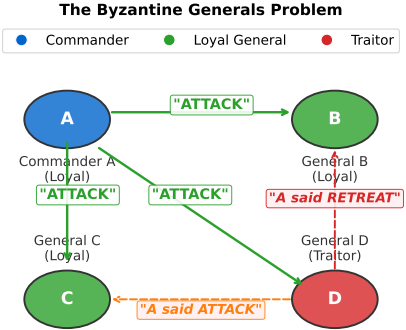
Leslie Lamport, Robert Shostak, and Marshall Pease formulated this thought experiment to describe the challenge of achieving consensus in distributed systems with potentially faulty or malicious actors.

The Scenario:

- Byzantine army surrounds an enemy city
- Army divided into divisions, each led by a general
- Generals must coordinate: **ATTACK** or **RETREAT**
- Communication only via messengers
- Some generals may be traitors (Byzantine faults)

Challenge: How can loyal generals reach consensus when traitors send conflicting messages?

Byzantine Generals: The Communication Challenge



Problem: How can loyal generals reach consensus when traitors send conflicting messages?

Problem: Traitor D sends conflicting messages to B and C, causing coordination failure.

Byzantine Generals: Example Scenario

Setup: 4 Generals (A, B, C, D), 1 is a traitor

Round 1 - Commander A sends orders:

- To General B: "ATTACK"
- To General C: "ATTACK"
- To General D (traitor): "ATTACK"

Round 2 - Traitor D sends conflicting messages:

- To General B: "A said RETREAT" (lie)
- To General C: "A said ATTACK" (truth)

Result Without Byzantine Fault Tolerance:

- General B thinks majority said RETREAT (withdraws alone)
- General C thinks majority said ATTACK (attacks alone)
- Army coordination fails, both divisions defeated

Byzantine Fault Tolerance (BFT)

Formal Result

Consensus is achievable if and only if at least $\frac{2}{3}$ of the actors are honest. Formally: $n \geq 3f + 1$ where n = total nodes, f = faulty nodes.

BFT Solution Requirements:

1. **Agreement**: All honest nodes decide on the same value
2. **Validity**: If all honest nodes propose value v, then v is decided
3. **Termination**: All honest nodes eventually decide

Blockchain Context:

- Bitcoin's Proof-of-Work solves Byzantine Generals Problem
- Nakamoto Consensus: Longest chain = majority decision
- Tolerates up to 49% malicious hash power (in practice, 51% attack possible)
- Practical BFT (PBFT) used in permissioned blockchains (Hyperledger)

Types of Faults in Distributed Systems

Crash Faults (Simpler)

- Node fails and stops responding
- Predictable behavior
- Detectable by timeout
- Example: Server power loss

Handling:

- Majority voting
- Heartbeat monitoring
- Leader election

Example: Apache Zookeeper, etcd (use Paxos/Raft)

Byzantine Faults (Complex)

- Node sends incorrect/conflicting information
- Malicious or software bugs
- Unpredictable behavior
- Example: Hacked node

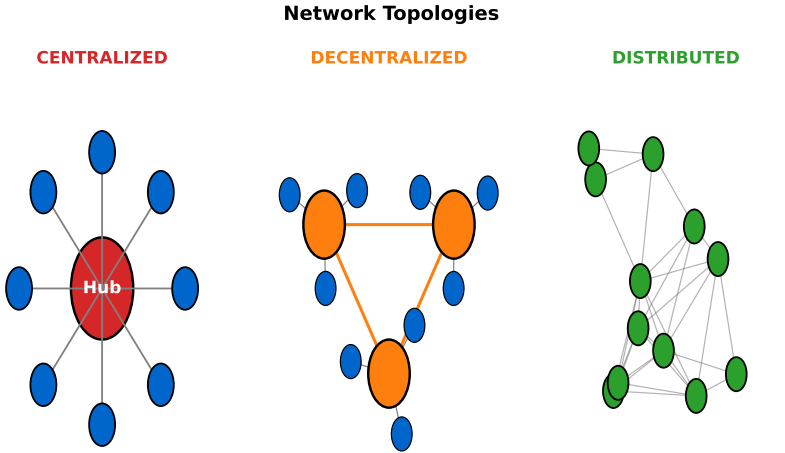
Handling:

- Cryptographic proofs
- Economic incentives
- Supermajority consensus ($> 2/3$)

Example: Bitcoin (PoW), Tendermint (BFT)

Key Insight: Public blockchains assume Byzantine environment; private blockchains may assume only crash faults

Network Topologies Comparison



Key Trade-off: Centralized is fast but fragile; Distributed is resilient but slower.

Centralized Networks

Architecture:

- Single central node (hub)
- All communication flows through hub
- Clients connect to central server
- Hub controls access and data

Advantages:

- Fast and efficient
- Easy to manage and update
- Low coordination overhead

Disadvantages:

- Single point of failure
- Censorship possible
- Privacy concerns (hub sees all data)

Examples: Traditional banking systems, Facebook, Gmail

Decentralized Networks

Architecture:

- Multiple hubs (federated model)
- Each hub serves subset of nodes
- Hubs communicate with each other
- No single central authority

Advantages:

- More resilient than centralized
- Regional autonomy
- Balanced between efficiency and resilience

Disadvantages:

- Hubs still represent points of failure
- Coordination between hubs needed
- Potential for fragmentation

Examples: Email (SMTP), Tor network, Mastodon (federated social media)

Distributed Networks

Architecture:

- Peer-to-peer (P2P) topology
- No hubs or central points
- Every node equal (or nearly equal)
- Direct node-to-node communication

Advantages:

- Maximum resilience (no single point of failure)
- Censorship resistant
- Highly fault-tolerant

Disadvantages:

- Slower coordination (consensus overhead)
- Complex to manage and upgrade
- Higher resource requirements per node

Examples: Bitcoin, Ethereum, BitTorrent, IPFS

Topology Comparison Table

Property	Centralized	Decentralized	Distributed
Control	Single entity	Multiple entities	All participants
Speed	Very fast	Fast	Slower
Resilience	Low (SPOF)	Medium	High
Censorship Resistance	None	Moderate	Strong
Coordination Overhead	Minimal	Moderate	High
Scalability	Easy (vertical)	Moderate	Hard (horizontal)
Trust Required	High	Medium	Low
Examples	Banks, Facebook	Email, Mastodon	Bitcoin, IPFS

Blockchain networks typically use fully distributed topology for maximum trustlessness

Anatomy of a Block: Overview

A blockchain block contains two main parts:

1. **Block Header** (80 bytes in Bitcoin)
   - Metadata about the block
   - Links to previous block
   - Proof-of-Work evidence
2. **Block Body** (variable size)
   - Transaction data
   - Can contain hundreds to thousands of transactions

Block Size Limits:

- Bitcoin: 1 MB (base block) to 4 MB (with SegWit)
- Ethereum: Dynamic gas limit ($\approx$ 30M gas, $\approx$ 15 MB)
- Bitcoin Cash: 32 MB

(c) Joerg Osterrieder 2025

Block Header Components

Bitcoin Block Header Fields (80 bytes):

1. **Version** (4 bytes): Block version number (for protocol upgrades)
2. **Previous Block Hash** (32 bytes): Hash of the previous block header
3. **Merkle Root** (32 bytes): Hash of all transactions in this block
4. **Timestamp** (4 bytes): Unix epoch time (seconds since Jan 1, 1970)
5. **Difficulty Target** (4 bytes): Required difficulty for PoW
6. **Nonce** (4 bytes): Counter used for PoW mining

Key Insight:

$$\text{Block Hash} = \text{SHA256}(\text{SHA256}(\text{Header}))$$

The hash must be below the difficulty target for the block to be valid.

Merkle Trees: Efficient Transaction Verification

Merkle Tree Definition

A **Merkle tree** is a binary hash tree where each leaf node is a hash of a transaction, and each non-leaf node is a hash of its two children.

Construction Process:

1. Hash each transaction: $H(Tx_1), H(Tx_2), ..., H(Tx_n)$
2. Pair hashes and hash again: $H(H(Tx_1)||H(Tx_2))$
3. Repeat until single root hash (Merkle Root)

Benefits:

- **Compact Proof**: Verify transaction inclusion with $O(\log n)$ hashes
- **Efficient Storage**: Light clients store only 80-byte headers
- **Integrity**: Any transaction change alters Merkle Root

Example: Prove transaction in block with 1,000 tx requires only 10 hashes ($\log_2 1000 \approx 10$)

Merkle Proof Example

Scenario: Block contains 8 transactions, prove Tx_3 is included

Tree Structure:

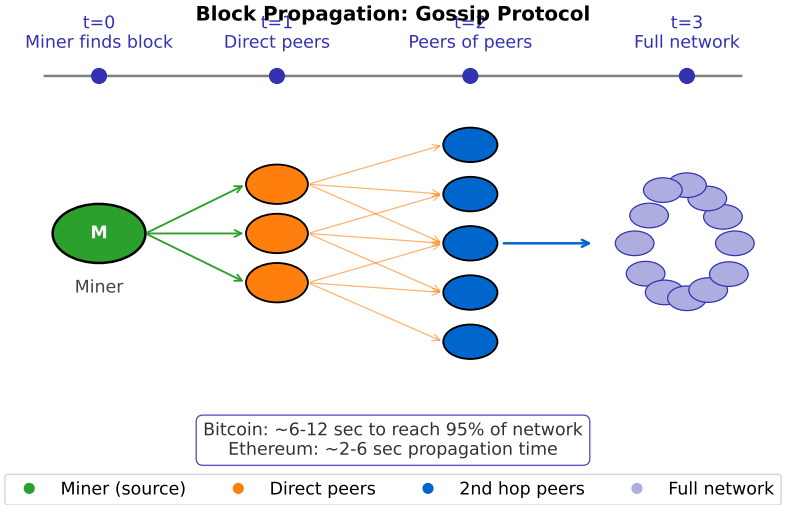
- Level 3 (Root): $R = H(AB||CD)$ where $AB = H(A||B)$, $CD = H(C||D)$
- Level 2: $A = H(Tx_1||Tx_2)$, $B = H(Tx_3||Tx_4)$, etc.
- Level 1: Tx_1, Tx_2, Tx_3, Tx_4, ..., Tx_8

Merkle Proof for Tx_3:

1. Verifier has: Block header with Merkle Root R
2. Prover provides: Tx_3, $H(Tx_4)$, $H(A)$, $H(CD)$
3. Verifier computes: $H(Tx_3)$, then $B = H(H(Tx_3)||H(Tx_4))$
4. Then: $AB = H(H(A)||B)$, finally $R' = H(AB||H(CD))$
5. If $R' = R$, then Tx_3 is proven to be in the block

Only 3 hashes needed instead of downloading all 8 transactions

Block Propagation via Gossip Protocol



Timeline: Miner broadcasts to peers, who propagate to their peers, until full network coverage.

(c) Joerg Osterrieder 2025

Block Propagation Details

How New Blocks Spread Through Network:

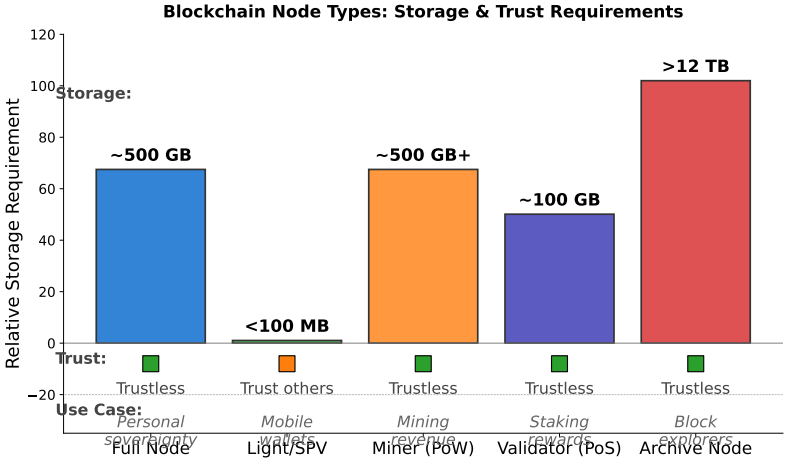
1. Miner finds valid block (solves PoW puzzle)
2. Miner broadcasts block to connected peers ($\approx$ 8-125 peers)
3. Peers validate block:
   - Check block hash meets difficulty target
   - Verify all transactions are valid
   - Ensure no double-spends
4. Valid block propagated to peers' peers (gossip protocol)
5. Process repeats until entire network has the block

Propagation Time:

- Bitcoin: $\approx$ 6-12 seconds to reach 95% of network
- Ethereum (pre-merge): $\approx$ 2-6 seconds
- Faster propagation reduces orphan block rate

Network latency creates temporary forks (resolved by longest chain rule)

Blockchain Node Types: Storage and Trust



Trade-off: Higher storage requirements enable trustless verification; lower requirements require trusting others.

Full Nodes

Full Node Definition

A **full node** downloads and validates the entire blockchain history, enforcing all consensus rules without relying on third parties.

Responsibilities:

- Store complete blockchain (Bitcoin: $\approx$ 600 GB, Ethereum: $\approx$ 2 TB)
- Validate all blocks and transactions independently
- Relay valid transactions and blocks to peers
- Serve blockchain data to light clients

Benefits:

- Maximum security (trust no one)
- Support network decentralization
- Can verify historical transactions

Requirements: $\approx$ 500 GB storage, $\approx$ 5 GB/day bandwidth, moderate CPU

Light Nodes (SPV Nodes)

Simplified Payment Verification (SPV)

Described in Bitcoin whitepaper: Light nodes download only block headers ($\approx$ 80 bytes each) instead of full blocks, relying on Merkle proofs to verify transactions.

Operation:

- Download all block headers ($\approx$ 50 MB for Bitcoin)
- Request Merkle proofs from full nodes for relevant transactions
- Verify transaction inclusion in block
- Assume longest chain is valid

Trade-offs:

+ Low storage ($<$ 100 MB vs. 500 GB)
+ Suitable for mobile devices
- Must trust full nodes for transaction data
- Vulnerable to bloom filter privacy leaks

Examples: Mobile wallets (Electrum, MetaMask mobile)

Miner Nodes (PoW)

Specialized Nodes in Proof-of-Work Blockchains

Functions:

1. Collect unconfirmed transactions from mempool
2. Construct candidate block (select transactions based on fees)
3. Attempt to find valid nonce (compute millions of hashes/second)
4. Broadcast valid block if found
5. Receive block reward + transaction fees

Requirements:

- Specialized hardware (ASICs for Bitcoin, GPUs for some altcoins)
- High electricity consumption (Bitcoin: $\approx$ 150 TWh/year globally)
- Cooling infrastructure
- High-bandwidth internet connection

Economics:

- Bitcoin block reward: 3.125 BTC (post-April 2024 halving)
- Break-even depends on: Hash rate, electricity cost, BTC price

Validator Nodes (PoS)

Specialized Nodes in Proof-of-Stake Blockchains

Functions:

1. Stake cryptocurrency as collateral (Ethereum: 32 ETH minimum)
2. Selected to propose/attest blocks based on stake
3. Earn rewards for honest participation
4. Risk slashing (stake confiscation) for malicious behavior

Ethereum Validator Requirements:

- 32 ETH staked (locked)
- Run validator client 24/7 ($>$ 99% uptime)
- Consumer-grade hardware (4 GB RAM, 100 GB SSD)
- Stable internet (10 Mbps)

Comparison to Mining:

+ 99.95% less energy consumption
+ Lower hardware requirements
- Capital locked (opportunity cost)
- Slashing risk if offline or malicious

Archive Nodes

Full Historical State Storage

- Store every state of the blockchain at every block height
- Enable queries like: "What was Alice's balance at block 1,000,000?"
- Required for block explorers (Etherscan, Blockchain.com)
- Needed for advanced analytics and forensics

Storage Requirements:

- Bitcoin archive node: $\approx$ 500 GB (same as full node, UTXO model)
- Ethereum archive node: $\approx$ 12 TB (account model stores all states)
- Grows continuously (Ethereum: $+1$ TB/year)

Use Cases:

- Block explorers
- Tax reporting services
- Academic research
- Forensic analysis

Most users do not need archive nodes; full nodes are sufficient

Node Type Comparison

Node Type	Storage	Validation	Trust Model	Use Case
Full Node	$\approx$ 500 GB	All blocks & txs	Trustless	Personal sovereignty
Light/SPV	$<$ 100 MB	Headers only	Trust full nodes	Mobile wallets
Miner (PoW)	$\approx$ 500 GB +	Full validation	Trustless	Mining revenue
Validator (PoS)	$\approx$ 100 GB	Full validation	Trustless	Staking rewards
Archive Node	$>$ 10 TB	Full + history	Trustless	Analytics, explorers

Decentralization Trade-off:

- More full nodes = more decentralization
- High storage requirements = fewer full nodes
- Blockchain scalability trilemma: Security, Decentralization, Scalability

Permissionless Blockchains (Public)

Definition

Permissionless (public) blockchains allow anyone to join, read, write, and participate in consensus without approval from a central authority.

Characteristics:

- Open participation (anyone can run a node)
- Pseudonymous identities (addresses, not real names)
- Transparent transaction history (all data public)
- Censorship resistant
- Token-based incentives (mining/staking rewards)

Examples: Bitcoin, Ethereum, Cardano, Solana

Best For:

- Global, trustless applications (DeFi, NFTs)
- Censorship-resistant systems
- Public goods (identity, voting)

Permissioned Blockchains (Private/Consortium)

Definition

Permissioned blockchains restrict participation to verified entities. Access to read, write, or validate is controlled by administrators.

Characteristics:

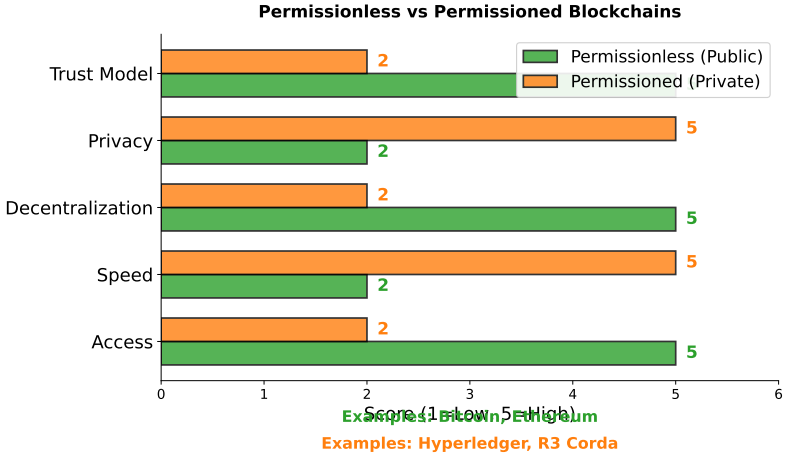
- Controlled participation (invitation-only)
- Known identities (KYC/AML compliance)
- Selective transparency (private channels possible)
- Efficient consensus (no mining, BFT-based)
- No native cryptocurrency (optional)

Examples: Hyperledger Fabric, R3 Corda, JP Morgan Quorum

Best For:

- Enterprise consortia (supply chain, trade finance)
- Regulatory compliance scenarios
- Inter-organizational workflows

Permissioned vs Permissionless: Key Dimensions



Trade-off: Permissionless maximizes decentralization/trust; Permissioned maximizes speed/privacy.

Comparison: Permissionless vs. Permissioned

Permissionless (Public)

Advantages:

- Maximum decentralization
- Censorship resistant
- Network effects (large user base)
- Innovation without permission

Disadvantages:

- Slower throughput (5-30 TPS)
- Higher costs (gas fees)
- Energy intensive (PoW)
- No privacy by default

Permissioned (Private)

Advantages:

- High throughput (1,000+ TPS)
- Low/no transaction fees
- Energy efficient (BFT)
- Configurable privacy

Disadvantages:

- Central point of control
- Limited network effects
- Potential for censorship
- Requires trust in admins

Hybrid models exist: Public with private sidechains (e.g., Polygon for Ethereum)

(c) Joerg Osterrieder 2025

When to Choose Each Type

Criterion	Permissionless	Permissioned
Trust Model	No trust required	Parties partially trust each other
Participants	Unknown, global	Known, verified entities
Governance	Decentralized (hard forks)	Centralized/consortium voting
Performance	5-30 TPS	1,000-10,000+ TPS
Privacy	Pseudonymous, transparent	Configurable, private channels
Compliance	Challenging	Built-in (KYC/AML)
Cost	High (gas fees)	Low (no mining)
Use Cases	DeFi, NFTs, payments	Supply chain, trade finance, CBDCs

Key Takeaways

What You Should Remember:

1. **DLT** is broader than blockchain; includes DAGs, Holochain, etc.
2. **Byzantine Generals Problem**: Achieving consensus with potentially malicious actors requires $> 2/3$ honest nodes
3. **Network Topologies**: Centralized (fast, fragile), Decentralized (balanced), Distributed (resilient, slow)
4. **Block Structure**: Header (80 bytes) + Body (transactions), linked via cryptographic hashes
5. **Merkle Trees**: Enable efficient transaction verification ($O(\log n)$ proof size)
6. **Node Types**: Full (trustless), Light (trust others), Miner/Validator (consensus), Archive (historical queries)
7. **Permissioned vs. Permissionless**: Public for trustless apps, private for enterprise consortia

Discussion Questions

Consider and discuss:

1. **Decentralization Trade-offs**: At what point does storage cost compromise decentralization?
   - If only enterprises can afford archive nodes, is the network still decentralized?
2. **Byzantine Assumptions**: Are public blockchains too conservative?
   - Could permissioned chains with known actors be more efficient?
3. **Privacy vs. Transparency**: How can we enable audits without sacrificing user privacy?
   - Explore: zk-SNARKs, confidential transactions

References & Resources

Foundational Papers

- Lamport et al. (1982): *Byzantine Generals Problem*
- Nakamoto (2008): *Bitcoin Whitepaper* (Section 8: SPV)
- Castro & Liskov (1999): *Practical Byzantine Fault Tolerance*

Technical Resources

- Bitcoin Developer Guide
- Ethereum Yellow Paper
- Hyperledger Fabric Docs

Interactive Tools

- Blockchain Demo (andersbrownworth.com)
- Merkle Tree Visualizer
- Node map: bitnodes.io

Books

- Antonopoulos (2023): *Mastering Bitcoin* (Chapter 6: Transactions)
- Narayanan et al. (2016): *Bitcoin and Cryptocurrency Technologies* (Chapter 2)

(c) Joerg Osterrieder 2025

Next Lesson Preview

L03: Cryptographic Hash Functions

We will explore:

- Properties of cryptographic hash functions (deterministic, fixed-length, avalanche effect)
- SHA-256 algorithm and its use in Bitcoin
- Collision resistance and birthday paradox
- Hash functions as digital fingerprints
- Merkle trees in-depth (construction and verification)
- Applications beyond blockchain

Preparation: Review binary representation of data and basic probability theory

Thank you

Questions?

See you in Lesson 3: Cryptographic Hash Functions

Quiz Questions (1/4)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., DAGs like IOTA).

Q2. In the Byzantine Generals Problem, what minimum fraction of nodes must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – The formal requirement is $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed (P2P) networks have no central hubs, maximizing resilience.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes (6 fields).

Q5. What is the purpose of the Merkle Root in a block header?
A) Identify previous block B) Prove all transactions included C) Set mining difficulty D) Store timestamp
Answer: B – Merkle Root commits to all transactions, enabling efficient verification.

Quiz Questions (2/4)

Q6. How many hashes are needed to verify a transaction in a block with 1,024 transactions using a Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes needed for Merkle proof.

Q7. Which fault type is more challenging for distributed systems to handle?
A) Crash faults B) Network partitions C) Byzantine faults D) Timeout errors
Answer: C – Byzantine faults involve malicious/conflicting behavior, harder than simple crashes.

Q8. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of 2025).

Q9. What does SPV stand for in the context of light nodes?
A) Secure Payment Validation B) Simplified Payment Verification C) Shared Proof Verification D) Synchronized Peer Validation
Answer: B – SPV (Simplified Payment Verification) described in Bitcoin whitepaper.

Q10. How much storage does a light/SPV node typically require?
A) Less than 100 MB B) 50 GB C) 500 GB D) 2 TB
Answer: A – SPV nodes download only headers ($<$ 100 MB), not full blocks.

Quiz Questions (3/4)

Q11. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q12. Which node type stores every historical state at every block height?
A) Full node B) Light node C) Archive node D) Miner node
Answer: C – Archive nodes store complete historical state (e.g., 12 TB for Ethereum).

Q13. What is Bitcoin's current block reward after the April 2024 halving?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – After April 2024 halving, reward is 3.125 BTC per block.

Q14. Which consensus mechanism uses approximately 99.95% less energy than Proof-of-Work?
A) Proof-of-Authority B) Proof-of-Stake C) Delegated PoS D) Practical BFT
Answer: B – Proof-of-Stake (like Ethereum post-merge) reduces energy by 99.95%.

Q15. In permissionless blockchains, what determines who can participate?
A) Central administrator approval B) KYC verification C) No restrictions, anyone can join D) Consortium voting
Answer: C – Permissionless means open participation without approval.

Quiz Questions (4/4)

Q16. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public chains B) Permissioned private chains C) Both equal D) Depends only on hardware
Answer: B – Permissioned chains achieve 1,000+ TPS vs. 5-30 TPS for public chains.

Q17. What protocol do Bitcoin nodes use to propagate new blocks?
A) HTTP B) FTP C) Gossip protocol D) TCP handshake
Answer: C – Gossip protocol: nodes relay to peers, who relay to their peers.

Q18. Which DLT architecture uses a Directed Acyclic Graph instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger Fabric D) Cardano
Answer: B – IOTA uses DAG (Tangle) where transactions reference previous transactions.

Q19. What is the main advantage of centralized networks over distributed ones?
A) Censorship resistance B) Speed and efficiency C) No single point of failure D) Maximum decentralization
Answer: B – Centralized networks are faster/more efficient but have single point of failure.

Q20. Which field in the Bitcoin block header links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp
Answer: C – Previous Block Hash (32 bytes) creates the cryptographic chain.

L02: Distributed Ledger Technology

Mini-Lecture (30 min) – Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

January 2026

Learning Objectives:

- Define DLT and distinguish it from blockchain
- Explain Byzantine Generals Problem and consensus
- Compare network topologies and node types
- Contrast permissioned vs permissionless architectures

What is Distributed Ledger Technology?

DLT Definition

A **Distributed Ledger Technology (DLT)** is a database where data is synchronized, replicated, and shared across multiple nodes without a central administrator.

Key Characteristics:

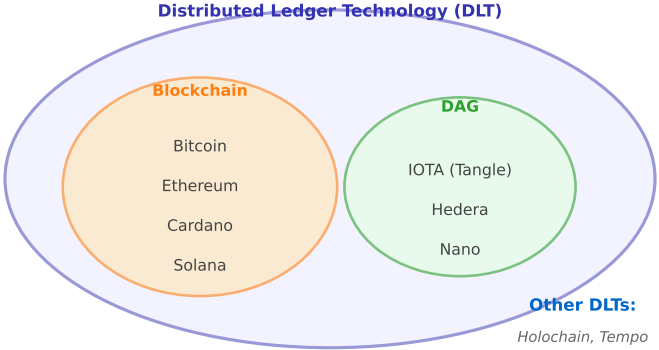
- **Distributed**: Data stored across many nodes
- **Synchronized**: Nodes maintain consistent state via consensus
- **Replicated**: Each node has a copy of the ledger
- **Consensus-driven**: Agreement mechanism validates changes

All blockchains are DLTs, but not all DLTs are blockchains

Other DLT types: DAGs (IOTA), Holochain, Tempo (Radix)

DLT Taxonomy

DLT Taxonomy: Types of Distributed Ledgers



All blockchains are DLTs, but not all DLTs are blockchains

Blockchain is a subset of DLT – different architectures optimize for different trade-offs

Byzantine Generals Problem (1982)

The Challenge: Achieve consensus with potentially malicious actors

The Scenario:

- Army divisions must coordinate: ATTACK or RETREAT
- Communication only via messengers
- Some generals may be traitors
- How can loyal generals reach agreement?

Solution:

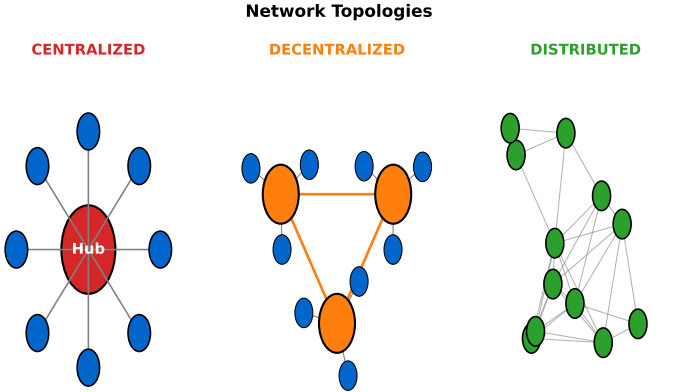
BFT Threshold

Consensus achievable if $\geq 2/3$ nodes are honest: $n \geq 3f + 1$

Blockchain Solution: Bitcoin's PoW solves this – longest chain = majority decision

Lamport, Shostak & Pease (1982) formalized this distributed systems problem

Network Topologies Comparison



Centralized = fast but fragile; Distributed = resilient but slower

Anatomy of a Block

Block Header (80 bytes):

1. Version (4 bytes)
2. Previous Block Hash (32 bytes)
3. Merkle Root (32 bytes)
4. Timestamp (4 bytes)
5. Difficulty Target (4 bytes)
6. Nonce (4 bytes)

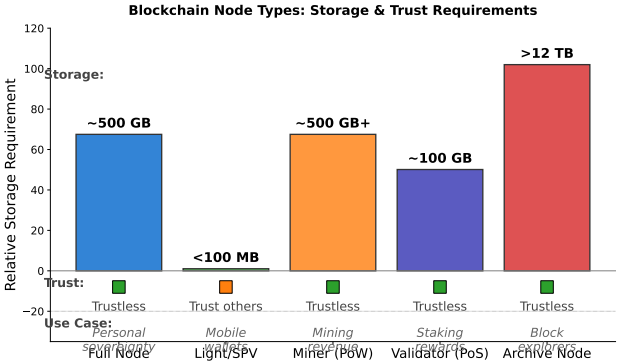
Merkle Tree Benefits:

- Verify transaction with $O(\log n)$ hashes
- 1,000 tx block needs only 10 hashes
- Light clients store 80-byte headers
- Any change alters root hash

$$\text{Block Hash} = \text{SHA256}(\text{SHA256}(\text{Header}))$$

Hash must be below difficulty target for valid block

Blockchain Node Types



Type	Storage	Trust	Use Case
Full Node	600 GB	Trustless	Personal sovereignty
Light/SPV	$<$100 MB	Trust full nodes	Mobile wallets
Validator	100 GB + 32 ETH	Trustless	Staking rewards
Archive	$>$12 TB	Trustless	Block explorers

More full nodes = more decentralization; high storage = fewer nodes

Permissioned vs Permissionless Blockchains

Permissionless (Public)

- Anyone can join/read/write
- Pseudonymous identities
- Censorship resistant
- 5-30 TPS, high fees
- Examples: Bitcoin, Ethereum

Best for: DeFi, NFTs, global trustless apps

Permissioned (Private)

- Invitation-only, KYC required
- Known identities
- High throughput (1,000+ TPS)
- Low/no fees, BFT consensus
- Examples: Hyperledger, Corda

Best for: Enterprise, supply chain, CBDCs

Hybrid models exist: Public chains with private sidechains (e.g., Polygon)

Key Takeaways

1. **DLT** is broader than blockchain – includes DAGs, Holochain, etc.
2. **Byzantine Fault Tolerance**: Requires $> 2/3$ honest nodes for consensus
3. **Network Topologies**: Distributed P2P maximizes resilience at cost of speed
4. **Merkle Trees**: Enable $O(\log n)$ transaction verification
5. **Node Types**: Full nodes provide trustless verification; light nodes trade security for convenience
6. **Permissioned vs Permissionless**: Public for trustless, private for enterprise

Key Equation: BFT threshold $n \geq 3f + 1$ (tolerate f faulty nodes)

Next: L03 Cryptographic Hash Functions – SHA-256, collision resistance, Merkle trees in depth

Quiz Questions (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) They are synonyms D) Blockchains cannot use consensus

Quiz Questions (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) They are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains.

Q2. What minimum fraction of nodes must be honest for Byzantine consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%

Quiz Questions (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) They are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains.

Q2. What minimum fraction of nodes must be honest for Byzantine consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$ (at least 2/3 honest).

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated

Quiz Questions (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) They are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains.

Q2. What minimum fraction of nodes must be honest for Byzantine consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$ (at least 2/3 honest).

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed P2P networks have no central hubs.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB

Quiz Questions (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) They are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains.

Q2. What minimum fraction of nodes must be honest for Byzantine consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$ (at least 2/3 honest).

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed P2P networks have no central hubs.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes.

Q5. How many hashes verify a transaction in a 1,024-tx block using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024

Quiz Questions (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) They are synonyms D) Blockchains cannot use consensus
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains.

Q2. What minimum fraction of nodes must be honest for Byzantine consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$ (at least 2/3 honest).

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed P2P networks have no central hubs.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes.

Q5. How many hashes verify a transaction in a 1,024-tx block using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes needed.

Quiz Questions (6–10)

Q6. What storage does a Bitcoin full node require?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB

Quiz Questions (6–10)

Q6. What storage does a Bitcoin full node require?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Full nodes require approximately 600 GB (2025).

Q7. What is the minimum ETH stake to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH

Quiz Questions (6–10)

Q6. What storage does a Bitcoin full node require?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Full nodes require approximately 600 GB (2025).

Q7. What is the minimum ETH stake to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type achieves higher throughput?
A) Permissionless public B) Permissioned private C) Both equal D) Depends on hardware

Quiz Questions (6–10)

Q6. What storage does a Bitcoin full node require?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Full nodes require approximately 600 GB (2025).

Q7. What is the minimum ETH stake to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type achieves higher throughput?
A) Permissionless public B) Permissioned private C) Both equal D) Depends on hardware
Answer: B – Permissioned: 1,000+ TPS vs. 5-30 TPS for public.

Q9. Which DLT uses a DAG instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger D) Cardano

Quiz Questions (6–10)

Q6. What storage does a Bitcoin full node require?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Full nodes require approximately 600 GB (2025).

Q7. What is the minimum ETH stake to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type achieves higher throughput?
A) Permissionless public B) Permissioned private C) Both equal D) Depends on hardware
Answer: B – Permissioned: 1,000+ TPS vs. 5-30 TPS for public.

Q9. Which DLT uses a DAG instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger D) Cardano
Answer: B – IOTA uses DAG where transactions reference previous transactions.

Q10. Which block header field links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp

Quiz Questions (6–10)

Q6. What storage does a Bitcoin full node require?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Full nodes require approximately 600 GB (2025).

Q7. What is the minimum ETH stake to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type achieves higher throughput?
A) Permissionless public B) Permissioned private C) Both equal D) Depends on hardware
Answer: B – Permissioned: 1,000+ TPS vs. 5-30 TPS for public.

Q9. Which DLT uses a DAG instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger D) Cardano
Answer: B – IOTA uses DAG where transactions reference previous transactions.

Q10. Which block header field links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp
Answer: C – Previous Block Hash (32 bytes) creates the chain.

Quiz: DLT Concepts

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Neither relates to the other

Quiz (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Neither relates to the other
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., IOTA's DAG).

Q2. In the Byzantine Generals Problem, what minimum fraction must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%

Quiz (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Neither relates to the other
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., IOTA's DAG).

Q2. In the Byzantine Generals Problem, what minimum fraction must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated

Quiz (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Neither relates to the other
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., IOTA's DAG).

Q2. In the Byzantine Generals Problem, what minimum fraction must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed (P2P) networks have no central hubs, maximizing resilience.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB

Quiz (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Neither relates to the other
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., IOTA's DAG).

Q2. In the Byzantine Generals Problem, what minimum fraction must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed (P2P) networks have no central hubs, maximizing resilience.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes (6 fields).

Q5. How many hashes verify a tx in a block with 1,024 transactions using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024

Quiz (1–5)

Q1. Which statement correctly distinguishes DLT from blockchain?
A) All DLTs are blockchains B) All blockchains are DLTs C) DLT and blockchain are synonyms D) Neither relates to the other
Answer: B – All blockchains are DLTs, but not all DLTs are blockchains (e.g., IOTA's DAG).

Q2. In the Byzantine Generals Problem, what minimum fraction must be honest for consensus?
A) 1/2 B) 2/3 C) 3/4 D) 100%
Answer: B – Formal requirement: $n \geq 3f + 1$, meaning at least 2/3 honest nodes.

Q3. Which network topology has NO single point of failure?
A) Centralized B) Decentralized C) Distributed D) Federated
Answer: C – Distributed (P2P) networks have no central hubs, maximizing resilience.

Q4. What is the size of a Bitcoin block header?
A) 32 bytes B) 80 bytes C) 256 bytes D) 1 MB
Answer: B – Bitcoin block headers are exactly 80 bytes (6 fields).

Q5. How many hashes verify a tx in a block with 1,024 transactions using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes needed for Merkle proof.

Quiz (6–10)

Q6. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB

Quiz (6–10)

Q6. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of Dec 2025).

Q7. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH

Quiz (6–10)

Q6. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of Dec 2025).

Q7. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public B) Permissioned private C) Both equal D) Depends only on hardware

Quiz (6–10)

Q6. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of Dec 2025).

Q7. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public B) Permissioned private C) Both equal D) Depends only on hardware
Answer: B – Permissioned chains achieve 1,000+ TPS vs. 5-30 TPS for public chains.

Q9. Which DLT architecture uses a Directed Acyclic Graph instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger Fabric D) Cardano

Quiz (6–10)

Q6. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of Dec 2025).

Q7. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public B) Permissioned private C) Both equal D) Depends only on hardware
Answer: B – Permissioned chains achieve 1,000+ TPS vs. 5-30 TPS for public chains.

Q9. Which DLT architecture uses a Directed Acyclic Graph instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger Fabric D) Cardano
Answer: B – IOTA uses DAG (Tangle) where transactions reference previous transactions.

Q10. Which field in the Bitcoin block header links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp

Quiz (6–10)

Q6. What approximate storage is required for a Bitcoin full node?
A) 50 MB B) 10 GB C) 600 GB D) 12 TB
Answer: C – Bitcoin full nodes require approximately 600 GB (as of Dec 2025).

Q7. What is the minimum stake required to run an Ethereum validator?
A) 1 ETH B) 10 ETH C) 32 ETH D) 100 ETH
Answer: C – Ethereum requires exactly 32 ETH to activate a validator.

Q8. Which blockchain type typically achieves higher throughput (TPS)?
A) Permissionless public B) Permissioned private C) Both equal D) Depends only on hardware
Answer: B – Permissioned chains achieve 1,000+ TPS vs. 5-30 TPS for public chains.

Q9. Which DLT architecture uses a Directed Acyclic Graph instead of blocks?
A) Bitcoin B) IOTA Tangle C) Hyperledger Fabric D) Cardano
Answer: B – IOTA uses DAG (Tangle) where transactions reference previous transactions.

Q10. Which field in the Bitcoin block header links blocks together?
A) Merkle Root B) Nonce C) Previous Block Hash D) Timestamp
Answer: C – Previous Block Hash (32 bytes) creates the cryptographic chain.

Lesson 3: Cryptographic Hash Functions

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Define cryptographic hash functions and their key properties
2. Explain the avalanche effect with concrete examples
3. Describe the SHA-256 algorithm and its role in Bitcoin
4. Analyze collision resistance and the birthday paradox
5. Construct and verify Merkle trees step-by-step
6. Identify real-world applications of hash functions beyond blockchain

Prerequisites: L02 - DLT Concepts (Merkle trees introduction)

The Problem: How can we prove data integrity without revealing the data?

Part 1/2: Hash Functions (Fundamentals)

The Challenge

How can we compress any data (a single byte or an entire database) to a fixed-size "fingerprint" that uniquely identifies it and proves it hasn't been tampered with?

Why It Matters

- Without hash functions, we cannot detect tampering in blockchain blocks
- Every Bitcoin block must prove integrity of thousands of transactions

What We Need

- Collision resistance (no two inputs produce same output)
- Preimage resistance (cannot reverse the hash)
- Second preimage resistance (cannot forge alternate data)

The Cryptoeconomics Question

How do we create trust in data without a central authority?

Today's lesson: How cryptographic hash functions provide the foundation for blockchain security

What is a Hash Function?

Hash Function Definition

A **hash function** is a mathematical function that takes an input (message) of arbitrary length and produces a fixed-size output (hash/digest).

Mathematical Notation:

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

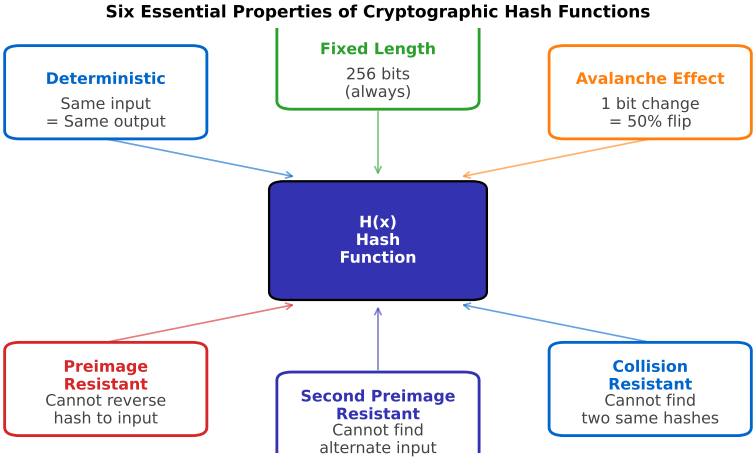
Where $\{0,1\}^*$ is any binary string, and $\{0,1\}^n$ is a fixed n-bit output.

Example (SHA-256):

- Input: "Hello World" (any length)
- Output: `a591a6d40bf420404...` (always 256 bits = 64 hex characters)

Hash functions are "digital fingerprints" - unique identifiers for data

Six Essential Properties of Cryptographic Hashes



Key Insight: All six properties are required for cryptographic security.

Non-Cryptographic vs. Cryptographic Hashes

Non-Cryptographic Hashes

- Fast computation
- Designed for hash tables, checksums
- NOT resistant to adversarial attacks
- Collision attacks are easy

Examples:

- CRC32 (cyclic redundancy check)
- MD5 (broken, not cryptographic anymore)
- MurmurHash (fast, non-crypto)

Cryptographic Hashes

- Slower, but secure
- Collision resistant
- Preimage resistant
- Unpredictable (pseudorandom)

Examples:

- SHA-256 (Bitcoin, SSL/TLS)
- SHA-3 (Keccak, used in Ethereum)
- BLAKE2 (fast, modern)

Key Difference: Cryptographic hashes must withstand deliberate attacks

Property 1: Deterministic

Deterministic Property

The same input always produces the same output. No randomness involved.

Example:

- $H(\text{“blockchain”}) = \texttt{ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1}$
- Computing this hash 1,000 times yields the same result every time

Why This Matters:

- Enables verification: Anyone can recompute the hash
- Makes auditing possible: Deterministic proofs
- Foundation for digital signatures

Contrast with Random Functions:

- Random: $f(x)$ might return different values each time
- Hash: $H(x)$ is a pure function (functional programming)

Property 2: Fixed-Length Output

Fixed-Length Property

Regardless of input size, the hash output is always the same fixed length.

Examples (SHA-256):

- $H(\text{“a”}) = 256$ bits (64 hex characters)
- $H(\text{entire Bitcoin whitepaper}) = 256$ bits (same length)
- $H(\text{1 GB video file}) = 256$ bits (still 64 hex chars)

Common Hash Sizes:

Algorithm	Output Size (bits)	Hex Characters
MD5 (broken)	128	32
SHA-1 (deprecated)	160	40
SHA-256 (Bitcoin)	256	64
SHA-512	512	128

Implication: Infinite inputs map to finite outputs $\Rightarrow$ collisions must exist (pigeonhole principle)

Property 3: Avalanche Effect (Sensitivity)

Avalanche Effect

A tiny change in input (even 1 bit) causes a massive, unpredictable change in the output. Approximately 50% of output bits flip.

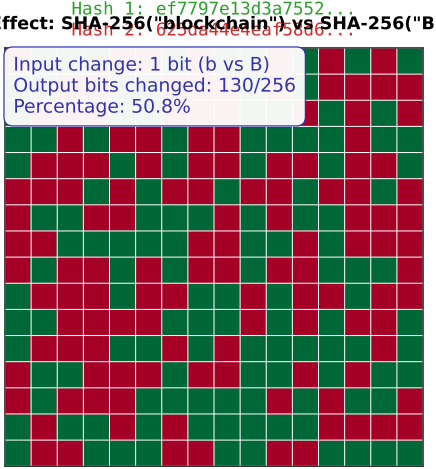
Example (SHA-256):

- Input: "blockchain"
  - Hash: `ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1`
- Input: "Blockchain" (capital B)
  - Hash: `625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1`

Analysis:

- Only 1 bit changed in input (ASCII: b = 01100010, B = 01000010)
- Output is completely different (no pattern recognizable)
- Approximately 128 out of 256 bits flipped (50%)

Avalanche Effect: Visual Demonstration



Green = Same bit | Red = Different bit

Observation: 1-bit input change causes approximately 50% of output bits to flip.

Property 4: Preimage Resistance (One-Way)

Preimage Resistance

Given a hash output h, it is computationally infeasible to find any input m such that $H(m) = h$.

Analogy: Easy to scramble an egg, impossible to unscramble it

Mathematical Formulation:

- Computing $h = H(m)$ is fast ($\approx$ microseconds)
- Finding m given h requires trying all 2^{256} possibilities (for SHA-256)
- At 1 trillion hashes/second, this would take 10^{58} years

Practical Implications:

- Password storage: Store H(password), not password itself
- Blockchain integrity: Cannot reverse-engineer block data from hash
- Commitment schemes: Hash your choice before revealing

Property 5: Second Preimage Resistance

Second Preimage Resistance

Given input m_1 and its hash $h = H(m_1)$, it is computationally infeasible to find a different input $m_2 \neq m_1$ such that $H(m_2) = h$.

Scenario:

- You sign a contract: "Pay Alice $1,000"
- Hash: $H(\text{contract}) = h$
- Attacker tries to find alternate message: "Pay Bob $1,000,000" with same hash h
- Second preimage resistance prevents this attack

Difference from Preimage Resistance:

- **Preimage**: Given h, find any m where $H(m) = h$
- **Second Preimage**: Given m_1 and $h = H(m_1)$, find different m_2 where $H(m_2) = h$

Property 6: Collision Resistance

Collision Resistance

It is computationally infeasible to find any two different inputs $m_1 \neq m_2$ such that $H(m_1) = H(m_2)$.

Theoretical Guarantee:

- Pigeonhole principle: Collisions MUST exist (infinite inputs, finite outputs)
- But finding them should be practically impossible

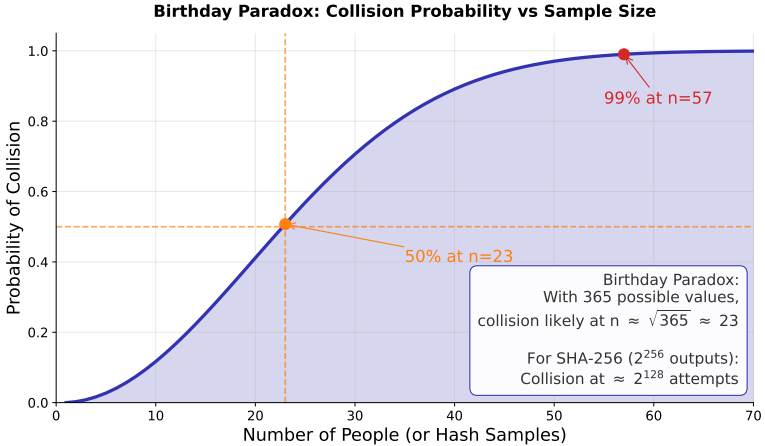
Birthday Paradox Attack:

- For n-bit hash, finding collision requires $\approx 2^{n/2}$ attempts (not 2^n)
- SHA-256: 2^{128} operations needed ($\approx 10^{38}$ hashes)
- Still infeasible with current technology

Broken Examples:

- MD5 collisions found in 2004 (now insecure)
- SHA-1 collisions demonstrated in 2017 (deprecated for security)

The Birthday Paradox



Implication: Collision resistance scales as $2^{n/2}$, not 2^n. This is why we need large hash outputs.

SHA-256 Overview

SHA-256

Secure Hash Algorithm 256-bit is a cryptographic hash function designed by the NSA, published by NIST in 2001 as part of the SHA-2 family.

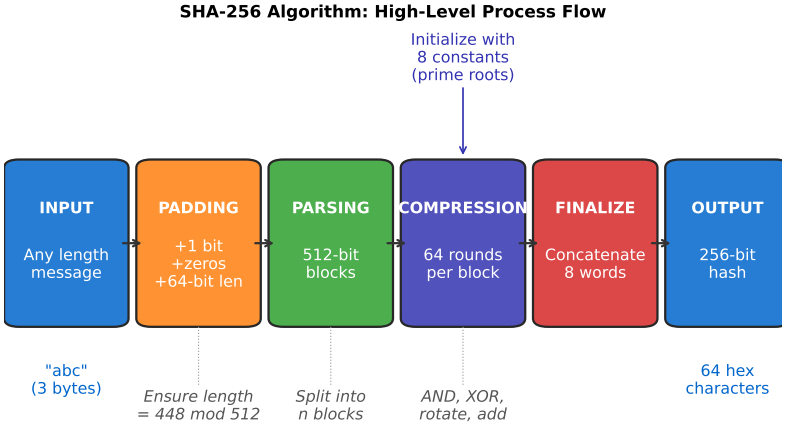
Specifications:

- Output: 256 bits (32 bytes, 64 hex characters)
- Block size: 512 bits (processes data in 512-bit chunks)
- Internal state: Eight 32-bit words (256 bits total)
- Rounds: 64 compression iterations per block

Uses in Bitcoin:

- Block hashing: Double SHA-256 (SHA256(SHA256(header)))
- Transaction IDs: SHA-256 hash of transaction data
- Address generation: SHA-256 + RIPEMD-160
- Merkle tree construction

SHA-256 High-Level Process



Key Steps: Padding ensures proper length; compression uses 64 rounds of bitwise operations.

SHA-256 Example Calculation

Input: "abc" (3 bytes)

Step 1 - Padding:

- Binary: `01100001 01100010 01100011` (24 bits)
- Add 1 bit: `01100001 01100010 01100011 1...`
- Pad with zeros until length $\equiv 448 \pmod{512}$
- Append 64-bit length: `...0000011000` (24 in binary)

Step 2 - Initialize Hash Values (first 8 primes):

- $H_0 =$ `6a09e667`, $H_1 =$ `bb67ae85`, ..., $H_7 =$ `5be0cd19`

Step 3 - Compression (64 rounds):

- Complex bitwise operations (Ch, Maj, Σ_0, Σ_1, etc.)

Final Output:

$$H(\text{"abc"}) = \texttt{ba7816bf8f01cfea414140de5dae2223b00361a396177a9cb410ff61f20015ad}$$

Double SHA-256 in Bitcoin

Why Double Hashing?

Bitcoin uses SHA256(SHA256(x)) instead of single SHA-256 to guard against length-extension attacks (theoretical vulnerability in Merkle-Damgard construction).

Process:

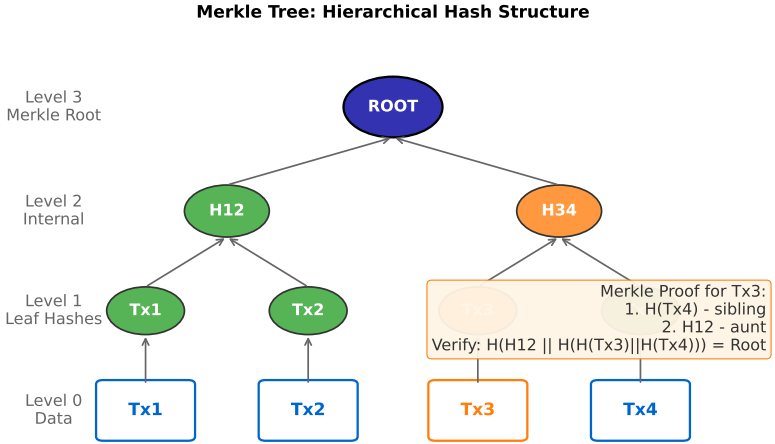
1. Compute $h_1 = \text{SHA256}(\text{data})$
2. Compute $h_2 = \text{SHA256}(h_1)$
3. Use h_2 as final hash

Example - Bitcoin Block Hash:

- Input: 80-byte block header
- First hash: $h_1 = \text{SHA256}(\text{header})$
- Second hash: $h_2 = \text{SHA256}(h_1)$
- Result: h_2 must be below difficulty target to be valid

Performance: Modern hardware computes millions of double-SHA256 per second

Merkle Tree Construction



Key Insight: Merkle proofs enable $O(\log n)$ verification of transaction inclusion.

Merkle Tree Construction Algorithm

Goal: Efficiently verify transaction inclusion without downloading all data

Construction Algorithm:

1. Start with n transactions: $Tx_1, Tx_2, ..., Tx_n$
2. Hash each transaction: $H_1 = H(Tx_1), H_2 = H(Tx_2), ..., H_n = H(Tx_n)$
3. Pair and hash: $H_{12} = H(H_1||H_2)$, $H_{34} = H(H_3||H_4)$, ...
4. If odd number, duplicate last hash: $H_{nn} = H(H_n||H_n)$
5. Repeat until single root hash (Merkle Root)

Example (4 transactions):

- Level 0: Tx_1, Tx_2, Tx_3, Tx_4
- Level 1: H_1, H_2, H_3, H_4
- Level 2: $H_{12} = H(H_1||H_2)$, $H_{34} = H(H_3||H_4)$
- Level 3 (Root): $R = H(H_{12}||H_{34})$

Merkle Proof Verification

Scenario: Light client wants to verify Tx_3 is in block (4 transactions total)

Verifier Has:

- Block header with Merkle Root R
- Transaction Tx_3

Prover Sends (Merkle Proof):

- H_4 (sibling of H_3)
- H_{12} (sibling of H_{34})

Verification Steps:

1. Compute $H_3 = H(Tx_3)$
2. Compute $H_{34} = H(H_3||H_4)$ (using provided H_4)
3. Compute $R' = H(H_{12}||H_{34})$ (using provided H_{12})
4. If $R' = R$, then Tx_3 is proven to be in the block

Efficiency: Only 2 hashes sent instead of 3 other transactions

Merkle Tree Efficiency Analysis

Space Complexity:

- For n transactions, tree has $\approx 2n$ nodes
- Merkle proof requires $\log_2(n)$ hashes

Proof Size Comparison:

Transactions in Block	Full Data	Merkle Proof
10	$\approx$ 2.5 KB	4 hashes (128 bytes)
100	$\approx$ 25 KB	7 hashes (224 bytes)
1,000	$\approx$ 250 KB	10 hashes (320 bytes)
10,000	$\approx$ 2.5 MB	14 hashes (448 bytes)

Real-World Impact:

- Bitcoin block: $\approx$ 2,000 transactions $\Rightarrow$ 11-hash proof ($\approx$ 352 bytes)
- Full block: $\approx$ 1 MB
- Savings: $\frac{352}{1{,}000{,}000} = 0.035\%$ of data needed

Merkle Tree Variants

Binary Merkle Tree

- Each node has 2 children
- Used in Bitcoin
- Proof size: $O(\log_2 n)$
- Simple to implement

Merkle Patricia Trie (Ethereum)

- Combines Merkle tree + Patricia trie
- Supports key-value storage
- Enables state root (all accounts)
- More complex, but more powerful

Verkle Trees (Future Ethereum)

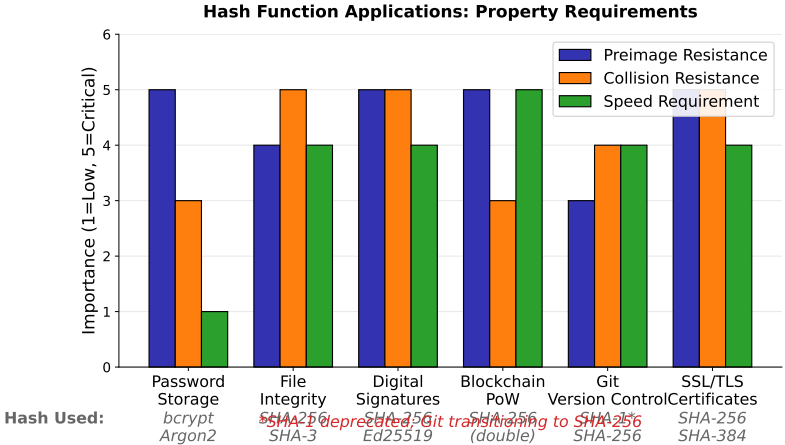
- Uses polynomial commitments
- Constant-size proofs (regardless of tree size)
- Enables stateless clients
- Based on vector commitments

Sparse Merkle Trees

- Fixed depth (e.g., 256 levels)
- Most branches empty (pruned)
- Supports non-membership proofs
- Used in some zero-knowledge systems

(c) Joerg Osterrieder 2025

Hash Function Applications Overview



Note: Different applications prioritize different hash properties.

Password Storage

Problem: Storing passwords in plaintext is insecure (database breach exposes all passwords)

Solution: Store $H(\text{password})$ instead

1. User creates account with password "mypassword123"
2. System computes $h = H(\text{"mypassword123"})$
3. Database stores only h, not the password
4. Login: User enters password, system hashes it, compares with stored h
5. Attacker with database cannot reverse h to get password (preimage resistance)

Enhancements:

- **Salting**: Add random data before hashing to prevent rainbow tables
  - Store $h = H(\text{password}||\text{salt})$ and salt
- **Key Stretching**: Use slow hash functions (bcrypt, Argon2) to resist brute-force

File Integrity Verification

Use Case: Ensure downloaded file hasn't been tampered with

Process:

1. Software developer publishes file hash on official website
   - Example: Ubuntu ISO hash on ubuntu.com
2. User downloads file from mirror site
3. User computes hash of downloaded file locally
4. User compares computed hash with official hash
5. If hashes match, file is authentic and unmodified

Real-World Example:

- Download Ubuntu 24.04 LTS ISO (4 GB)
- Official SHA-256: `c2e6f4dc37ac944e2f8b21de00e9610c79c61d11...`
- Compute: `sha256sum ubuntu-24.04-desktop-amd64.iso`
- Match confirms integrity

Git Version Control

How Git Uses Hash Functions:

- Every commit has a SHA-1 hash (Git transitioning to SHA-256)
- Hash is computed from:
  - Commit message
  - Author/committer metadata
  - Tree object (directory structure)
  - Parent commit hash(es)
- Forms a Merkle tree of commits (immutable history)

Example:

- Commit: `a3f5c79...` points to parent `b2e4d31...`
- Changing history requires recomputing all subsequent hashes
- Makes history tampering detectable

Similarity to Blockchain:

- Git is a content-addressed storage system
- Hashes link commits, just like blocks in blockchain

Digital Signatures & SSL/TLS

Digital Signatures (Overview - more in L05):

- Hash the message: $h = H(m)$
- Sign the hash with private key: $\sigma = \text{Sign}(h, sk)$
- Verify signature: $\text{Verify}(\sigma, h, pk)$
- Signing hash (32 bytes) is faster than signing entire message (MB+)

SSL/TLS (HTTPS):

- Certificate authorities (CAs) sign website certificates
- CA computes $h = H(\text{certificate})$
- CA signs h with private key
- Your browser verifies signature using CA's public key
- Ensures you're connected to legitimate website, not impostor

Hash Functions Used:

- Modern TLS 1.3: SHA-256, SHA-384
- Legacy systems: SHA-1 (deprecated due to collision attacks)

Proof-of-Work (Bitcoin Mining)

Mining Process:

1. Collect transactions into candidate block
2. Construct block header (80 bytes)
3. Compute: $h = \text{SHA256}(\text{SHA256}(\text{header}))$
4. Check if $h <$ target (difficulty requirement)
5. If no: increment nonce (4-byte counter), repeat step 3
6. If yes: broadcast valid block, receive reward

Example Difficulty (Block 800,000):

- Target: 00000000000000000000... (19 leading zeros)
- Probability of success per hash: $\frac{1}{2^{76}} \approx 10^{-23}$
- Network hash rate: $\approx$ 500 EH/s (Block 800,000, July 2023; now $\sim$1,000 EH/s, surpassing 1 ZH/s)

Why Hashes Enable PoW:

- Unpredictable output (no shortcut, must try all nonces)
- Fast verification (anyone can check $h <$ target instantly)

Problem Solved? Hash Functions

The Original Problem

How can we prove data integrity without revealing the data?

How Hash Functions Solve It

- SHA-256 provides 256-bit security level (computationally infeasible to break)
- Merkle trees enable efficient verification of large datasets ($O(\log n)$ proofs)
- Collision resistance ensures unique fingerprints for different data

Remaining Limitations

- Quantum computers threaten current hash functions (Grover's algorithm reduces security)
- MD5 and SHA-1 already broken (collision attacks found)

Open Questions

- When should blockchain migrate to post-quantum hash functions?
- Can we develop hash functions resistant to quantum attacks?
- Risk: Coordination challenge in decentralized networks for hash function upgrades

Hash functions solve data integrity verification but face future quantum threats

Key Takeaways

What You Should Remember:

1. **Hash Functions**: Transform arbitrary input to fixed-size output (digital fingerprints)
2. **Core Properties**: Deterministic, fixed-length, avalanche effect, preimage resistance, collision resistance
3. **SHA-256**: 256-bit output, used in Bitcoin (double hashing), computationally infeasible to break
4. **Collision Resistance**: Birthday paradox reduces attack from 2^n to $2^{n/2}$ operations
5. **Merkle Trees**: Binary hash trees enable $O(\log n)$ proofs for transaction inclusion
6. **Applications**: Passwords, file integrity, Git, digital signatures, Proof-of-Work

Critical Insight

Cryptographic hash functions are the foundation of blockchain security. Without collision resistance and preimage resistance, the entire system collapses.

Discussion Questions

Consider and discuss:

1. **Quantum Computing Threat**: Will quantum computers break SHA-256?
   - Research: Grover's algorithm reduces preimage attack to 2^{128} operations
2. **Hash Function Lifespan**: When should we migrate to SHA-3 or BLAKE3?
   - Consider: Coordination challenge in decentralized networks
3. **Environmental Impact**: Can we reduce PoW energy consumption without sacrificing security?
   - Explore: Alternative consensus mechanisms (PoS, PoSpace)

References & Resources

Standards & Specs

- NIST FIPS 180-4 (SHA-2 specification)
- RFC 6234 (SHA and HMAC-SHA)
- Keccak Team (SHA-3 documentation)

Academic Papers

- Merkle (1987): *A Digital Signature Based on a Conventional Encryption Function*
- Wang et al. (2005): *Finding Collisions in SHA-1*

Tools

- `sha256sum` (Linux command-line)
- Online SHA-256 calculator
- Python `hashlib` library

Learning Resources

- Computerphile: "Hashing Algorithms"
- Khan Academy: Cryptography course
- 3Blue1Brown: "But what is a hash function?"

Next Lesson Preview

L04: Lab - Hash Experiments

Hands-on exercises:

- Generate SHA-256 hashes using Python `hashlib`
- Visualize the avalanche effect (1-bit input change)
- Build a Merkle tree from scratch
- Verify Merkle proofs manually
- Experiment with collision search (limited scale)
- Analyze hash distribution properties

Required Setup: Python 3.8+, Jupyter Notebook or Python IDE

Deliverables: Lab report with code snippets and visualizations

Thank you

Questions?

See you in Lab 4: Hash Experiments

Quiz - Part 1

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit (32-byte) output, regardless of input size.

Q2. Which property ensures the same input always produces the same hash?
A) Avalanche effect B) Collision resistance C) Deterministic D) Preimage resistance
Answer: C – Deterministic means no randomness; same input = same output always.

Q3. What percentage of output bits typically flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% of output bits to flip.

Q4. Which hash algorithm is broken and no longer considered secure?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions were found in 2004; it's not cryptographically secure.

Q5. What does preimage resistance prevent?
A) Finding input from hash B) Finding two inputs with same hash C) Fast computation D) Fixed output length
Answer: A – Preimage resistance means you cannot reverse a hash to find the original input.

Quiz - Part 2

Q6. How many rounds of compression does SHA-256 perform per 512-bit block?
A) 16 B) 32 C) 64 D) 128
Answer: C – SHA-256 uses 64 rounds of bitwise operations per block.

Q7. Why does Bitcoin use double SHA-256 instead of single hashing?
A) Faster computation B) Smaller output C) Guard against length-extension attacks D) Easier implementation
Answer: C – Double hashing protects against theoretical length-extension vulnerabilities.

Q8. What is the birthday paradox complexity for finding hash collisions?
A) 2^n B) $2^{n/2}$ C) 2^{2n} D) $\log n$
Answer: B – Birthday attack reduces collision search from 2^n to $2^{n/2}$ operations.

Q9. For SHA-256, approximately how many operations are needed for birthday attack?
A) 2^{64} B) 2^{128} C) 2^{256} D) 2^{512}
Answer: B – $2^{256/2} = 2^{128}$ operations, still computationally infeasible.

Q10. What distinguishes second preimage resistance from preimage resistance?
A) Faster computation B) You're given the original input C) Shorter output D) No difference
Answer: B – Second preimage: find different m_2 for given m_1 where $H(m_1) = H(m_2)$.

Quiz - Part 3

Q11. How many hashes are needed for a Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed for proof path to root.

Q12. What happens if a Merkle tree has an odd number of leaf nodes?
A) Error occurs B) Last hash is duplicated C) Tree is invalid D) Extra node is discarded
Answer: B – The last hash is duplicated to create a pair for hashing.

Q13. Which Merkle tree variant does Ethereum use?
A) Binary Merkle Tree B) Merkle Patricia Trie C) Verkle Tree D) Sparse Merkle Tree
Answer: B – Ethereum uses Merkle Patricia Trie for state storage with key-value support.

Q14. What is the space complexity of a Merkle proof for n transactions?
A) $O(n)$ B) $O(n^2)$ C) $O(\log n)$ D) $O(1)$
Answer: C – Proof size grows logarithmically with number of transactions.

Q15. In password storage, what is the purpose of salting?
A) Make hash faster B) Prevent rainbow table attacks C) Reduce output size D) Enable reversibility
Answer: B – Salt (random data) prevents precomputed hash tables (rainbow tables).

Quiz - Part 4

Q16. Which hash function is Git transitioning to from SHA-1?
A) MD5 B) SHA-256 C) SHA-3 D) BLAKE2
Answer: B – Git is migrating to SHA-256 due to SHA-1 collision vulnerabilities.

Q17. What makes collision resistance critical for digital signatures?
A) Faster signing B) Prevents forged documents with same hash C) Smaller signatures D) Easier verification
Answer: B – Without collision resistance, attacker could create alternate message with identical hash.

Q18. In Bitcoin mining, what must the hash be less than?
A) Merkle root B) Previous block hash C) Difficulty target D) Nonce value
Answer: C – Hash must be below difficulty target (e.g., certain number of leading zeros).

Q19. What is the block size that SHA-256 processes data in?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: C – SHA-256 processes input in 512-bit (64-byte) blocks.

Q20. Which quantum algorithm threatens preimage resistance of hash functions?
A) Shor's algorithm B) Grover's algorithm C) Deutsch-Jozsa D) Simon's algorithm
Answer: B – Grover's algorithm reduces preimage search from 2^{256} to 2^{128} operations.

Lesson 3: Cryptographic Hash Functions

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Define cryptographic hash functions and their key properties
2. Explain the avalanche effect with concrete examples
3. Describe the SHA-256 algorithm and its role in Bitcoin
4. Analyze collision resistance and the birthday paradox
5. Construct and verify Merkle trees step-by-step
6. Identify real-world applications of hash functions beyond blockchain

Prerequisites: L02 - DLT Concepts (Merkle trees introduction)
Building on L02b: DLT Architecture

Fingerprinting Everything

[COMIC: A detective examining a tiny grain of sand with a magnifying glass, and a giant "fingerprint" (hash) floating above it. Caption: "Every piece of data has a unique fingerprint – even this grain of sand."]

[Comic placeholder – to be illustrated]

- Hash functions create unique "fingerprints" for any data – a single byte or an entire database
- Change one bit, and the fingerprint transforms completely

The Problem: How can we prove data integrity without revealing the data?

Part 1/2: Hash Functions (Fundamentals)

The Challenge

How can we compress any data (a single byte or an entire database) to a fixed-size "fingerprint" that uniquely identifies it and proves it hasn't been tampered with?

Why It Matters

- Without hash functions, we cannot detect tampering in blockchain blocks
- Every Bitcoin block must prove integrity of thousands of transactions

What We Need

- Collision resistance (no two inputs produce same output)
- Preimage resistance (cannot reverse the hash)
- Second preimage resistance (cannot forge alternate data)

The Cryptoeconomics Question

How do we create trust in data without a central authority?

Today's lesson: How cryptographic hash functions provide the foundation for blockchain security

(c) Joerg Osterrieder 2025

How Do Hash Functions Create Digital Fingerprints?

Hash Function Definition

A **hash function** is a mathematical function that takes an input (message) of arbitrary length and produces a fixed-size output (hash/digest).

Mathematical Notation:

$$H : \{0,1\}^* \rightarrow \{0,1\}^n$$

(takes any binary input $\rightarrow$ outputs fixed-length binary)
Where $\{0,1\}^*$ is any binary string, and $\{0,1\}^n$ is a fixed n-bit output.

Example (SHA-256):

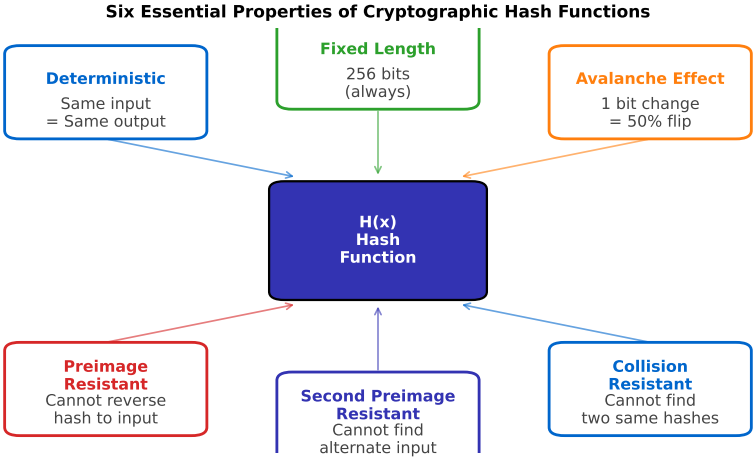
- Input: "Hello World" (any length)
- Output: `a591a6d40bf420404...` (always 256 bits = 64 hex characters)

Hash functions are "digital fingerprints" - unique identifiers for data

---

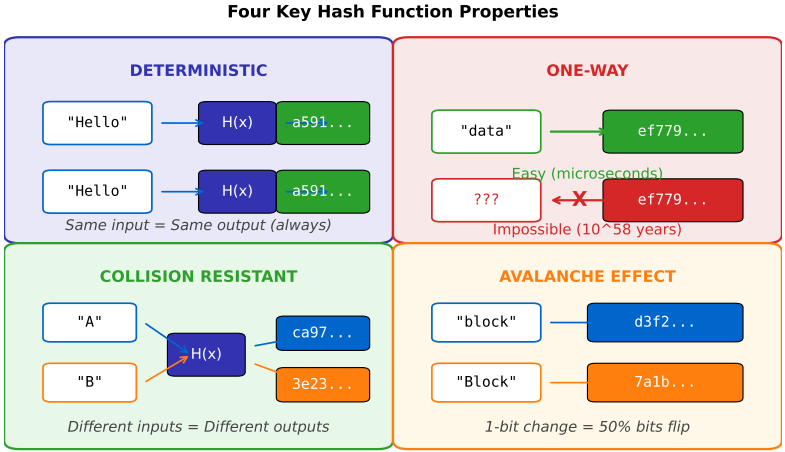
Hash functions create fixed-size fingerprints that prove data integrity without revealing the original data

What Are the Six Essential Properties of Cryptographic Hashes?



Key Insight: All six properties are required for cryptographic security.

How Do Hash Properties Work in Practice?



Key Insight: Each property serves a distinct security purpose in blockchain systems.

What's the Difference Between Cryptographic and Non-Cryptographic Hashes?

Non-Cryptographic Hashes

- Fast computation
- Designed for hash tables, checksums
- NOT resistant to adversarial attacks
- Collision attacks are easy

Examples:

- CRC32 (cyclic redundancy check)
- MD5 (broken, not cryptographic anymore)
- MurmurHash (fast, non-crypto)

Cryptographic Hashes

- Slower, but secure
- Collision resistant
- Preimage resistant
- Unpredictable (pseudorandom)

Examples:

- SHA-256 (Bitcoin, SSL/TLS)
- SHA-3 (Keccak, used in Ethereum)
- BLAKE2 (fast, modern)

Key Difference: Cryptographic hashes must withstand deliberate attacks

Why Must Hash Functions Be Deterministic?

Deterministic Property

The same input always produces the same output. No randomness involved.

Example: $H(\text{“blockchain”}) = \texttt{ef7797e1...}$ – computing 1,000 times yields the same result

Why This Matters:

- Enables verification: Anyone can recompute the hash
- Makes auditing possible: Deterministic proofs
- Foundation for digital signatures

Contrast with Random Functions:

- Random: $f(x)$ might return different values each time
- Hash: $H(x)$ is a pure function (functional programming)

Determinism enables trustless verification: anyone can independently recompute and confirm a hash

Why Do Hash Functions Produce Fixed-Length Output?

Fixed-Length Property

Regardless of input size, the hash output is always the same fixed length.

Examples (SHA-256):

- $H(\text{“a”}) = 256$ bits (64 hex characters)
- $H(\text{entire Bitcoin whitepaper}) = 256$ bits (same length)
- $H(\text{1 GB video file}) = 256$ bits (still 64 hex chars)

Common Hash Sizes:

Algorithm	Output Size (bits)	Hex Characters
MD5 (broken)	128	32
SHA-1 (deprecated)	160	40
SHA-256 (Bitcoin)	256	64
SHA-512	512	128

Implication: Infinite inputs map to finite outputs $\Rightarrow$ collisions must exist (pigeonhole principle)

What Is the Avalanche Effect?

Avalanche Effect

A tiny change in input (even 1 bit) causes a massive, unpredictable change in the output. Approximately 50% of output bits flip.

Example (SHA-256):

- Input: "blockchain"
  - Hash: `ef7797e13d3a75526946a3bcf00daec9fc9c9c4d51ddc7cc5df888f74dd434d1`
- Input: "Blockchain" (capital B)
  - Hash: `625da44e4eaf58d61cf048d168aa6f5e492dea166d8bb54ec06c30de07db57e1`

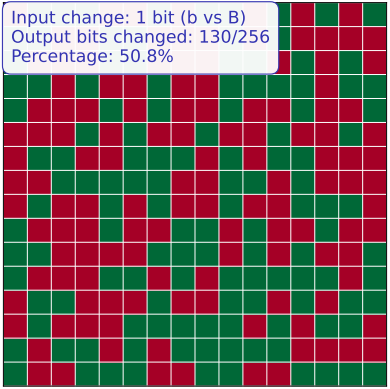
Analysis:

- Only 1 bit changed in input (ASCII: b = 01100010, B = 01000010)
- Output is completely different (no pattern recognizable)
- Approximately 128 out of 256 bits flipped (50%)

How Does the Avalanche Effect Prevent Tampering?

Hash 1: ef7797e13d3a7552...
Hash 2: e258d4f4e4e8af58d0...

Avalanche Effect: SHA-256("blockchain") vs SHA-256("Blockchain")



Green = Same bit | Red = Different bit

Observation: 1-bit input change causes approximately 50% of output bits to flip.

The avalanche effect ensures that even minor tampering produces completely different hashes, enabling detection

Why Is Preimage Resistance Critical?

Preimage Resistance

Given a hash output h, it is computationally infeasible to find any input m such that $H(m) = h$.

Analogy: Easy to scramble an egg, impossible to unscramble it

Mathematical Formulation:

- Computing $h = H(m)$ is fast ($\approx$ microseconds)
- Finding m given h requires trying all 2^{256} possibilities
- At 1 trillion hashes/sec: 10^{58} years

Practical Implications:

- Password storage: Store H(password), not password itself
- Blockchain integrity: Cannot reverse-engineer block data from hash
- Commitment schemes: Hash your choice before revealing

One-wayness is the foundation: easy to compute forward, infeasible to reverse

How Does Second Preimage Resistance Prevent Forgery?

Second Preimage Resistance

Given input m_1 and its hash $h = H(m_1)$, it is computationally infeasible to find a different input $m_2 \neq m_1$ such that $H(m_2) = h$.

Scenario:

- You sign a contract: "Pay Alice \$1,000"
- Hash: $H(\text{contract}) = h$
- Attacker tries to find alternate message: "Pay Bob \$1,000,000" with same hash h
- Second preimage resistance prevents this attack

Difference from Preimage Resistance:

- **Preimage**: Given h, find any m where $H(m) = h$
- **Second Preimage**: Given m_1 and $h = H(m_1)$, find different m_2 where $H(m_2) = h$

Why Is Collision Resistance Challenging?

Collision Resistance

It is computationally infeasible to find any two different inputs $m_1 \neq m_2$ such that $H(m_1) = H(m_2)$.

Theoretical Guarantee:

- Pigeonhole principle: Collisions MUST exist (infinite inputs, finite outputs)
- But finding them should be practically impossible

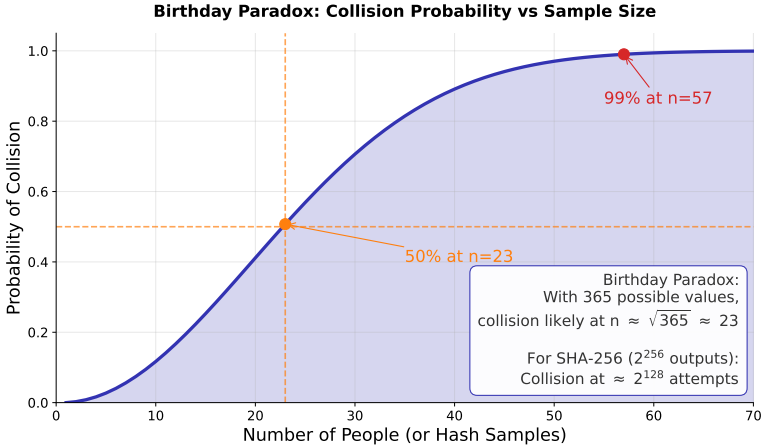
Birthday Paradox Attack:

- For n-bit hash, finding collision requires $\approx 2^{n/2}$ attempts (not 2^n) – (Like in a room of just 23 people, there's a 50% chance two share a birthday)
- SHA-256: 2^{128} operations needed ($\approx 10^{38}$ hashes)
- Still infeasible with current technology

Broken Examples:

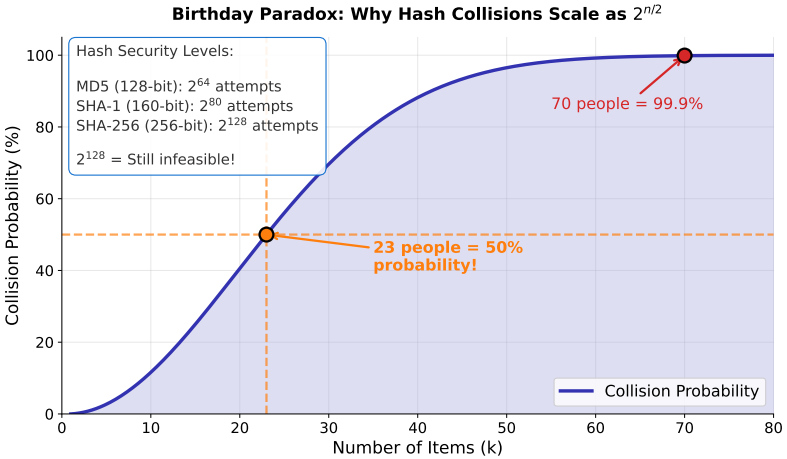
- MD5 collisions found in 2004 (now insecure)
- SHA-1 collisions demonstrated in 2017 (deprecated for security)

How Does the Birthday Paradox Threaten Hash Functions?



Implication: Collision resistance scales as $2^{n/2}$, not 2^n. This is why we need large hash outputs.

What Is the Collision Probability for SHA-256?



Security Implication: SHA-256 requires 2^{128} operations for birthday attack, still computationally infeasible.

How Does SHA-256 Work?

SHA-256

Secure Hash Algorithm 256-bit is a cryptographic hash function designed by the NSA, published by NIST in 2001 as part of the SHA-2 family.

Specifications:

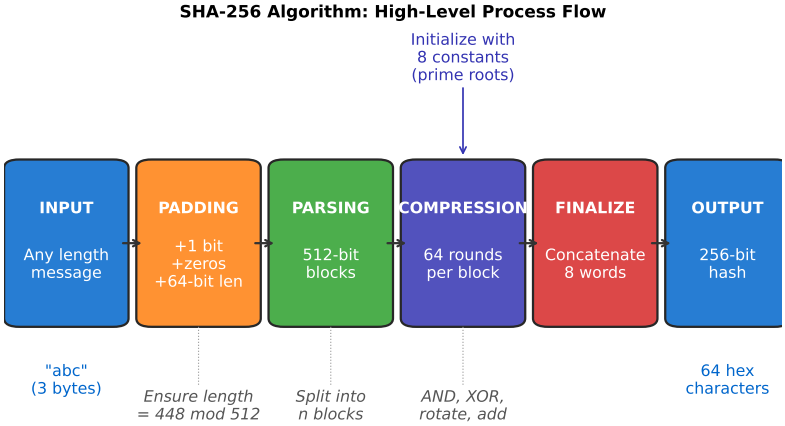
- Output: 256 bits (32 bytes, 64 hex characters)
- Block size: 512 bits (processes data in 512-bit chunks)
- Internal state: Eight 32-bit words (256 bits total)
- Rounds: 64 compression iterations per block

Uses in Bitcoin:

- Block hashing: Double SHA-256 (SHA256(SHA256(header)))
- Transaction IDs: SHA-256 hash of transaction data
- Address generation: SHA-256 + RIPEMD-160
- Merkle tree construction

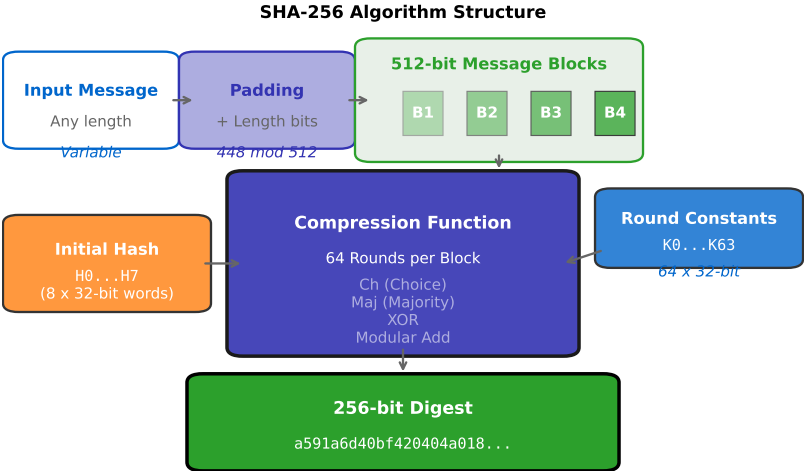
SHA-256 is the cryptographic backbone of Bitcoin – used for blocks, transactions, addresses, and Merkle trees

What Are the Key Steps in SHA-256 Processing?



Key Steps: Padding ensures proper length; compression uses 64 rounds of bitwise operations.

How Is SHA-256's Internal Structure Designed?



Key Insight: The compression function processes 512-bit blocks using 64 rounds of bitwise operations.

Problem Check-In: Hash Functions

Recall Our Problem

How do we prove knowledge without revealing secrets?

What We've Learned So Far

- Six essential properties of cryptographic hash functions
- SHA-256 algorithm and collision resistance guarantees
- Hash properties enable tamper detection and data integrity proofs

Still to Address

- Merkle trees and efficient verification of large datasets
- How do we verify data integrity at scale efficiently?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we prove knowledge without..."?

How Do You Calculate a SHA-256 Hash?

Input: "abc" (3 bytes)

Step 1 – Padding:

- Binary: `01100001 01100010 01100011`
- Add `1` bit, pad zeros until $\equiv 448 \pmod{512}$
- Append 64-bit length

Step 2 – Initialize:

- 8 hash values from first 8 primes
- $H_0 =$ `6a09e667`, ..., $H_7 =$ `5be0cd19`

Step 3 – Compression (64 rounds):

- Bitwise operations (Ch, Maj, Σ_0, Σ_1)
- Each round mixes message schedule with state

Final Output:

$H(\text{"abc"}) =$ `ba7816bf...f20015ad`

Always 256 bits (64 hex chars), regardless of input size.

SHA-256's deterministic computation allows anyone to verify data integrity by recomputing the hash

Why Does Bitcoin Use Double SHA-256?

Why Double Hashing?

Bitcoin uses SHA256(SHA256(x)) instead of single SHA-256 to guard against length-extension attacks (theoretical vulnerability in Merkle-Damgard construction).

Process:

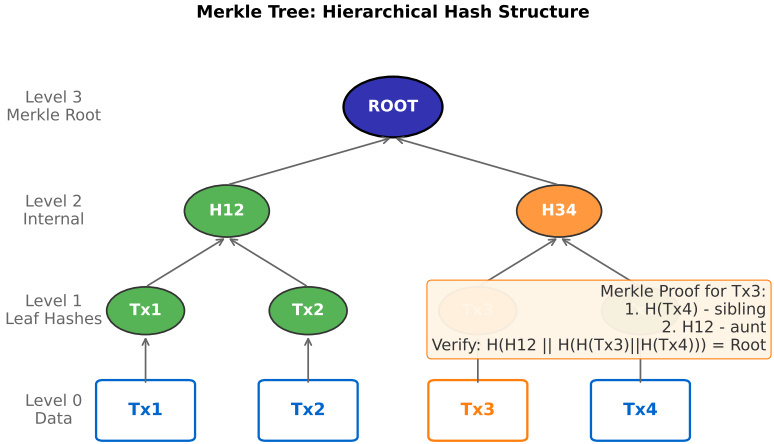
1. Compute $h_1 = \text{SHA256}(\text{data})$
2. Compute $h_2 = \text{SHA256}(h_1)$
3. Use h_2 as final hash

Example - Bitcoin Block Hash:

- Input: 80-byte block header
- First hash: $h_1 = \text{SHA256}(\text{header})$
- Second hash: $h_2 = \text{SHA256}(h_1)$
- Result: h_2 must be below difficulty target to be valid

Performance: Modern hardware computes millions of double-SHA256 per second

How Are Merkle Trees Built?



Key Insight: Merkle proofs enable $O(\log n)$ verification of transaction inclusion.

How Are Merkle Trees Constructed?

Goal: Efficiently verify transaction inclusion without downloading all data

Construction Algorithm:

1. Start with n transactions: $Tx_1, ..., Tx_n$
2. Hash each: $H_i = H(Tx_i)$
3. Pair and hash: $H_{12} = H(H_1||H_2)$
4. If odd, duplicate last hash
5. Repeat until single Merkle Root

Example (4 transactions):

- Level 0: Tx_1, Tx_2, Tx_3, Tx_4
- Level 1: H_1, H_2, H_3, H_4
- Level 2: H_{12}, H_{34}
- Level 3 (Root): $R = H(H_{12}||H_{34})$

Merkle trees compress thousands of transactions into a single 32-byte root hash

How Do You Verify a Merkle Proof?

Scenario: Light client verifies Tx_3 is in block (4 transactions total)

Verifier Has:

- Block header with Merkle Root R
- Transaction Tx_3

Prover Sends (Proof):

- H_4 (sibling of H_3)
- H_{12} (sibling of H_{34})

Verification Steps:

1. Compute $H_3 = H(Tx_3)$
2. Compute $H_{34} = H(H_3 || H_4)$
3. Compute $R' = H(H_{12} || H_{34})$
4. If $R' = R$: Tx_3 is in the block

Only 2 hashes sent instead of 3 other transactions – $O(\log n)$ verification

How Efficient Are Merkle Trees?

Space Complexity:

- For n transactions, tree has $\approx 2n$ nodes
- Merkle proof requires $\log_2(n)$ hashes

Proof Size Comparison:

Transactions in Block	Full Data	Merkle Proof
10	$\approx$ 2.5 KB	4 hashes (128 bytes)
100	$\approx$ 25 KB	7 hashes (224 bytes)
1,000	$\approx$ 250 KB	10 hashes (320 bytes)
10,000	$\approx$ 2.5 MB	14 hashes (448 bytes)

Real-World Impact:

- Bitcoin block: $\approx$ 2,000 transactions $\Rightarrow$ 11-hash proof ($\approx$ 352 bytes)
- Full block: $\approx$ 1 MB
- Savings: $\frac{352}{1{,}000{,}000} = 0.035\%$ of data needed

What Are the Different Merkle Tree Variants?

Binary Merkle Tree

- Each node has 2 children
- Used in Bitcoin
- Proof size: $O(\log_2 n)$
- Simple to implement

Merkle Patricia Trie (Ethereum)

- Combines Merkle tree + Patricia trie
- Supports key-value storage
- Enables state root (all accounts)
- More complex, but more powerful

Verkle Trees (Future Ethereum)

- Uses polynomial commitments
- Constant-size proofs (regardless of tree size)
- Enables stateless clients
- Based on vector commitments

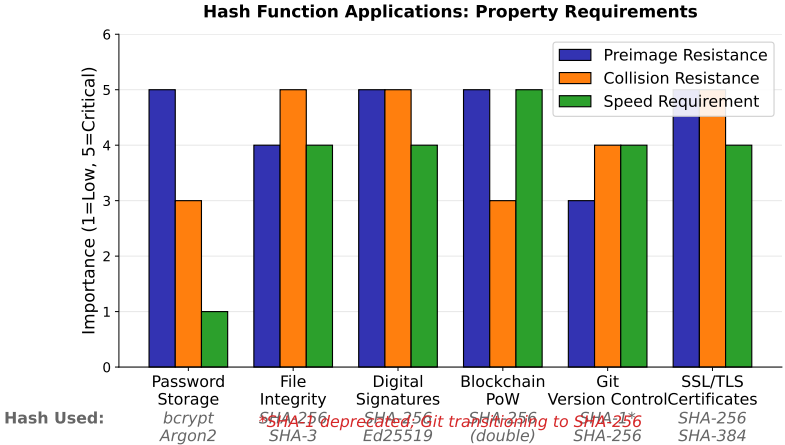
Sparse Merkle Trees

- Fixed depth (e.g., 256 levels)
- Most branches empty (pruned)
- Supports non-membership proofs
- Used in some zero-knowledge systems

Merkle tree variants optimize for different use cases while maintaining the core integrity proof property

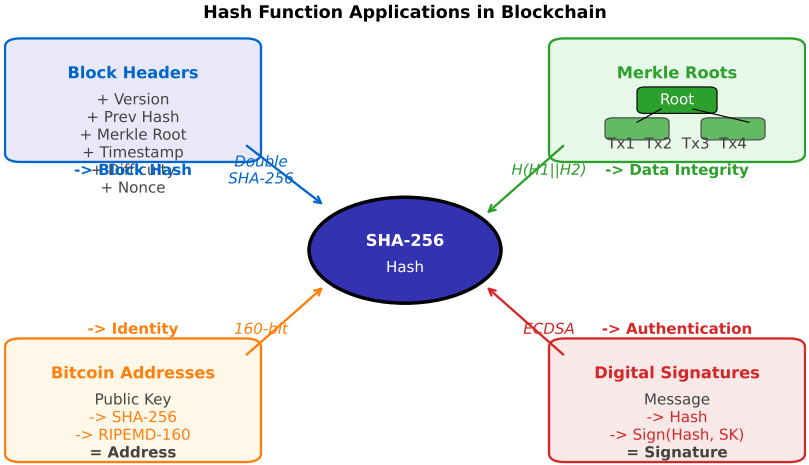
(c) Joerg Osterrieder 2025

Where Are Hash Functions Used Beyond Blockchain?



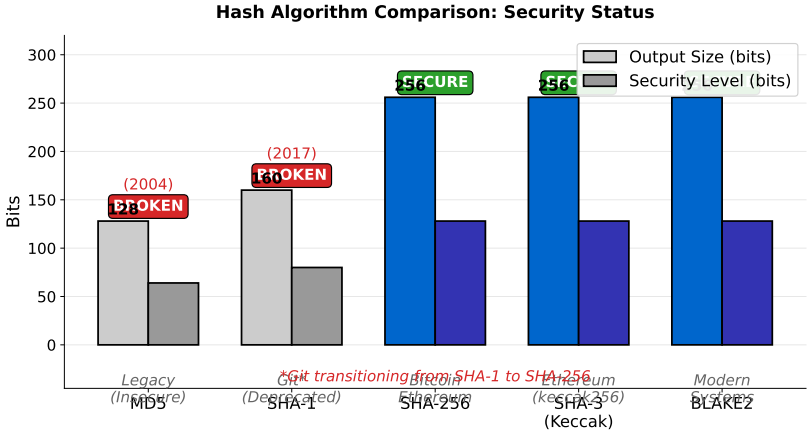
Note: Different applications prioritize different hash properties.

How Do Hash Functions Connect Blockchain Components?



Key Insight: SHA-256 is the cryptographic backbone connecting all blockchain components.

Which Hash Algorithms Are Secure?



Warning: MD5 and SHA-1 are broken. Always use SHA-256, SHA-3, or BLAKE2 for security applications.

How Should Passwords Be Stored Securely?

Problem: Storing passwords in plaintext is insecure (breach exposes all passwords)

Solution: Store $H(\text{password})$ instead

1. User creates password "mypassword123"
2. System computes $h = H(\text{password})$
3. Database stores only h
4. Login: hash input, compare with h
5. Preimage resistance prevents reversal

Enhancements:

- **Salting**: Add random data before hashing to prevent rainbow tables
  - Store $h = H(\text{pwd}||\text{salt})$ and salt
- **Key Stretching**: Slow hash functions (bcrypt, Argon2) resist brute-force

---

Hash-based password storage means even database breaches don't reveal user passwords

How Can We Verify File Integrity?

Use Case: Ensure downloaded file hasn't been tampered with

Process:

1. Software developer publishes file hash on official website
   - Example: Ubuntu ISO hash on ubuntu.com
2. User downloads file from mirror site
3. User computes hash of downloaded file locally
4. User compares computed hash with official hash
5. If hashes match, file is authentic and unmodified

Real-World Example:

- Download Ubuntu 24.04 LTS ISO (4 GB)
- Official SHA-256: `c2e6f4dc37ac944e2f8b21de00e9610c79c61d11...`
- Compute: `sha256sum ubuntu-24.04-desktop-amd64.iso`
- Match confirms integrity

How Does Git Use Hash Functions?

Git's Hash-Based Design:

- Every commit has a SHA-1 hash (transitioning to SHA-256)
- Hash computed from: message, author, tree object, parent hash(es)
- Forms a Merkle tree of commits (immutable history)

Example:

- `a3f5c79...` $\rightarrow$ parent `b2e4d31...`
- Changing history requires recomputing all subsequent hashes

Similarity to Blockchain:

- Git is a content-addressed storage system
- Hashes link commits, just like blocks in blockchain
- History tampering is detectable via hash chain breaks

Git and blockchain share the same core principle: hash-linked immutable history

How Do Hash Functions Enable Digital Signatures?

Digital Signatures (more in L05):

- Hash the message: $h = H(m)$
- Sign the hash: $\sigma = \text{Sign}(h, sk)$
- Verify: $\text{Verify}(\sigma, h, pk)$
- Signing 32-byte hash is faster than signing MB+ message

SSL/TLS (HTTPS):

- CAs sign website certificates
- CA computes $h = H(\text{cert})$, signs with private key
- Browser verifies using CA's public key
- Ensures legitimate connection

Algorithms: TLS 1.3 uses SHA-256/384; SHA-1 deprecated

Hashing before signing is both faster and more secure than signing raw data

How Does Proof-of-Work Mining Use Hash Functions?

Mining Process:

1. Collect transactions into candidate block
2. Construct block header (80 bytes)
3. Compute: $h = \text{SHA256}(\text{SHA256}(\text{header}))$
4. Check if $h < \text{target}$
5. If no: increment nonce, repeat
6. If yes: broadcast block, earn reward

Example (Block 800,000):

- Target: 19 leading zeros
- Success probability: $\frac{1}{2^{76}} \approx 10^{-23}$
- Network: $\sim$500 EH/s (now $>$1 ZH/s)

Why Hashes Enable PoW:

- Unpredictable output (no shortcut)
- Fast verification ($h <$ target? instant)

Hash unpredictability forces brute-force search; hash speed enables instant verification

The Avalanche Effect Butterfly

[COMIC: A butterfly flapping its wings on one side, causing a massive "hash avalanche" on the other side – a tsunami of completely different 1s and 0s. Caption: "One bit flaps, and the entire hash transforms."]

[Comic placeholder – to be illustrated]

- The avalanche effect is cryptography's "butterfly effect" – tiny changes cascade into complete transformation
- This unpredictability is what makes tampering instantly detectable

Problem Solved? Hash Functions

The Original Problem

How can we prove data integrity without revealing the data?

How Hash Functions Solve It

- SHA-256 provides 256-bit security level (computationally infeasible to break)
- Merkle trees enable efficient verification of large datasets ($O(\log n)$ proofs)
- Collision resistance ensures unique fingerprints for different data

Remaining Limitations

- Quantum computers threaten current hash functions (Grover's algorithm reduces security)
- MD5 and SHA-1 already broken (collision attacks found)

Open Questions

- When should blockchain migrate to post-quantum hash functions?
- Can we develop hash functions resistant to quantum attacks?
- Risk: Coordination challenge in decentralized networks for hash function upgrades

Hash functions solve data integrity verification but face future quantum threats

The Economics of Hash Functions

Incentive Structure

- **Core Problem:** Miners invest in hash computation; reward = block subsidy + fees
- **Why act honestly?** Mining reward exceeds cost only for valid blocks
- **Value Flow:** Users pay fees → miners earn rewards for securing the network

Economic Security

- Attack cost = majority of network hash rate
- Cost of 51% attack: billions in hardware + electricity

Key Economic Question

Who Pays, Who Earns?

Users pay transaction fees; miners earn block rewards for hash computation. Security scales with total hash rate investment.

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Hash functions convert electricity into security: the more energy spent mining, the harder it is to attack

Design Space: Hash Functions

Hash Function Choices

1. **SHA-256** (Bitcoin): Battle-tested, ASIC-dominated, 256-bit security
2. **Keccak-256** (Ethereum): ASIC-resistant design (initially), different construction
3. **BLAKE2** (Zcash): Faster computation, smaller output available

Trade-offs Made

- SHA-256: Proven security vs ASIC centralization
- Keccak: ASIC resistance vs less battle-tested

Design Questions

- Should hash functions resist ASICs (fair mining) or embrace them (more security)?
- How large should the output be? 256-bit vs 512-bit?
- When should a blockchain migrate to a new hash function?

Key Insight

Design Is Context-Dependent

Bitcoin chose SHA-256 for proven security; Ethereum chose Keccak for independence from NSA-influenced designs.

Every hash function choice trades off speed, security margin, hardware fairness, and proven track record

Failure Modes: Hash Functions

Critical Failure Modes

- **What breaks:** Collision found in the hash function
- **Why it matters:** Forged blocks, double spends, broken Merkle proofs

Historical Precedents

- **MD5 collision (2004)**: Practical attacks demonstrated
- **SHA-1 collision (2017)**: Google's SHAttered attack (2^{63} operations)
- Pattern: Hash functions weaken over time as attacks improve

Quantum Computing Threat

- Grover's algorithm halves security bits (256 $\rightarrow$ 128 effective)
- SHA-256 remains safe at 128-bit post-quantum security
- ECDSA signatures are more vulnerable than hashes

Early Warning Signs

- ! Reduced collision resistance in academic papers
- ! Practical quantum computers reaching 1000+ qubits
- ! NIST deprecation announcements

Assumption: SHA-256 is computationally infeasible to break. MD5 and SHA-1 show that assumptions can fail.

Key Takeaways

What You Should Remember:

1. **Hash Functions**: Transform arbitrary input to fixed-size output (digital fingerprints)
2. **Core Properties**: Deterministic, fixed-length, avalanche effect, preimage resistance, collision resistance
3. **SHA-256**: 256-bit output, used in Bitcoin (double hashing), computationally infeasible to break
4. **Collision Resistance**: Birthday paradox reduces attack from 2^n to $2^{n/2}$ operations
5. **Merkle Trees**: Binary hash trees enable $O(\log n)$ proofs for transaction inclusion
6. **Applications**: Passwords, file integrity, Git, digital signatures, Proof-of-Work

Critical Insight

Cryptographic hash functions are the foundation of blockchain security. Without collision resistance and preimage resistance, the entire system collapses.

Next Lesson: L04 – Lab: Hash Experiments

What Questions Should We Consider?

Consider and discuss:

1. **Quantum Computing Threat**: Will quantum computers break SHA-256?
   - Research: Grover's algorithm reduces preimage attack to 2^{128} operations
2. **Hash Function Lifespan**: When should we migrate to SHA-3 or BLAKE3?
   - Consider: Coordination challenge in decentralized networks
3. **Environmental Impact**: Can we reduce PoW energy consumption without sacrificing security?
   - Explore: Alternative consensus mechanisms (PoS, PoSpace)

Where Can You Learn More?

Standards & Specs

- NIST FIPS 180-4 (SHA-2 specification)
- RFC 6234 (SHA and HMAC-SHA)
- Keccak Team (SHA-3 documentation)

Academic Papers

- Merkle (1987): *A Digital Signature Based on a Conventional Encryption Function*
- Wang et al. (2005): *Finding Collisions in SHA-1*

Tools

- `sha256sum` (Linux command-line)
- Online SHA-256 calculator
- Python `hashlib` library

Learning Resources

- Computerphile: "Hashing Algorithms"
- Khan Academy: Cryptography course
- 3Blue1Brown: "But what is a hash function?"

What's Next?

L04: Lab - Hash Experiments

Hands-on exercises:

- Generate SHA-256 hashes using Python `hashlib`
- Visualize the avalanche effect (1-bit input change)
- Build a Merkle tree from scratch
- Verify Merkle proofs manually
- Experiment with collision search (limited scale)
- Analyze hash distribution properties

Required Setup: Python 3.8+, Jupyter Notebook or Python IDE

Deliverables: Lab report with code snippets and visualizations

Thank you

Questions?

See you in Lab 4: Hash Experiments

Quiz - Part 1

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit (32-byte) output, regardless of input size.

Q2. Which property ensures the same input always produces the same hash?
A) Avalanche effect B) Collision resistance C) Deterministic D) Preimage resistance
Answer: C – Deterministic means no randomness; same input = same output always.

Q3. What percentage of output bits typically flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% of output bits to flip.

Q4. Which hash algorithm is broken and no longer considered secure?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions were found in 2004; it's not cryptographically secure.

Q5. What does preimage resistance prevent?
A) Finding input from hash B) Finding two inputs with same hash C) Fast computation D) Fixed output length
Answer: A – Preimage resistance means you cannot reverse a hash to find the original input.

Quiz - Part 2

Q6. How many rounds of compression does SHA-256 perform per 512-bit block?
A) 16 B) 32 C) 64 D) 128
Answer: C – SHA-256 uses 64 rounds of bitwise operations per block.

Q7. Why does Bitcoin use double SHA-256 instead of single hashing?
A) Faster computation B) Smaller output C) Guard against length-extension attacks D) Easier implementation
Answer: C – Double hashing protects against theoretical length-extension vulnerabilities.

Q8. What is the birthday paradox complexity for finding hash collisions?
A) 2^n B) $2^{n/2}$ C) 2^{2n} D) $\log n$
Answer: B – Birthday attack reduces collision search from 2^n to $2^{n/2}$ operations.

Q9. For SHA-256, approximately how many operations are needed for birthday attack?
A) 2^{64} B) 2^{128} C) 2^{256} D) 2^{512}
Answer: B – $2^{256/2} = 2^{128}$ operations, still computationally infeasible.

Q10. What distinguishes second preimage resistance from preimage resistance?
A) Faster computation B) You're given the original input C) Shorter output D) No difference
Answer: B – Second preimage: find different m_2 for given m_1 where $H(m_1) = H(m_2)$.

Quiz - Part 3

Q11. How many hashes are needed for a Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed for proof path to root.

Q12. What happens if a Merkle tree has an odd number of leaf nodes?
A) Error occurs B) Last hash is duplicated C) Tree is invalid D) Extra node is discarded
Answer: B – The last hash is duplicated to create a pair for hashing.

Q13. Which Merkle tree variant does Ethereum use?
A) Binary Merkle Tree B) Merkle Patricia Trie C) Verkle Tree D) Sparse Merkle Tree
Answer: B – Ethereum uses Merkle Patricia Trie for state storage with key-value support.

Q14. What is the space complexity of a Merkle proof for n transactions?
A) $O(n)$ B) $O(n^2)$ C) $O(\log n)$ D) $O(1)$
Answer: C – Proof size grows logarithmically with number of transactions.

Q15. In password storage, what is the purpose of salting?
A) Make hash faster B) Prevent rainbow table attacks C) Reduce output size D) Enable reversibility
Answer: B – Salt (random data) prevents precomputed hash tables (rainbow tables).

Quiz - Part 4

Q16. Which hash function is Git transitioning to from SHA-1?
A) MD5 B) SHA-256 C) SHA-3 D) BLAKE2
Answer: B – Git is migrating to SHA-256 due to SHA-1 collision vulnerabilities.

Q17. What makes collision resistance critical for digital signatures?
A) Faster signing B) Prevents forged documents with same hash C) Smaller signatures D) Easier verification
Answer: B – Without collision resistance, attacker could create alternate message with identical hash.

Q18. In Bitcoin mining, what must the hash be less than?
A) Merkle root B) Previous block hash C) Difficulty target D) Nonce value
Answer: C – Hash must be below difficulty target (e.g., certain number of leading zeros).

Q19. What is the block size that SHA-256 processes data in?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: C – SHA-256 processes input in 512-bit (64-byte) blocks.

Q20. Which quantum algorithm threatens preimage resistance of hash functions?
A) Shor's algorithm B) Grover's algorithm C) Deutsch-Jozsa D) Simon's algorithm
Answer: B – Grover's algorithm reduces preimage search from 2^{256} to 2^{128} operations.

L03: Cryptographic Hash Functions

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Define cryptographic hash functions and their key properties
- Explain the avalanche effect and why it matters
- Understand SHA-256 and its role in Bitcoin
- Construct and verify Merkle trees for efficient proofs

What is a Hash Function?

Hash Function Definition

A **hash function** takes input of arbitrary length and produces a fixed-size output (hash/digest).

Mathematical Notation:

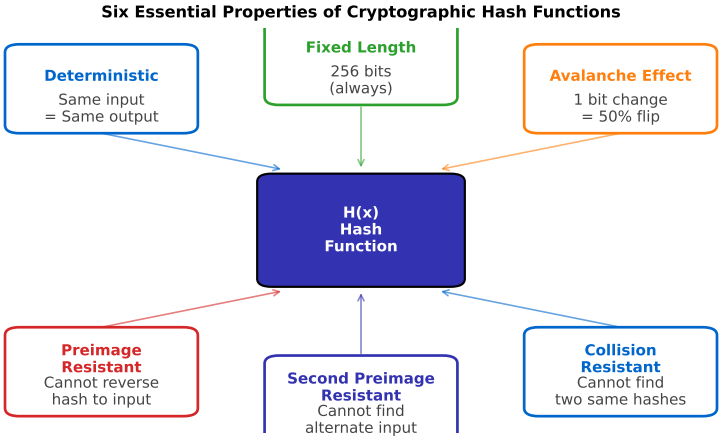
$$H : \{0,1\}^* \to \{0,1\}^n$$

Example (SHA-256):

- Input: "Hello World" (any length)
- Output: `a591a6d40bf420404...` (always 256 bits = 64 hex)

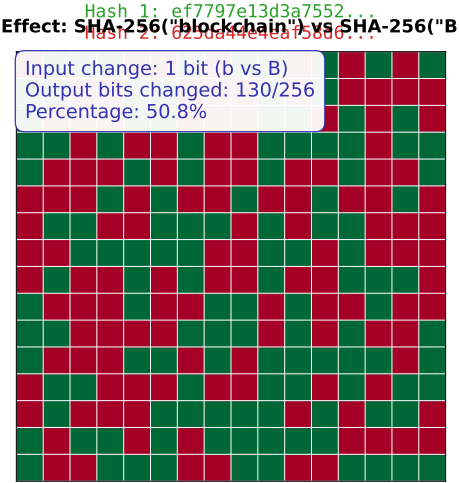
Hash functions are "digital fingerprints" – unique identifiers for data

Six Essential Properties



Key Insight: All six properties are required for cryptographic security.

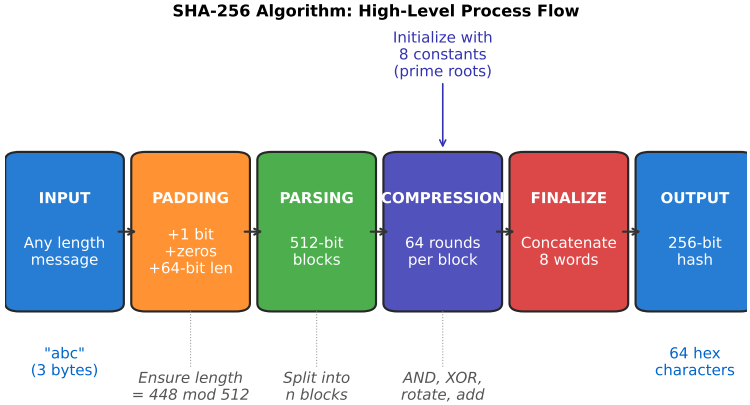
Avalanche Effect: 1 Bit Changes Everything



Green = Same bit | Red = Different bit

1-bit input change causes approximately **50%** of output bits to flip – completely unpredictable output.

SHA-256: The Workhorse



Bitcoin uses double SHA-256: $H(H(x))$ guards against length-extension attacks.

Collision Resistance & Birthday Paradox

Collision: Two different inputs $m_1 \neq m_2$ where $H(m_1) = H(m_2)$

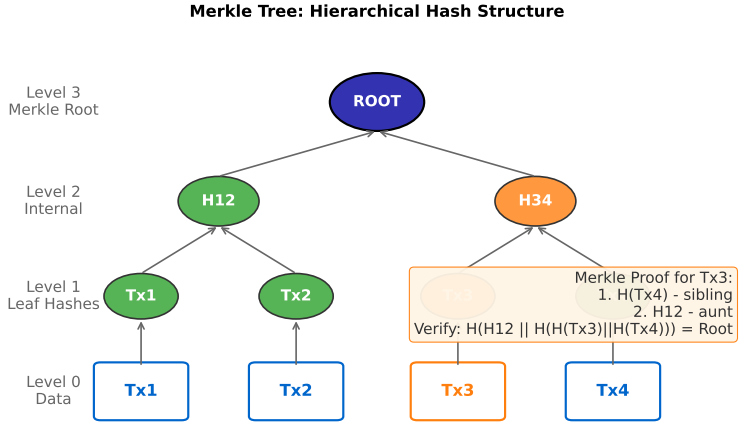
Birthday Paradox Attack:

- For n-bit hash, finding collision requires $\approx 2^{n/2}$ attempts (not 2^n)
- SHA-256: 2^{128} operations needed ($\approx 10^{38}$ hashes)
- Still computationally infeasible with current technology

Broken Examples:

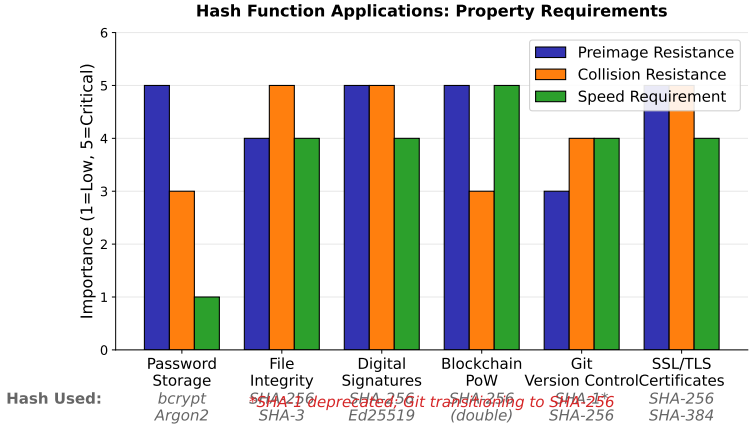
- MD5 collisions found 2004 (insecure)
- SHA-1 collisions demonstrated 2017 (deprecated)

Merkle Trees: Efficient Verification



Key Insight: Merkle proofs enable $O(\log n)$ verification – prove 1 transaction in 1,000 with only 10 hashes.

Real-World Applications



Beyond Blockchain: Passwords, file integrity, Git, SSL/TLS, digital signatures.

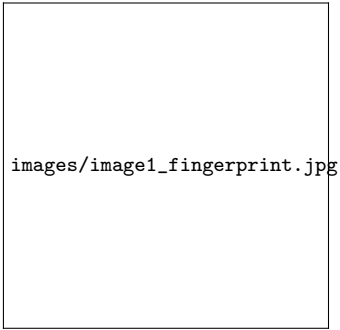
Key Takeaways

1. **Hash Functions:** Transform arbitrary input to fixed-size output (digital fingerprints)
2. **Core Properties:** Deterministic, fixed-length, avalanche effect, preimage resistance, collision resistance
3. **SHA-256:** 256-bit output, Bitcoin uses double hashing, computationally infeasible to break
4. **Merkle Trees:** Binary hash trees enable $O(\log n)$ proofs for transaction inclusion

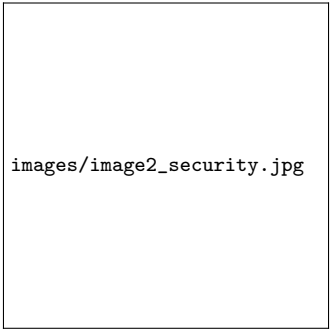
Critical Insight

Cryptographic hash functions are the foundation of blockchain security. Without collision and preimage resistance, the entire system collapses.

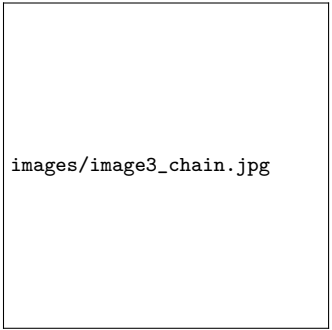
Hash Functions in the Real World



Digital Fingerprints



Cryptographic Security



Blockchain Chains

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits

Quiz (1/2)

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit output.

Q2. What percentage of output bits flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%

Quiz (1/2)

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit output.

Q2. What percentage of output bits flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% flip.

Q3. Which hash algorithm is broken and insecure?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2

Quiz (1/2)

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit output.

Q2. What percentage of output bits flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% flip.

Q3. Which hash algorithm is broken and insecure?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions were found in 2004.

Q4. What is the birthday paradox complexity for collision attacks?
A) 2^n B) $2^{n/2}$ C) 2^{2n} D) $\log n$

Quiz (1/2)

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit output.

Q2. What percentage of output bits flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% flip.

Q3. Which hash algorithm is broken and insecure?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions were found in 2004.

Q4. What is the birthday paradox complexity for collision attacks?
A) 2^n B) $2^{n/2}$ C) 2^{2n} D) $\log n$
Answer: B – Birthday attack reduces from 2^n to $2^{n/2}$.

Q5. Why does Bitcoin use double SHA-256?
A) Faster B) Smaller output C) Length-extension protection D) Easier

Quiz (1/2)

Q1. What is the output size of SHA-256?
A) 128 bits B) 256 bits C) 512 bits D) 1024 bits
Answer: B – SHA-256 produces a fixed 256-bit output.

Q2. What percentage of output bits flip when 1 input bit changes?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% flip.

Q3. Which hash algorithm is broken and insecure?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions were found in 2004.

Q4. What is the birthday paradox complexity for collision attacks?
A) 2^n B) $2^{n/2}$ C) 2^{2n} D) $\log n$
Answer: B – Birthday attack reduces from 2^n to $2^{n/2}$.

Q5. Why does Bitcoin use double SHA-256?
A) Faster B) Smaller output C) Length-extension protection D) Easier
Answer: C – Guards against length-extension attacks.

Quiz (2/2)

Q6. How many hashes needed for Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500

Quiz (2/2)

Q6. How many hashes needed for Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed.

Q7. What does preimage resistance prevent?
A) Finding input from hash B) Finding collisions C) Fast computation D) Fixed output

Quiz (2/2)

Q6. How many hashes needed for Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed.

Q7. What does preimage resistance prevent?
A) Finding input from hash B) Finding collisions C) Fast computation D) Fixed output
Answer: A – Cannot reverse a hash to find original input.

Q8. Which Merkle tree variant does Ethereum use?
A) Binary B) Merkle Patricia Trie C) Verkle D) Sparse

Quiz (2/2)

Q6. How many hashes needed for Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed.

Q7. What does preimage resistance prevent?
A) Finding input from hash B) Finding collisions C) Fast computation D) Fixed output
Answer: A – Cannot reverse a hash to find original input.

Q8. Which Merkle tree variant does Ethereum use?
A) Binary B) Merkle Patricia Trie C) Verkle D) Sparse
Answer: B – Ethereum uses Merkle Patricia Trie for state storage.

Q9. What is the purpose of salting passwords?
A) Faster hash B) Prevent rainbow tables C) Reduce size D) Enable reversibility

Quiz (2/2)

Q6. How many hashes needed for Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed.

Q7. What does preimage resistance prevent?
A) Finding input from hash B) Finding collisions C) Fast computation D) Fixed output
Answer: A – Cannot reverse a hash to find original input.

Q8. Which Merkle tree variant does Ethereum use?
A) Binary B) Merkle Patricia Trie C) Verkle D) Sparse
Answer: B – Ethereum uses Merkle Patricia Trie for state storage.

Q9. What is the purpose of salting passwords?
A) Faster hash B) Prevent rainbow tables C) Reduce size D) Enable reversibility
Answer: B – Salt prevents precomputed hash tables.

Q10. Which quantum algorithm threatens hash preimage resistance?
A) Shor's B) Grover's C) Deutsch-Jozsa D) Simon's

Quiz (2/2)

Q6. How many hashes needed for Merkle proof with 1,000 transactions?
A) 5 B) 10 C) 100 D) 500
Answer: B – $\log_2(1000) \approx 10$ hashes needed.

Q7. What does preimage resistance prevent?
A) Finding input from hash B) Finding collisions C) Fast computation D) Fixed output
Answer: A – Cannot reverse a hash to find original input.

Q8. Which Merkle tree variant does Ethereum use?
A) Binary B) Merkle Patricia Trie C) Verkle D) Sparse
Answer: B – Ethereum uses Merkle Patricia Trie for state storage.

Q9. What is the purpose of salting passwords?
A) Faster hash B) Prevent rainbow tables C) Reduce size D) Enable reversibility
Answer: B – Salt prevents precomputed hash tables.

Q10. Which quantum algorithm threatens hash preimage resistance?
A) Shor's B) Grover's C) Deutsch-Jozsa D) Simon's
Answer: B – Grover's reduces search from 2^{256} to 2^{128}.

Thank you

Questions?

Next: L04 Lab – Hash Experiments

Quiz: Hash Functions

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3
Answer: C – Bitcoin uses double SHA-256 for block hashes.

Q4. Preimage resistance means:
A) Fast computation B) Cannot reverse hash to find input C) Fixed output size D) No collisions

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3
Answer: C – Bitcoin uses double SHA-256 for block hashes.

Q4. Preimage resistance means:
A) Fast computation B) Cannot reverse hash to find input C) Fixed output size D) No collisions
Answer: B – Given hash output, infeasible to find any matching input.

Q5. How many hashes verify a tx in 1,024-tx block using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024

Quiz (1–5)

Q1. What is the output size of SHA-256?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – SHA-256 always produces 256-bit (64 hex character) output.

Q2. The avalanche effect means:
A) Hash grows exponentially B) 1-bit change flips 50% output C) Hash cascades D) Network congests
Answer: B – Small input change causes large, unpredictable output change.

Q3. Which hash algorithm is used by Bitcoin?
A) MD5 B) SHA-1 C) SHA-256 D) SHA-3
Answer: C – Bitcoin uses double SHA-256 for block hashes.

Q4. Preimage resistance means:
A) Fast computation B) Cannot reverse hash to find input C) Fixed output size D) No collisions
Answer: B – Given hash output, infeasible to find any matching input.

Q5. How many hashes verify a tx in 1,024-tx block using Merkle proof?
A) 5 B) 10 C) 512 D) 1,024
Answer: B – $\log_2 1024 = 10$ hashes for Merkle proof.

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy
Answer: B – Merkle proofs verify tx inclusion with $O(\log n)$ hashes.

Q9. Why does Bitcoin use double SHA-256?
A) More secure B) Faster C) Prevents length extension attacks D) Smaller output

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy
Answer: B – Merkle proofs verify tx inclusion with $O(\log n)$ hashes.

Q9. Why does Bitcoin use double SHA-256?
A) More secure B) Faster C) Prevents length extension attacks D) Smaller output
Answer: C – Double hashing prevents length extension attacks on SHA-256.

Q10. A collision occurs when:
A) Hash fails B) Two inputs produce same hash C) Output is too long D) Network splits

Quiz (6–10)

Q6. The birthday paradox implies collision attacks need:
A) 2^n attempts B) $2^{n/2}$ attempts C) n attempts D) $\log n$ attempts
Answer: B – Birthday bound: $2^{n/2}$ for n-bit hash (SHA-256: 2^{128}).

Q7. Which hash algorithm is considered broken?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 collisions can be found in seconds; deprecated.

Q8. Merkle trees enable:
A) Faster mining B) Efficient transaction verification C) Larger blocks D) Privacy
Answer: B – Merkle proofs verify tx inclusion with $O(\log n)$ hashes.

Q9. Why does Bitcoin use double SHA-256?
A) More secure B) Faster C) Prevents length extension attacks D) Smaller output
Answer: C – Double hashing prevents length extension attacks on SHA-256.

Q10. A collision occurs when:
A) Hash fails B) Two inputs produce same hash C) Output is too long D) Network splits
Answer: B – Collision: $H(m_1) = H(m_2)$ where $m_1 \neq m_2$.

Lab Session: Hash Function Experiments

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Use Python's `hashlib` library to compute SHA-256 hashes
- Demonstrate the avalanche effect experimentally
- Analyze collision resistance through brute-force attempts
- Build a simple proof-of-work mining simulation
- Verify hash-based integrity in practical scenarios

The Problem: Proving Work Without Trust

The Challenge
How can we force computational honesty in a system where anyone can claim to have done work? Traditional systems rely on trusted authorities to verify effort, but blockchain needs trustless proof of computational expenditure.

Why It Matters

- Without computational cost, attackers can rewrite history cheaply
- Sybil attacks: One actor creates thousands of fake identities

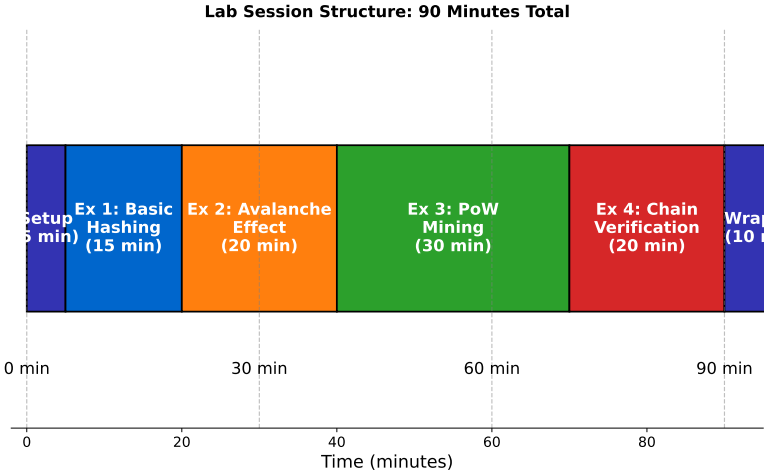
What We Need

- Verifiable proof that computational work was performed
- Work that is hard to produce but easy to verify
- Difficulty that adjusts to maintain consistent block times

The Cryptoeconomics Question
How do we make honest behavior computationally cheaper than attacks?

Today's lab: Explore how hash functions enable provable computational expense

Lab Session Structure



Total duration: 90 minutes with 4 hands-on exercises

Environment Setup

Required Libraries:

- `hashlib` (standard library)
- `time` (standard library)
- `json` (standard library)

Setup Instructions:

1. Create a new directory: `hash_lab`
2. Create a Python file: `hash_experiments.py`
3. Import required libraries
4. Test installation by computing a simple hash

Verification: Hash "Hello, Blockchain!" and verify output

Exercise 1: Basic Hashing

Objectives:

- Compute SHA-256 hashes of strings
- Compute SHA-256 hashes of files
- Compare different hash algorithms (MD5, SHA-1, SHA-256)

Tasks:

1. Create a function that takes a string and returns its SHA-256 hash
2. Hash: "Blockchain", "blockchain", "Blockchain " (with space)
3. Compare the outputs and observe differences
4. Create a text file and compute its hash
5. Modify one character and recompute

Expected Outcome: Tiny input changes produce completely different hashes

Exercise 2: Avalanche Effect Demonstration

Objective: Experimentally verify the avalanche effect

The Avalanche Effect:

- Changing a single bit should change approximately 50% of output bits
- Critical property for cryptographic security

Tasks:

1. Create a function that compares two hashes bit-by-bit
2. Hash "The quick brown fox jumps over the lazy dog"
3. Hash "The quick brown fox jumps over the lazy dof" (last letter changed)
4. Count how many bits differ between the two hashes
5. Calculate the percentage of bits that changed

Expected Result: Approximately 50% of bits should differ

Exercise 3: Simple Proof-of-Work Mining

Objective: Build a basic mining simulation

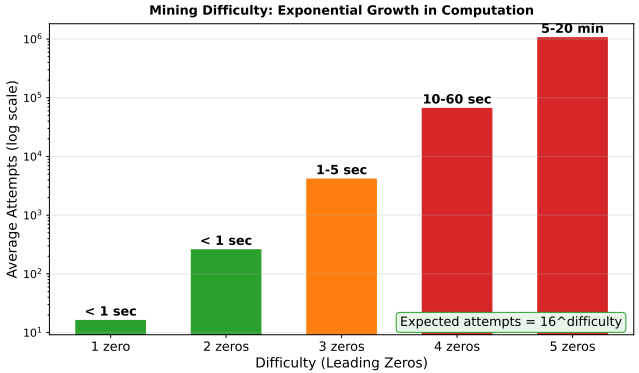
Concept Review:

- Mining = finding a nonce such that hash meets difficulty target
- Difficulty target = hash must start with N leading zeros
- No shortcut: must try different nonces sequentially

Tasks:

1. Create a block structure (number, data, previous hash, nonce)
2. Implement mining function that increments nonce until valid
3. Mine blocks with difficulty 1, 2, 3, 4
4. Record time taken and nonces tried for each difficulty

Mining Difficulty: Exponential Growth



Each additional zero increases difficulty by approximately 16x

Exercise 4: Hash Chain Verification

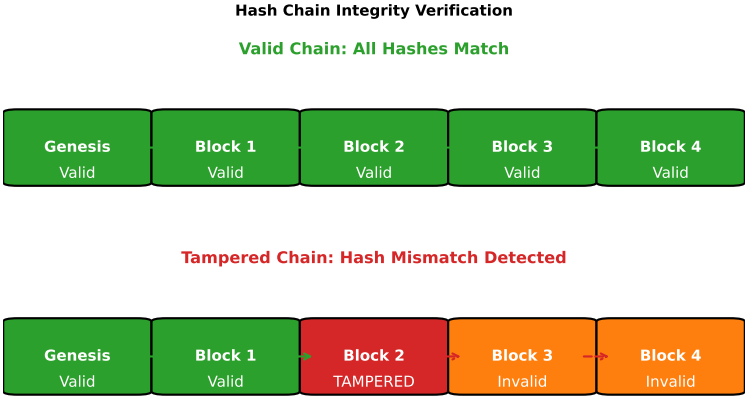
Objective: Build and verify a simple blockchain

Tasks:

1. Create a genesis block (first block with previous_hash = "0")
2. Create a function to add new blocks
3. Build a chain of 5 blocks
4. Implement a verification function that checks:
   - Each block's hash is valid
   - Each block correctly references previous hash
5. Tamper with block 3's data and observe verification failure

Expected Outcome: Understand immutability through hash chains

Chain Integrity Verification



Tampering breaks hash links, making modifications immediately detectable

Lab Deliverables

Submit the following:

1. **Python script** (`hash_experiments.py`) containing:
   - All four exercises implemented
   - Clear function names and comments
   - Test cases demonstrating functionality
2. **Lab report** (PDF, 2-3 pages) including:
   - Avalanche effect results (bit difference percentages)
   - Mining performance table (difficulty vs. time)
   - Screenshot of chain verification before and after tampering

Submission Deadline: One week from lab session date

Problem Solved? Computational Security

The Original Problem

Proving work without trusted authorities

How Hash-Based Mining Solves It

- **Proof-of-Work**: Hash difficulty forces computational expenditure (electricity + hardware costs)
- **Economic Incentive**: Block rewards (6.25 BTC) + transaction fees justify mining expense
- **Easy Verification**: Network nodes verify valid hashes instantly without re-mining

Remaining Limitations

- **Energy Consumption**: Bitcoin network uses 110 TWh/year (comparable to Netherlands)
- **51% Attack Risk**: If mining becomes too centralized, attacker can rewrite history

Open Questions

- Can we achieve security with less energy? (Proof-of-Stake alternatives)
- What happens when block rewards decrease? (Fee market dependency)

Hash-based mining converts computational cost into economic security, but at energy expense

Key Takeaways

- Hash functions are easy to compute but infeasible to reverse
- The avalanche effect ensures unpredictable output changes
- Proof-of-work mining is computationally expensive by design
- Hash chains create tamper-evident data structures
- Blockchain immutability comes from re-mining cost

Real-World Applications:

- Bitcoin/Ethereum mining
- Git version control (commit hashes)
- File integrity verification (checksums)

Discussion Questions

1. Why is it important that hash functions are deterministic?
2. Did you notice any patterns in which nonces produced valid hashes?
3. If you wanted to modify block 3 of a 100-block chain, how many hashes would you need to recompute?
4. How does increasing difficulty affect blockchain security?
5. What would happen if a hash function did not exhibit the avalanche effect?

(c) Joerg Osterrieder 2025

Quiz - Part 1

Q1. Which Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256 D) security
Answer: B – The `hashlib` library is Python's standard library for hash computations.

Q2. When demonstrating the avalanche effect, approximately what percentage of bits change?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% of bits to flip with a single bit input change.

Q3. In proof-of-work mining, what are we searching for?
A) A specific hash value B) A nonce that produces valid hash C) The private key D) The block data
Answer: B – Mining involves finding a nonce that makes the hash meet the difficulty target.

Q4. Each additional leading zero in difficulty target increases work by approximately:
A) 2x B) 8x C) 16x D) 256x
Answer: C – Each hex digit is 4 bits, so each zero increases difficulty by $2^4 = 16$ times.

Quiz - Part 2

Q5. What does the genesis block have as its previous hash?
A) Its own hash B) All zeros or null C) Random value D) Block 1's hash
Answer: B – The genesis block has no predecessor, so previous_hash is typically "0" or null.

Q6. If you tamper with block 3's data, verification fails because:
A) Block 3's hash changes B) Block 4's previous hash no longer matches C) Both A and B D) Neither
Answer: C – Tampering changes block 3's hash AND breaks block 4's previous hash reference.

Q7. Why must miners try different nonces sequentially?
A) Hash output is predictable B) Hash output is unpredictable C) Nonces are sequential D) Hardware limitation
Answer: B – Hash function output is unpredictable, so no shortcut exists to find valid nonces.

Q8. In a 100-block chain, modifying block 3 requires recomputing how many hashes?
A) 3 B) 97 C) 98 D) 100
Answer: C – Block 3 plus all subsequent blocks (4-100) = 98 blocks need recomputation.

Lab Session: Hash Function Experiments

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Use Python's `hashlib` library to compute SHA-256 hashes
- Demonstrate the avalanche effect experimentally
- Analyze collision resistance through brute-force attempts
- Build a simple proof-of-work mining simulation
- Verify hash-based integrity in practical scenarios

Building on L03: Cryptographic Hash Functions

Try to Reverse This!

[COMIC: A frustrated hacker staring at a hash output on screen, surrounded by crumpled papers with failed attempts. The hash mocks him: "Good luck finding my input!" Caption: "2^{256} possibilities, infinite frustration."]

[Comic placeholder – to be illustrated]

- Cryptographic hashes are one-way functions – easy to compute, impossible to reverse
- Today you'll experience why brute-force is the only option

The Problem: Proving Work Without Trust

The Challenge
How can we force computational honesty in a system where anyone can claim to have done work? Traditional systems rely on trusted authorities to verify effort, but blockchain needs trustless proof of computational expenditure.

Why It Matters

- Without computational cost, attackers can rewrite history cheaply
- Sybil attacks (creating fake identities to gain disproportionate influence): One actor creates thousands of fake identities

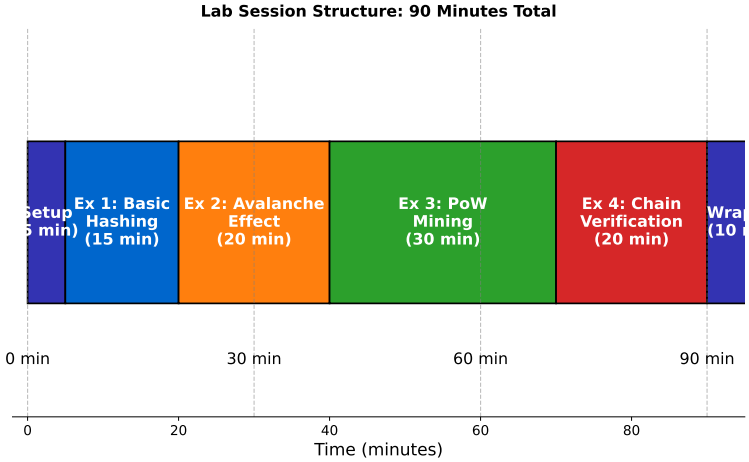
What We Need

- Verifiable proof that computational work was performed
- Work that is hard to produce but easy to verify
- Difficulty that adjusts to maintain consistent block times

The Cryptoeconomics Question
How do we make honest behavior computationally cheaper than attacks?

Today's lab: Explore how hash functions enable provable computational expense

What Will We Do Today?



Total duration: 90 minutes with 4 hands-on exercises

How Do You Set Up Your Environment?

Required Libraries:

- `hashlib` (standard library)
- `time` (standard library)
- `json` (standard library)

Setup Instructions:

1. Create a new directory: `hash_lab`
2. Create a Python file: `hash_experiments.py`
3. Import required libraries
4. Test installation by computing a simple hash

Verification: Hash "Hello, Blockchain!" and verify output

How Do You Hash Text and Files?

Objectives:

- Compute SHA-256 hashes of strings
- Compute SHA-256 hashes of files
- Compare different hash algorithms (MD5, SHA-1, SHA-256)

Tasks:

1. Create a function that takes a string and returns its SHA-256 hash
2. Hash: “Blockchain”, “blockchain”, “Blockchain ” (with space)
3. Compare the outputs and observe differences
4. Create a text file and compute its hash
5. Modify one character and recompute

Expected Outcome: Tiny input changes produce completely different hashes

(c) Joerg Osterrieder 2025

Why Does One Bit Change Everything?

Objective: Experimentally verify the avalanche effect

The Avalanche Effect:

- Changing a single bit should change approximately 50% of output bits
- Critical property for cryptographic security

Tasks:

1. Create a function that compares two hashes bit-by-bit
2. Hash "The quick brown fox jumps over the lazy dog"
3. Hash "The quick brown fox jumps over the lazy dof" (last letter changed)
4. Count how many bits differ between the two hashes
5. Calculate the percentage of bits that changed

Expected Result: Approximately 50% of bits should differ

(c) Joerg Osterrieder 2025

How Does Mining Actually Work?

Objective: Build a basic mining simulation

Concept Review:

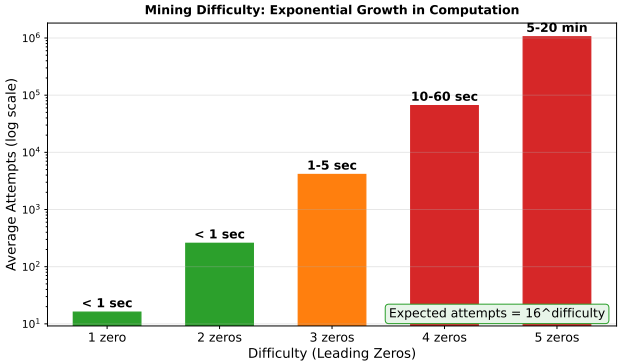
- Mining = finding a nonce such that hash meets difficulty target
- Difficulty target = hash must start with N leading zeros
- No shortcut: must try different nonces sequentially

Tasks:

1. Create a block structure (number, data, previous hash, nonce)
2. Implement mining function that increments nonce until valid
3. Mine blocks with difficulty 1, 2, 3, 4
4. Record time taken and nonces tried for each difficulty

(c) Joerg Osterrieder 2025

Why Does Mining Get Exponentially Harder?



Each additional zero increases difficulty by approximately 16x

How Do You Verify a Blockchain?

Objective: Build and verify a simple blockchain

Tasks:

1. Create a genesis block (first block with previous_hash = "0")
2. Create a function to add new blocks
3. Build a chain of 5 blocks
4. Implement a verification function that checks:
   - Each block's hash is valid
   - Each block correctly references previous hash
5. Tamper with block 3's data and observe verification failure

Expected Outcome: Understand immutability through hash chains

What Happens When You Tamper With a Block?

Hash Chain Integrity Verification

Valid Chain: All Hashes Match

Tampered Chain: Hash Mismatch Detected

Tampering breaks hash links, making modifications immediately detectable

(c) Joerg Osterrieder 2025

What Should You Submit?

Submit the following:

1. **Python script** (`hash_experiments.py`) containing:
   - All four exercises implemented
   - Clear function names and comments
   - Test cases demonstrating functionality
2. **Lab report** (PDF, 2-3 pages) including:
   - Avalanche effect results (bit difference percentages)
   - Mining performance table (difficulty vs. time)
   - Screenshot of chain verification before and after tampering

Submission Deadline: One week from lab session date

Problem Solved? Computational Security

The Original Problem

Proving work without trusted authorities

How Hash-Based Mining Solves It

- **Proof-of-Work**: Hash difficulty forces computational expenditure (electricity + hardware costs)
- **Economic Incentive**: Block rewards (3.125 BTC since April 2024 halving) + transaction fees justify mining expense
- **Easy Verification**: Network nodes verify valid hashes instantly without re-mining

Remaining Limitations

- **Energy Consumption**: Bitcoin network uses 110 TWh/year (comparable to Netherlands)
- **51% Attack Risk**: If mining becomes too centralized, attacker can rewrite history

Open Questions

- Can we achieve security with less energy? (Proof-of-Stake alternatives)
- What happens when block rewards decrease? (Fee market dependency)

Hash-based mining converts computational cost into economic security, but at energy expense

The Economics of Computational Security

Incentive Structure

- **Core Problem:** Coordinating without trusted intermediaries
- **Why act honestly?** Participants verify rather than trust
- **Value Flow:** Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Proof-of-Work Mining

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Hash-Based Security

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

The Birthday Paradox Surprise

[COMIC: A crowded room of 23 people at a party, two discovering they share a birthday. A cryptographer in the corner thinks: "Same principle breaks weak hashes!" Caption: "23 people, 50% collision chance – security lesson learned."]

[Comic placeholder – to be illustrated]

- The birthday paradox explains why hash collisions are easier to find than expected
- SHA-256's 256-bit output means 2^{128} operations for collision – still safe (for now)

Key Takeaways

- Hash functions are easy to compute but infeasible to reverse
- The avalanche effect ensures unpredictable output changes
- Proof-of-work mining is computationally expensive by design
- Hash chains create tamper-evident data structures
- Blockchain immutability comes from re-mining cost

Real-World Applications:

- Bitcoin/Ethereum mining
- Git version control (commit hashes)
- File integrity verification (checksums)

Next Lesson: L05 – Public Key Cryptography

Discussion Questions

1. Why is it important that hash functions are deterministic?
2. Did you notice any patterns in which nonces produced valid hashes?
3. If you wanted to modify block 3 of a 100-block chain, how many hashes would you need to recompute?
4. How does increasing difficulty affect blockchain security?
5. What would happen if a hash function did not exhibit the avalanche effect?

(c) Joerg Osterrieder 2025

Quiz - Part 1

Q1. Which Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256 D) security
Answer: B – The `hashlib` library is Python's standard library for hash computations.

Q2. When demonstrating the avalanche effect, approximately what percentage of bits change?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect causes approximately 50% of bits to flip with a single bit input change.

Q3. In proof-of-work mining, what are we searching for?
A) A specific hash value B) A nonce that produces valid hash C) The private key D) The block data
Answer: B – Mining involves finding a nonce that makes the hash meet the difficulty target.

Q4. Each additional leading zero in difficulty target increases work by approximately:
A) 2x B) 8x C) 16x D) 256x
Answer: C – Each hex digit is 4 bits, so each zero increases difficulty by $2^4 = 16$ times.

Quiz - Part 2

Q5. What does the genesis block have as its previous hash?
A) Its own hash B) All zeros or null C) Random value D) Block 1's hash
Answer: B – The genesis block has no predecessor, so previous_hash is typically "0" or null.

Q6. If you tamper with block 3's data, verification fails because:
A) Block 3's hash changes B) Block 4's previous hash no longer matches C) Both A and B D) Neither
Answer: C – Tampering changes block 3's hash AND breaks block 4's previous hash reference.

Q7. Why must miners try different nonces sequentially?
A) Hash output is predictable B) Hash output is unpredictable C) Nonces are sequential D) Hardware limitation
Answer: B – Hash function output is unpredictable, so no shortcut exists to find valid nonces.

Q8. In a 100-block chain, modifying block 3 requires recomputing how many hashes?
A) 3 B) 97 C) 98 D) 100
Answer: C – Block 3 plus all subsequent blocks (4-100) = 98 blocks need recomputation.

Quiz: Lab Hash Experiments

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256lib D) securelib

Quiz (1–5)

Q1. What Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256lib D) securelib
Answer: B – hashlib is the standard library for hash functions in Python.

Q2. What is the output length of a SHA-256 hash in hexadecimal characters?
A) 32 B) 64 C) 128 D) 256

Quiz (1–5)

Q1. What Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256lib D) securelib
Answer: B – hashlib is the standard library for hash functions in Python.

Q2. What is the output length of a SHA-256 hash in hexadecimal characters?
A) 32 B) 64 C) 128 D) 256
Answer: B – SHA-256 produces 256 bits = 32 bytes = 64 hex characters.

Q3. If you hash "Blockchain" and "blockchain", what will happen?
A) Same hash B) Similar hashes C) Completely different hashes D) Error

Quiz (1–5)

Q1. What Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256lib D) securelib
Answer: B – hashlib is the standard library for hash functions in Python.

Q2. What is the output length of a SHA-256 hash in hexadecimal characters?
A) 32 B) 64 C) 128 D) 256
Answer: B – SHA-256 produces 256 bits = 32 bytes = 64 hex characters.

Q3. If you hash "Blockchain" and "blockchain", what will happen?
A) Same hash B) Similar hashes C) Completely different hashes D) Error
Answer: C – Hash functions are case-sensitive; any input change produces a completely different output.

Q4. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Determinism B) Collision resistance C) Preimage resistance D) Avalanche effect

Quiz (1–5)

Q1. What Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256lib D) securelib
Answer: B – hashlib is the standard library for hash functions in Python.

Q2. What is the output length of a SHA-256 hash in hexadecimal characters?
A) 32 B) 64 C) 128 D) 256
Answer: B – SHA-256 produces 256 bits = 32 bytes = 64 hex characters.

Q3. If you hash "Blockchain" and "blockchain", what will happen?
A) Same hash B) Similar hashes C) Completely different hashes D) Error
Answer: C – Hash functions are case-sensitive; any input change produces a completely different output.

Q4. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Determinism B) Collision resistance C) Preimage resistance D) Avalanche effect
Answer: B – Collision resistance means it's practically impossible to find two different inputs producing the same hash.

Q5. What happens if you add a single space to the end of a string before hashing?
A) Hash unchanged B) Hash slightly modified C) Completely different hash D) Hashing fails

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What Python library is used for computing SHA-256 hashes?
A) cryptolib B) hashlib C) sha256lib D) securelib
Answer: B – hashlib is the standard library for hash functions in Python.

Q2. What is the output length of a SHA-256 hash in hexadecimal characters?
A) 32 B) 64 C) 128 D) 256
Answer: B – SHA-256 produces 256 bits = 32 bytes = 64 hex characters.

Q3. If you hash "Blockchain" and "blockchain", what will happen?
A) Same hash B) Similar hashes C) Completely different hashes D) Error
Answer: C – Hash functions are case-sensitive; any input change produces a completely different output.

Q4. Which property ensures that finding two inputs with the same hash is computationally infeasible?
A) Determinism B) Collision resistance C) Preimage resistance D) Avalanche effect
Answer: B – Collision resistance means it's practically impossible to find two different inputs producing the same hash.

Q5. What happens if you add a single space to the end of a string before hashing?
A) Hash unchanged B) Hash slightly modified C) Completely different hash D) Hashing fails
Answer: C – Even tiny changes (one space) produce completely different hashes due to avalanche effect.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What percentage of bits should change when one input bit is flipped (avalanche effect)?
A) 10% B) 25% C) 50% D) 100%

Quiz (6–10)

Q6. What percentage of bits should change when one input bit is flipped (avalanche effect)?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect means approximately 50% of output bits should change.

Q7. In the lab exercise, changing "dog" to "dof" in the input resulted in what?
A) No change B) Small change C) About 50% bit change D) Complete reversal

Quiz (6–10)

Q6. What percentage of bits should change when one input bit is flipped (avalanche effect)?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect means approximately 50% of output bits should change.

Q7. In the lab exercise, changing "dog" to "dof" in the input resulted in what?
A) No change B) Small change C) About 50% bit change D) Complete reversal
Answer: C – This demonstrates the avalanche effect with approximately 50% of bits differing.

Q8. What is a "nonce" in proof-of-work mining?
A) A timestamp B) A counter incremented to find valid hash C) The block data D) The previous hash

Quiz (6–10)

Q6. What percentage of bits should change when one input bit is flipped (avalanche effect)?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect means approximately 50% of output bits should change.

Q7. In the lab exercise, changing "dog" to "dof" in the input resulted in what?
A) No change B) Small change C) About 50% bit change D) Complete reversal
Answer: C – This demonstrates the avalanche effect with approximately 50% of bits differing.

Q8. What is a "nonce" in proof-of-work mining?
A) A timestamp B) A counter incremented to find valid hash C) The block data D) The previous hash
Answer: B – A nonce (number used once) is incremented until the hash meets the difficulty target.

Q9. If mining difficulty increases from 3 to 4 leading zeros, how much harder does it become?
A) 2x B) 4x C) 10x D) 16x

Quiz (6–10)

Q6. What percentage of bits should change when one input bit is flipped (avalanche effect)?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect means approximately 50% of output bits should change.

Q7. In the lab exercise, changing "dog" to "dof" in the input resulted in what?
A) No change B) Small change C) About 50% bit change D) Complete reversal
Answer: C – This demonstrates the avalanche effect with approximately 50% of bits differing.

Q8. What is a "nonce" in proof-of-work mining?
A) A timestamp B) A counter incremented to find valid hash C) The block data D) The previous hash
Answer: B – A nonce (number used once) is incremented until the hash meets the difficulty target.

Q9. If mining difficulty increases from 3 to 4 leading zeros, how much harder does it become?
A) 2x B) 4x C) 10x D) 16x
Answer: D – Each additional hex zero increases difficulty by 16x (one hex digit has 16 possible values).

Q10. What is the only way to find a valid nonce in proof-of-work?
A) Mathematical formula B) Brute-force trial and error C) Reverse the hash D) Use quantum computing

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What percentage of bits should change when one input bit is flipped (avalanche effect)?
A) 10% B) 25% C) 50% D) 100%
Answer: C – The avalanche effect means approximately 50% of output bits should change.

Q7. In the lab exercise, changing "dog" to "dof" in the input resulted in what?
A) No change B) Small change C) About 50% bit change D) Complete reversal
Answer: C – This demonstrates the avalanche effect with approximately 50% of bits differing.

Q8. What is a "nonce" in proof-of-work mining?
A) A timestamp B) A counter incremented to find valid hash C) The block data D) The previous hash
Answer: B – A nonce (number used once) is incremented until the hash meets the difficulty target.

Q9. If mining difficulty increases from 3 to 4 leading zeros, how much harder does it become?
A) 2x B) 4x C) 10x D) 16x
Answer: D – Each additional hex zero increases difficulty by 16x (one hex digit has 16 possible values).

Q10. What is the only way to find a valid nonce in proof-of-work?
A) Mathematical formula B) Brute-force trial and error C) Reverse the hash D) Use quantum computing
Answer: B – No shortcut exists; miners must try nonces sequentially until finding a valid hash.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the “previous hash” field in a block used for?
A) Encrypt data B) Link blocks into chain C) Store transaction data D) Calculate difficulty

Quiz (11–15)

Q11. What is the "previous hash" field in a block used for?

A) Encrypt data B) Link blocks into chain C) Store transaction data D) Calculate difficulty

Answer: B – Previous hash links the current block to its predecessor, creating the chain structure.

Q12. What value does the genesis block (first block) use for previous_hash?

A) Empty string B) "0" or all zeros C) Random value D) Hash of timestamp

Quiz (11–15)

Q11. What is the "previous hash" field in a block used for?
A) Encrypt data B) Link blocks into chain C) Store transaction data D) Calculate difficulty
Answer: B – Previous hash links the current block to its predecessor, creating the chain structure.

Q12. What value does the genesis block (first block) use for previous_hash?
A) Empty string B) "0" or all zeros C) Random value D) Hash of timestamp
Answer: B – Genesis block has no predecessor, so previous_hash is typically "0" or all zeros.

Q13. If you tamper with block 3 in a 10-block chain, how many blocks are invalidated?
A) Only block 3 B) Blocks 3-10 C) All 10 blocks D) None

Quiz (11–15)

Q11. What is the "previous hash" field in a block used for?
A) Encrypt data B) Link blocks into chain C) Store transaction data D) Calculate difficulty
Answer: B – Previous hash links the current block to its predecessor, creating the chain structure.

Q12. What value does the genesis block (first block) use for previous_hash?
A) Empty string B) "0" or all zeros C) Random value D) Hash of timestamp
Answer: B – Genesis block has no predecessor, so previous_hash is typically "0" or all zeros.

Q13. If you tamper with block 3 in a 10-block chain, how many blocks are invalidated?
A) Only block 3 B) Blocks 3-10 C) All 10 blocks D) None
Answer: B – Tampering invalidates block 3 and all subsequent blocks (4-10) since their previous hashes no longer match.

Q14. What does the chain verification function check for each block?
A) Only the nonce B) Hash validity and previous hash link C) Transaction signatures D) Timestamp order

Quiz (11–15)

Q11. What is the "previous hash" field in a block used for?
A) Encrypt data B) Link blocks into chain C) Store transaction data D) Calculate difficulty
Answer: B – Previous hash links the current block to its predecessor, creating the chain structure.

Q12. What value does the genesis block (first block) use for previous_hash?
A) Empty string B) "0" or all zeros C) Random value D) Hash of timestamp
Answer: B – Genesis block has no predecessor, so previous_hash is typically "0" or all zeros.

Q13. If you tamper with block 3 in a 10-block chain, how many blocks are invalidated?
A) Only block 3 B) Blocks 3-10 C) All 10 blocks D) None
Answer: B – Tampering invalidates block 3 and all subsequent blocks (4-10) since their previous hashes no longer match.

Q14. What does the chain verification function check for each block?
A) Only the nonce B) Hash validity and previous hash link C) Transaction signatures D) Timestamp order
Answer: B – Verification checks that each block's hash is valid and correctly references the previous block's hash.

Q15. Why can't an attacker simply modify one block without detection?
A) Encryption prevents it B) Hash links break C) Network rejects it D) Signatures fail

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the "previous hash" field in a block used for?
A) Encrypt data B) Link blocks into chain C) Store transaction data D) Calculate difficulty
Answer: B – Previous hash links the current block to its predecessor, creating the chain structure.

Q12. What value does the genesis block (first block) use for previous_hash?
A) Empty string B) "0" or all zeros C) Random value D) Hash of timestamp
Answer: B – Genesis block has no predecessor, so previous_hash is typically "0" or all zeros.

Q13. If you tamper with block 3 in a 10-block chain, how many blocks are invalidated?
A) Only block 3 B) Blocks 3-10 C) All 10 blocks D) None
Answer: B – Tampering invalidates block 3 and all subsequent blocks (4-10) since their previous hashes no longer match.

Q14. What does the chain verification function check for each block?
A) Only the nonce B) Hash validity and previous hash link C) Transaction signatures D) Timestamp order
Answer: B – Verification checks that each block's hash is valid and correctly references the previous block's hash.

Q15. Why can't an attacker simply modify one block without detection?
A) Encryption prevents it B) Hash links break C) Network rejects it D) Signatures fail
Answer: B – Modifying block data changes its hash, breaking the link to the next block and invalidating the chain.

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. Which hash algorithm is considered cryptographically broken and should NOT be used?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2

Quiz (16–20)

Q16. Which hash algorithm is considered cryptographically broken and should NOT be used?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 has known collision vulnerabilities and is no longer secure for cryptographic use.

Q17. How does Git version control use hash functions?
A) Encrypt repositories B) Generate commit IDs C) Compress files D) Authenticate users

Quiz (16–20)

Q16. Which hash algorithm is considered cryptographically broken and should NOT be used?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 has known collision vulnerabilities and is no longer secure for cryptographic use.

Q17. How does Git version control use hash functions?
A) Encrypt repositories B) Generate commit IDs C) Compress files D) Authenticate users
Answer: B – Git uses SHA-1 (moving to SHA-256) to generate unique commit identifiers based on content.

Q18. What computational property makes blockchain immutability expensive to break?
A) Encryption strength B) Network size C) Re-mining cost D) Disk space

Quiz (16–20)

Q16. Which hash algorithm is considered cryptographically broken and should NOT be used?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 has known collision vulnerabilities and is no longer secure for cryptographic use.

Q17. How does Git version control use hash functions?
A) Encrypt repositories B) Generate commit IDs C) Compress files D) Authenticate users
Answer: B – Git uses SHA-1 (moving to SHA-256) to generate unique commit identifiers based on content.

Q18. What computational property makes blockchain immutability expensive to break?
A) Encryption strength B) Network size C) Re-mining cost D) Disk space
Answer: C – To tamper with history, attackers must re-mine all subsequent blocks faster than the network.

Q19. In the lab, you computed file hashes. What's the practical use of this?
A) File compression B) Integrity verification C) File encryption D) Access control

Quiz (16–20)

Q16. Which hash algorithm is considered cryptographically broken and should NOT be used?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 has known collision vulnerabilities and is no longer secure for cryptographic use.

Q17. How does Git version control use hash functions?
A) Encrypt repositories B) Generate commit IDs C) Compress files D) Authenticate users
Answer: B – Git uses SHA-1 (moving to SHA-256) to generate unique commit identifiers based on content.

Q18. What computational property makes blockchain immutability expensive to break?
A) Encryption strength B) Network size C) Re-mining cost D) Disk space
Answer: C – To tamper with history, attackers must re-mine all subsequent blocks faster than the network.

Q19. In the lab, you computed file hashes. What's the practical use of this?
A) File compression B) Integrity verification C) File encryption D) Access control
Answer: B – File hashing verifies integrity; if the hash changes, the file was modified or corrupted.

Q20. If a hash function were NOT deterministic, what would fail?
A) Mining would be faster B) Verification would be impossible C) Security would improve D) Nothing

Quiz (16–20)

Q16. Which hash algorithm is considered cryptographically broken and should NOT be used?
A) SHA-256 B) SHA-3 C) MD5 D) BLAKE2
Answer: C – MD5 has known collision vulnerabilities and is no longer secure for cryptographic use.

Q17. How does Git version control use hash functions?
A) Encrypt repositories B) Generate commit IDs C) Compress files D) Authenticate users
Answer: B – Git uses SHA-1 (moving to SHA-256) to generate unique commit identifiers based on content.

Q18. What computational property makes blockchain immutability expensive to break?
A) Encryption strength B) Network size C) Re-mining cost D) Disk space
Answer: C – To tamper with history, attackers must re-mine all subsequent blocks faster than the network.

Q19. In the lab, you computed file hashes. What's the practical use of this?
A) File compression B) Integrity verification C) File encryption D) Access control
Answer: B – File hashing verifies integrity; if the hash changes, the file was modified or corrupted.

Q20. If a hash function were NOT deterministic, what would fail?
A) Mining would be faster B) Verification would be impossible C) Security would improve D) Nothing
Answer: B – Determinism (same input = same output) is essential; otherwise you couldn't verify by recomputing the hash.

(c) Joerg Osterrieder 2025

Lesson 5: Public Key Cryptography

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Explain the fundamental difference between symmetric and asymmetric cryptography
2. Explain how public-private key pairs enable secure communication
3. Describe the Elliptic Curve Digital Signature Algorithm (ECDSA)
4. Generate and verify digital signatures
5. Derive blockchain addresses from public keys
6. Recognize key security best practices for cryptocurrency wallets

Prerequisites: L03 - Cryptographic Hash Functions

The Problem: How can we prove ownership and authorize transactions without revealing secrets?

Part 2/2: Public Key Cryptography (Integration)

The Challenge

How can we prove ownership and authorize transactions on a public blockchain without revealing our secret credentials to everyone watching?

Why It Matters

- Anyone who can sign your transactions controls your funds permanently
- RSA digital signatures introduced in 1977, ECDSA adopted by Bitcoin in 2009 for efficiency

What We Need

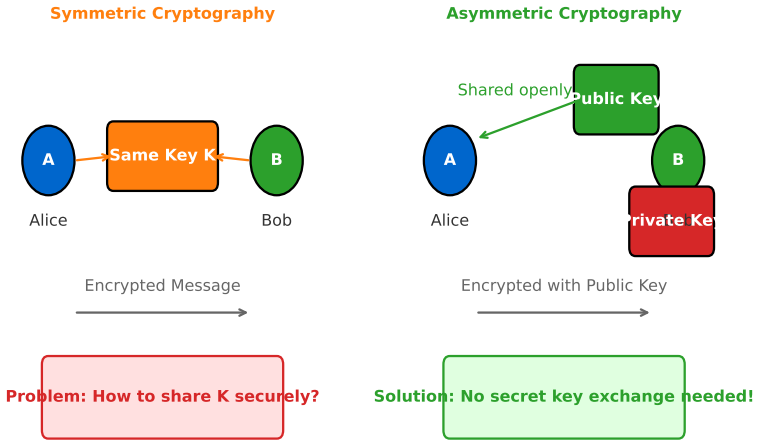
- Trustless verification mechanism
- Unforgeable signatures that anyone can verify without accessing secrets

The Cryptoeconomics Question

Coordinating without trusted intermediaries

Today's lesson: How Public Key Cryptography addresses this challenge

Symmetric vs. Asymmetric Cryptography



Key Insight: Blockchains use asymmetric cryptography because it solves the key distribution problem.

Symmetric vs. Asymmetric: Comparison

Symmetric Cryptography

- Same key for encryption and decryption
- Fast and efficient
- Key distribution problem
- Examples: AES, DES, 3DES

Use Case:

- Encrypting large data volumes
- Disk encryption
- VPN tunnels

Asymmetric Cryptography

- Different keys: public and private
- Slower than symmetric
- No key distribution problem
- Examples: RSA, ECC, ECDSA

Use Case:

- Digital signatures
- Key exchange
- Blockchain transactions

Key Insight: Blockchains rely exclusively on asymmetric cryptography for identity and authorization

(c) Joerg Osterrieder 2025

Public-Private Key Pairs

Core Concept:

- Mathematically related pair of keys
- Public key: freely shared, used to verify signatures
- Private key: kept secret, used to create signatures
- One-way mathematical relationship (hard to derive private from public)

Mathematical Property:
If Alice has key pair (PK_A, SK_A):

- Message encrypted with PK_A can only be decrypted with SK_A
- Signature created with SK_A can only be verified with PK_A

Blockchain Usage:

- Private key = your "password" to control funds
- Public key (or address) = your account identifier
- Losing private key = losing access to funds permanently
- No password reset mechanism exists

RSA vs. Elliptic Curve Cryptography

RSA (Rivest-Shamir-Adleman)

- Based on factoring large primes
- Key sizes: 2048-4096 bits
- Computationally intensive
- Well-established (1977)
- Used in TLS/SSL certificates

Security:

- 2048-bit key = 112-bit security
- 3072-bit key = 128-bit security

Elliptic Curve (ECC)

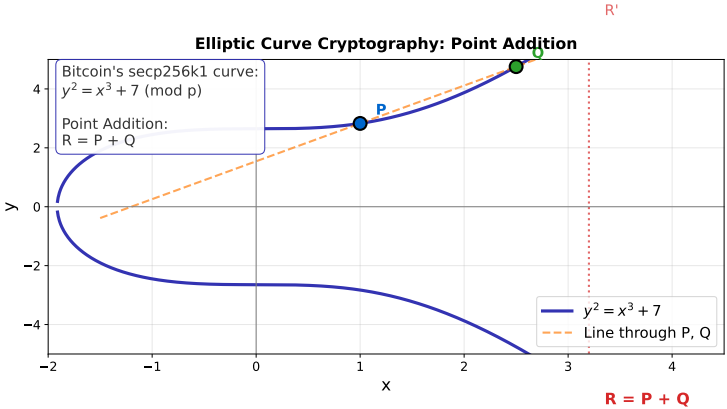
- Based on discrete logarithm problem
- Key sizes: 256 bits
- More efficient computation
- Newer (1985)
- Used in Bitcoin, Ethereum

Security:

- 256-bit key = 128-bit security
- Equivalent to 3072-bit RSA

Why Blockchains Use ECC: Smaller key sizes = less storage, faster verification, mobile-friendly

Elliptic Curve: Point Addition



Key Generation: Choose random k (private key), compute $Q = k \cdot G$ (public key).

Elliptic Curve Mathematics

Elliptic Curve Equation:

$$y^2 = x^3 + ax + b$$

Bitcoin's Curve (secp256k1):

$$y^2 = x^3 + 7 \quad \text{(parameters: } a = 0, b = 7\text{)}$$

Key Mathematical Properties:

- Defined over finite field (modulo large prime)
- Point addition operation creates a group
- Scalar multiplication: $Q = k \cdot G$ (k = private key, G = generator point, Q = public key)
- Easy to compute Q from k, infeasible to compute k from Q

Intuition:

- Private key = random 256-bit number
- Public key = point on elliptic curve (x, y coordinates)
- Trapdoor function ensures one-way relationship

(c) Joerg Osterrieder 2025

The Discrete Logarithm Problem

Security Foundation:

Given:

- Generator point G (known)
- Public key $Q = k \cdot G$ (known)

Find:

- Private key k (unknown)

Computational Complexity:

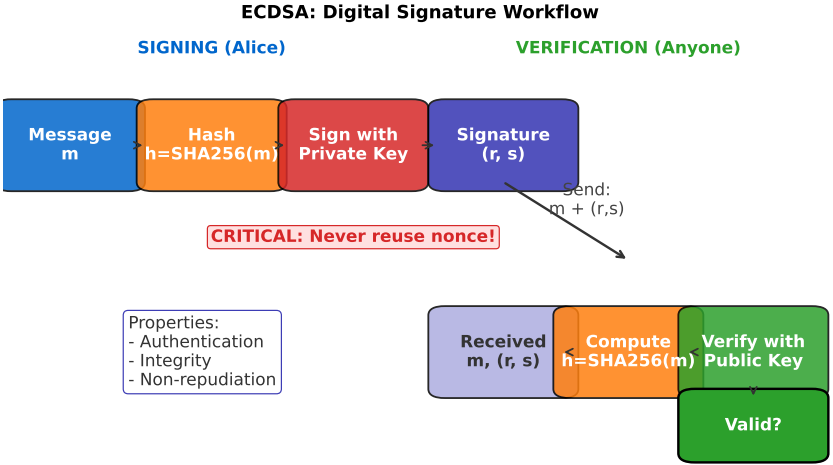
- No known efficient algorithm to solve this
- Best attack: Pollard's rho algorithm
- For 256-bit keys: requires 2^{128} operations (infeasible)
- Quantum computers: Shor's algorithm reduces to polynomial time (future threat)

Practical Implication:

- Cannot derive private key from public key
- Cannot forge signatures without private key
- Blockchain security relies on this hardness assumption

(c) Joerg Osterrieder 2025

ECDSA: Digital Signature Workflow



Properties: Authentication, Integrity, Non-repudiation, Unforgeability.

Digital Signatures: Purpose and Properties

What is a Digital Signature?

- Cryptographic proof that a message was created by the holder of a private key
- Anyone with the public key can verify authenticity
- Provides authentication, integrity, and non-repudiation

Required Properties:

1. **Authentication:** Proves who created the signature
2. **Integrity:** Any modification to message invalidates signature
3. **Non-repudiation:** Signer cannot deny creating signature
4. **Unforgeable:** Impossible to create valid signature without private key

Blockchain Applications:

- Authorize cryptocurrency transactions
- Prove ownership of funds
- Create immutable audit trails
- Smart contract execution authorization

ECDSA: Mathematical Details

Signature Generation:
Given message m and private key k:

1. Compute message hash: $h = \text{SHA-256}(m)$
2. Generate random nonce: n (must be unique per signature)
3. Compute point: $R = n \cdot G$, extract x-coordinate as r
4. Compute: $s = n^{-1}(h + r \cdot k) \mod p$
5. Signature is pair: (r, s)

Signature Verification:
Given message m, signature (r, s), and public key Q:

1. Compute message hash: $h = \text{SHA-256}(m)$
2. Compute: $u_1 = h \cdot s^{-1} \mod p$, $u_2 = r \cdot s^{-1} \mod p$
3. Compute point: $R' = u_1 \cdot G + u_2 \cdot Q$
4. Extract x-coordinate r'
5. Verify: $r' = r$ (signature valid if true)

Critical Security: Nonce Reuse Vulnerability

The Danger of Reusing Nonces:

If the same nonce n is used to sign two different messages m_1 and m_2:

- Attacker obtains signatures: (r, s_1) and (r, s_2)
- Notice that r is the same (same nonce used)
- Can compute: $s_1 - s_2 = n^{-1}(h_1 - h_2) \mod p$
- Solve for n, then solve for private key k

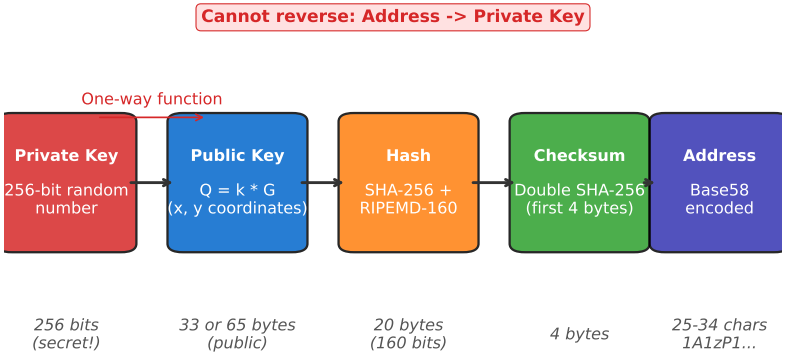
Real-World Incident: Sony PlayStation 3 (2010)

- Sony used ECDSA to sign PS3 firmware
- Used the same nonce for all signatures
- Hackers recovered Sony's private key
- Enabled homebrew software and piracy

Best Practice: Use deterministic nonce generation (RFC 6979) - nonce derived from message hash and private key

From Private Key to Blockchain Address

Bitcoin Address Derivation: From Private Key to Address



Security: One-way functions ensure addresses cannot be reversed to private keys.

Bitcoin Address Derivation Details

Step-by-Step Process:

1. Generate random 256-bit private key k
2. Compute public key: $Q = k \cdot G$ (33 bytes compressed or 65 bytes uncompressed)
3. Hash public key: $h_1 = \text{SHA-256}(Q)$
4. Hash again: $h_2 = \text{RIPEMD-160}(h_1)$ (20 bytes)
5. Add version byte: $0x00$ for mainnet (21 bytes)
6. Compute checksum: first 4 bytes of SHA-256(SHA-256(version + h_2))
7. Concatenate: version + h_2 + checksum (25 bytes)
8. Encode in Base58: produces address like "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa"

Why Multiple Hash Functions?

- SHA-256: widely trusted, fast
- RIPEMD-160: reduces address size (160 bits instead of 256 bits)
- Double hashing: additional security layer

Ethereum Address Derivation

Simplified Process:

1. Generate random 256-bit private key k
2. Compute public key: $Q = k \cdot G$ (uncompressed, 64 bytes excluding prefix)
3. Hash public key: $h = \text{Keccak-256}(Q)$ (32 bytes)
4. Take last 20 bytes of hash
5. Add "0x" prefix
6. Result: address like "0x742d35Cc6634C0532925a3b844Bc9e7595f0bEb"

Key Differences from Bitcoin:

- Uses Keccak-256 instead of SHA-256 + RIPEMD-160
- No checksum in base address (EIP-55 adds mixed-case checksum)
- Hexadecimal encoding instead of Base58
- Always 20 bytes (40 hex characters)

Public Key Compression

Uncompressed (65 bytes):

- Format: $04 \| x \| y$
- Prefix 0x04 + 32B x + 32B y

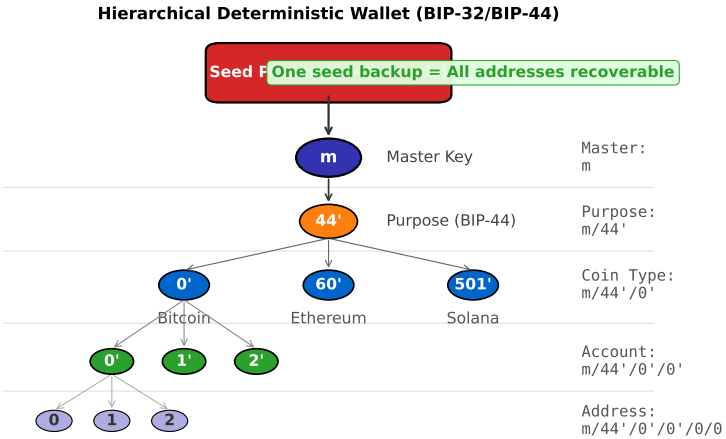
Compressed (33 bytes):

- Format: $02/03 \| x$
- Prefix indicates y parity
- y derived from curve equation

Why Compression Matters:

- 50% storage reduction
- Faster propagation, lower fees
- Bitcoin: both formats valid
- Ethereum: uncompressed only

Hierarchical Deterministic Wallets (BIP-32)



Advantage: Backup once (seed phrase), recover all addresses forever.

HD Wallet Details

Problem with Random Key Generation:

- Need to back up every new private key separately
- Managing hundreds of keys becomes impractical
- Risk of losing individual keys

HD Wallet Solution:

- Generate all keys from single master seed (usually 12-24 words)
- Deterministic derivation: same seed always produces same keys
- Hierarchical structure: master key -¿ account keys -¿ address keys
- Only need to back up seed phrase once

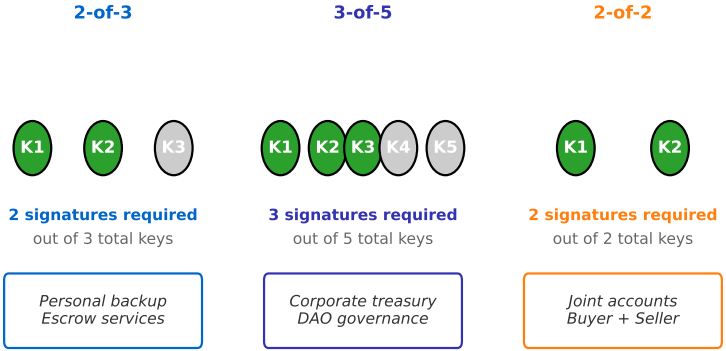
Derivation Path Example:

- Bitcoin: `m/44'/0'/0'/0/0`
- Ethereum: `m/44'/60'/0'/0/0`
- Each level represents: purpose / coin type / account / change / index

BIP-39 Mnemonic: Seed phrase = 12-24 English words encoding 128-256 bits of entropy

Multi-Signature Wallets

Multi-Signature (M-of-N) Wallet Configurations



Green = Required for signing | Gray = Spare/backup key

Security: No single point of failure; attacker must compromise multiple keys.

(c) Joerg Osterrieder 2025

Multi-Signature Use Cases

Concept:

- Require multiple signatures to authorize a transaction
- Common schemes: 2-of-3, 3-of-5, etc.
- M-of-N threshold: need M signatures out of N total keys

Use Cases:

- Corporate treasuries (require CEO + CFO approval)
- Estate planning (family members hold keys)
- Escrow services (buyer + seller + mediator)
- Enhanced security (attacker must compromise multiple keys)

Bitcoin Implementation:

- P2SH (Pay-to-Script-Hash) addresses start with "3"
- Redeem script specifies signature requirements

Ethereum Implementation:

- Smart contract-based (e.g., Gnosis Safe)
- More flexible logic (time delays, spending limits)

(c) Joerg Osterrieder 2025

Key Security Best Practices

Private Key Protection:

- Never share keys or seed phrases
- Use hardware wallets for large amounts
- Multiple secure backup locations

Common Threats:

- Phishing (fake wallet sites)
- Clipboard malware, keyloggers
- SIM swapping, physical theft

Defense Strategies:

- Multi-sig wallets (M-of-N keys)
- Air-gapped signing (offline)
- Test small amounts first
- Strong passwords + encryption

Hardware wallets (Ledger, Trezor) provide best protection for significant holdings.

Problem Solved? Public Key Cryptography

The Original Problem

How can we prove ownership and authorize transactions without revealing secrets?

How Public Key Cryptography Solves It

- ECDSA on secp256k1 curve provides 128-bit security with only 256-bit keys
- HD wallets (BIP-32/44) enable deterministic key derivation from single seed phrase
- Multi-signature schemes distribute control across multiple private keys

Remaining Limitations

- Private key security remains user's sole responsibility – no password reset mechanism
- Nonce reuse in ECDSA can leak private key (Sony PS3 2010 incident)

Open Questions

- Can threshold signatures and multi-party computation provide institutional-grade custody without single points of failure?
- Risk: Sybil attacks, eclipse attacks

Public Key Cryptography partially solves "proving ownership without revealing secrets" but introduces new trade-offs around key management and quantum resistance

Key Takeaways

- Public key cryptography solves the key distribution problem
- Private keys must remain absolutely secret
- ECDSA provides efficient digital signatures for blockchains
- Nonce reuse is a critical vulnerability
- Bitcoin and Ethereum use different address derivation schemes
- HD wallets enable convenient key management from a single seed
- Multi-signature wallets add an extra security layer

Core Principle

"Not your keys, not your coins."
If you do not control the private keys to your cryptocurrency addresses, you do not truly own the funds. Exchanges and custodians can be hacked, frozen, or shut down.

Discussion Questions

1. Why do blockchains use elliptic curve cryptography instead of RSA?
2. What would happen if two users randomly generated the same private key?
3. How does address derivation protect privacy compared to reusing the same address?
4. Why is the discrete logarithm problem crucial for blockchain security?
5. What are the trade-offs between convenience and security when storing private keys?
6. How would quantum computing impact ECDSA-based blockchains?

Next Lesson Preview: L06 Bitcoin Protocol Deep Dive

Topics to be covered:

- Unspent Transaction Output (UTXO) model
- Bitcoin transaction structure in detail
- Transaction inputs and outputs
- Bitcoin Script language
- Transaction verification process
- Common transaction types (P2PKH, P2SH, SegWit)
- Transaction lifecycle from creation to confirmation

Preparation:

- Review how digital signatures work
- Explore a Bitcoin block explorer (e.g., blockchain.com)
- Observe transaction structure in real blocks

Thank you

Questions?

See you in Lesson 6: Bitcoin Protocol Deep Dive

Quiz Questions (1/4)

Q1. What is the primary advantage of asymmetric cryptography over symmetric cryptography for blockchain applications?
A) Faster encryption B) Smaller key sizes C) No key distribution problem D) Lower computational cost
Answer: C – Asymmetric cryptography eliminates the need to securely share keys between parties, making it ideal for decentralized networks.

Q2. In elliptic curve cryptography, what relationship exists between the private key and public key?
A) They are identical B) Public key = hash of private key C) Public key = private key × generator point D) They are randomly generated
Answer: C – The public key Q is computed as $Q = k \cdot G$, where k is the private key and G is the generator point.

Q3. Which elliptic curve does Bitcoin use for ECDSA?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with the equation $y^2 = x^3 + 7$.

Q4. What is the approximate security level of a 256-bit elliptic curve key?
A) 64-bit security B) 128-bit security C) 256-bit security D) 512-bit security
Answer: B – A 256-bit ECC key provides approximately 128-bit security, equivalent to a 3072-bit RSA key.

Q5. What cryptographic problem ensures that deriving a private key from a public key is computationally infeasible?
A) Factorization problem B) Discrete logarithm problem C) Traveling salesman problem D) Halting problem
Answer: B – The elliptic curve discrete logarithm problem makes it infeasible to find k given $Q = k \cdot G$.

Quiz Questions (2/4)

Q6. What four properties must a digital signature scheme provide?
A) Speed, size, cost, privacy B) Authentication, integrity, non-repudiation, unforgeable C) Encryption, decryption, hashing, compression D) Storage, transmission, verification, deletion
Answer: B – Digital signatures must provide authentication, integrity, non-repudiation, and be unforgeable.

Q7. In ECDSA signature generation, what must be unique for every signature to prevent private key leakage?
A) The message hash B) The private key C) The nonce D) The public key
Answer: C – Reusing a nonce allows attackers to recover the private key from two different signatures.

Q8. What real-world incident demonstrated the danger of nonce reuse in ECDSA?
A) Mt. Gox hack B) Sony PlayStation 3 breach (2010) C) DAO hack D) Parity wallet freeze
Answer: B – Sony used the same nonce for all PS3 firmware signatures, allowing hackers to recover the private key.

Q9. In Bitcoin address derivation, why are both SHA-256 and RIPEMD-160 hash functions used?
A) Redundancy for security B) SHA-256 for speed, RIPEMD-160 to reduce address size C) Legal compliance D) Compatibility with older systems
Answer: B – SHA-256 provides security and speed, while RIPEMD-160 reduces the address from 256 bits to 160 bits.

Q10. How long is an Ethereum address (excluding the "0x" prefix)?
A) 20 characters B) 32 characters C) 40 characters D) 64 characters
Answer: C – Ethereum addresses are 20 bytes represented as 40 hexadecimal characters.

Quiz Questions (3/4)

Q11. What is the main difference between compressed and uncompressed public keys?
A) Compressed keys are encrypted B) Compressed keys store only x-coordinate and sign of y C) Compressed keys use different curves D) Compressed keys are hashed differently
Answer: B – Compressed keys (33 bytes) store the x-coordinate and a prefix (02/03) indicating y's parity; uncompressed keys (65 bytes) store both x and y.

Q12. What is the primary benefit of Hierarchical Deterministic (HD) wallets?
A) Faster transactions B) Lower fees C) Single backup recovers all keys D) Stronger encryption
Answer: C – HD wallets derive all keys from a single master seed, so backing up the seed phrase once recovers all addresses.

Q13. What is a BIP-39 mnemonic seed phrase typically composed of?
A) Random letters and numbers B) 12-24 English words C) Binary data D) Hexadecimal string
Answer: B – BIP-39 seed phrases use 12-24 English words encoding 128-256 bits of entropy.

Q14. In a 2-of-3 multi-signature wallet, how many signatures are required to authorize a transaction?
A) 1 B) 2 C) 3 D) All signatures must be present
Answer: B – A 2-of-3 multisig requires any 2 out of 3 possible signatures to authorize a transaction.

Q15. What does the Bitcoin derivation path "m/44'/0'/0'/0/0" represent?
A) Account version B) Hierarchical levels: purpose/coin/account/change/index C) Encryption parameters D) Network identifier
Answer: B – The path represents purpose (44' for BIP-44), coin type (0' for Bitcoin), account (0'), change (0), and address index (0).

Quiz Questions (4/4)

Q16. What is the primary threat mitigated by using a hardware wallet?
A) Network congestion B) High transaction fees C) Malware on internet-connected devices D) Quantum computing attacks
Answer: C – Hardware wallets keep private keys offline, protecting them from malware and remote attacks.

Q17. Which hashing algorithm does Ethereum use for address derivation?
A) SHA-256 B) RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: C – Ethereum uses Keccak-256 to hash the public key and derives the address from the last 20 bytes.

Q18. What is the best practice for preventing nonce reuse in ECDSA signatures?
A) Use random nonces B) Use sequential nonces C) Use deterministic nonce generation (RFC 6979) D) Reuse nonces from previous signatures
Answer: C – RFC 6979 deterministically derives nonces from the message hash and private key, preventing reuse while maintaining security.

Q19. What does the principle "Not your keys, not your coins" mean?
A) Keys must be physically printed B) Only own cryptocurrency if you control the private keys C) Keys should be shared with trusted parties D) Public keys determine ownership
Answer: B – If you don't control the private keys (e.g., funds on an exchange), you don't truly own the cryptocurrency.

Q20. How does quantum computing threaten ECDSA-based blockchains?
A) Quantum computers can mine faster B) Shor's algorithm can solve discrete logarithm in polynomial time C) Quantum computers increase transaction fees D) Quantum computers corrupt blockchain data
Answer: B – Shor's algorithm can efficiently solve the discrete logarithm problem on quantum computers, potentially allowing derivation of private keys from public keys.

Lesson 5: Public Key Cryptography

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Explain the fundamental difference between symmetric and asymmetric cryptography
2. Explain how public-private key pairs enable secure communication
3. Describe the Elliptic Curve Digital Signature Algorithm (ECDSA)
4. Generate and verify digital signatures
5. Derive blockchain addresses from public keys
6. Recognize key security best practices for cryptocurrency wallets

Prerequisites: L03 - Cryptographic Hash Functions
Building on L04: Lab: Hash Experiments

The Lock and Key Metaphor

[COMIC: A mailbox with a slot anyone can drop letters into (public key), but only the owner has the key to open it (private key). A thief tries to fish letters out but fails. Caption: "Everyone can send, only you can receive."]

[Comic placeholder – to be illustrated]

- Public keys are like open mailbox slots – anyone can encrypt messages to you
- Private keys are like your mailbox key – only you can decrypt and sign

The Problem: How can we prove ownership and authorize transactions without revealing secrets?

Part 2/2: Public Key Cryptography (Integration)

The Challenge

How can we prove ownership and authorize transactions on a public blockchain without revealing our secret credentials to everyone watching?

Why It Matters

- Anyone who can sign your transactions controls your funds permanently
- RSA digital signatures introduced in 1977, ECDSA adopted by Bitcoin in 2009 for efficiency

What We Need

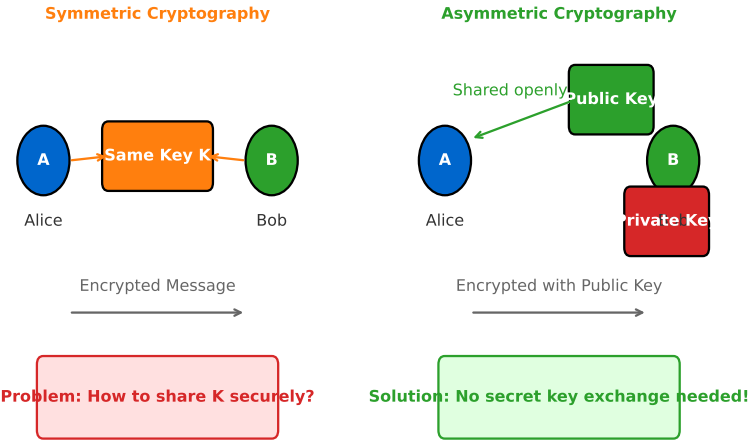
- Trustless verification mechanism
- Unforgeable signatures that anyone can verify without accessing secrets

The Cryptoeconomics Question

Coordinating without trusted intermediaries

Today's lesson: How Public Key Cryptography addresses this challenge

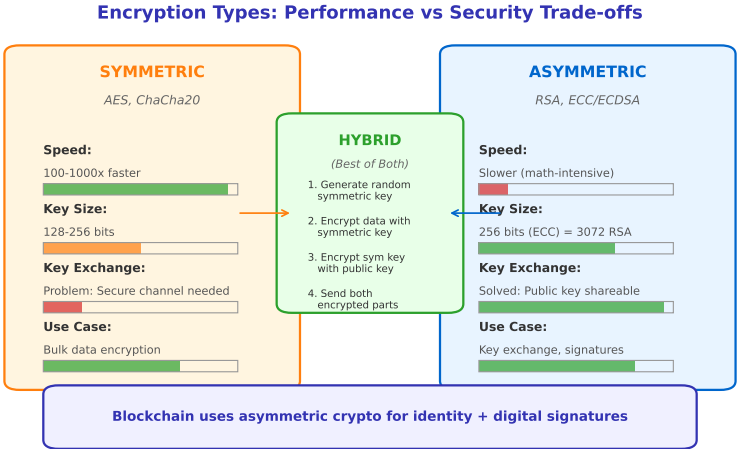
How Does Symmetric Differ from Asymmetric Cryptography



Key Insight: Blockchains use asymmetric cryptography because it solves the key distribution problem.

Asymmetric cryptography solves the secret-sharing problem: public keys can be distributed openly while private keys remain secret

How Do Encryption Types Compare in Performance?



Key Insight: Symmetric is 100-1000x faster but requires secure key exchange; asymmetric solves key exchange but is slower.

Hybrid encryption combines both: asymmetric for key exchange, symmetric for bulk data encryption

What Are the Key Differences Between Symmetric and Asymmetric Cryptography?

Symmetric Cryptography

- Same key for encryption and decryption
- Fast and efficient
- Key distribution problem
- Examples: AES, DES, 3DES

Use Case:

- Encrypting large data volumes
- Disk encryption
- VPN tunnels

Asymmetric Cryptography

- Different keys: public and private
- Slower than symmetric
- No key distribution problem
- Examples: RSA, ECC, ECDSA

Use Case:

- Digital signatures
- Key exchange
- Blockchain transactions

Key Insight: Blockchains rely exclusively on asymmetric cryptography for identity and authorization

(c) Joerg Osterrieder 2025

How Do Public-Private Key Pairs Work?

Core Concept:

- Mathematically related pair of keys
- Public key: freely shared, verifies signatures
- Private key: kept secret, creates signatures
- One-way relationship (hard to reverse)

Mathematical Property:
If Alice has key pair (PK_A, SK_A):

- Encrypted with $PK_A \rightarrow$ only SK_A decrypts
- Signed with $SK_A \rightarrow$ only PK_A verifies

Blockchain Usage:

- Private key = your "password" to control funds
- Public key (or address) = account identifier
- Losing private key = losing access permanently
- No password reset mechanism exists

Key pairs enable trustless ownership: only the private key holder can authorize transactions

How Does ECC Compare to RSA?

RSA (Rivest-Shamir-Adleman)

- Based on factoring large primes
- Key sizes: 2048-4096 bits
- Computationally intensive
- Well-established (1977)
- Used in TLS/SSL certificates

Security:

- 2048-bit key = 112-bit security
- 3072-bit key = 128-bit security

Elliptic Curve (ECC)

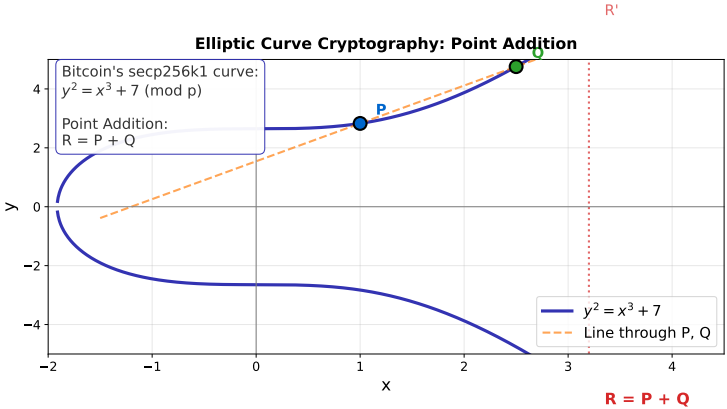
- Based on discrete logarithm problem (finding k given $Q = k \cdot G$ – like finding the exponent in $b^k = x$)
- Key sizes: 256 bits
- More efficient computation
- Newer (1985)
- Used in Bitcoin, Ethereum

Security:

- 256-bit key = 128-bit security
- Equivalent to 3072-bit RSA

Why Blockchains Use ECC: Smaller key sizes = less storage, faster verification, mobile-friendly

How Does Elliptic Curve Point Addition Work?



Key Generation: Choose random k (private key), compute $Q = k \cdot G$ (public key).

Scalar Multiplication: $2G = G + G$; $3G = G + G + G$; kG = add G to itself k times.

Scalar multiplication is fast (double-and-add); reversing it (finding k from kG) is infeasible

What is the Mathematics Behind Elliptic Curves?

Elliptic Curve Equation:

$$y^2 = x^3 + ax + b$$

Bitcoin's Curve (secp256k1):

$$y^2 = x^3 + 7 \quad \text{(parameters: } a = 0, b = 7\text{)}$$

Key Mathematical Properties:

- Defined over finite field (modulo large prime)
- Point addition operation creates a group
- Scalar multiplication: $Q = k \cdot G$ (k = private key, G = generator point, Q = public key)
- Easy to compute Q from k, infeasible to compute k from Q

Intuition:

- Private key = random 256-bit number
- Public key = point on elliptic curve (x, y coordinates)
- Trapdoor function ensures one-way relationship

The discrete logarithm problem makes it computationally infeasible to reverse-engineer private keys from public keys, enabling trustless verification

(c) Joerg Osterrieder 2025

What is the Discrete Logarithm Problem?

Security Foundation:

Given:

- Generator point G (known)
- Public key $Q = k \cdot G$ (known)

Find:

- Private key k (unknown)

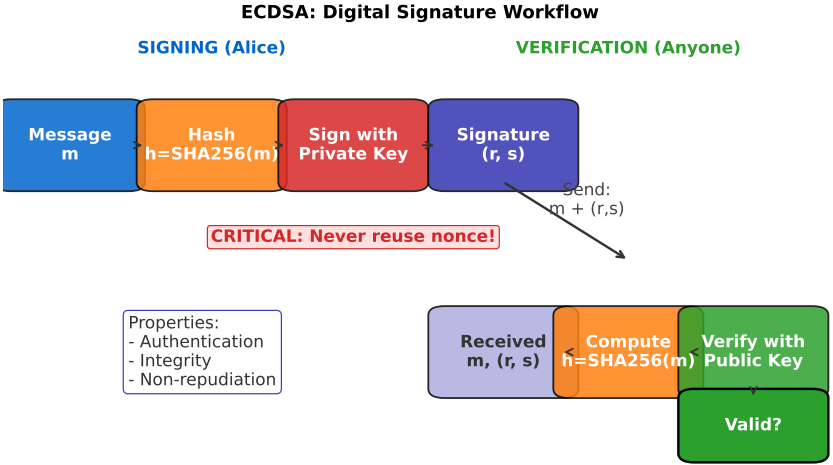
Computational Complexity:

- No known efficient algorithm to solve this
- Best attack: Pollard's rho algorithm
- For 256-bit keys: requires 2^{128} operations (infeasible)
- Quantum computers: Shor's algorithm reduces to polynomial time (future threat)

Practical Implication:

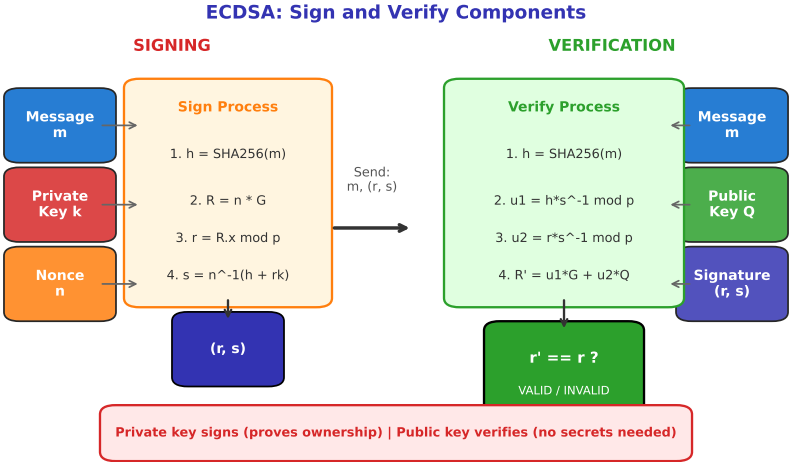
- Cannot derive private key from public key
- Cannot forge signatures without private key
- Blockchain security relies on this hardness assumption

How Does the ECDSA Digital Signature Workflow Work?



Properties: Authentication, Integrity, Non-repudiation, Unforgeability.

What Are the Components of ECDSA Sign and Verify?



Mathematical Foundation: Signing uses private key k and nonce n; verification uses public key Q without needing any secrets.

The verification equation $R' = u_1 \cdot G + u_2 \cdot Q$ proves the signer knew k without revealing it

What Are Digital Signatures and What Do They Provide?

What is a Digital Signature?

- Cryptographic proof created by private key holder
- Anyone with public key can verify authenticity
- Provides authentication, integrity, non-repudiation

Required Properties:

1. **Authentication:** Proves who signed
2. **Integrity:** Modification invalidates signature
3. **Non-repudiation:** Cannot deny signing
4. **Unforgeable:** Needs private key

Blockchain Applications:

- Authorize cryptocurrency transactions
- Prove ownership of funds
- Create immutable audit trails
- Smart contract execution authorization

Digital signatures are the cryptographic foundation of all blockchain transaction authorization

What is Modular Arithmetic?

Definition:
Modular arithmetic is "clock arithmetic" – numbers wrap around after reaching a limit.

Key Concepts:

- **Modulo (mod):** Remainder after division. Example: $17 \mod 5 = 2$ (since $17 = 3 \times 5 + 2$)
- **Modular inverse:** The number a^{-1} such that $a \cdot a^{-1} \equiv 1 \mod p$
  - Example: $3^{-1} \mod 7 = 5$ because $3 \times 5 = 15 \equiv 1 \mod 7$

Why It Matters for ECDSA:

- All elliptic curve operations use modular arithmetic
- Modular inverses are essential for signature generation and verification
- The large prime p ensures computations stay within a finite range

---

Modular arithmetic keeps calculations bounded – essential for digital cryptography

What Are the Mathematical Details of ECDSA?

Signature Generation:
Given message m and private key k:

1. Compute message hash: $h = \text{SHA-256}(m)$
2. Generate random nonce: n (must be unique per signature)
3. Compute point: $R = n \cdot G$, extract x-coordinate as r
4. Compute: $s = n^{-1}(h + r \cdot k) \mod p$
5. Signature is pair: (r, s)

Signature Verification:
Given message m, signature (r, s), and public key Q:

1. Compute message hash: $h = \text{SHA-256}(m)$
2. Compute: $u_1 = h \cdot s^{-1} \mod p$, $u_2 = r \cdot s^{-1} \mod p$
3. Compute point: $R' = u_1 \cdot G + u_2 \cdot Q$
4. Extract x-coordinate r'
5. Verify: $r' = r$ (signature valid if true)

Problem Check-In: Cryptographic Foundations

Recall Our Problem

How do we prove knowledge without revealing secrets?

What We've Learned So Far

- Asymmetric cryptography eliminates the key distribution problem
- ECDSA provides efficient signatures with 256-bit keys
- Public keys enable verification without revealing private secrets

Still to Address

- Address derivation and hierarchical deterministic wallets
- How do we manage private keys securely at scale?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we prove knowledge without..."?

Why Is Nonce Reuse a Critical Security Vulnerability?

The Danger of Reusing Nonces:
If the same nonce n signs two messages m_1, m_2:

- Attacker obtains (r, s_1) and (r, s_2)
- Same r reveals nonce reuse
- Compute: $s_1 - s_2 = n^{-1}(h_1 - h_2) \mod p$
- Solve for n, then derive private key k

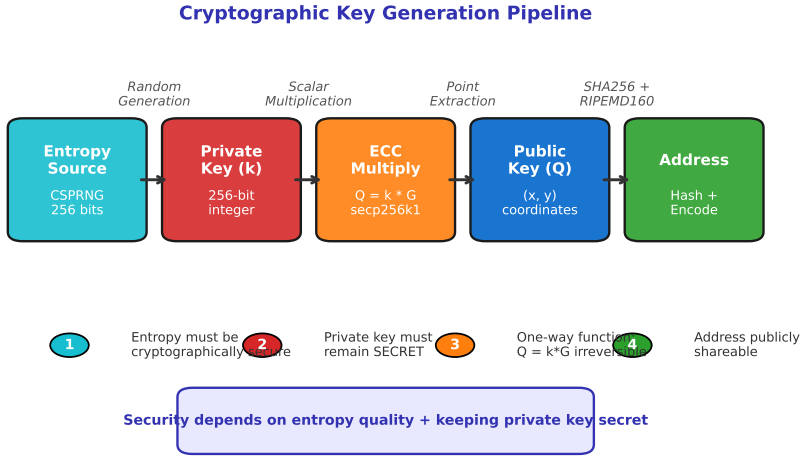
Best Practice: Deterministic nonce generation (RFC 6979)

Real-World: Sony PS3 (2010)

- Sony signed PS3 firmware with ECDSA
- Used the same nonce for all signatures
- Hackers recovered Sony's private key
- Enabled homebrew software and piracy

Nonce reuse breaks the security proof: proper implementation is critical to maintaining the "secrets remain secret" guarantee

How Does the Key Generation Pipeline Work?



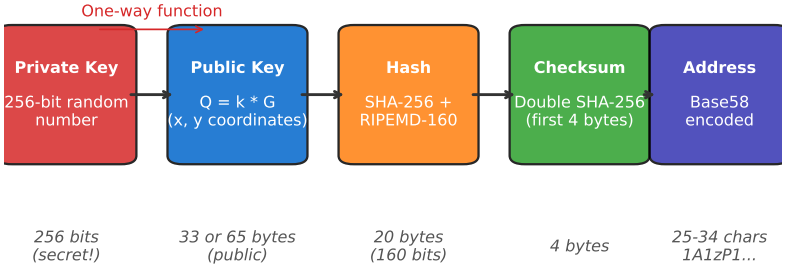
Critical Steps: Entropy quality determines security; private key must remain secret throughout.

CSPRNG = Cryptographically Secure Pseudo-Random Number Generator; secp256k1 = Bitcoin's elliptic curve

How Do We Derive a Blockchain Address from a Private Key?

Bitcoin Address Derivation: From Private Key to Address

Cannot reverse: Address -> Private Key



Security: One-way functions ensure addresses cannot be reversed to private keys.

What Are the Details of Bitcoin Address Derivation?

Step-by-Step Process:

1. Generate random 256-bit private key k
2. Compute public key: $Q = k \cdot G$ (33 bytes compressed or 65 bytes uncompressed)
3. Hash public key: $h_1 = \text{SHA-256}(Q)$
4. Hash again: $h_2 = \text{RIPEMD-160}(h_1)$ (20 bytes)
5. Add version byte: $0x00$ for mainnet (21 bytes)
6. Compute checksum: first 4 bytes of SHA-256(SHA-256(version + h_2))
7. Concatenate: version + h_2 + checksum (25 bytes)
8. Encode in Base58: produces address like "1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa"

Why Multiple Hash Functions?

- SHA-256: widely trusted, fast
- RIPEMD-160: reduces address size (160 bits instead of 256 bits)
- Double hashing: additional security layer

How Does Ethereum Address Derivation Work?

Simplified Process:

1. Generate random 256-bit private key k
2. Compute public key: $Q = k \cdot G$ (uncompressed, 64 bytes excluding prefix)
3. Hash public key: $h = \text{Keccak-256}(Q)$ (32 bytes)
4. Take last 20 bytes of hash
5. Add "0x" prefix
6. Result: address like "0x742d35Cc6634C0532925a3b844Bc9e7595f0bEbF"

Key Differences from Bitcoin:

- Uses Keccak-256 instead of SHA-256 + RIPEMD-160
- No checksum in base address (EIP-55 adds mixed-case checksum)
- Hexadecimal encoding instead of Base58
- Always 20 bytes (40 hex characters)

How Does Public Key Compression Work?

Uncompressed (65 bytes):

- Format: $04 \| x \| y$
- Prefix 0x04 + 32B x + 32B y

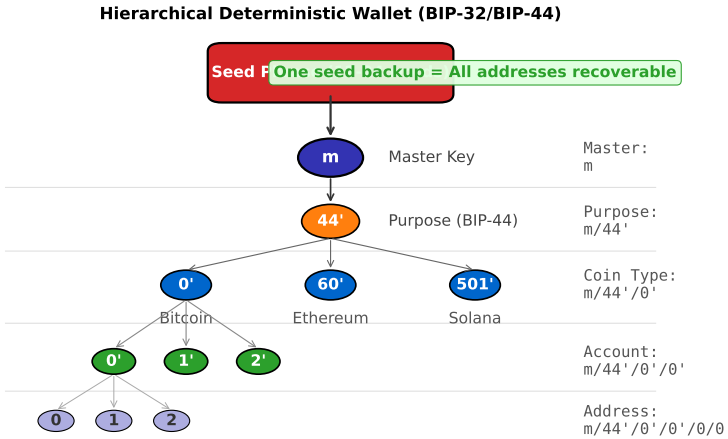
Compressed (33 bytes):

- Format: $02/03 \| x$
- Prefix indicates y parity
- y derived from curve equation

Why Compression Matters:

- 50% storage reduction
- Faster propagation, lower fees
- Bitcoin: both formats valid
- Ethereum: uncompressed only

Hierarchical Deterministic Wallets (BIP-32)



Advantage: Backup once (seed phrase), recover all addresses forever.

HD wallets enable secure key management at scale: single seed phrase protects unlimited addresses without revealing any private keys

How Do HD Wallets Work?

Problem with Random Keys:

- Back up every new private key separately
- Managing hundreds of keys is impractical
- Risk of losing individual keys

HD Wallet Solution:

- All keys from single master seed (12-24 words)
- Deterministic: same seed $\rightarrow$ same keys
- Hierarchical: master $\rightarrow$ account $\rightarrow$ address
- Only back up seed phrase once

Derivation Path Example:

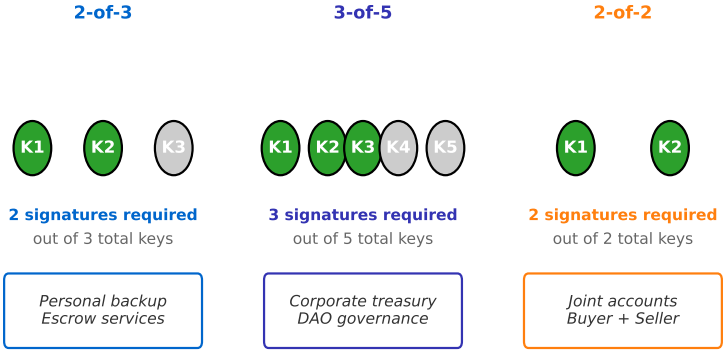
- Bitcoin: `m/44'/0'/0'/0/0`
- Ethereum: `m/44'/60'/0'/0/0`
- Levels: purpose / coin / account / change / index

BIP-39 Mnemonic:
Seed phrase = 12-24 English words encoding 128-256 bits of entropy

HD wallets solve the key management problem: one seed phrase protects unlimited addresses

Multi-Signature Wallets

Multi-Signature (M-of-N) Wallet Configurations



Green = Required for signing | Gray = Spare/backup key

Security: No single point of failure; attacker must compromise multiple keys.

(c) Joerg Osterrieder 2025

What Are the Use Cases for Multi-Signature Wallets?

Concept:

- Multiple signatures to authorize a transaction
- Common: 2-of-3, 3-of-5 threshold schemes
- M-of-N: need M signatures out of N keys

Use Cases:

- Corporate treasuries (CEO + CFO)
- Estate planning (family members)
- Escrow (buyer + seller + mediator)
- Enhanced security (multiple keys)

Bitcoin Implementation:

- P2SH addresses start with "3"
- Redeem script specifies requirements

Ethereum Implementation:

- Smart contract-based (Gnosis Safe)
- Flexible: time delays, spending limits

Multi-sig eliminates single points of failure in key management

(c) Joerg Osterrieder 2025

What Are the Key Security Best Practices?

Private Key Protection:

- Never share keys or seed phrases
- Use hardware wallets for large amounts
- Multiple secure backup locations

Common Threats:

- Phishing (fake wallet sites)
- Clipboard malware, keyloggers
- SIM swapping, physical theft

Defense Strategies:

- Multi-sig wallets (M-of-N keys)
- Air-gapped signing (offline)
- Test small amounts first
- Strong passwords + encryption

Hardware wallets (Ledger, Trezor) provide best protection for significant holdings.

Problem Solved? Public Key Cryptography

The Original Problem

How can we prove ownership and authorize transactions without revealing secrets?

How Public Key Cryptography Solves It

- ECDSA on secp256k1 curve provides 128-bit security with only 256-bit keys
- HD wallets (BIP-32/44) enable deterministic key derivation from single seed phrase
- Multi-signature schemes distribute control across multiple private keys

Remaining Limitations

- Private key security remains user's sole responsibility – no password reset mechanism
- Nonce reuse in ECDSA can leak private key (Sony PS3 2010 incident)

Open Questions

- Can threshold signatures and multi-party computation provide institutional-grade custody without single points of failure?
- Risk: Sybil attacks, eclipse attacks

Public Key Cryptography partially solves "proving ownership without revealing secrets" but introduces new trade-offs around key management and quantum resistance

Key Backup Horror Stories

[COMIC: A person crying over a crashed hard drive, with ghost coins floating away. A wise elder holds a steel plate with seed words: "Always backup your keys in multiple locations." Caption: "$200M lost to forgotten passwords – don't be a statistic."]

[Comic placeholder – to be illustrated]

- Millions in cryptocurrency are permanently lost due to poor key management
- "Not your keys, not your coins" – but also "lost keys, lost coins forever"

(c) Joerg Osterrieder 2025

The Economics of Cryptographic Foundations

Incentive Structure

- **Core Problem:** Coordinating without trusted intermediaries
- **Why act honestly?** Participants verify rather than trust
- **Value Flow:** Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Cryptographic Foundations

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Cryptographic Foundations

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Key Takeaways

Cryptographic Foundations:

- Public key crypto solves key distribution
- Private keys must remain absolutely secret
- ECDSA provides efficient digital signatures
- Nonce reuse is a critical vulnerability

Practical Applications:

- BTC and ETH use different address derivation
- HD wallets: single seed manages all keys
- Multi-sig adds extra security layer

Core Principle

"Not your keys, not your coins." If you do not control the private keys, you do not truly own the funds.

Next Lesson: L06 – Bitcoin Protocol

Discussion Questions

1. Why do blockchains use elliptic curve cryptography instead of RSA?
2. What would happen if two users randomly generated the same private key?
3. How does address derivation protect privacy compared to reusing the same address?
4. Why is the discrete logarithm problem crucial for blockchain security?
5. What are the trade-offs between convenience and security when storing private keys?
6. How would quantum computing impact ECDSA-based blockchains?

Next Lesson Preview: L06 Bitcoin Protocol Deep Dive

Topics to be covered:

- Unspent Transaction Output (UTXO) model
- Bitcoin transaction structure in detail
- Transaction inputs and outputs
- Bitcoin Script language
- Transaction verification process
- Common transaction types (P2PKH, P2SH, SegWit)
- Transaction lifecycle from creation to confirmation

Preparation:

- Review how digital signatures work
- Explore a Bitcoin block explorer (e.g., blockchain.com)
- Observe transaction structure in real blocks

Thank you

Questions?

See you in Lesson 6: Bitcoin Protocol Deep Dive

Quiz Questions (1/4)

Q1. What is the primary advantage of asymmetric cryptography over symmetric cryptography for blockchain applications?
A) Faster encryption B) Smaller key sizes C) No key distribution problem D) Lower computational cost
Answer: C – Asymmetric cryptography eliminates the need to securely share keys between parties, making it ideal for decentralized networks.

Q2. In elliptic curve cryptography, what relationship exists between the private key and public key?
A) They are identical B) Public key = hash of private key C) Public key = private key × generator point D) They are randomly generated
Answer: C – The public key Q is computed as $Q = k \cdot G$, where k is the private key and G is the generator point.

Q3. Which elliptic curve does Bitcoin use for ECDSA?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with the equation $y^2 = x^3 + 7$.

Q4. What is the approximate security level of a 256-bit elliptic curve key?
A) 64-bit security B) 128-bit security C) 256-bit security D) 512-bit security
Answer: B – A 256-bit ECC key provides approximately 128-bit security, equivalent to a 3072-bit RSA key.

Q5. What cryptographic problem ensures that deriving a private key from a public key is computationally infeasible?
A) Factorization problem B) Discrete logarithm problem C) Traveling salesman problem D) Halting problem
Answer: B – The elliptic curve discrete logarithm problem makes it infeasible to find k given $Q = k \cdot G$.

Quiz Questions (2/4)

Q6. What four properties must a digital signature scheme provide?
A) Speed, size, cost, privacy B) Authentication, integrity, non-repudiation, unforgeable C) Encryption, decryption, hashing, compression D) Storage, transmission, verification, deletion
Answer: B – Digital signatures must provide authentication, integrity, non-repudiation, and be unforgeable.

Q7. In ECDSA signature generation, what must be unique for every signature to prevent private key leakage?
A) The message hash B) The private key C) The nonce D) The public key
Answer: C – Reusing a nonce allows attackers to recover the private key from two different signatures.

Q8. What real-world incident demonstrated the danger of nonce reuse in ECDSA?
A) Mt. Gox hack B) Sony PlayStation 3 breach (2010) C) DAO hack D) Parity wallet freeze
Answer: B – Sony used the same nonce for all PS3 firmware signatures, allowing hackers to recover the private key.

Q9. In Bitcoin address derivation, why are both SHA-256 and RIPEMD-160 hash functions used?
A) Redundancy for security B) SHA-256 for speed, RIPEMD-160 to reduce address size C) Legal compliance D) Compatibility with older systems
Answer: B – SHA-256 provides security and speed, while RIPEMD-160 reduces the address from 256 bits to 160 bits.

Q10. How long is an Ethereum address (excluding the "0x" prefix)?
A) 20 characters B) 32 characters C) 40 characters D) 64 characters
Answer: C – Ethereum addresses are 20 bytes represented as 40 hexadecimal characters.

Quiz Questions (3/4)

Q11. What is the main difference between compressed and uncompressed public keys?
A) Compressed keys are encrypted B) Compressed keys store only x-coordinate and sign of y C) Compressed keys use different curves D) Compressed keys are hashed differently
Answer: B – Compressed keys (33 bytes) store the x-coordinate and a prefix (02/03) indicating y's parity; uncompressed keys (65 bytes) store both x and y.

Q12. What is the primary benefit of Hierarchical Deterministic (HD) wallets?
A) Faster transactions B) Lower fees C) Single backup recovers all keys D) Stronger encryption
Answer: C – HD wallets derive all keys from a single master seed, so backing up the seed phrase once recovers all addresses.

Q13. What is a BIP-39 mnemonic seed phrase typically composed of?
A) Random letters and numbers B) 12-24 English words C) Binary data D) Hexadecimal string
Answer: B – BIP-39 seed phrases use 12-24 English words encoding 128-256 bits of entropy.

Q14. In a 2-of-3 multi-signature wallet, how many signatures are required to authorize a transaction?
A) 1 B) 2 C) 3 D) All signatures must be present
Answer: B – A 2-of-3 multisig requires any 2 out of 3 possible signatures to authorize a transaction.

Q15. What does the Bitcoin derivation path "m/44'/0'/0'/0/0" represent?
A) Account version B) Hierarchical levels: purpose/coin/account/change/index C) Encryption parameters D) Network identifier
Answer: B – The path represents purpose (44' for BIP-44), coin type (0' for Bitcoin), account (0'), change (0), and address index (0).

Quiz Questions (4/4)

Q16. What is the primary threat mitigated by using a hardware wallet?
A) Network congestion B) High transaction fees C) Malware on internet-connected devices D) Quantum computing attacks
Answer: C – Hardware wallets keep private keys offline, protecting them from malware and remote attacks.

Q17. Which hashing algorithm does Ethereum use for address derivation?
A) SHA-256 B) RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: C – Ethereum uses Keccak-256 to hash the public key and derives the address from the last 20 bytes.

Q18. What is the best practice for preventing nonce reuse in ECDSA signatures?
A) Use random nonces B) Use sequential nonces C) Use deterministic nonce generation (RFC 6979) D) Reuse nonces from previous signatures
Answer: C – RFC 6979 deterministically derives nonces from the message hash and private key, preventing reuse while maintaining security.

Q19. What does the principle "Not your keys, not your coins" mean?
A) Keys must be physically printed B) Only own cryptocurrency if you control the private keys C) Keys should be shared with trusted parties D) Public keys determine ownership
Answer: B – If you don't control the private keys (e.g., funds on an exchange), you don't truly own the cryptocurrency.

Q20. How does quantum computing threaten ECDSA-based blockchains?
A) Quantum computers can mine faster B) Shor's algorithm can solve discrete logarithm in polynomial time C) Quantum computers increase transaction fees D) Quantum computers corrupt blockchain data
Answer: B – Shor's algorithm can efficiently solve the discrete logarithm problem on quantum computers, potentially allowing derivation of private keys from public keys.

L05: Public Key Cryptography

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

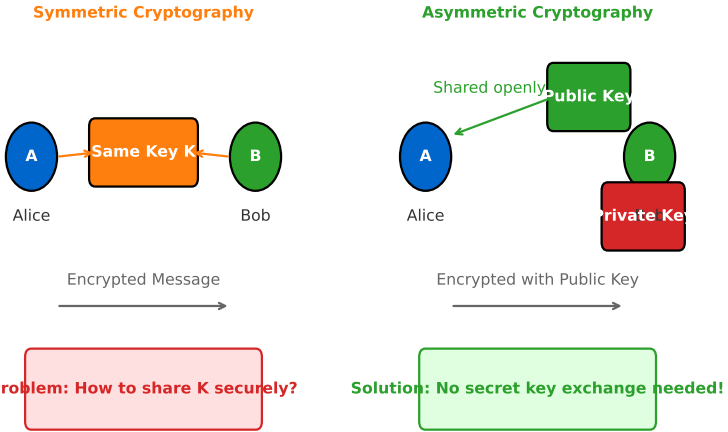
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

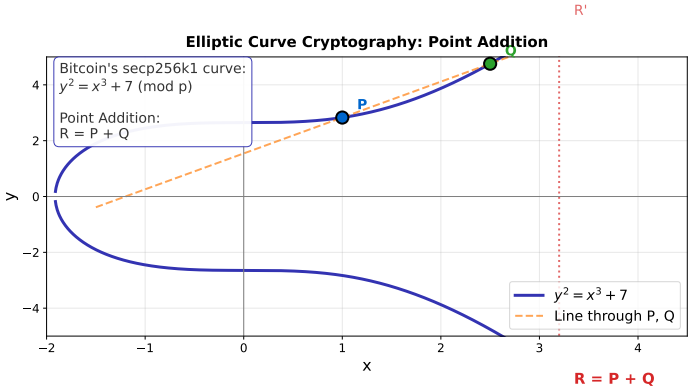
- Explain the difference between symmetric and asymmetric cryptography
- Understand how ECDSA digital signatures work
- Derive blockchain addresses from public keys
- Apply key security best practices

Symmetric vs. Asymmetric Cryptography



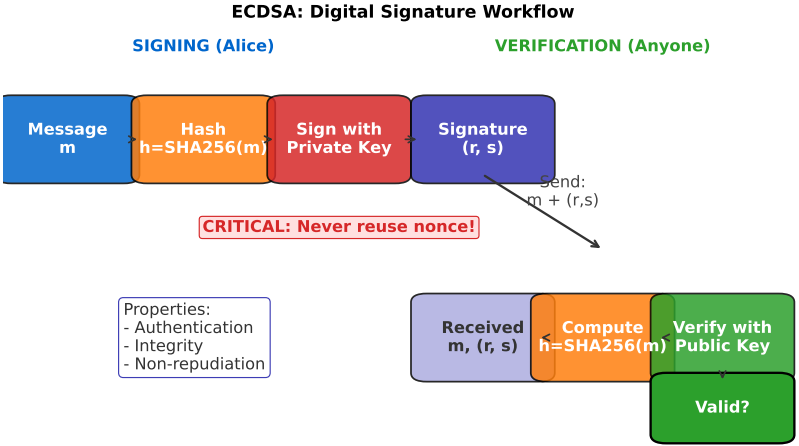
Key Insight: Blockchains use asymmetric cryptography because it solves the key distribution problem.

Elliptic Curve Cryptography (ECC)



Bitcoin's secp256k1: $y^2 = x^3 + 7$. Private key k derives public key $Q = k \cdot G$.

ECDSA Digital Signatures



Properties: Authentication, Integrity, Non-repudiation, Unforgeable.

Critical Security: Nonce Reuse

The Danger of Reusing Nonces:

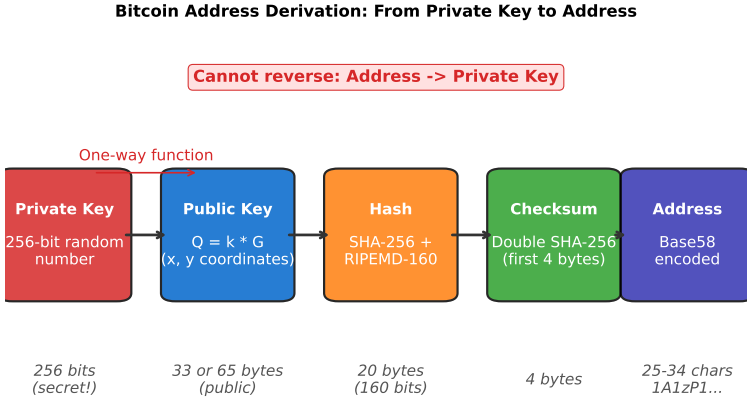
- If same nonce n signs two different messages
- Attacker obtains signatures (r, s_1) and (r, s_2) with same r
- Can compute private key k from equations

Real-World Incident: Sony PlayStation 3 (2010)

- Sony used same nonce for all PS3 firmware signatures
- Hackers recovered Sony's private key
- Enabled homebrew software and piracy

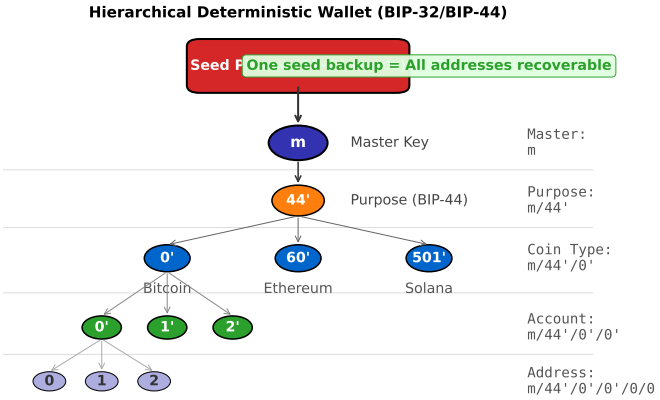
Best Practice: Use deterministic nonce generation (RFC 6979)

From Private Key to Address



One-way: Cannot reverse addresses to private keys.

HD Wallets: One Seed, All Keys



BIP-39: 12-24 word seed phrase recovers all addresses forever.

Key Security Best Practices

Private Key Protection:

- Never share private keys or seed phrases
- Use hardware wallets (Ledger, Trezor) for large amounts
- Store backups in multiple secure physical locations

Common Threats:

- Phishing attacks (fake wallet websites)
- Clipboard malware (replaces copied addresses)
- SIM swapping (hijack 2FA)

Core Principle

"Not your keys, not your coins."

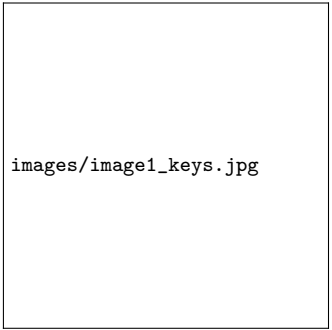
Key Takeaways

1. **Asymmetric Crypto:** Public/private key pairs solve key distribution
2. **ECC:** 256-bit keys provide 128-bit security (efficient, mobile-friendly)
3. **ECDSA:** Digital signatures prove ownership without revealing private key
4. **Nonce Security:** Never reuse nonces – use RFC 6979 deterministic generation
5. **HD Wallets:** Single seed phrase derives unlimited addresses

Critical Insight: The discrete logarithm problem ensures private keys cannot be derived from public keys – blockchain security depends on this.

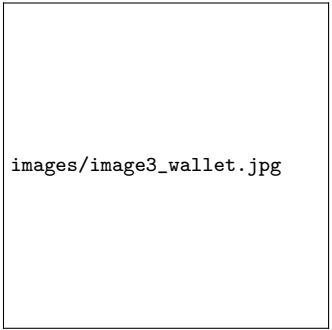
(c) Joerg Osterrieder 2025

Cryptography in the Real World



Public-Private Keys

Digital Security



Crypto Wallets

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the main advantage of asymmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost

Quiz (1/2)

Q1. What is the main advantage of asymmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519

Quiz (1/2)

Q1. What is the main advantage of asymmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q3. What must be unique for every ECDSA signature?
A) Message hash B) Private key C) Nonce D) Public key

Quiz (1/2)

Q1. What is the main advantage of asymmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q3. What must be unique for every ECDSA signature?
A) Message hash B) Private key C) Nonce D) Public key
Answer: C – Reusing a nonce allows attackers to recover the private key.

Q4. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars

Quiz (1/2)

Q1. What is the main advantage of asymmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q3. What must be unique for every ECDSA signature?
A) Message hash B) Private key C) Nonce D) Public key
Answer: C – Reusing a nonce allows attackers to recover the private key.

Q4. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q5. What is a BIP-39 seed phrase composed of?
A) Random letters B) 12-24 English words C) Binary data D) Hex string

Quiz (1/2)

Q1. What is the main advantage of asymmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q3. What must be unique for every ECDSA signature?
A) Message hash B) Private key C) Nonce D) Public key
Answer: C – Reusing a nonce allows attackers to recover the private key.

Q4. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q5. What is a BIP-39 seed phrase composed of?
A) Random letters B) 12-24 English words C) Binary data D) Hex string
Answer: B – 12-24 words encoding 128-256 bits of entropy.

Quiz (2/2)

Q6. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit

Quiz (2/2)

Q6. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC = 128-bit security = 3072-bit RSA equivalent.

Q7. In a 2-of-3 multisig, how many signatures are required?
A) 1 B) 2 C) 3 D) All

Quiz (2/2)

Q6. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC = 128-bit security = 3072-bit RSA equivalent.

Q7. In a 2-of-3 multisig, how many signatures are required?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 out of 3 possible signatures.

Q8. What does "Not your keys, not your coins" mean?
A) Keys must be printed B) Control private keys to own crypto C) Share keys D) Public keys matter

Quiz (2/2)

Q6. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC = 128-bit security = 3072-bit RSA equivalent.

Q7. In a 2-of-3 multisig, how many signatures are required?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 out of 3 possible signatures.

Q8. What does "Not your keys, not your coins" mean?
A) Keys must be printed B) Control private keys to own crypto C) Share keys D) Public keys matter
Answer: B – If you don't control private keys, you don't truly own the funds.

Q9. Which hash does Ethereum use for address derivation?
A) SHA-256 B) RIPEMD-160 C) Keccak-256 D) Blake2b

Quiz (2/2)

Q6. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC = 128-bit security = 3072-bit RSA equivalent.

Q7. In a 2-of-3 multisig, how many signatures are required?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 out of 3 possible signatures.

Q8. What does "Not your keys, not your coins" mean?
A) Keys must be printed B) Control private keys to own crypto C) Share keys D) Public keys matter
Answer: B – If you don't control private keys, you don't truly own the funds.

Q9. Which hash does Ethereum use for address derivation?
A) SHA-256 B) RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: C – Ethereum uses Keccak-256, takes last 20 bytes.

Q10. How does quantum computing threaten ECDSA?
A) Faster mining B) Shor's algorithm solves discrete log C) Higher fees D) Data corruption

Quiz (2/2)

Q6. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC = 128-bit security = 3072-bit RSA equivalent.

Q7. In a 2-of-3 multisig, how many signatures are required?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 out of 3 possible signatures.

Q8. What does "Not your keys, not your coins" mean?
A) Keys must be printed B) Control private keys to own crypto C) Share keys D) Public keys matter
Answer: B – If you don't control private keys, you don't truly own the funds.

Q9. Which hash does Ethereum use for address derivation?
A) SHA-256 B) RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: C – Ethereum uses Keccak-256, takes last 20 bytes.

Q10. How does quantum computing threaten ECDSA?
A) Faster mining B) Shor's algorithm solves discrete log C) Higher fees D) Data corruption
Answer: B – Shor's algorithm can derive private keys from public keys.

Thank you

Questions?

Next: L06 – Bitcoin Protocol Deep Dive

Quiz: Public Key Cryptography

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q4. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q4. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC provides 128-bit security, equivalent to 3072-bit RSA.

Q5. What must be unique for every ECDSA signature to prevent key leakage?
A) Message hash B) Private key C) Nonce D) Public key

Quiz (1–5)

Q1. What is the primary advantage of asymmetric over symmetric cryptography for blockchains?
A) Faster encryption B) Smaller keys C) No key distribution problem D) Lower cost
Answer: C – No need to securely share keys between parties.

Q2. In ECC, how is the public key derived from the private key?
A) Hash function B) $Q = k \cdot G$ C) Random generation D) Encryption
Answer: B – Public key Q = private key k multiplied by generator point G.

Q3. Which elliptic curve does Bitcoin use?
A) secp192k1 B) secp256k1 C) NIST P-256 D) Ed25519
Answer: B – Bitcoin uses secp256k1 with equation $y^2 = x^3 + 7$.

Q4. What security level does a 256-bit ECC key provide?
A) 64-bit B) 128-bit C) 256-bit D) 512-bit
Answer: B – 256-bit ECC provides 128-bit security, equivalent to 3072-bit RSA.

Q5. What must be unique for every ECDSA signature to prevent key leakage?
A) Message hash B) Private key C) Nonce D) Public key
Answer: C – Reusing a nonce allows recovery of the private key.

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption
Answer: C – Backing up seed phrase once recovers all derived addresses.

Q9. In a 2-of-3 multisig, how many signatures authorize a transaction?
A) 1 B) 2 C) 3 D) All

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption
Answer: C – Backing up seed phrase once recovers all derived addresses.

Q9. In a 2-of-3 multisig, how many signatures authorize a transaction?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 of 3 possible signatures required.

Q10. What does "Not your keys, not your coins" mean?
A) Print keys physically B) Control private keys to own crypto C) Share keys D) Public keys = ownership

Quiz (6–10)

Q6. Which hash functions does Bitcoin address derivation use?
A) MD5 + SHA1 B) SHA-256 + RIPEMD-160 C) Keccak-256 D) Blake2b
Answer: B – SHA-256 for security, RIPEMD-160 to reduce address size.

Q7. How long is an Ethereum address (excluding 0x prefix)?
A) 20 chars B) 32 chars C) 40 chars D) 64 chars
Answer: C – 20 bytes = 40 hexadecimal characters.

Q8. What is the main benefit of HD wallets?
A) Faster transactions B) Lower fees C) Single backup for all keys D) Stronger encryption
Answer: C – Backing up seed phrase once recovers all derived addresses.

Q9. In a 2-of-3 multisig, how many signatures authorize a transaction?
A) 1 B) 2 C) 3 D) All
Answer: B – Any 2 of 3 possible signatures required.

Q10. What does "Not your keys, not your coins" mean?
A) Print keys physically B) Control private keys to own crypto C) Share keys D) Public keys = ownership
Answer: B – Without private key control, you depend on third-party custody.

Bitcoin Protocol Deep Dive

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the UTXO (Unspent Transaction Output) model
- Describe the structure of a Bitcoin transaction
- Describe transaction inputs and outputs
- Recognize different Bitcoin Script types
- Trace the lifecycle of a transaction from creation to confirmation
- Distinguish between legacy and SegWit transaction formats

The Problem: How do we prevent digital counterfeiting?

The Challenge
How do we prevent digital counterfeiting and double-spending without a central authority tracking who owns what? Digital files can be copied infinitely at zero cost – how can digital money have scarcity?

Why It Matters

- Every pre-Bitcoin digital currency required trusted intermediaries who could be shut down, hacked, or corrupted
- Historical examples: DigiCash (centralized issuer, bankrupt 1998), E-gold (central database, seized by FBI 2007), Liberty Reserve (prosecuted for money laundering 2013)

What We Need

- Trustless verification mechanism
- Unforgeable, publicly verifiable transaction history where anyone can verify ownership without trusting a third party

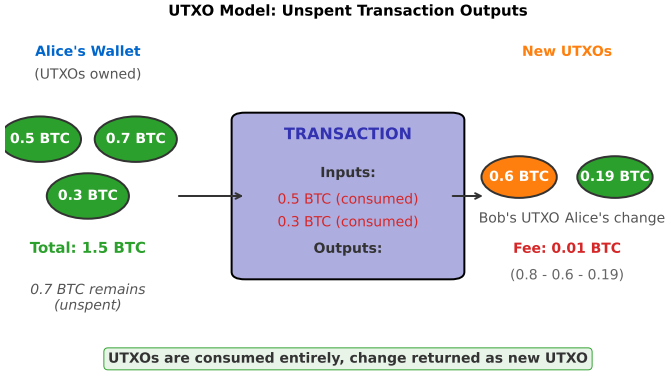
The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How Bitcoin's transaction protocol addresses this challenge

The UTXO Model: Core Concept

What is a UTXO?

- Unspent Transaction Output = a chunk of bitcoin that can be spent
- Bitcoin does not track account balances (unlike Ethereum)
- Instead, tracks individual "coins" (UTXOs)



UTXO Properties and Cash Analogy

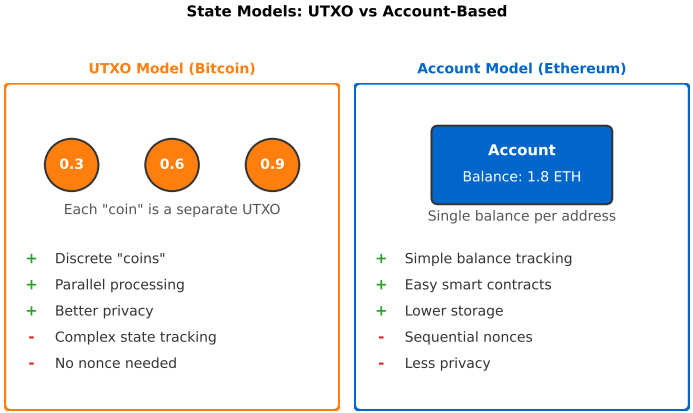
Analogy: Physical Cash

- UTXOs = bills in your wallet
- No "balance" – just individual coins
- Pay 30 EUR: use 20 + 10 bills
- Pay 25 EUR with 50: get 25 change

Key Principles:

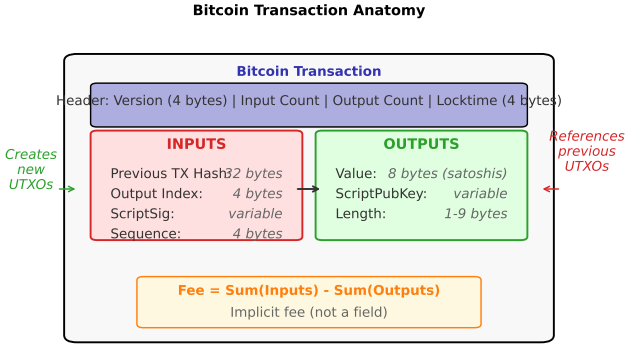
- Each UTXO spent once (consumed)
- Spending creates new UTXOs
- Blockchain tracks unspent UTXOs
- Balance = sum of your UTXOs

UTXO Model vs. Account Model



Why Bitcoin Uses UTXO: Easier to verify (check UTXO existence), no global state needed, natural double-spend prevention.

Bitcoin Transaction Structure



Transaction Hash (txid):

- Double SHA-256 of entire transaction – unique identifier
- Used to reference transaction in inputs

Transaction Inputs

Each Input Contains:

1. **Previous TX Hash:** txid of UTXO
2. **Output Index:** which output (0,1,2...)
3. **ScriptSig:** signature + pubkey
4. **Sequence Number:** for replacement

Example Input:

- Prev tx: `5a3c7b...` (3 BTC)
- Output index: 0
- ScriptSig: ownership proof

Multiple Inputs:
Combine UTXOs; each signed separately

Transaction Outputs

Each Output Contains:

1. **Value:** satoshis (1 BTC = 10^8 sat)
2. **ScriptPubKey:** spending conditions

Change Outputs:

- Input ¿ payment → create change
- Change to sender (new address)
- 5 BTC → 3 + 1.999 change

Transaction Fee:

- Fee = Inputs − Outputs
- Implicit (not stated)
- Miner collects difference

Bitcoin Script: A Stack-Based Language

What is Bitcoin Script?

- Simple, stack-based programming language
- Not Turing-complete (no loops, limited expressiveness)
- Executed during transaction validation
- Determines whether transaction is valid

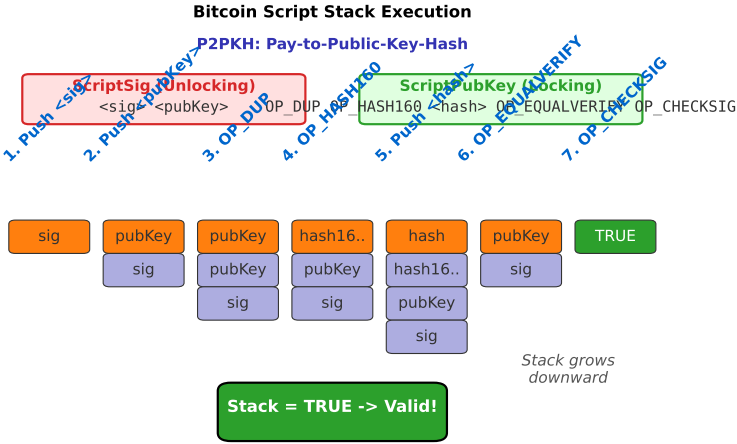
How It Works:

1. Combine ScriptSig (from input) + ScriptPubKey (from previous output)
2. Execute script operations left to right
3. Use a stack (LIFO data structure)
4. Transaction valid if final stack value is TRUE

Basic Operations:

- `OP_DUP`: duplicate top stack item
- `OP_HASH160`: hash with SHA-256 then RIPEMD-160
- `OP_EQUALVERIFY`: check equality, fail if not
- `OP_CHECKSIG`: verify signature against public key

P2PKH Script Execution



Why Public Key Hash? Shorter addresses (20 vs 33 bytes), extra security (quantum resistance until spending).

P2SH: Pay-to-Script-Hash

Purpose:

- Allows complex spending conditions (multi-signature, time-locks)
- Hides complexity until spending time
- Sender only needs recipient's P2SH address

ScriptPubKey:

```
OP_HASH160 <ScriptHash> OP_EQUAL
```

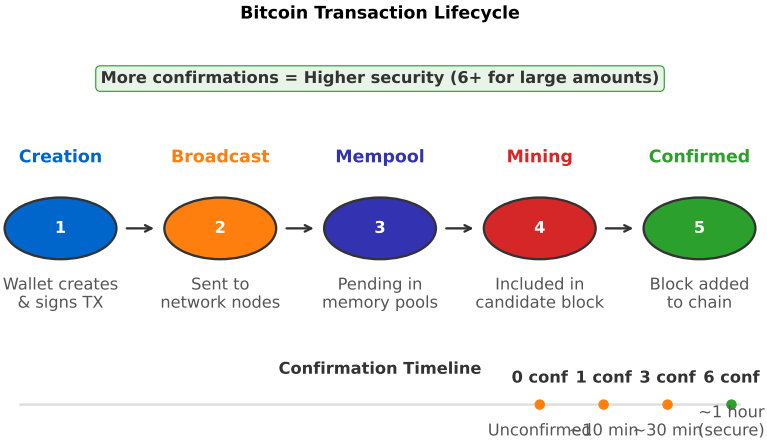
ScriptSig:

```
<Signature1> <Signature2> ... <RedeemScript>
```

Verification Process:

1. Hash the redeem script
2. Verify hash matches ScriptHash in ScriptPubKey
3. Execute redeem script with provided signatures
4. Transaction valid if redeem script evaluates to TRUE

Transaction Lifecycle



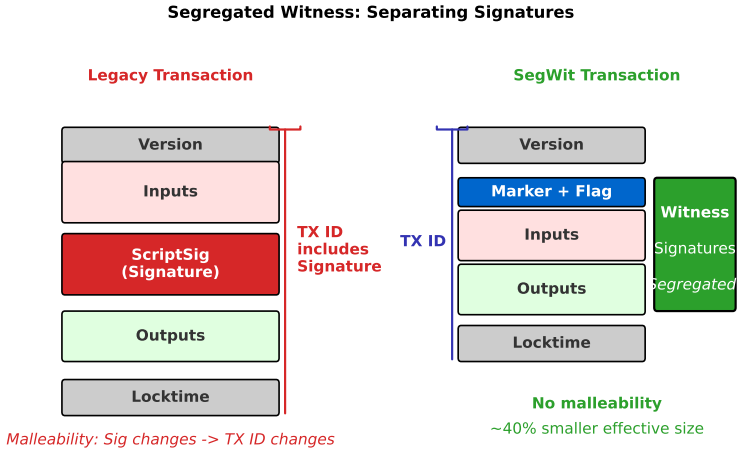
Key Stages:

- Creation → Signing → Broadcast → Mempool → Mining → Confirmation

Transaction Lifecycle: Details

1. **Creation and Signing:**
   - Wallet selects UTXOs, constructs inputs/outputs, calculates fee
   - Signs each input with corresponding private key
2. **Broadcast and Mempool:**
   - Transaction sent to connected nodes, validated, added to mempool
   - Nodes relay to peers (propagation across network)
   - Transactions sorted by fee rate in mempool
3. **Mining and Confirmation:**
   - Miner includes transaction in candidate block
   - Block mined, broadcast, validated by network
   - Each new block adds one confirmation
   - 6 confirmations typically considered final ($\sim$1 hour)

SegWit: Segregated Witness



Problem with Legacy: Signature in TX hash → malleability
SegWit Solution (BIP 141, 2017): Separate witness data from TX ID

SegWit Benefits

Block Capacity:

- Legacy: 1 MB limit
- SegWit: 4M weight units
- Witness: 1 byte = 1 WU
- Effective: 2-2.7 MB/block

Lower Fees:
Witness data 75% discount

Address Formats:

- P2WPKH: “bc1q...” (Bech32)
- P2SH-wrapped: “3...”

Enables Lightning:
Fixes malleability for payment channels

Taproot: SegWit v1 (Activated 2021)

Key Improvements:

- **Schnorr:** Signature aggregation
- **MAST:** Hidden scripts until used
- **Privacy:** Uniform tx appearance

Address: "bc1p..." (Bech32m)

Benefits:

- Multi-sig = single-sig appearance
- Complex contracts look simple
- Smaller transaction size

(c) Joerg Osterrieder 2025

Transaction Validation Rules

Syntax:

- Size within limits
- Values non-negative
- No duplicate inputs

Semantic:

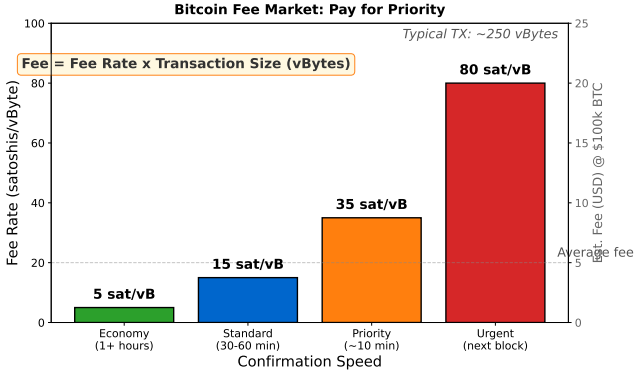
- UTXOs exist, unspent
- Valid signatures
- Scripts succeed
- Locktime satisfied

Rejection:

- Invalid sig = fraud
- Double-spend
- Dust output (spam)

(c) Joerg Osterrieder 2025

Transaction Fees: Economics



Fee Market Dynamics:

- Block space is scarce (∼4 MB weight per 10 minutes)
- Users compete for inclusion via fees
- Fee estimation based on mempool state and target confirmation time

Replace-by-Fee (RBF) and CPFP

RBF (BIP 125):

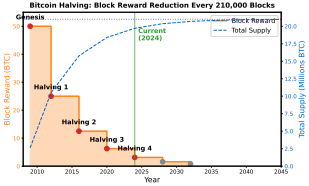
- Replace tx with same inputs
- Increase fee (+1 sat/byte)
- Signal via sequence number
- Sender controls

CPFP:

- Spend unconfirmed output
- High-fee child tx
- Miners include both
- Receiver controls

Key Difference: RBF = sender bumps; CPFP = receiver bumps

Coinbase Transactions and Block Rewards



Coinbase Properties:

- First transaction in every block, creates new bitcoins
- Miner collects block reward + all transaction fees
- Must wait 100 confirmations before spending (maturity rule)

2024-2025 Milestone: Bitcoin ETFs and Institutional Adoption

Jan 10, 2024: ETF Approval

- SEC approved 11 spot ETFs
- BlackRock, Fidelity, Grayscale
- $140B+ AUM (Jan 2026)

Market Impact:

- Institutional legitimization
- Rivals major commodity ETFs
- Regulated custody

Transaction Implications:

- Large on-chain tx for ETFs
- Institutional UTXO consolidation
- Increased block space demand

Problem Solved? Bitcoin's Transaction Protocol

The Original Problem

How do we prevent digital counterfeiting?

How Bitcoin's Protocol Solves It

- **UTXO Model:** Tracks coin ownership cryptographically – each UTXO has a unique digital signature proving ownership, making counterfeiting computationally infeasible
- **Transaction Fees:** Create economic incentives for miners to include transactions in blocks, ensuring the system processes payments without centralized payment processors
- **Coinbase + Halving:** Bootstrap network security by rewarding early miners, gradually transitioning to fee-only economy by 2140

Remaining Limitations

- **Throughput:** 7 transactions per second (TPS) limit vs Visa's 24,000 TPS – Bitcoin sacrificed scalability for decentralization and security
- **Confirmation Time:** 10-minute average block time means 1-hour wait for 6 confirmations, making point-of-sale payments impractical

Open Questions

- **Post-2140:** How will the network maintain security when all 21M coins are mined and only transaction fees remain? Will fees alone suffice?
- **Risk:** Sybil attacks, eclipse attacks, quantum computing threat to ECDSA signatures

Bitcoin's transaction protocol solves digital counterfeiting but introduces throughput and latency trade-offs

Key Takeaways

- UTXO model: consume old, create new
- Inputs + outputs structure
- Bitcoin Script: flexible, not Turing-complete
- P2PKH → P2SH → SegWit → Taproot
- Lifecycle: create → sign → broadcast → mine
- Fee market competition
- SegWit/Taproot: scalability + privacy

Design Philosophy: Security and decentralization over throughput

Discussion Questions

1. Why does Bitcoin use the UTXO model instead of the account model?
2. How does the fee market incentivize miners to include transactions?
3. What are the trade-offs between legacy addresses, SegWit, and Taproot?
4. How does transaction malleability affect second-layer solutions?
5. Why is the coinbase maturity rule (100 confirmations) necessary?
6. How could you design a transaction that can only be spent after a certain date?

Next Lesson Preview: L07 Proof of Work Consensus

Topics to be covered:

- Mining mechanics and the proof-of-work algorithm
- Nonce searching and difficulty adjustment
- Block header structure and hash rate
- 51% attacks and mining centralization risks
- Energy consumption and environmental concerns

Preparation:

- Review hash function properties (pre-image resistance)
- Explore Bitcoin mining pools and hash rate distribution
- Consider the economics of mining profitability

Quiz - Part 1

Q1. What does UTXO stand for?
A) Unified Transaction Exchange Output B) Unspent Transaction Output C) Universal Token Exchange Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output, representing spendable bitcoin.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage of amount B) Sum of inputs minus sum of outputs C) Set by miners D) Based on recipient address
Answer: B – Fee = Total Input Value - Total Output Value (implicit, not explicitly stated).

Q3. What is the purpose of the ScriptSig in a transaction input?
A) Lock the output B) Set the transaction fee C) Provide proof of ownership (signature) D) Specify the recipient
Answer: C – ScriptSig provides the unlocking script with signature proving ownership of the UTXO.

Q4. How many satoshis are in one Bitcoin?
A) 1,000 B) 1,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis (eight decimal places).

Quiz - Part 2

Q5. Which statement about Bitcoin Script is correct?
A) It is Turing-complete B) It uses a stack-based execution model C) It supports loops D) It runs on Ethereum
Answer: B – Bitcoin Script is stack-based and intentionally NOT Turing-complete (no loops).

Q6. What does P2PKH stand for?
A) Pay to Protocol Key Hash B) Pay to Public Key Hash C) Private to Public Key Handler D) Peer to Peer Key Hash
Answer: B – P2PKH = Pay to Public Key Hash, the standard legacy transaction type.

Q7. What problem did SegWit solve?
A) Block size limit B) Transaction malleability C) Mining centralization D) Key generation
Answer: B – SegWit separates witness data from txid, fixing transaction malleability.

Q8. What prefix do native SegWit (Bech32) addresses start with?
A) 1 B) 3 C) bc1q D) 0x
Answer: C – Native SegWit addresses use Bech32 encoding starting with "bc1q".

Quiz - Part 3

Q9. How many confirmations are typically considered final for a Bitcoin transaction?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is the standard for high-value transaction finality.

Q10. What is RBF (Replace-by-Fee) used for?
A) Reduce transaction size B) Increase fee to speed up confirmation C) Cancel already confirmed transactions D) Create multi-sig wallets
Answer: B – RBF allows replacing an unconfirmed transaction with a higher-fee version.

Q11. What is a coinbase transaction?
A) Transaction on Coinbase exchange B) First transaction creating new BTC in each block C) Multi-signature transaction D) Fee refund transaction
Answer: B – Coinbase transaction is the first tx in each block, creating the block reward.

Q12. How long must a miner wait before spending coinbase outputs?
A) 10 blocks B) 50 blocks C) 100 blocks D) 144 blocks
Answer: C – Coinbase maturity rule requires 100 confirmations before spending.

Quiz - Part 4

Q13. What did Taproot introduce to Bitcoin (activated 2021)?
A) Proof of Stake B) Schnorr signatures and MAST C) Smart contract execution D) Larger block size
Answer: B – Taproot introduced Schnorr signatures and Merkelized Abstract Syntax Trees (MAST).

Q14. In the UTXO model, what happens to your "balance" after spending?
A) It decreases incrementally B) Old UTXOs are consumed, new ones created C) Balance is updated in global state D) Nothing changes
Answer: B – UTXOs are consumed entirely; change creates new UTXOs.

Q15. Why is Bitcoin's UTXO model considered more privacy-friendly than account models?
A) UTXOs are encrypted B) No global balance visible, each UTXO is independent C) Addresses are hidden D) Transactions are anonymous
Answer: B – UTXO model has no visible balance; coins can be spread across many addresses.

Q16. What is a "dust" output in Bitcoin?
A) A high-value transaction B) An output too small to be economically spent C) A mining reward D) A test transaction
Answer: B – Dust outputs are so small that the fee to spend them exceeds their value.

Bitcoin Protocol Deep Dive

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the UTXO (Unspent Transaction Output) model
- Describe the structure of a Bitcoin transaction
- Describe transaction inputs and outputs
- Recognize different Bitcoin Script types
- Trace the lifecycle of a transaction from creation to confirmation
- Distinguish between legacy and SegWit transaction formats

Building on L05: Public Key Cryptography

UTXO Confusion

[COMIC: A confused person at a cash register trying to pay $25, but their wallet contains only $20 and $10 bills – no $25 bill exists. The cashier explains: "You give me $30, I give you $5 change." Caption: "Bitcoin doesn't have balances – just unspent coins."]

[Comic placeholder – to be illustrated]

- Unlike bank accounts, Bitcoin tracks individual "coins" (UTXOs), not balances
- Spending requires consuming entire UTXOs and creating change outputs

The Problem: How do we prevent digital counterfeiting?

The Challenge
How do we prevent digital counterfeiting and double-spending without a central authority tracking who owns what? Digital files can be copied infinitely at zero cost – how can digital money have scarcity?

Why It Matters

- Every pre-Bitcoin digital currency required trusted intermediaries who could be shut down, hacked, or corrupted
- Historical examples: DigiCash (centralized issuer, bankrupt 1998), E-gold (central database, seized by FBI 2007), Liberty Reserve (prosecuted for money laundering 2013)

What We Need

- Trustless verification mechanism
- Unforgeable, publicly verifiable transaction history where anyone can verify ownership without trusting a third party

The Cryptoeconomics Question
Coordinating without trusted intermediaries

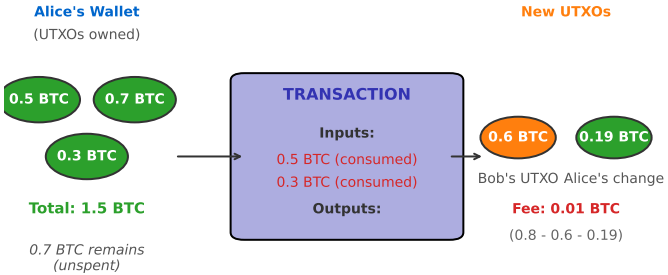
Today's lesson: How Bitcoin's transaction protocol addresses this challenge

How Does the UTXO Model Track Ownership?

What is a UTXO?

- Unspent Transaction Output = a chunk of bitcoin that can be spent
- Bitcoin does not track account balances (unlike Ethereum)
- Instead, tracks individual "coins" (UTXOs)

UTXO Model: Unspent Transaction Outputs



UTXOs are consumed entirely, change returned as new UTXO

UTXOs create unforgeable ownership – each coin spent only once with valid signature

How Are UTXOs Like Physical Cash?

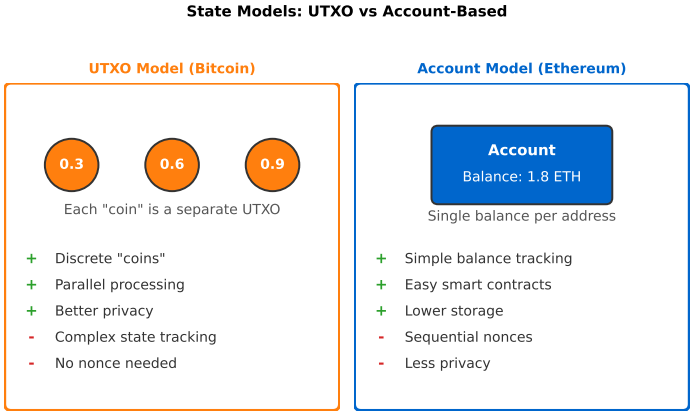
Analogy: Physical Cash

- UTXOs = bills in your wallet
- No "balance" – just individual coins
- Pay 30 EUR: use 20 + 10 bills
- Pay 25 EUR with 50: get 25 change

Key Principles:

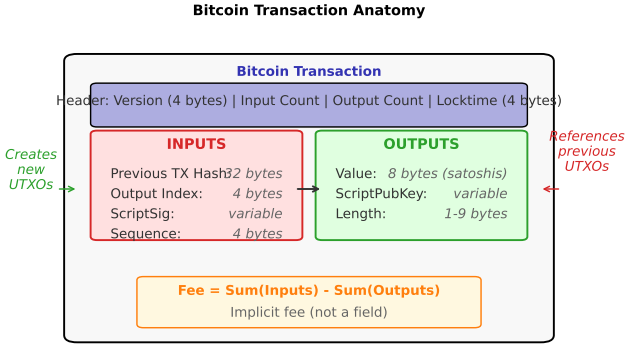
- Each UTXO spent once (consumed)
- Spending creates new UTXOs
- Blockchain tracks unspent UTXOs
- Balance = sum of your UTXOs

Why Did Bitcoin Choose UTXOs Over Accounts?



Why Bitcoin Uses UTXO: Easier to verify (check UTXO existence), no global state needed, natural double-spend prevention.

How is a Bitcoin Transaction Structured?



Transaction Hash (txid):

- Double SHA-256 of entire transaction – unique identifier
- Used to reference transaction in inputs

What Information Do Transaction Inputs Contain?

Each Input Contains:

1. **Previous TX Hash:** txid of UTXO
2. **Output Index:** which output (0,1,2...)
3. **ScriptSig:** signature + pubkey
4. **Sequence Number:** for replacement

Example Input:

- Prev tx: `5a3c7b...` (3 BTC)
- Output index: 0
- ScriptSig: ownership proof

Multiple Inputs:
Combine UTXOs; each signed separately

→ **Problem: How do we prevent digital... — Transaction Inputs — Every input must prove ownership via digital signature, preventing unauthorized spending**

How Do Transaction Outputs Work?

Each Output Contains:

1. **Value:** satoshis (1 BTC = 10^8 sat)
2. **ScriptPubKey:** spending conditions

Change Outputs:

- Input ¿ payment $\rightarrow$ create change
- Change to sender (new address)
- 5 BTC $\rightarrow$ 3 + 1.999 change

Transaction Fee:

- Fee = Inputs − Outputs
- Implicit (not stated)
- Miner collects difference

How Does Bitcoin Script Verify Transactions?

What is Bitcoin Script?

- Simple, stack-based programming language
- Not Turing-complete (no loops, limited expressiveness)
- Executed during transaction validation
- Determines whether transaction is valid

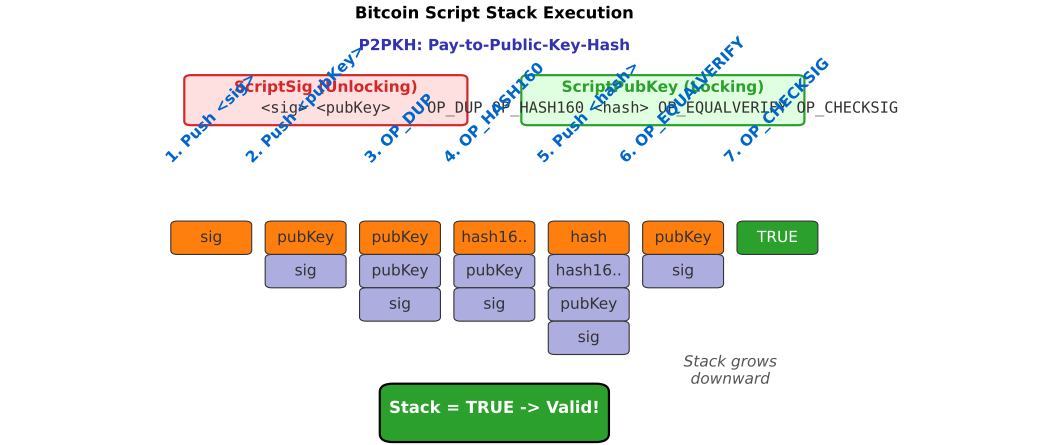
How It Works:

1. Combine ScriptSig (from input) + ScriptPubKey (from previous output)
2. Execute script operations left to right
3. Use a stack (LIFO data structure)
4. Transaction valid if final stack value is TRUE

Basic Operations:

- `OP_DUP`: duplicate top stack item
- `OP_HASH160`: hash with SHA-256 then RIPEMD-160
- `OP_EQUALVERIFY`: check equality, fail if not
- `OP_CHECKSIG`: verify signature against public key

How Does P2PKH Script Execution Work?



Why Public Key Hash? Shorter addresses (20 vs 33 bytes), extra security (quantum resistance until spending).

How Does Pay-to-Script-Hash Enable Complex Transactions?

Purpose:

- Allows complex spending conditions (multi-signature, time-locks)
- Hides complexity until spending time
- Sender only needs recipient's P2SH address

ScriptPubKey:

```
OP_HASH160 <ScriptHash> OP_EQUAL
```

ScriptSig:

```
<Signature1> <Signature2> ... <RedeemScript>
```

Verification Process:

1. Hash the redeem script
2. Verify hash matches ScriptHash in ScriptPubKey
3. Execute redeem script with provided signatures
4. Transaction valid if redeem script evaluates to TRUE

Problem Check-In: Mining Economics

Recall Our Problem

How do we prevent digital counterfeiting?

What We've Learned So Far

- UTXO model tracks coin ownership cryptographically – each output is spent exactly once
- Bitcoin Script verifies spending conditions without trusted intermediaries
- Together, these prevent counterfeiting: no valid signature = no spending

Still to Address

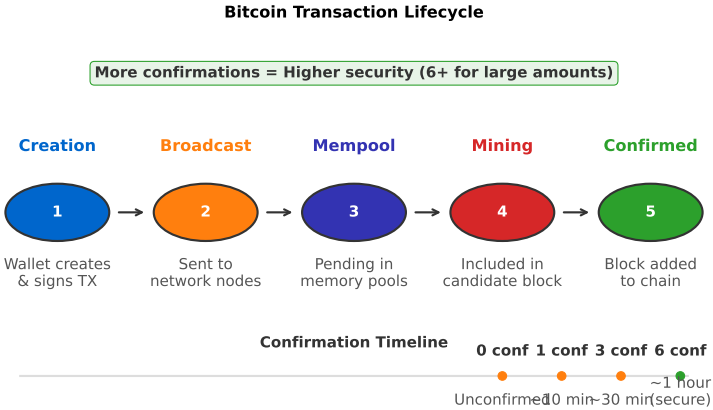
- Transaction lifecycle from creation to confirmation
- How do miners decide which transactions to include?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we prevent digital..."?

What Happens to a Transaction from Creation to Confirmation?



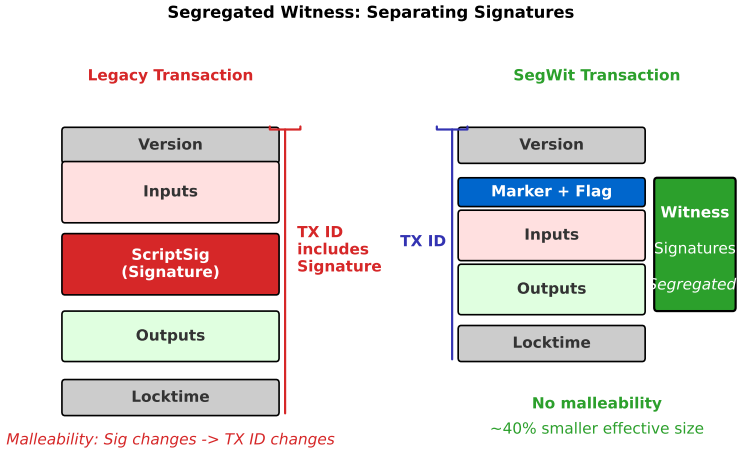
Key Stages: Creation → Signing → Broadcast → Mempool → Mining → Confirmation

Each stage adds verification – unconfirmed transactions can still be double-spent

What Are the Key Stages in Transaction Processing?

1. **Creation and Signing:**
   - Wallet selects UTXOs, constructs inputs/outputs, calculates fee
   - Signs each input with corresponding private key
2. **Broadcast and Mempool:**
   - Transaction sent to connected nodes, validated, added to mempool
   - Nodes relay to peers (propagation across network)
   - Transactions sorted by fee rate in mempool
3. **Mining and Confirmation:**
   - Miner includes transaction in candidate block
   - Block mined, broadcast, validated by network
   - Each new block adds one confirmation
   - 6 confirmations typically considered final ($\sim$1 hour)

How Did SegWit Fix Transaction Malleability?



Problem with Legacy: Signature in TX hash → malleability
SegWit Solution (BIP 141, 2017): Separate witness data from TX ID

What Benefits Did SegWit Bring to Bitcoin?

Block Capacity:

- Legacy: 1 MB limit
- SegWit: 4M weight units
- Witness: 1 byte = 1 WU
- Effective: 2-2.7 MB/block

Lower Fees:
Witness data 75% discount

Address Formats:

- P2WPKH: “bc1q...” (Bech32)
- P2SH-wrapped: “3...”

Enables Lightning:
Fixes malleability for payment channels

What Improvements Did Taproot Introduce?

Key Improvements:

- **Schnorr:** Signature aggregation
- **MAST:** Hidden scripts until used
- **Privacy:** Uniform tx appearance

Address: "bc1p..." (Bech32m)

Benefits:

- Multi-sig = single-sig appearance
- Complex contracts look simple
- Smaller transaction size

How Are Transactions Validated by Nodes?

Syntax:

- Size within limits
- Values non-negative
- No duplicate inputs

Semantic:

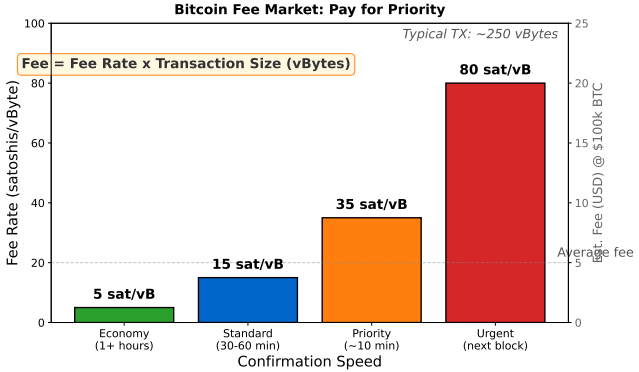
- UTXOs exist, unspent
- Valid signatures
- Scripts succeed
- Locktime satisfied

Rejection:

- Invalid sig = fraud
- Double-spend
- Dust output (spam)

→ Problem: How do we prevent digital... — Transaction Validation Rules — Validation rules are the network's defense against counterfeiting – invalid transactions rejected by all nodes

How Does Bitcoin's Fee Market Work?



Fee Market Dynamics:

- Block space is scarce (∼4 MB weight per 10 minutes)
- Users compete for inclusion via fees
- Fee estimation based on mempool state and target confirmation time

How Can You Speed Up Stuck Transactions?

RBF (BIP 125):

- Replace tx with same inputs
- Increase fee (+1 sat/byte)
- Signal via sequence number
- Sender controls

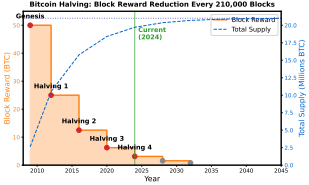
CPFP:

- Spend unconfirmed output
- High-fee child tx
- Miners include both
- Receiver controls

Key Difference: RBF = sender bumps; CPFP = receiver bumps

(c) Joerg Osterrieder 2025

How Do Miners Get Paid for Securing the Network?



Coinbase Properties:

- First transaction in every block, creates new bitcoins
- Miner collects block reward + all transaction fees
- Must wait 100 confirmations before spending (maturity rule)

How Have Bitcoin ETFs Changed the Landscape?

Jan 10, 2024: ETF Approval

- SEC approved 11 spot ETFs
- BlackRock, Fidelity, Grayscale
- $140B+ AUM (Jan 2026)

Market Impact:

- Institutional legitimization
- Rivals major commodity ETFs
- Regulated custody

Transaction Implications:

- Large on-chain tx for ETFs
- Institutional UTXO consolidation
- Increased block space demand

Problem Solved? Bitcoin's Transaction Protocol

The Original Problem

How do we prevent digital counterfeiting?

How Bitcoin's Protocol Solves It

- **UTXO Model:** Tracks coin ownership cryptographically – each UTXO has a unique digital signature proving ownership, making counterfeiting computationally infeasible
- **Transaction Fees:** Create economic incentives for miners to include transactions in blocks, ensuring the system processes payments without centralized payment processors
- **Coinbase + Halving:** Bootstrap network security by rewarding early miners, gradually transitioning to fee-only economy by 2140

Remaining Limitations

- **Throughput:** 7 transactions per second (TPS) limit vs Visa's 24,000 TPS – Bitcoin sacrificed scalability for decentralization and security
- **Confirmation Time:** 10-minute average block time means 1-hour wait for 6 confirmations, making point-of-sale payments impractical

Open Questions

- **Post-2140:** How will the network maintain security when all 21M coins are mined and only transaction fees remain? Will fees alone suffice?
- **Risk:** Sybil attacks, eclipse attacks, quantum computing threat to ECDSA signatures

Bitcoin's transaction protocol solves digital counterfeiting but introduces throughput and latency trade-offs

The Economics of Mining Economics

Incentive Structure

- **Core Problem:** Coordinating without trusted intermediaries
- **Why act honestly?** Participants verify rather than trust
- **Value Flow:** Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Mining Economics

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Mining Economics

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Script Puzzle Complexity

[COMIC: A Bitcoin Script as a Rube Goldberg machine – signatures push data onto stacks, operations verify and transform, finally a green "TRUE" light illuminates. A developer sighs: "All that just to prove I own 0.001 BTC." Caption: "Simple concept, complex execution."]

[Comic placeholder – to be illustrated]

- Bitcoin Script is intentionally limited – no loops, no Turing-completeness
- This simplicity is a security feature: predictable execution, no infinite loops

Key Takeaways

- UTXO model: consume old, create new
- Inputs + outputs structure
- Bitcoin Script: flexible, not Turing-complete
- P2PKH → P2SH → SegWit → Taproot
- Lifecycle: create → sign → broadcast → mine
- Fee market competition
- SegWit/Taproot: scalability + privacy

Design Philosophy: Security and decentralization over throughput

Next Lesson: L07 – Proof of Work

Discussion Questions

1. Why does Bitcoin use the UTXO model instead of the account model?
2. How does the fee market incentivize miners to include transactions?
3. What are the trade-offs between legacy addresses, SegWit, and Taproot?
4. How does transaction malleability affect second-layer solutions?
5. Why is the coinbase maturity rule (100 confirmations) necessary?
6. How could you design a transaction that can only be spent after a certain date?

Next Lesson Preview: L07 Proof of Work Consensus

Topics to be covered:

- Mining mechanics and the proof-of-work algorithm
- Nonce searching and difficulty adjustment
- Block header structure and hash rate
- 51% attacks and mining centralization risks
- Energy consumption and environmental concerns

Preparation:

- Review hash function properties (pre-image resistance)
- Explore Bitcoin mining pools and hash rate distribution
- Consider the economics of mining profitability

Quiz - Part 1

Q1. What does UTXO stand for?
A) Unified Transaction Exchange Output B) Unspent Transaction Output C) Universal Token Exchange Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output, representing spendable bitcoin.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage of amount B) Sum of inputs minus sum of outputs C) Set by miners D) Based on recipient address
Answer: B – Fee = Total Input Value - Total Output Value (implicit, not explicitly stated).

Q3. What is the purpose of the ScriptSig in a transaction input?
A) Lock the output B) Set the transaction fee C) Provide proof of ownership (signature) D) Specify the recipient
Answer: C – ScriptSig provides the unlocking script with signature proving ownership of the UTXO.

Q4. How many satoshis are in one Bitcoin?
A) 1,000 B) 1,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis (eight decimal places).

Quiz - Part 2

Q5. Which statement about Bitcoin Script is correct?
A) It is Turing-complete B) It uses a stack-based execution model C) It supports loops D) It runs on Ethereum
Answer: B – Bitcoin Script is stack-based and intentionally NOT Turing-complete (no loops).

Q6. What does P2PKH stand for?
A) Pay to Protocol Key Hash B) Pay to Public Key Hash C) Private to Public Key Handler D) Peer to Peer Key Hash
Answer: B – P2PKH = Pay to Public Key Hash, the standard legacy transaction type.

Q7. What problem did SegWit solve?
A) Block size limit B) Transaction malleability C) Mining centralization D) Key generation
Answer: B – SegWit separates witness data from txid, fixing transaction malleability.

Q8. What prefix do native SegWit (Bech32) addresses start with?
A) 1 B) 3 C) bc1q D) 0x
Answer: C – Native SegWit addresses use Bech32 encoding starting with "bc1q".

Quiz - Part 3

Q9. How many confirmations are typically considered final for a Bitcoin transaction?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is the standard for high-value transaction finality.

Q10. What is RBF (Replace-by-Fee) used for?
A) Reduce transaction size B) Increase fee to speed up confirmation C) Cancel already confirmed transactions D) Create multi-sig wallets
Answer: B – RBF allows replacing an unconfirmed transaction with a higher-fee version.

Q11. What is a coinbase transaction?
A) Transaction on Coinbase exchange B) First transaction creating new BTC in each block C) Multi-signature transaction D) Fee refund transaction
Answer: B – Coinbase transaction is the first tx in each block, creating the block reward.

Q12. How long must a miner wait before spending coinbase outputs?
A) 10 blocks B) 50 blocks C) 100 blocks D) 144 blocks
Answer: C – Coinbase maturity rule requires 100 confirmations before spending.

Quiz - Part 4

Q13. What did Taproot introduce to Bitcoin (activated 2021)?
A) Proof of Stake B) Schnorr signatures and MAST C) Smart contract execution D) Larger block size
Answer: B – Taproot introduced Schnorr signatures and Merkelized Abstract Syntax Trees (MAST).

Q14. In the UTXO model, what happens to your "balance" after spending?
A) It decreases incrementally B) Old UTXOs are consumed, new ones created C) Balance is updated in global state D) Nothing changes
Answer: B – UTXOs are consumed entirely; change creates new UTXOs.

Q15. Why is Bitcoin's UTXO model considered more privacy-friendly than account models?
A) UTXOs are encrypted B) No global balance visible, each UTXO is independent C) Addresses are hidden D) Transactions are anonymous
Answer: B – UTXO model has no visible balance; coins can be spread across many addresses.

Q16. What is a "dust" output in Bitcoin?
A) A high-value transaction B) An output too small to be economically spent C) A mining reward D) A test transaction
Answer: B – Dust outputs are so small that the fee to spend them exceeds their value.

L06: Bitcoin Protocol Deep Dive

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

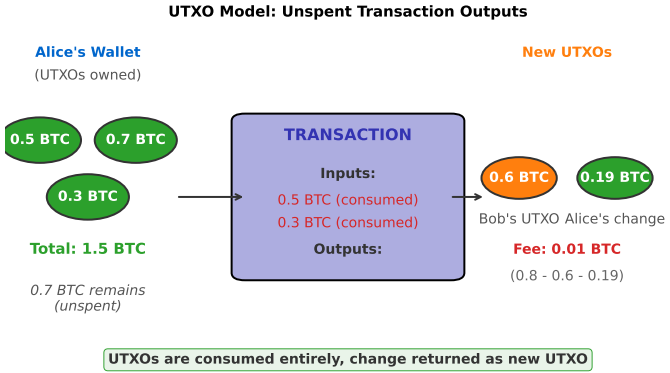
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

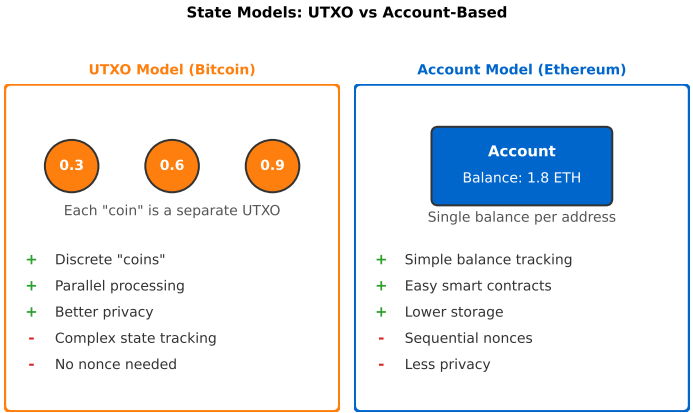
- Explain the UTXO (Unspent Transaction Output) model
- Describe the structure of Bitcoin transactions
- Understand Bitcoin Script and transaction validation
- Distinguish between legacy, SegWit, and Taproot formats

The UTXO Model: Core Concept



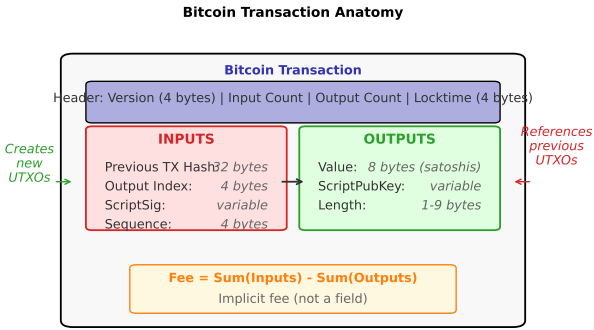
Key Insight: Bitcoin tracks individual "coins" (UTXOs), not account balances. Like cash bills, each UTXO must be spent entirely.

UTXO vs. Account Model



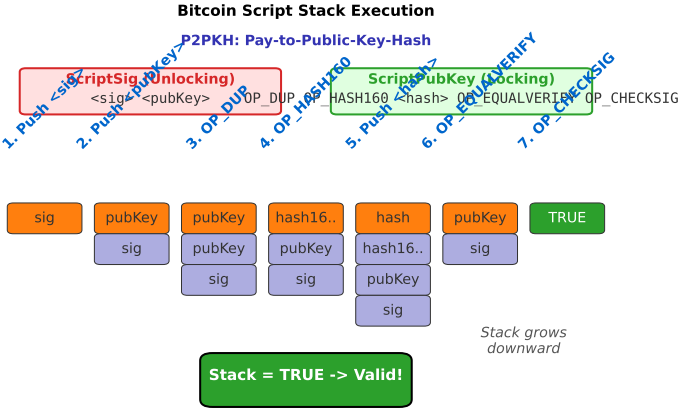
Why UTXO: Easier verification, no global state needed, natural double-spend prevention.

Bitcoin Transaction Structure



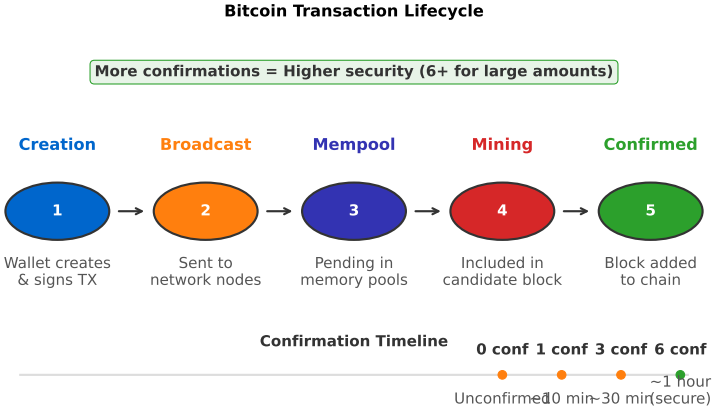
Fee = Sum of inputs - Sum of outputs (implicit, not stated in transaction).

Bitcoin Script: Stack-Based Validation



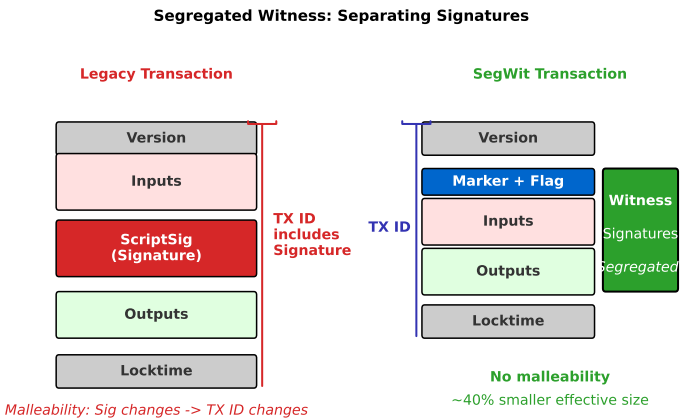
Not Turing-complete: Intentionally limited (no loops) for security.

Transaction Lifecycle



Stages: Creation → Signing → Broadcast → Mempool → Mining → Confirmation (6 blocks ≈ 1 hour).

SegWit and Taproot: Modern Upgrades



SegWit (2017): Fixes malleability, enables Lightning, lower fees
Taproot (2021): Schnorr signatures, MAST, privacy improvements
Address prefixes: Legacy "1", P2SH "3", SegWit "bc1q", Taproot "bc1p"

2024-2025: Institutional Adoption

January 10, 2024: Spot Bitcoin ETF Approval

- SEC approved 11 spot Bitcoin ETFs (first time in US)
- Major issuers: BlackRock (IBIT), Fidelity (FBTC), Grayscale (GBTC)
- Accumulated $140B+ in assets under management (Jan 2026)

Transaction Implications:

- ETF creation/redemption uses large on-chain transactions
- Institutional custody drives UTXO consolidation
- Increased demand for block space during high activity

Key Takeaways

1. **UTXO Model:** Transactions consume old outputs, create new ones
2. **Inputs/Outputs:** Each input references previous UTXO; outputs create new UTXOs
3. **Bitcoin Script:** Stack-based, not Turing-complete, validates spending conditions
4. **SegWit/Taproot:** Fix malleability, improve scalability and privacy
5. **Transaction Fees:** Determined by market competition for limited block space

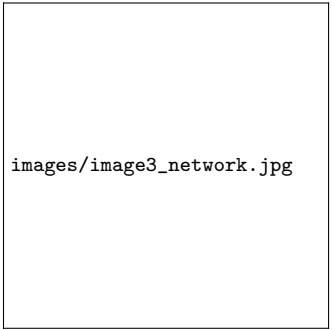
Design Philosophy: Bitcoin prioritizes security and decentralization over transaction throughput.

(c) Joerg Osterrieder 2025

Bitcoin Protocol in Action

Bitcoin Network

Transaction Flow



Global Network

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What does UTXO stand for?
A) Unified Transaction Exchange B) Unspent Transaction Output C) Universal Token Order D) Unverified Transaction Object

Quiz (1/2)

Q1. What does UTXO stand for?
A) Unified Transaction Exchange B) Unspent Transaction Output C) Universal Token Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage B) Sum of inputs minus outputs C) Set by miners D) Based on recipient

Quiz (1/2)

Q1. What does UTXO stand for?
A) Unified Transaction Exchange B) Unspent Transaction Output C) Universal Token Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage B) Sum of inputs minus outputs C) Set by miners D) Based on recipient
Answer: B – Fee = Total Inputs - Total Outputs (implicit).

Q3. How many satoshis are in one Bitcoin?
A) 1,000 B) 1,000,000 C) 100,000,000 D) 1,000,000,000

Quiz (1/2)

Q1. What does UTXO stand for?
A) Unified Transaction Exchange B) Unspent Transaction Output C) Universal Token Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage B) Sum of inputs minus outputs C) Set by miners D) Based on recipient
Answer: B – Fee = Total Inputs - Total Outputs (implicit).

Q3. How many satoshis are in one Bitcoin?
A) 1,000 B) 1,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis.

Q4. What problem did SegWit solve?
A) Block size B) Transaction malleability C) Mining centralization D) Key generation

Quiz (1/2)

Q1. What does UTXO stand for?
A) Unified Transaction Exchange B) Unspent Transaction Output C) Universal Token Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage B) Sum of inputs minus outputs C) Set by miners D) Based on recipient
Answer: B – Fee = Total Inputs - Total Outputs (implicit).

Q3. How many satoshis are in one Bitcoin?
A) 1,000 B) 1,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis.

Q4. What problem did SegWit solve?
A) Block size B) Transaction malleability C) Mining centralization D) Key generation
Answer: B – SegWit separates witness data, fixing malleability.

Q5. What prefix do native SegWit addresses start with?
A) 1 B) 3 C) bc1q D) 0x

Quiz (1/2)

Q1. What does UTXO stand for?
A) Unified Transaction Exchange B) Unspent Transaction Output C) Universal Token Order D) Unverified Transaction Object
Answer: B – UTXO = Unspent Transaction Output.

Q2. How is a Bitcoin transaction fee calculated?
A) Fixed percentage B) Sum of inputs minus outputs C) Set by miners D) Based on recipient
Answer: B – Fee = Total Inputs - Total Outputs (implicit).

Q3. How many satoshis are in one Bitcoin?
A) 1,000 B) 1,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis.

Q4. What problem did SegWit solve?
A) Block size B) Transaction malleability C) Mining centralization D) Key generation
Answer: B – SegWit separates witness data, fixing malleability.

Q5. What prefix do native SegWit addresses start with?
A) 1 B) 3 C) bc1q D) 0x
Answer: C – Native SegWit uses Bech32 encoding starting with "bc1q".

Quiz (2/2)

Q6. How many confirmations are considered final?
A) 1 B) 3 C) 6 D) 10

Quiz (2/2)

Q6. How many confirmations are considered final?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is standard.

Q7. What is a coinbase transaction?
A) Exchange transaction B) First tx creating new BTC in each block C) Multi-sig tx D) Fee refund

Quiz (2/2)

Q6. How many confirmations are considered final?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is standard.

Q7. What is a coinbase transaction?
A) Exchange transaction B) First tx creating new BTC in each block C) Multi-sig tx D) Fee refund
Answer: B – Coinbase creates the block reward.

Q8. What did Taproot introduce (2021)?
A) Proof of Stake B) Schnorr signatures and MAST C) Smart contracts D) Larger blocks

Quiz (2/2)

Q6. How many confirmations are considered final?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is standard.

Q7. What is a coinbase transaction?
A) Exchange transaction B) First tx creating new BTC in each block C) Multi-sig tx D) Fee refund
Answer: B – Coinbase creates the block reward.

Q8. What did Taproot introduce (2021)?
A) Proof of Stake B) Schnorr signatures and MAST C) Smart contracts D) Larger blocks
Answer: B – Schnorr signatures and Merkelized Abstract Syntax Trees.

Q9. What is RBF (Replace-by-Fee) used for?
A) Reduce size B) Increase fee to speed confirmation C) Cancel confirmed tx D) Create multisig

Quiz (2/2)

Q6. How many confirmations are considered final?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is standard.

Q7. What is a coinbase transaction?
A) Exchange transaction B) First tx creating new BTC in each block C) Multi-sig tx D) Fee refund
Answer: B – Coinbase creates the block reward.

Q8. What did Taproot introduce (2021)?
A) Proof of Stake B) Schnorr signatures and MAST C) Smart contracts D) Larger blocks
Answer: B – Schnorr signatures and Merkelized Abstract Syntax Trees.

Q9. What is RBF (Replace-by-Fee) used for?
A) Reduce size B) Increase fee to speed confirmation C) Cancel confirmed tx D) Create multisig
Answer: B – Replace unconfirmed tx with higher fee version.

Q10. What is a "dust" output?
A) High-value tx B) Output too small to economically spend C) Mining reward D) Test tx

Quiz (2/2)

Q6. How many confirmations are considered final?
A) 1 B) 3 C) 6 D) 10
Answer: C – 6 confirmations ($\sim$1 hour) is standard.

Q7. What is a coinbase transaction?
A) Exchange transaction B) First tx creating new BTC in each block C) Multi-sig tx D) Fee refund
Answer: B – Coinbase creates the block reward.

Q8. What did Taproot introduce (2021)?
A) Proof of Stake B) Schnorr signatures and MAST C) Smart contracts D) Larger blocks
Answer: B – Schnorr signatures and Merkelized Abstract Syntax Trees.

Q9. What is RBF (Replace-by-Fee) used for?
A) Reduce size B) Increase fee to speed confirmation C) Cancel confirmed tx D) Create multisig
Answer: B – Replace unconfirmed tx with higher fee version.

Q10. What is a "dust" output?
A) High-value tx B) Output too small to economically spend C) Mining reward D) Test tx
Answer: B – Fee to spend exceeds the output value.

Thank you

Questions?

Next: L07 – Proof of Work Consensus

Quiz: Bitcoin Protocol

Instructions: 21 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?
A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?
A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object
Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?
A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?
A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object
Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?
A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?
A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?
A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object
Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?
A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?
A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig
Answer: C – ScriptPubKey is in the output, not input. Inputs have ScriptSig (unlocking script).

Q4. How is the transaction fee calculated?
A) Fixed 0.001 BTC B) Sum of inputs minus sum of outputs C) Explicitly stated in tx D) Based on block height

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?
A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object
Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?
A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?
A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig
Answer: C – ScriptPubKey is in the output, not input. Inputs have ScriptSig (unlocking script).

Q4. How is the transaction fee calculated?
A) Fixed 0.001 BTC B) Sum of inputs minus sum of outputs C) Explicitly stated in tx D) Based on block height
Answer: B – Fee is implicit: total input value minus total output value.

Q5. What happens to a UTXO when it is spent?
A) Balance decremented B) Marked as spent C) Consumed entirely D) Split into smaller pieces

Quiz (1–5)

Q1. What is a UTXO in Bitcoin?
A) A user account balance B) An unspent transaction output C) A unified transaction output D) A transaction verification object
Answer: B – UTXO stands for Unspent Transaction Output, representing a chunk of bitcoin that can be spent.

Q2. How many satoshis are in 1 Bitcoin?
A) 1,000,000 B) 10,000,000 C) 100,000,000 D) 1,000,000,000
Answer: C – 1 BTC = 100,000,000 satoshis (smallest unit).

Q3. Which component is NOT part of a transaction input?
A) Previous transaction hash B) Output index C) ScriptPubKey D) ScriptSig
Answer: C – ScriptPubKey is in the output, not input. Inputs have ScriptSig (unlocking script).

Q4. How is the transaction fee calculated?
A) Fixed 0.001 BTC B) Sum of inputs minus sum of outputs C) Explicitly stated in tx D) Based on block height
Answer: B – Fee is implicit: total input value minus total output value.

Q5. What happens to a UTXO when it is spent?
A) Balance decremented B) Marked as spent C) Consumed entirely D) Split into smaller pieces
Answer: C – UTXOs must be consumed entirely; change is returned via new output.

Quiz (6–10)

Q6. What is the purpose of Bitcoin Script?
A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol

Quiz (6–10)

Q6. What is the purpose of Bitcoin Script?
A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol
Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?
A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash

Quiz (6–10)

Q6. What is the purpose of Bitcoin Script?
A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol
Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?
A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash
Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?
A) Starts with "1" B) Starts with "3" C) Starts with "bc1q" D) Starts with "bc1p"

Quiz (6–10)

Q6. What is the purpose of Bitcoin Script?
A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol
Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?
A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash
Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?
A) Starts with "1" B) Starts with "3" C) Starts with "bc1q" D) Starts with "bc1p"
Answer: C – "bc1q" addresses use Bech32 encoding for native SegWit (P2WPKH).

Q9. What problem does SegWit solve?
A) High fees B) Transaction malleability C) 51% attacks D) Double spending

Quiz (6–10)

Q6. What is the purpose of Bitcoin Script?
A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol
Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?
A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash
Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?
A) Starts with "1" B) Starts with "3" C) Starts with "bc1q" D) Starts with "bc1p"
Answer: C – "bc1q" addresses use Bech32 encoding for native SegWit (P2WPKH).

Q9. What problem does SegWit solve?
A) High fees B) Transaction malleability C) 51% attacks D) Double spending
Answer: B – SegWit fixes transaction malleability by separating witness data from transaction ID.

Q10. How many confirmations are typically considered final for a Bitcoin transaction?
A) 1 B) 3 C) 6 D) 12

Quiz (6–10)

Q6. What is the purpose of Bitcoin Script?
A) Smart contracts B) Transaction validation C) Mining algorithm D) Network protocol
Answer: B – Bitcoin Script determines whether a transaction is valid during execution.

Q7. What does OP_CHECKSIG do in Bitcoin Script?
A) Checks tx size B) Verifies signature against public key C) Checks balance D) Validates block hash
Answer: B – OP_CHECKSIG verifies the signature using the provided public key.

Q8. Which address format indicates a native SegWit transaction?
A) Starts with "1" B) Starts with "3" C) Starts with "bc1q" D) Starts with "bc1p"
Answer: C – "bc1q" addresses use Bech32 encoding for native SegWit (P2WPKH).

Q9. What problem does SegWit solve?
A) High fees B) Transaction malleability C) 51% attacks D) Double spending
Answer: B – SegWit fixes transaction malleability by separating witness data from transaction ID.

Q10. How many confirmations are typically considered final for a Bitcoin transaction?
A) 1 B) 3 C) 6 D) 12
Answer: C – Six confirmations (about 1 hour) are standard for finality.

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?
A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?
A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB
Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?
A) SegWit B) Taproot C) P2SH D) Lightning Network

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?
A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB
Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?
A) SegWit B) Taproot C) P2SH D) Lightning Network
Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?
A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?
A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB
Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?
A) SegWit B) Taproot C) P2SH D) Lightning Network
Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?
A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations
Answer: C – Coinbase outputs must wait 100 confirmations before being spent.

Q14. What does RBF (Replace-by-Fee) allow?
A) Cancel any transaction B) Replace unconfirmed tx with higher fee C) Refund fees D) Merge transactions

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?
A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB
Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?
A) SegWit B) Taproot C) P2SH D) Lightning Network
Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?
A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations
Answer: C – Coinbase outputs must wait 100 confirmations before being spent.

Q14. What does RBF (Replace-by-Fee) allow?
A) Cancel any transaction B) Replace unconfirmed tx with higher fee C) Refund fees D) Merge transactions
Answer: B – RBF (BIP 125) allows replacing unconfirmed transactions with higher-fee versions.

Q15. How often does Bitcoin halving occur?
A) Every year B) Every 100,000 blocks C) Every 210,000 blocks D) Every 500,000 blocks

Quiz (11–15)

Q11. What is the maximum block weight in SegWit?
A) 1 MB B) 2 MB C) 4 million weight units D) 8 MB
Answer: C – SegWit uses weight units (max 4 million), allowing effective capacity of 2-2.7 MB.

Q12. Which upgrade introduced Schnorr signatures?
A) SegWit B) Taproot C) P2SH D) Lightning Network
Answer: B – Taproot (2021) introduced Schnorr signatures for efficiency and privacy.

Q13. What is the maturity rule for coinbase transactions?
A) 10 confirmations B) 50 confirmations C) 100 confirmations D) 144 confirmations
Answer: C – Coinbase outputs must wait 100 confirmations before being spent.

Q14. What does RBF (Replace-by-Fee) allow?
A) Cancel any transaction B) Replace unconfirmed tx with higher fee C) Refund fees D) Merge transactions
Answer: B – RBF (BIP 125) allows replacing unconfirmed transactions with higher-fee versions.

Q15. How often does Bitcoin halving occur?
A) Every year B) Every 100,000 blocks C) Every 210,000 blocks D) Every 500,000 blocks
Answer: C – Halving occurs every 210,000 blocks (approximately every 4 years).

Quiz (16–20)

Q16. What is the first transaction in every Bitcoin block called?
A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction

Quiz (16–20)

Q16. What is the first transaction in every Bitcoin block called?
A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction
Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?
A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection

Quiz (16–20)

Q16. What is the first transaction in every Bitcoin block called?
A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction
Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?
A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection
Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?
A) SegWit B) Lightning C) Taproot D) P2SH

Quiz (16–20)

Q16. What is the first transaction in every Bitcoin block called?
A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction
Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?
A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection
Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?
A) SegWit B) Lightning C) Taproot D) P2SH
Answer: C – Taproot (SegWit v1) was activated in November 2021.

Q19. What does P2SH stand for?
A) Pay-to-Script-Hash B) Pay-to-Secure-Hash C) Peer-to-Script-Hash D) Protocol-to-Script-Hash

Quiz (16–20)

Q16. What is the first transaction in every Bitcoin block called?
A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction
Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?
A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection
Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?
A) SegWit B) Lightning C) Taproot D) P2SH
Answer: C – Taproot (SegWit v1) was activated in November 2021.

Q19. What does P2SH stand for?
A) Pay-to-Script-Hash B) Pay-to-Secure-Hash C) Peer-to-Script-Hash D) Protocol-to-Script-Hash
Answer: A – P2SH (Pay-to-Script-Hash) enables complex spending conditions.

Q20. When were spot Bitcoin ETFs approved in the US?
A) 2020 B) 2022 C) January 2024 D) December 2024

Quiz (16–20)

Q16. What is the first transaction in every Bitcoin block called?
A) Genesis transaction B) Coinbase transaction C) Root transaction D) Base transaction
Answer: B – The coinbase transaction creates new bitcoins and collects fees.

Q17. What is CPFP (Child-Pays-for-Parent)?
A) Mining strategy B) Fee bumping by receiver C) Block propagation D) UTXO selection
Answer: B – CPFP allows recipient to create high-fee tx spending unconfirmed output.

Q18. Which Bitcoin upgrade was activated in 2021?
A) SegWit B) Lightning C) Taproot D) P2SH
Answer: C – Taproot (SegWit v1) was activated in November 2021.

Q19. What does P2SH stand for?
A) Pay-to-Script-Hash B) Pay-to-Secure-Hash C) Peer-to-Script-Hash D) Protocol-to-Script-Hash
Answer: A – P2SH (Pay-to-Script-Hash) enables complex spending conditions.

Q20. When were spot Bitcoin ETFs approved in the US?
A) 2020 B) 2022 C) January 2024 D) December 2024
Answer: C – SEC approved 11 spot Bitcoin ETFs on January 10, 2024.

Quiz (21–21)

Q21. How many confirmations are typically considered final?
A) 1 B) 3 C) 6 D) 12

Quiz (21–21)

Q21. How many confirmations are typically considered final?
A) 1 B) 3 C) 6 D) 12
Answer: C – Six confirmations (about 1 hour) are standard for finality.

Proof of Work Consensus

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the proof-of-work consensus mechanism
- Describe the mining process and nonce searching
- Explain difficulty adjustment and its purpose
- Calculate mining profitability and hash rate economics
- Recognize the security guarantees and vulnerabilities of PoW
- Evaluate the 51% attack threat model
- Discuss energy consumption and environmental impact

The Problem: How do we make attacks economically irrational?

The Challenge
In a decentralized network, anyone can participate. How do we make attacks so expensive that honest behavior becomes the dominant strategy? Without economic skin-in-the-game, attackers could cheaply rewrite history and steal coins.

Why It Matters

- Without attack costs $>$ potential profit, no double-spend security
- Historical: GHash.IO mining pool reached 55% in 2014, threatening Bitcoin's security assumptions

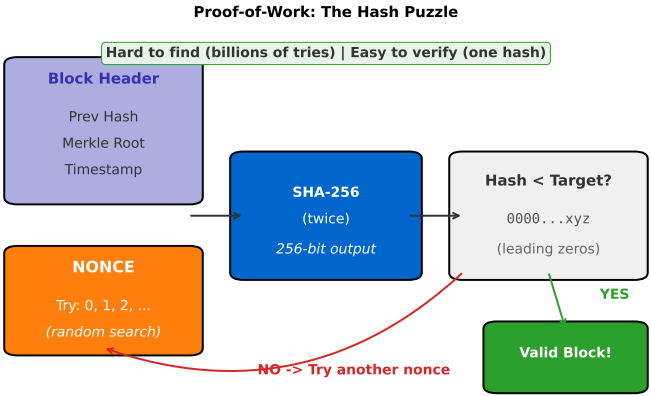
Today's lesson: How Proof of Work addresses this challenge

What We Need

- Economic alignment of actors
- Attack cost must exceed potential profit from double-spending
- Security that scales with network value

The Cryptoeconomics Question
Aligning individual and collective interests

What is Proof of Work?



Core Concept: Find a nonce such that the hash of block header is below the target. No shortcut: must try nonces randomly until one works.

Proof-of-Work Properties

Key Properties:

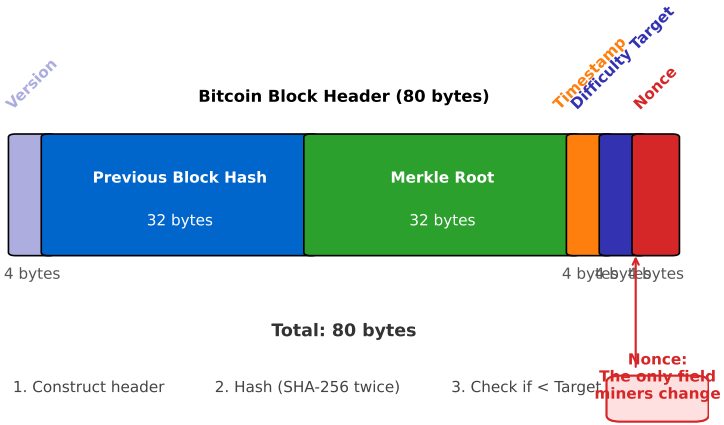
1. **Asymmetry:** Hard to find, easy to verify
2. **Probabilistic:** Expected time to find solution, no guarantee
3. **Adjustable difficulty:** Target changes to maintain block time
4. **Progress-free:** Past attempts do not help future attempts

Mathematical Formulation:

$$\text{SHA-256}(\text{SHA-256}(\text{BlockHeader})) < \text{Target}$$

Analogy: Rolling dice until you get 10 sixes in a row. Each roll is independent. Expected number of attempts: 6^{10}. Verification: just look at the result.

Bitcoin Block Header Structure



Mining Process: Construct block → Set timestamp/difficulty → Try nonces → If hash $<$ target: success, else repeat.

Nonce Space and Extra Nonce

Nonce Space Exhaustion:

- 4 bytes = 2^{32} = 4.3 billion possible nonces
- Modern ASICs exceed this in milliseconds
- Solution: modify coinbase transaction (extra nonce), recompute Merkle root

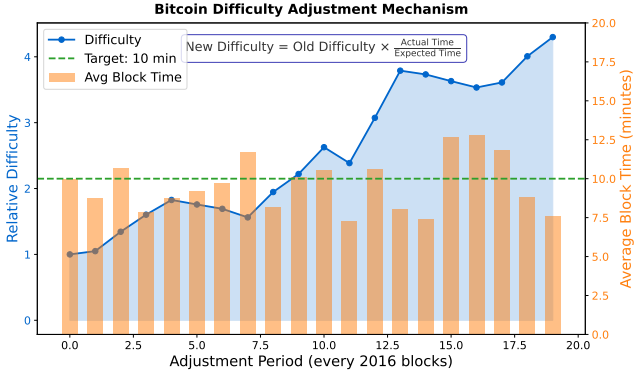
Merkle Trees:

- Commit to all transactions with single 32-byte hash
- Tree height: $\log_2(n)$ for n transactions
- Proof size: $\log_2(n)$ hashes to prove inclusion
- Example: 1000 transactions $\rightarrow$ 10 hashes ($\sim$320 bytes proof)

Extra Nonce Trick:

- Miners modify coinbase transaction (includes extra nonce field)
- Recompute Merkle root (different root for each extra nonce)
- Expands search space beyond 2^{32} nonces

Difficulty Adjustment



Adjustment Rule (Every 2016 Blocks):

$$\text{New Target} = \text{Old Target} \times \frac{\text{Actual Time}}{\text{Expected Time (20,160 min)}}$$

Clamped to $[T/4, T \times 4]$ to prevent extreme changes.

Hash Rate and Mining Probability

Hash Rate:

- Number of hashes computed per second
- Units: H/s, KH/s, MH/s, GH/s, TH/s, PH/s, EH/s
- Bitcoin network (Dec 2024): $\sim$1,200 EH/s (all-time high)

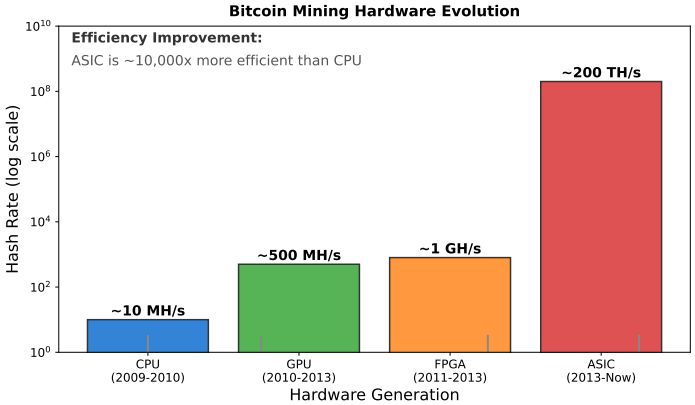
Mining Probability:

$$P(\text{find block}) = \frac{\text{Your Hash Rate}}{\text{Network Hash Rate}}$$

Example:

- Miner: 100 TH/s, Network: 500 EH/s
- Probability: $0.0000002 = 0.00002\%$
- Expected time to find block: $\sim$100 years solo mining
- Solution: Join mining pools for steady income

Mining Hardware Evolution



Implications: Mining centralization, high barrier to entry, geographic concentration in low-electricity regions.

Mining Profitability

Revenue:

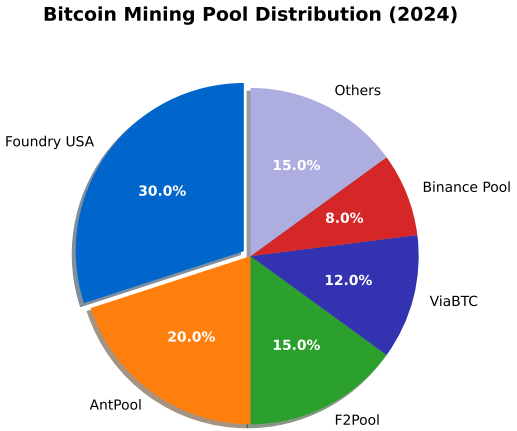
$$\text{Daily Revenue} = \frac{\text{Hash Rate}}{\text{Network Hash Rate}} \times 144 \times (\text{Reward} + \text{Fees})$$

Example (Antminer S19 Pro):

- Hash rate: 110 TH/s, Power: 3250 W = 78 kWh/day
- Electricity: \$0.05/kWh $\times$ 78 = \$3.90/day
- Revenue (@\$40k BTC): $\sim$\$7.92/day
- Profit: \$4.02/day, Payback: $\sim$2 years

Risk Factors: BTC price volatility, difficulty increases, hardware obsolescence, electricity cost changes.

Mining Pools



Top 5 pools control ~85% of hash rate

(Miners can switch pools - pools do not own hardware)

Payout Schemes: PPS (fixed/share), PPLNS (share recent blocks), FPPS (PPS + fees).

Mining Pool Operation

Why Pools Exist:

- Solo mining: high variance (might wait years for block)
- Pooled mining: steady income (proportional to hash rate)

Pool Operation:

1. Pool coordinator distributes mining tasks (shares)
2. Miners submit partial solutions (lower difficulty)
3. Pool tracks contribution of each miner
4. When pool finds block, reward distributed proportionally
5. Pool takes fee (1-3%)

Centralization Concern:

- Pools do not own hardware (miners can switch pools)
- Mitigation: decentralized pool protocols (P2Pool, Stratum V2)

Block Rewards and Halving

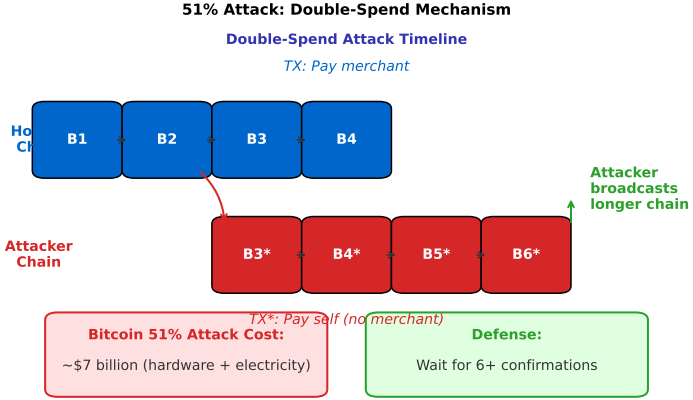
Block Reward Components:

$$\text{Total Reward} = \text{Block Subsidy} + \text{Transaction Fees}$$

Period	Reward	Cumulative Supply
2009-2012	50 BTC	10.5M BTC
2012-2016	25 BTC	15.75M BTC
2016-2020	12.5 BTC	18.375M BTC
2020-2024	6.25 BTC	19.6875M BTC
2024-2028 (current)	3.125 BTC	20.34M BTC

Future: Transaction fees must eventually sustain mining as block subsidy approaches zero ($\sim$2140).

The 51% Attack



CAN do: Double-spend, censor transactions.
CANNOT do: Steal coins without keys, create coins out of thin air.

51% Attack Economics

Cost of Attack (Bitcoin):

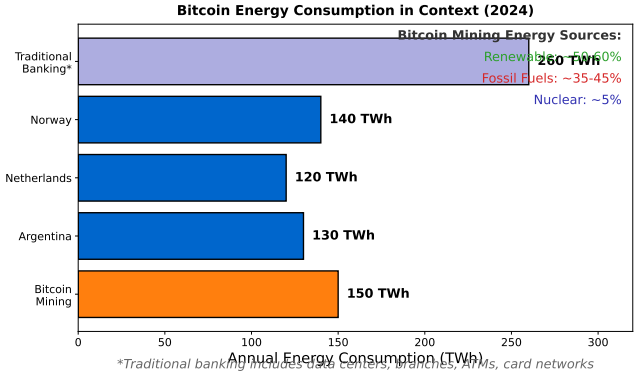
- Need 255 EH/s (>50% of network)
- Hardware: ∼2.3 million ASICs = $6.9 billion
- Electricity (1 week): ∼$63 million
- Total: ∼$7 billion

Consequences:

- Attack becomes public immediately
- Bitcoin price crashes (attacker's hardware worthless)
- Community may hard fork (bricks attacker's ASICs)

Vulnerable Chains: Small PoW chains, shared mining algorithms. Historical: Bitcoin Gold, Ethereum Classic, Verge.

Energy Consumption



Counterarguments: Incentivizes renewable development, facilitates grid balancing, security proportional to value.

ASIC Resistance Alternatives

ASIC-Resistant Algorithms:

- **Scrypt (Litecoin):** Memory-hard hashing (ASICs developed 2014)
- **Ethash (Ethereum pre-merge):** Memory-hard with large DAG
- **RandomX (Monero):** CPU-optimized, frequently updated

Trade-offs:

- ASIC resistance $\rightarrow$ lower security per watt
- Easier for botnets to attack (commodity hardware)
- Algorithm changes create hard fork risks
- Debate: specialization increases security investment

Problem Solved? Proof of Work

The Original Problem

How do we make attacks economically irrational?

How Proof of Work Solves It

- Mining requires real-world energy expenditure (150 TWh/year for Bitcoin)
- Difficulty adjustment maintains 10-minute blocks regardless of hash rate
- Attack cost: $7 billion in hardware + $63 million/week in electricity (Bitcoin)

Remaining Limitations

- Energy consumption equivalent to Argentina's annual usage
- Mining pool centralization (top 4 pools >50% of hash rate)
- Geographic concentration in low-electricity regions (China, Kazakhstan, USA)

Open Questions

- Is PoW's energy use justified by its security guarantees?
- Risk: What happens when block rewards approach zero and fees remain low?

Proof of Work partially solves attack rationality but introduces energy and centralization trade-offs

(c) Joerg Osterrieder 2025

Key Takeaways

- Proof-of-work provides Sybil resistance via computational cost
- Mining searches for nonces to produce valid block hashes
- Difficulty adjusts every 2016 blocks to maintain 10-minute block time
- Mining profitability depends on hash rate, electricity cost, and BTC price
- 51% attacks are economically infeasible for large PoW chains
- Block rewards halve every 4 years, shifting incentives toward fees
- Energy consumption is significant but incentivizes renewable energy

Core Insight: Proof-of-work converts energy into cryptographic security. The cost of attacking equals cumulative computational work by honest miners.

(c) Joerg Osterrieder 2025

Discussion Questions

1. Why is proof-of-work described as “progress-free”?
2. How does difficulty adjustment make Bitcoin resilient to hash rate fluctuations?
3. What would happen if block rewards fell to zero but fees remained low?
4. Is ASIC mining centralization a threat to Bitcoin’s decentralization?
5. How does mining pool concentration differ from miner concentration?
6. Can proof-of-work be justified from an environmental perspective?

Next Lesson Preview: L08 Lab - Wallet Setup

Lab activities:

- Install and configure MetaMask wallet
- Understand seed phrase security and backup
- Connect to Ethereum testnet (Sepolia)
- Obtain testnet ETH from faucets
- Execute first testnet transaction

Preparation:

- Install a modern web browser (Chrome, Firefox, Brave)
- Review public-private key concepts from Lesson 5
- Prepare a secure location for seed phrase backup

Quiz Questions (1/4)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks
Answer: B – Every 2,016 blocks (approximately 2 weeks at 10-minute block times).

Q3. What happens when a miner exhausts all 4.3 billion nonce values?
A) Mining fails B) Modify coinbase transaction (extra nonce) C) Restart blockchain D) Wait for next block
Answer: B – Miners modify the coinbase transaction's extra nonce field and recompute the Merkle root.

Q4. Which property makes PoW "progress-free"?
A) Past failed attempts help future attempts B) Each hash attempt is independent C) Mining gets easier over time D) Blocks build on each other
Answer: B – Each hash attempt is independent; previous failures provide no advantage for future attempts.

Q5. What is Bitcoin's current block reward after the 2024 halving?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – The April 2024 halving reduced the block subsidy from 6.25 to 3.125 BTC.

Quiz Questions (2/4)

Q6. How often does Bitcoin's block reward halve?
A) Every year B) Every 2 years C) Every 4 years (210,000 blocks) D) Every 10 years
Answer: C – The halving occurs every 210,000 blocks, approximately every 4 years.

Q7. Which hash algorithm does Bitcoin use for proof-of-work?
A) SHA-1 B) MD5 C) SHA-256 (double) D) Scrypt
Answer: C – Bitcoin uses double SHA-256: SHA-256(SHA-256(block_header)).

Q8. What percentage of network hash rate is theoretically needed for a 51% attack?
A) 25% B) 33% C) 51% D) 75%
Answer: C – More than 50% of hash rate allows an attacker to outpace the honest chain.

Q9. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions D) Decrypt encrypted wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures or create invalid coins.

Q10. Which mining hardware generation is most efficient for Bitcoin?
A) CPUs B) GPUs C) FPGAs D) ASICs
Answer: D – ASICs (Application-Specific Integrated Circuits) are purpose-built for SHA-256 mining with highest efficiency.

Quiz Questions (3/4)

Q11. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income through variance reduction D) Avoid difficulty adjustment
Answer: C – Pools reduce variance by distributing rewards proportionally to contributed hash rate.

Q12. If Bitcoin's hash rate doubles but block time remains 10 minutes, what happened?
A) Network failure B) Difficulty increased proportionally C) Miners got faster D) Block reward doubled
Answer: B – Difficulty adjusts every 2,016 blocks to maintain 10-minute average block times.

Q13. Approximately how much energy does Bitcoin mining consume annually?
A) Same as Ireland B) Same as Argentina C) Same as USA D) Same as Luxembourg
Answer: B – Bitcoin consumes approximately 140-150 TWh/year, comparable to Argentina's consumption.

Q14. What is the maximum clamping factor for Bitcoin difficulty adjustment?
A) 2x B) 4x C) 8x D) No limit
Answer: B – Difficulty can only change by factor of 4 maximum (either up or down) per adjustment period.

Q15. Which payout scheme pays miners a fixed amount per share submitted?
A) PPLNS B) PPS C) PROP D) SOLO
Answer: B – PPS (Pay Per Share) provides predictable income regardless of pool luck.

Quiz Questions (4/4)

Q16. What is the Bitcoin block header size?
A) 80 bytes B) 256 bytes C) 1 KB D) 1 MB
Answer: A – The block header is exactly 80 bytes (version, prev hash, merkle root, timestamp, difficulty, nonce).

Q17. What year will Bitcoin's final block reward halving occur (approximately)?
A) 2040 B) 2100 C) 2140 D) 2256
Answer: C – Around 2140, when the block subsidy becomes negligible (less than 1 satoshi).

Q18. Which cryptocurrency was designed to be ASIC-resistant using RandomX?
A) Bitcoin B) Litecoin C) Ethereum D) Monero
Answer: D – Monero uses RandomX, a CPU-optimized algorithm designed to resist ASIC mining.

Q19. What is the typical mining pool fee?
A) 0.1-0.5% B) 1-3% C) 5-10% D) 15-20%
Answer: B – Most pools charge 1-3% fees for coordinating mining and distributing rewards.

Q20. Why does increasing hash rate NOT increase your chance of finding the next block?
A) It does increase your chance B) Network difficulty adjusts automatically C) Pool fees increase D) Block time is fixed
Answer: B – While individual hash rate increases help, network difficulty adjusts to maintain constant block times globally.

Proof of Work Consensus

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Mining rig vs gaming setup

[COMIC: A split scene showing a gamer frustrated that his RTX 4090 can't compete with industrial mining rigs filling a warehouse, while his friend brags about mining Bitcoin "back when GPUs worked"]

The Evolution of Mining Hardware

- From CPU mining to GPU farms to purpose-built ASICs
- Why your gaming rig is 10,000x too slow for Bitcoin
- The arms race that transformed hobby mining into industrial operations

The jump from CPUs to ASICs represents a 10-million-fold efficiency improvement

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the proof-of-work consensus mechanism
- Describe the mining process and nonce searching
- Explain difficulty adjustment and its purpose
- Calculate mining profitability and hash rate economics
- Recognize the security guarantees and vulnerabilities of PoW
- Evaluate the 51% attack threat model
- Discuss energy consumption and environmental impact

Building on L06: Bitcoin Protocol

The Problem: How do we make attacks economically irrational?

The Challenge
In a decentralized network, anyone can participate. How do we make attacks so expensive that honest behavior becomes the dominant strategy? Without economic skin-in-the-game, attackers could cheaply rewrite history and steal coins.

Why It Matters

- Without attack costs $>$ potential profit, no double-spend security
- Historical: GHash.IO mining pool reached 55% in 2014, threatening Bitcoin's security assumptions

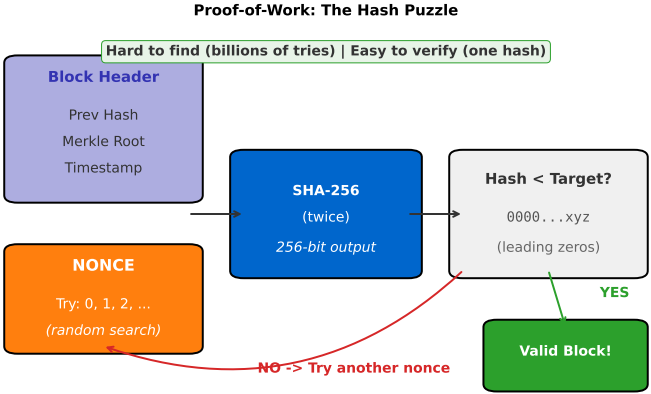
Today's lesson: How Proof of Work addresses this challenge

What We Need

- Economic alignment of actors
- Attack cost must exceed potential profit from double-spending
- Security that scales with network value

The Cryptoeconomics Question
Aligning individual and collective interests

What is Proof of Work?



Core Concept: Find a nonce such that the hash of block header is below the target. No shortcut: must try nonces randomly until one works.

→ **Problem: How do we make attacks economically... — What is Proof of Work? PoW transforms computational work into unforgeable proof of resource expenditure**

What Makes Proof-of-Work Secure?

Key Properties:

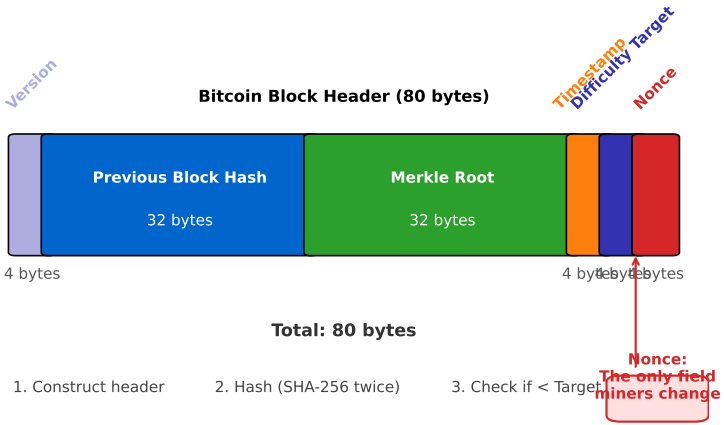
1. **Asymmetry:** Hard to find, easy to verify
2. **Probabilistic:** Expected time to find solution, no guarantee
3. **Adjustable difficulty:** Target changes to maintain block time
4. **Progress-free:** Past attempts do not help future attempts

Mathematical Formulation:

$$\text{SHA-256}(\text{SHA-256}(\text{BlockHeader})) < \text{Target}$$

Analogy: Rolling dice until you get 10 sixes in a row. Each roll is independent. Expected number of attempts: 6^{10}. Verification: just look at the result.

What Does a Bitcoin Block Header Contain?



Mining Process: Construct block → Set timestamp/difficulty → Try nonces → If hash $<$ target: success, else repeat.

What Happens When All Nonces Are Exhausted?

Nonce Space Exhaustion:

- 4 bytes = 2^{32} = 4.3B possible nonces
- Modern ASICs exhaust this in milliseconds
- Solution: extra nonce trick

Extra Nonce Trick:

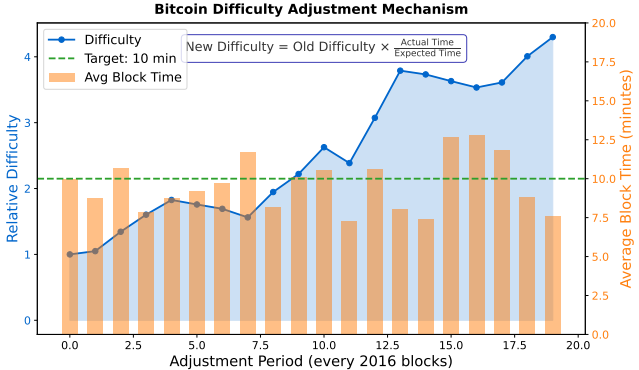
- Modify coinbase transaction (extra nonce field)
- Recompute Merkle root per extra nonce
- Expands search space beyond 2^{32}

Merkle Trees (Reminder):
Binary tree: each leaf is a tx hash, each parent is hash of children.

- Commit to all txs with single 32-byte root
- Tree height: $\log_2(n)$ for n transactions
- Proof: $\log_2(n)$ hashes for inclusion
- 1000 txs $\rightarrow$ 10 hashes ($\sim$320 bytes)

$\rightarrow$ Problem: How do we make attacks economically... — Nonce Space and Extra Nonce: The nonce search ensures miners cannot shortcut the computational work required for block creation

How Does Bitcoin Maintain 10-Minute Blocks?



Adjustment Rule (Every 2016 Blocks):

$$\text{New Target} = \text{Old Target} \times \frac{\text{Actual Time}}{\text{Expected Time (20,160 min)}}$$

Clamped to $[T/4, T \times 4]$ to prevent extreme changes.

How Likely Are You to Find a Block?

Hash Rate:

- Hashes computed per second
- Laptop $\approx$ 10 MH/s; ASIC $\approx$ 100 TH/s
- Bitcoin network (Dec 2024): $\sim$1,200 EH/s

Mining Probability:

$$P(\text{find block}) = \frac{\text{Your Hash Rate}}{\text{Network Hash Rate}}$$

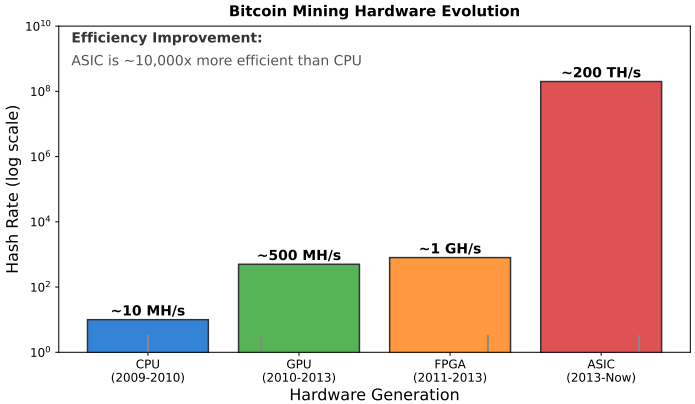
Example:

- Miner: 100 TH/s, Network: 500 EH/s
- Probability: 0.00002%
- Expected: $\sim$100 years solo mining
- Solution: Join mining pools

Unit Scale:
K=10^3, M=10^6, G=10^9, T=10^{12}, P=10^{15}, E=10^{18}

Solo mining is a lottery; pools provide steady, proportional income

How Has Mining Hardware Changed Over Time?



Implications: Mining centralization, high barrier to entry, geographic concentration in low-electricity regions.

Problem Check-In: Hash Power Distribution

Recall Our Problem

How do we make attacks economically irrational?

What We've Learned So Far

- PoW requires miners to find a nonce producing a hash below the difficulty target
- Mining probability equals your hash rate divided by total network hash rate
- Energy expenditure creates unforgeable real-world cost, making attacks economically irrational

Still to Address

- Security economics: attack cost vs potential profit analysis
- How do we balance security with energy efficiency?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we make attacks economically..."?

Is Bitcoin Mining Profitable?

Revenue Formula:

$$\text{Daily Revenue} = \frac{\text{Hash Rate}}{\text{Network Hash Rate}} \times 144 \times (\text{Reward} + \text{Fees})$$

Example (Antminer S19 Pro):

- Hash rate: 110 TH/s, Power: 3250 W
- Electricity: \$0.05/kWh $\times$ 78 = \$3.90/day
- Revenue (@\$40k BTC): $\sim$\$7.92/day
- Profit: \$4.02/day, Payback: $\sim$2 years

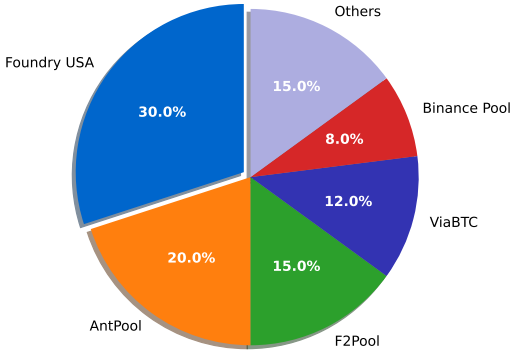
Risk Factors:

- BTC price volatility
- Difficulty increases over time
- Hardware obsolescence (2–3 year cycle)
- Electricity cost changes

Mining economics ensure honest behavior is more profitable than attacking the network

Why Do Miners Join Pools?

Bitcoin Mining Pool Distribution (2024)



Top 5 pools control ~85% of hash rate

(Miners can switch pools - pools do not own hardware)

Payout Schemes: PPS (fixed/share), PPLNS (share recent blocks), FPPS (PPS + fees).

How Do Mining Pools Work?

Why Pools Exist:

- Solo: high variance (years for a block)
- Pooled: steady income (proportional)

Pool Operation:

1. Coordinator distributes tasks (shares)
2. Miners submit partial solutions
3. Pool tracks each miner's contribution
4. Block found $\rightarrow$ reward split proportionally
5. Pool takes 1-3% fee

Centralization Concern:

- Pools don't own hardware (miners can switch)
- Mitigation: P2Pool, Stratum V2

Pools reduce variance but concentrate block production authority

How Do Block Rewards Change Over Time?

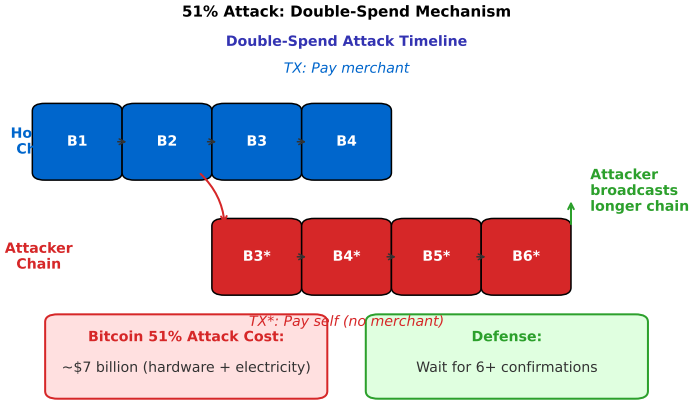
Block Reward Components:

$$\text{Total Reward} = \text{Block Subsidy} + \text{Transaction Fees}$$

Period	Reward	Cumulative Supply
2009-2012	50 BTC	10.5M BTC
2012-2016	25 BTC	15.75M BTC
2016-2020	12.5 BTC	18.375M BTC
2020-2024	6.25 BTC	19.6875M BTC
2024-2028 (current)	3.125 BTC	20.34M BTC

Future: Transaction fees must eventually sustain mining as block subsidy approaches zero ($\sim$2140).

What Can an Attacker with 51% Hash Rate Do?



CAN do: Double-spend, censor transactions.
CANNOT do: Steal coins without keys, create coins out of thin air.

→ **Problem: How do we make attacks economically... — The 51% Attack: Attack cost analysis demonstrates why PoW makes cheating economically irrational**

How Much Does a 51% Attack Cost?

Cost of Attack (Bitcoin):

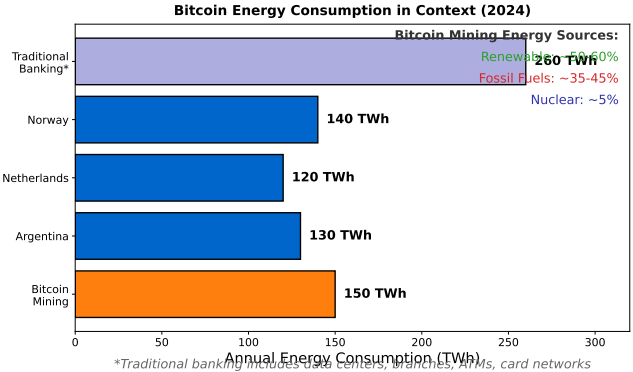
- Need 255 EH/s (>50% of network)
- Hardware: ∼2.3 million ASICs = $6.9 billion
- Electricity (1 week): ∼$63 million
- Total: ∼$7 billion

Consequences:

- Attack becomes public immediately
- Bitcoin price crashes (attacker's hardware worthless)
- Community may hard fork (bricks attacker's ASICs)

Vulnerable Chains: Small PoW chains, shared mining algorithms. Historical: Bitcoin Gold, Ethereum Classic, Verge.

How Much Energy Does Proof of Work Use?



Counterarguments: Incentivizes renewable development, facilitates grid balancing, security proportional to value.

Can We Make Mining More Accessible?

ASIC-Resistant Algorithms:

- **Scrypt (Litecoin):** Memory-hard hashing (ASICs developed 2014)
- **Ethash (Ethereum pre-merge):** Memory-hard with large DAG
- **RandomX (Monero):** CPU-optimized, frequently updated

Trade-offs:

- ASIC resistance $\rightarrow$ lower security per watt
- Easier for botnets to attack (commodity hardware)
- Algorithm changes create hard fork risks
- Debate: specialization increases security investment

ASIC resistance democratizes mining but may reduce overall network security

Problem Solved? Proof of Work

The Original Problem

How do we make attacks economically irrational?

How Proof of Work Solves It

- Mining requires real-world energy expenditure (150 TWh/year for Bitcoin)
- Difficulty adjustment maintains 10-minute blocks regardless of hash rate
- Attack cost: $7 billion in hardware + $63 million/week in electricity (Bitcoin)

Remaining Limitations

- Energy consumption equivalent to Argentina's annual usage
- Mining pool centralization (top 4 pools >50% of hash rate)
- Geographic concentration in low-electricity regions (China, Kazakhstan, USA)

Open Questions

- Is PoW's energy use justified by its security guarantees?
- Risk: What happens when block rewards approach zero and fees remain low?

Proof of Work partially solves attack rationality but introduces energy and centralization trade-offs

(c) Joerg Osterrieder 2025

The Economics of Hash Power Distribution

Incentive Structure

- **Core Problem:** Aligning individual and collective interests
- **Why act honestly?** Rewards for honest behavior, penalties for cheating
- **Value Flow:** Protocol gains security, participants earn rewards

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Protocol gains security, participants earn rewards

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Hash Power Distribution

Alternatives Considered

1. **Chosen Design:** Reward curves, slashing conditions
2. **Alternative:** Alternative reward mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Hash Power Distribution

Critical Failure Mode

- **What breaks:** Incentive misalignment, free-rider problems
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Difficulty adjustment whack-a-mole

[COMIC: Bitcoin protocol as a carnival whack-a-mole operator, constantly adjusting the mole pop-up speed as more and more miners (shown as giant hammers) crowd around the game]

The Self-Regulating System

- Every 2016 blocks, difficulty recalibrates to target 10-minute blocks
- More miners join? Difficulty increases. Miners leave? Difficulty decreases
- The only constant: blocks keep coming every 10 minutes (on average)

Difficulty has increased 50+ trillion times since Bitcoin's launch in 2009

Key Takeaways

- Proof-of-work provides Sybil resistance via computational cost
- Mining searches for nonces to produce valid block hashes
- Difficulty adjusts every 2016 blocks to maintain 10-minute block time
- Mining profitability depends on hash rate, electricity cost, and BTC price
- 51% attacks are economically infeasible for large PoW chains
- Block rewards halve every 4 years, shifting incentives toward fees
- Energy consumption is significant but incentivizes renewable energy

Core Insight: Proof-of-work converts energy into cryptographic security. The cost of attacking equals cumulative computational work by honest miners.

Next Lesson: L08 – Lab: Wallet Setup

Discussion Questions

1. Why is proof-of-work described as “progress-free”?
2. How does difficulty adjustment make Bitcoin resilient to hash rate fluctuations?
3. What would happen if block rewards fell to zero but fees remained low?
4. Is ASIC mining centralization a threat to Bitcoin’s decentralization?
5. How does mining pool concentration differ from miner concentration?
6. Can proof-of-work be justified from an environmental perspective?

Next Lesson Preview: L08 Lab - Wallet Setup

Lab activities:

- Install and configure MetaMask wallet
- Understand seed phrase security and backup
- Connect to Ethereum testnet (Sepolia)
- Obtain testnet ETH from faucets
- Execute first testnet transaction

Preparation:

- Install a modern web browser (Chrome, Firefox, Brave)
- Review public-private key concepts from Lesson 5
- Prepare a secure location for seed phrase backup

Quiz Questions (1/4)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks
Answer: B – Every 2,016 blocks (approximately 2 weeks at 10-minute block times).

Q3. What happens when a miner exhausts all 4.3 billion nonce values?
A) Mining fails B) Modify coinbase transaction (extra nonce) C) Restart blockchain D) Wait for next block
Answer: B – Miners modify the coinbase transaction's extra nonce field and recompute the Merkle root.

Q4. Which property makes PoW "progress-free"?
A) Past failed attempts help future attempts B) Each hash attempt is independent C) Mining gets easier over time D) Blocks build on each other
Answer: B – Each hash attempt is independent; previous failures provide no advantage for future attempts.

Q5. What is Bitcoin's current block reward after the 2024 halving?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – The April 2024 halving reduced the block subsidy from 6.25 to 3.125 BTC.

Quiz Questions (2/4)

Q6. How often does Bitcoin's block reward halve?
A) Every year B) Every 2 years C) Every 4 years (210,000 blocks) D) Every 10 years
Answer: C – The halving occurs every 210,000 blocks, approximately every 4 years.

Q7. Which hash algorithm does Bitcoin use for proof-of-work?
A) SHA-1 B) MD5 C) SHA-256 (double) D) Scrypt
Answer: C – Bitcoin uses double SHA-256: SHA-256(SHA-256(block_header)).

Q8. What percentage of network hash rate is theoretically needed for a 51% attack?
A) 25% B) 33% C) 51% D) 75%
Answer: C – More than 50% of hash rate allows an attacker to outpace the honest chain.

Q9. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions D) Decrypt encrypted wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures or create invalid coins.

Q10. Which mining hardware generation is most efficient for Bitcoin?
A) CPUs B) GPUs C) FPGAs D) ASICs
Answer: D – ASICs (Application-Specific Integrated Circuits) are purpose-built for SHA-256 mining with highest efficiency.

Quiz Questions (3/4)

Q11. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income through variance reduction D) Avoid difficulty adjustment
Answer: C – Pools reduce variance by distributing rewards proportionally to contributed hash rate.

Q12. If Bitcoin's hash rate doubles but block time remains 10 minutes, what happened?
A) Network failure B) Difficulty increased proportionally C) Miners got faster D) Block reward doubled
Answer: B – Difficulty adjusts every 2,016 blocks to maintain 10-minute average block times.

Q13. Approximately how much energy does Bitcoin mining consume annually?
A) Same as Ireland B) Same as Argentina C) Same as USA D) Same as Luxembourg
Answer: B – Bitcoin consumes approximately 140-150 TWh/year, comparable to Argentina's consumption.

Q14. What is the maximum clamping factor for Bitcoin difficulty adjustment?
A) 2x B) 4x C) 8x D) No limit
Answer: B – Difficulty can only change by factor of 4 maximum (either up or down) per adjustment period.

Q15. Which payout scheme pays miners a fixed amount per share submitted?
A) PPLNS B) PPS C) PROP D) SOLO
Answer: B – PPS (Pay Per Share) provides predictable income regardless of pool luck.

Quiz Questions (4/4)

Q16. What is the Bitcoin block header size?
A) 80 bytes B) 256 bytes C) 1 KB D) 1 MB
Answer: A – The block header is exactly 80 bytes (version, prev hash, merkle root, timestamp, difficulty, nonce).

Q17. What year will Bitcoin's final block reward halving occur (approximately)?
A) 2040 B) 2100 C) 2140 D) 2256
Answer: C – Around 2140, when the block subsidy becomes negligible (less than 1 satoshi).

Q18. Which cryptocurrency was designed to be ASIC-resistant using RandomX?
A) Bitcoin B) Litecoin C) Ethereum D) Monero
Answer: D – Monero uses RandomX, a CPU-optimized algorithm designed to resist ASIC mining.

Q19. What is the typical mining pool fee?
A) 0.1-0.5% B) 1-3% C) 5-10% D) 15-20%
Answer: B – Most pools charge 1-3% fees for coordinating mining and distributing rewards.

Q20. Why does increasing hash rate NOT increase your chance of finding the next block?
A) It does increase your chance B) Network difficulty adjusts automatically C) Pool fees increase D) Block time is fixed
Answer: B – While individual hash rate increases help, network difficulty adjusts to maintain constant block times globally.

L07: Proof of Work Consensus

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

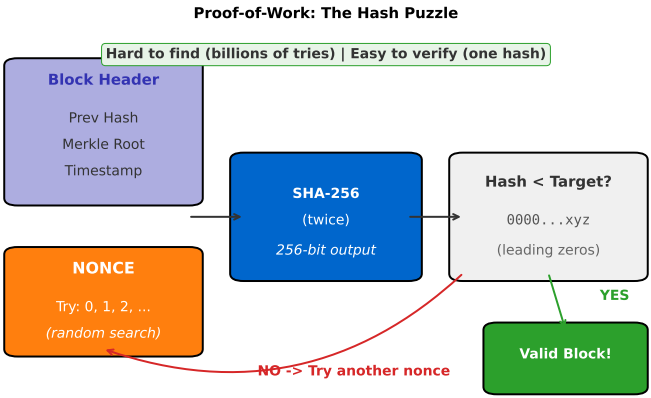
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

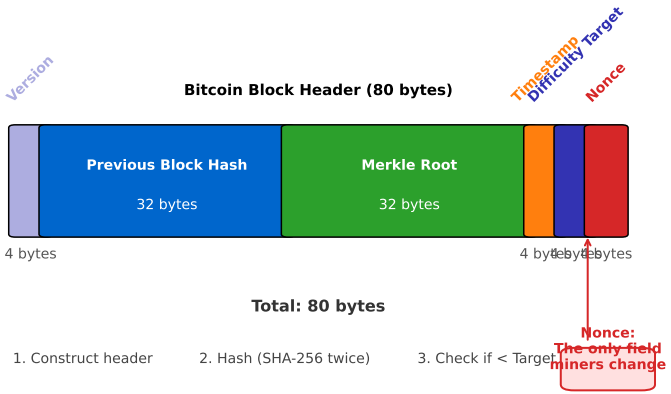
- Explain the proof-of-work consensus mechanism
- Describe mining and difficulty adjustment
- Analyze 51% attack economics
- Evaluate energy consumption trade-offs

What is Proof of Work?



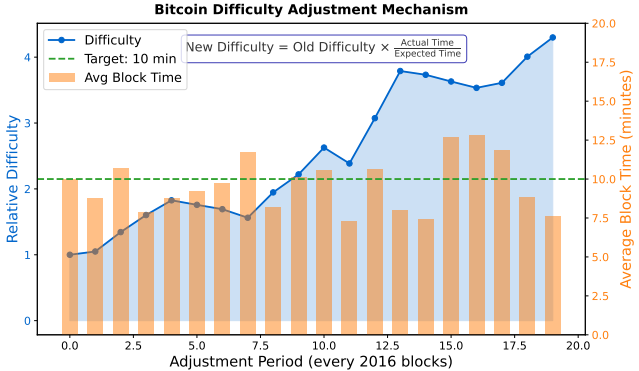
Core Concept: Find nonce where hash of block header is below target. No shortcut – must try nonces randomly.

Bitcoin Block Header Structure



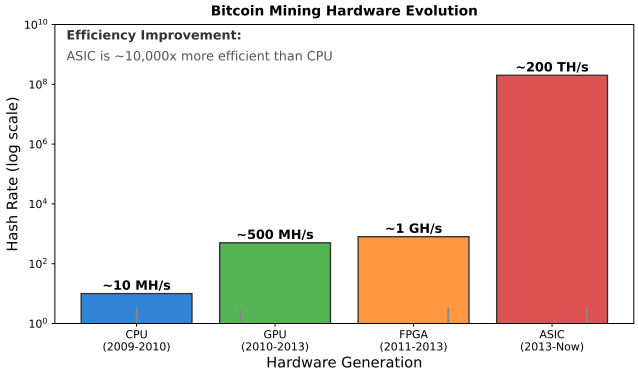
Mining: Construct block → Try nonces → If hash $<$ target: success, else repeat.

Difficulty Adjustment



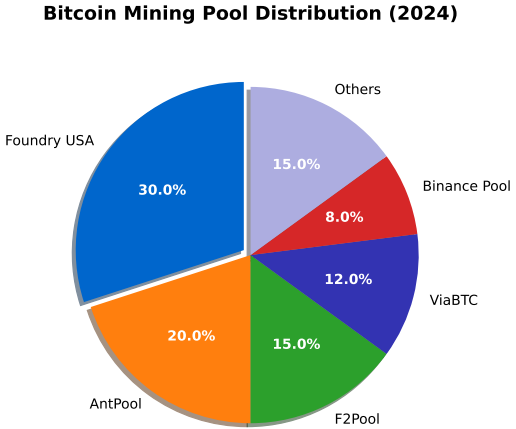
Every 2016 blocks: New Target = Old Target × (Actual Time / Expected Time).
Clamped to ±4x to prevent extreme changes.

Mining Hardware Evolution



Implications: Mining centralization, high barrier to entry, geographic concentration in low-electricity regions.

Mining Pools: Variance Reduction

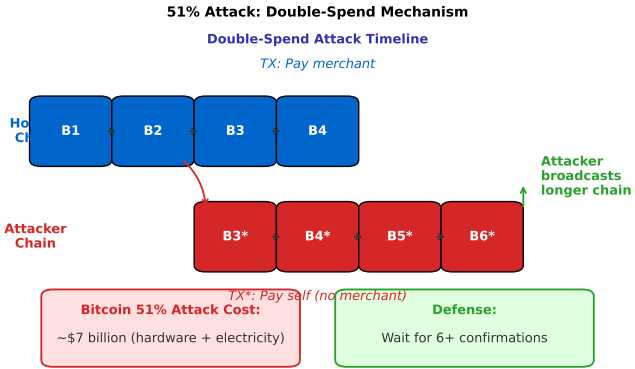


Top 5 pools control ~85% of hash rate

(Miners can switch pools - pools do not own hardware)

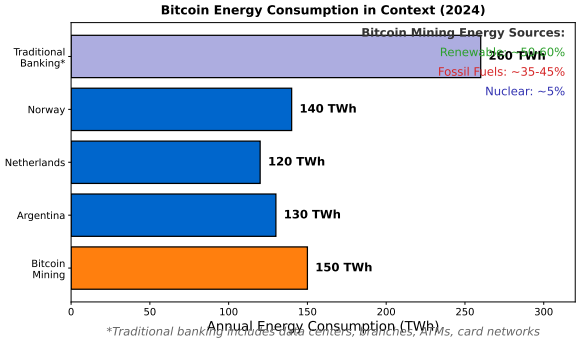
Why Pools: Solo mining has high variance (years between blocks). Pools provide steady income proportional to hash rate contribution.

The 51% Attack



CAN do: Double-spend, censor transactions.
CANNOT do: Steal coins without keys, create coins from nothing.
Bitcoin attack cost: ∼$7 billion (economically infeasible).

Energy Consumption: The Trade-off



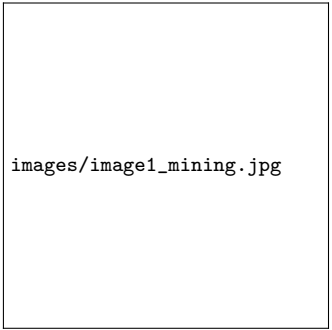
Counterarguments: Incentivizes renewable development, enables grid balancing, security proportional to value secured.

Key Takeaways

1. **PoW:** Provides Sybil resistance via computational cost
2. **Mining:** Search for nonces producing valid block hashes
3. **Difficulty:** Adjusts every 2016 blocks to maintain 10-min block time
4. **Block Reward:** 3.125 BTC (since April 2024 halving), halves every 4 years
5. **51% Attacks:** Economically infeasible for large PoW chains

Core Insight: Proof-of-work converts energy into cryptographic security. The cost of attacking equals cumulative work by honest miners.

Proof of Work in Practice



Bitcoin Mining

ASIC Hardware

Mining Datacenter

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify miner C) Vary header to find valid hash D) Encrypt block

Quiz (1/2)

Q1. What is the purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify miner C) Vary header to find valid hash D) Encrypt block
Answer: C – Nonce is incremented to produce different hash outputs.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 B) 2,016 C) 4,032 D) 10,000

Quiz (1/2)

Q1. What is the purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify miner C) Vary header to find valid hash D) Encrypt block
Answer: C – Nonce is incremented to produce different hash outputs.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 B) 2,016 C) 4,032 D) 10,000
Answer: B – Every 2,016 blocks (approximately 2 weeks).

Q3. What is Bitcoin's current block reward (post-2024 halving)?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC

Quiz (1/2)

Q1. What is the purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify miner C) Vary header to find valid hash D) Encrypt block
Answer: C – Nonce is incremented to produce different hash outputs.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 B) 2,016 C) 4,032 D) 10,000
Answer: B – Every 2,016 blocks (approximately 2 weeks).

Q3. What is Bitcoin's current block reward (post-2024 halving)?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – April 2024 halving reduced reward to 3.125 BTC.

Q4. What CAN an attacker with 51% hash rate do?
A) Steal coins without keys B) Create unlimited coins C) Double-spend their own tx D) Decrypt wallets

Quiz (1/2)

Q1. What is the purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify miner C) Vary header to find valid hash D) Encrypt block
Answer: C – Nonce is incremented to produce different hash outputs.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 B) 2,016 C) 4,032 D) 10,000
Answer: B – Every 2,016 blocks (approximately 2 weeks).

Q3. What is Bitcoin's current block reward (post-2024 halving)?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – April 2024 halving reduced reward to 3.125 BTC.

Q4. What CAN an attacker with 51% hash rate do?
A) Steal coins without keys B) Create unlimited coins C) Double-spend their own tx D) Decrypt wallets
Answer: C – Can double-spend but cannot break cryptographic signatures.

Q5. Which mining hardware is most efficient for Bitcoin?
A) CPUs B) GPUs C) FPGAs D) ASICs

Quiz (1/2)

Q1. What is the purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify miner C) Vary header to find valid hash D) Encrypt block
Answer: C – Nonce is incremented to produce different hash outputs.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 B) 2,016 C) 4,032 D) 10,000
Answer: B – Every 2,016 blocks (approximately 2 weeks).

Q3. What is Bitcoin's current block reward (post-2024 halving)?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – April 2024 halving reduced reward to 3.125 BTC.

Q4. What CAN an attacker with 51% hash rate do?
A) Steal coins without keys B) Create unlimited coins C) Double-spend their own tx D) Decrypt wallets
Answer: C – Can double-spend but cannot break cryptographic signatures.

Q5. Which mining hardware is most efficient for Bitcoin?
A) CPUs B) GPUs C) FPGAs D) ASICs
Answer: D – ASICs are purpose-built for SHA-256 mining.

Quiz (2/2)

Q6. Why do mining pools exist?
A) Centralize control B) Reduce electricity C) Provide steady income via variance reduction D) Avoid difficulty

Quiz (2/2)

Q6. Why do mining pools exist?
A) Centralize control B) Reduce electricity C) Provide steady income via variance reduction D) Avoid difficulty
Answer: C – Pools reduce variance by distributing rewards proportionally.

Q7. Which hash algorithm does Bitcoin use?
A) SHA-1 B) MD5 C) Double SHA-256 D) Scrypt

Quiz (2/2)

Q6. Why do mining pools exist?
A) Centralize control B) Reduce electricity C) Provide steady income via variance reduction D) Avoid difficulty
Answer: C – Pools reduce variance by distributing rewards proportionally.

Q7. Which hash algorithm does Bitcoin use?
A) SHA-1 B) MD5 C) Double SHA-256 D) Scrypt
Answer: C – SHA-256(SHA-256(block_header)).

Q8. When will Bitcoin's final halving occur (approximately)?
A) 2040 B) 2100 C) 2140 D) 2256

Quiz (2/2)

Q6. Why do mining pools exist?
A) Centralize control B) Reduce electricity C) Provide steady income via variance reduction D) Avoid difficulty
Answer: C – Pools reduce variance by distributing rewards proportionally.

Q7. Which hash algorithm does Bitcoin use?
A) SHA-1 B) MD5 C) Double SHA-256 D) Scrypt
Answer: C – SHA-256(SHA-256(block_header)).

Q8. When will Bitcoin's final halving occur (approximately)?
A) 2040 B) 2100 C) 2140 D) 2256
Answer: C – Around 2140 when block subsidy becomes negligible.

Q9. What is the Bitcoin block header size?
A) 80 bytes B) 256 bytes C) 1 KB D) 1 MB

Quiz (2/2)

Q6. Why do mining pools exist?
A) Centralize control B) Reduce electricity C) Provide steady income via variance reduction D) Avoid difficulty
Answer: C – Pools reduce variance by distributing rewards proportionally.

Q7. Which hash algorithm does Bitcoin use?
A) SHA-1 B) MD5 C) Double SHA-256 D) Scrypt
Answer: C – SHA-256(SHA-256(block_header)).

Q8. When will Bitcoin's final halving occur (approximately)?
A) 2040 B) 2100 C) 2140 D) 2256
Answer: C – Around 2140 when block subsidy becomes negligible.

Q9. What is the Bitcoin block header size?
A) 80 bytes B) 256 bytes C) 1 KB D) 1 MB
Answer: A – Exactly 80 bytes (version, prev hash, merkle root, timestamp, difficulty, nonce).

Q10. Which property makes PoW "progress-free"?
A) Past attempts help future B) Each attempt is independent C) Mining gets easier D) Blocks build up

Quiz (2/2)

Q6. Why do mining pools exist?
A) Centralize control B) Reduce electricity C) Provide steady income via variance reduction D) Avoid difficulty
Answer: C – Pools reduce variance by distributing rewards proportionally.

Q7. Which hash algorithm does Bitcoin use?
A) SHA-1 B) MD5 C) Double SHA-256 D) Scrypt
Answer: C – SHA-256(SHA-256(block_header)).

Q8. When will Bitcoin's final halving occur (approximately)?
A) 2040 B) 2100 C) 2140 D) 2256
Answer: C – Around 2140 when block subsidy becomes negligible.

Q9. What is the Bitcoin block header size?
A) 80 bytes B) 256 bytes C) 1 KB D) 1 MB
Answer: A – Exactly 80 bytes (version, prev hash, merkle root, timestamp, difficulty, nonce).

Q10. Which property makes PoW "progress-free"?
A) Past attempts help future B) Each attempt is independent C) Mining gets easier D) Blocks build up
Answer: B – Each hash attempt is independent; no advantage from failures.

Thank you

Questions?

Next: L08 Lab – Wallet Setup

Quiz: Proof of Work

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents

Quiz (1–5)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks

Quiz (1–5)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks
Answer: B – Every 2,016 blocks (approximately 2 weeks at 10-minute block times).

Q3. Which property makes PoW "progress-free"?
A) Past attempts help future attempts B) Each hash attempt is independent C) Mining gets easier over time
D) Blocks build on each other

Quiz (1–5)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks
Answer: B – Every 2,016 blocks (approximately 2 weeks at 10-minute block times).

Q3. Which property makes PoW "progress-free"?
A) Past attempts help future attempts B) Each hash attempt is independent C) Mining gets easier over time D) Blocks build on each other
Answer: B – Each hash attempt is independent; previous failures provide no advantage.

Q4. What is Bitcoin's current block reward after the 2024 halving?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC

Quiz (1–5)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks
Answer: B – Every 2,016 blocks (approximately 2 weeks at 10-minute block times).

Q3. Which property makes PoW "progress-free"?
A) Past attempts help future attempts B) Each hash attempt is independent C) Mining gets easier over time D) Blocks build on each other
Answer: B – Each hash attempt is independent; previous failures provide no advantage.

Q4. What is Bitcoin's current block reward after the 2024 halving?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – The April 2024 halving reduced the block subsidy from 6.25 to 3.125 BTC.

Q5. Which mining hardware generation is most efficient for Bitcoin?
A) CPUs B) GPUs C) FPGAs D) ASICs

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of the nonce in Bitcoin mining?
A) Store transaction data B) Identify the miner C) Vary block header to find valid hash D) Encrypt block contents
Answer: C – The nonce is incremented to produce different hash outputs until one meets the target difficulty.

Q2. Bitcoin's difficulty adjustment occurs every how many blocks?
A) 1,008 blocks B) 2,016 blocks C) 4,032 blocks D) 10,000 blocks
Answer: B – Every 2,016 blocks (approximately 2 weeks at 10-minute block times).

Q3. Which property makes PoW "progress-free"?
A) Past attempts help future attempts B) Each hash attempt is independent C) Mining gets easier over time
D) Blocks build on each other
Answer: B – Each hash attempt is independent; previous failures provide no advantage.

Q4. What is Bitcoin's current block reward after the 2024 halving?
A) 6.25 BTC B) 3.125 BTC C) 1.5625 BTC D) 12.5 BTC
Answer: B – The April 2024 halving reduced the block subsidy from 6.25 to 3.125 BTC.

Q5. Which mining hardware generation is most efficient for Bitcoin?
A) CPUs B) GPUs C) FPGAs D) ASICs
Answer: D – ASICs are purpose-built for SHA-256 mining with highest efficiency.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What CAN an attacker with 51% hash rate do?

A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions

D) Decrypt wallets

Quiz (6–10)

Q6. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions
D) Decrypt wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures.

Q7. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income via variance reduction
D) Avoid difficulty adjustment

Quiz (6–10)

Q6. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions
D) Decrypt wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures.

Q7. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income via variance reduction
D) Avoid difficulty adjustment
Answer: C – Pools reduce variance by distributing rewards proportionally to contributed hash rate.

Q8. Approximately how much energy does Bitcoin mining consume annually?
A) Same as Ireland B) Same as Argentina C) Same as USA D) Same as Luxembourg

Quiz (6–10)

Q6. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions
D) Decrypt wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures.

Q7. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income via variance reduction
D) Avoid difficulty adjustment
Answer: C – Pools reduce variance by distributing rewards proportionally to contributed hash rate.

Q8. Approximately how much energy does Bitcoin mining consume annually?
A) Same as Ireland B) Same as Argentina C) Same as USA D) Same as Luxembourg
Answer: B – Bitcoin consumes approximately 140-150 TWh/year, comparable to Argentina.

Q9. What is the maximum clamping factor for Bitcoin difficulty adjustment?
A) 2x B) 4x C) 8x D) No limit

Quiz (6–10)

Q6. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions
D) Decrypt wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures.

Q7. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income via variance reduction
D) Avoid difficulty adjustment
Answer: C – Pools reduce variance by distributing rewards proportionally to contributed hash rate.

Q8. Approximately how much energy does Bitcoin mining consume annually?
A) Same as Ireland B) Same as Argentina C) Same as USA D) Same as Luxembourg
Answer: B – Bitcoin consumes approximately 140-150 TWh/year, comparable to Argentina.

Q9. What is the maximum clamping factor for Bitcoin difficulty adjustment?
A) 2x B) 4x C) 8x D) No limit
Answer: B – Difficulty can only change by factor of 4 maximum per adjustment period.

Q10. Which cryptocurrency uses RandomX for ASIC resistance?
A) Bitcoin B) Litecoin C) Ethereum D) Monero

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What CAN an attacker with 51% hash rate do?
A) Steal coins without private keys B) Create unlimited new coins C) Double-spend their own transactions
D) Decrypt wallets
Answer: C – They can double-spend by creating a longer chain, but cannot break cryptographic signatures.

Q7. What is the purpose of mining pools?
A) Centralize mining control B) Reduce electricity costs C) Provide steady income via variance reduction
D) Avoid difficulty adjustment
Answer: C – Pools reduce variance by distributing rewards proportionally to contributed hash rate.

Q8. Approximately how much energy does Bitcoin mining consume annually?
A) Same as Ireland B) Same as Argentina C) Same as USA D) Same as Luxembourg
Answer: B – Bitcoin consumes approximately 140-150 TWh/year, comparable to Argentina.

Q9. What is the maximum clamping factor for Bitcoin difficulty adjustment?
A) 2x B) 4x C) 8x D) No limit
Answer: B – Difficulty can only change by factor of 4 maximum per adjustment period.

Q10. Which cryptocurrency uses RandomX for ASIC resistance?
A) Bitcoin B) Litecoin C) Ethereum D) Monero
Answer: D – Monero uses RandomX, a CPU-optimized algorithm designed to resist ASIC mining.

(c) Joerg Osterrieder 2025

Lab Session: Wallet Setup and First Transaction

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Install and configure MetaMask wallet extension
- Explain seed phrase importance and backup procedures
- Connect to Ethereum testnets (Sepolia)
- Obtain testnet ETH from faucets
- Send and receive testnet transactions
- Apply security best practices for wallet protection

The Problem: Self-Custody in Digital Finance

The Challenge
Traditional banks hold your money and control access. How do you prove ownership and control digital assets without a trusted intermediary like a bank?

Why It Matters

- Bank failures can freeze or lose customer funds (e.g., Cyprus 2013, Silicon Valley Bank 2023)
- Centralized custody creates single points of failure and censorship risk

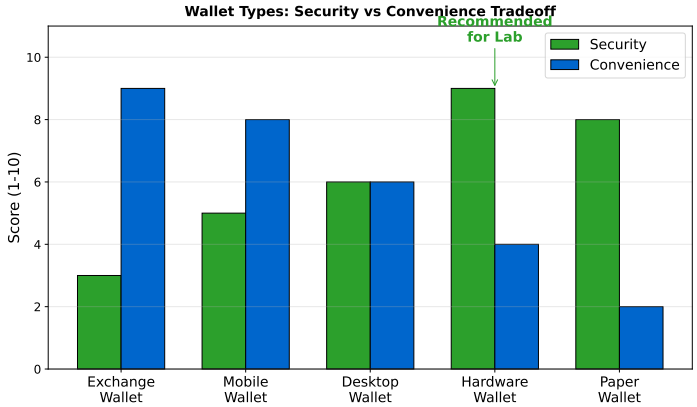
What We Need

- Cryptographic proof of ownership without intermediaries
- User-controlled key management system
- Secure backup mechanism for asset recovery

The Cryptoeconomics Question
How do private keys align economic incentives with security requirements?

Today's lab: Hands-on experience with self-custody wallet creation and key management

Wallet Types: Security vs Convenience



Hardware wallets offer best security; MetaMask provides good balance for learning

What is MetaMask?

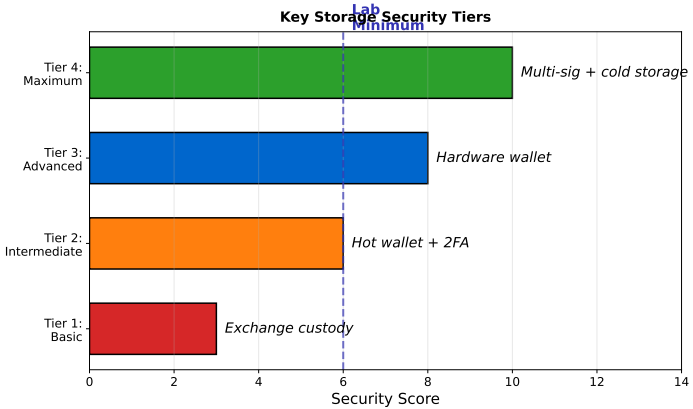
Overview:

- Browser extension and mobile app cryptocurrency wallet
- Supports Ethereum and EVM-compatible blockchains
- Non-custodial: you control private keys
- Most popular Ethereum wallet (30 million users)

Key Features:

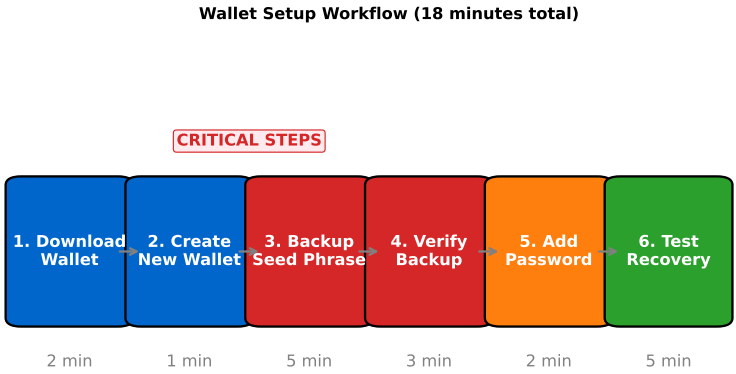
- Send and receive ETH and ERC-20 tokens
- Interact with decentralized applications (dApps)
- Multiple account management
- Network switching (Mainnet, testnets, custom networks)

Security Levels for Key Storage



For this lab, Tier 2 (hot wallet + 2FA) is the minimum acceptable level

Wallet Setup Workflow



Seed phrase backup (steps 3-4) is the most critical part of wallet setup

Exercise 1: Installing MetaMask

Installation Steps:

1. Visit official website: `https://metamask.io`
2. Click "Download" and select your browser
3. Install extension from official browser store
4. Pin extension to browser toolbar
5. Click MetaMask icon to launch setup wizard

Security Warning:

- Only install from official sources
- Beware of phishing sites (check URL carefully)
- Fake extensions exist in browser stores

Exercise 2: Creating Your Wallet

Setup Wizard Steps:

1. Click “Create a new wallet”
2. Set a strong password (8+ characters)
3. Reveal and record your 12-word seed phrase
4. Confirm seed phrase by selecting words in correct order

Critical: Seed Phrase vs. Password

- Seed phrase = master backup (recovers wallet on any device)
- Password = local device protection (cannot recover wallet)
- **Lose seed phrase -¿ lose wallet permanently**

Exercise 3: Adding Sepolia Testnet

Why Use Testnets?

- Practice without risking real money
- Free testnet ETH available from faucets
- Identical functionality to mainnet

Adding Sepolia Network:

1. Click network selector (top-right dropdown)
2. Settings -¿ Advanced -¿ Show test networks (enable)
3. Select “Sepolia test network”

Sepolia Faucets:

- Alchemy: `https://sepoliafaucet.com`
- Infura: `https://www.infura.io/faucet/sepolia`

Exercise 4: Sending Your First Transaction

Transaction Steps:

1. Ensure you have Sepolia ETH (from faucet)
2. Click "Send" button in MetaMask
3. Enter recipient address (create second account or use classmate's)
4. Enter amount (e.g., 0.1 Sepolia ETH)
5. Review transaction details (gas fee, total)
6. Click "Confirm"
7. View in Activity tab

Understanding Gas Fees:

- Fee = gas units $\times$ gas price (in gwei)
- Sepolia: fees are negligible (testnet)

Security Best Practices

Critical Security Rules:

1. **Seed Phrase:** Never share, never store digitally
2. **Phishing Protection:** Verify URLs, bookmark trusted sites
3. **Network Verification:** Confirm correct network before transacting
4. **Transaction Approval:** Review recipient and amounts carefully

Common Threats:

- Phishing websites requesting seed phrase
- Malicious dApps with unlimited token approvals
- Clipboard malware replacing copied addresses
- Fake support scams via DM

(c) Joerg Osterrieder 2025

Lab Deliverables

Submit the following:

1. **Screenshot Collection:**
   - MetaMask wallet showing Sepolia network
   - Transaction details from Activity tab
   - Etherscan transaction page (confirmed)
2. **Lab Report (1-2 pages):**
   - Your Sepolia address
   - Transaction hash of sent transaction
   - Reflection on seed phrase security

Submission Deadline: One week from lab session

Problem Solved? Self-Custody Trade-offs

The Original Problem

How to control digital assets without trusted intermediaries?

How Wallet Security Solves It

- Private keys provide cryptographic proof of ownership (ECDSA signatures)
- Seed phrases enable deterministic recovery across devices (BIP-39/HD wallets)
- Self-custody eliminates counterparty risk and censorship

Remaining Limitations

- User bears full responsibility for key security (no "forgot password" option)
- Lost seed phrase = permanent loss of funds (irreversible)
- Phishing and social engineering attacks target users directly

The Economic Trade-off

- Benefit: Full control, no intermediary fees, censorship resistance
- Cost: Security burden shifts to user (requires technical knowledge)

Self-custody solves intermediary risk but introduces user responsibility risk

(c) Joerg Osterrieder 2025

Key Takeaways

- MetaMask is a non-custodial wallet (you control private keys)
- Seed phrase is the master backup for all accounts
- Testnets provide safe environment for learning
- Gas fees vary by network congestion
- Blockchain transactions are irreversible
- Security requires vigilance against phishing and scams

(c) Joerg Osterrieder 2025

Quiz Questions - Part 1

Q1. What type of wallet is MetaMask?
A) Custodial wallet B) Non-custodial wallet C) Hardware wallet D) Paper wallet
Answer: B – MetaMask is non-custodial, meaning you control your private keys.

Q2. How many words are typically in a MetaMask seed phrase?
A) 6 words B) 12 words C) 24 words D) 32 words
Answer: B – MetaMask uses a 12-word seed phrase (BIP-39 standard).

Q3. What is the primary purpose of a seed phrase?
A) Login password B) Wallet recovery C) Transaction signing D) Network selection
Answer: B – Seed phrase is the master backup to recover your wallet on any device.

Q4. Which wallet type offers the highest security?
A) Mobile wallet B) Browser extension C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep private keys offline in secure hardware.

Q5. What happens if you lose your MetaMask password?
A) Wallet is lost forever B) Contact support C) Use seed phrase to recover D) Reset via email
Answer: C – Password is local; seed phrase recovers the wallet.

Quiz Questions - Part 2

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network identification D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. Can two people have the same Ethereum public address?
A) Yes, if on different networks B) Yes, addresses are reused C) No, addresses are unique D) Only on testnets
Answer: C – Addresses are cryptographically unique (collision probability negligible).

Q8. What is the purpose of using Sepolia testnet?
A) Faster transactions B) Lower fees C) Practice without risk D) Access exclusive dApps
Answer: C – Testnets allow safe practice with free testnet ETH.

Q9. How should you store your seed phrase?
A) Screenshot on phone B) Email to yourself C) Written on paper offline D) Cloud storage
Answer: C – Physical offline storage prevents digital theft or hacking.

Q10. What does "non-custodial" mean for wallets?
A) No fees B) You control keys C) Company holds keys D) No backups needed
Answer: B – Non-custodial means you (not a third party) control private keys.

Quiz Questions - Part 3

Q11. Which of these is a phishing attack vector?
A) Official MetaMask.io B) Fake site requesting seed phrase C) Hardware wallet D) Testnet faucets
Answer: B – Phishing sites impersonate legitimate services to steal seed phrases.

Q12. What is gas in Ethereum transactions?
A) Fuel for cars B) Computational work fee C) Token symbol D) Network name
Answer: B – Gas measures computational work; users pay miners/validators in ETH.

Q13. Can you reverse a confirmed blockchain transaction?
A) Yes, within 24 hours B) Yes, contact support C) No, transactions are irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q14. What information is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is meant to be shared for receiving funds.

Q15. How many accounts can you create from one seed phrase?
A) Only 1 B) Up to 5 C) Up to 100 D) Unlimited
Answer: D – HD wallets derive unlimited accounts from one seed phrase.

Quiz Questions - Part 4

Q16. What does MetaMask's password protect?
A) Seed phrase access B) Only local device access C) Network connections D) Transaction history
Answer: B – Password encrypts local storage; doesn't recover wallet without seed.

Q17. Which is NOT a recommended security practice?
A) Bookmark trusted sites B) Verify URLs carefully C) Share seed phrase with support D) Review transactions before confirming
Answer: C – Never share seed phrase; legitimate support never asks for it.

Q18. What is a hardware wallet example?
A) MetaMask B) Ledger Nano C) MyEtherWallet D) Trust Wallet
Answer: B – Ledger Nano is a hardware wallet; others are software wallets.

Q19. Where can you obtain Sepolia testnet ETH?
A) Exchanges B) Mining C) Faucets D) Purchase with credit card
Answer: C – Faucets distribute free testnet ETH for development/learning.

Q20. What does a transaction hash provide?
A) Sender's private key B) Unique transaction identifier C) Wallet password D) Gas price
Answer: B – Transaction hash (txhash) uniquely identifies transactions on blockchain.

Lab Session: Wallet Setup and First Transaction

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Not your keys, not your coins

[COMIC: A person confidently showing off their exchange balance on a phone, while behind them a shadowy exchange building has a "Sorry, withdrawals paused" sign and bankruptcy lawyers circling]

The Self-Custody Imperative

- Exchange custody means trusting someone else with your private keys
- Mt. Gox (2014), FTX (2022): billions lost when exchanges failed
- Today: you take control of your own cryptographic destiny

Over $10 billion lost to exchange failures and hacks since 2014

Learning Objectives

By the end of this lab session, you will be able to:

- Install and configure MetaMask wallet extension
- Explain seed phrase importance and backup procedures
- Connect to Ethereum testnets (Sepolia)
- Obtain testnet ETH from faucets
- Send and receive testnet transactions
- Apply security best practices for wallet protection

Building on L07: Proof of Work

The Problem: Self-Custody in Digital Finance

The Challenge
Traditional banks hold your money and control access. How do you prove ownership and control digital assets without a trusted intermediary like a bank?

Why It Matters

- Bank failures can freeze or lose customer funds (e.g., Cyprus 2013, Silicon Valley Bank 2023)
- Centralized custody creates single points of failure and censorship risk

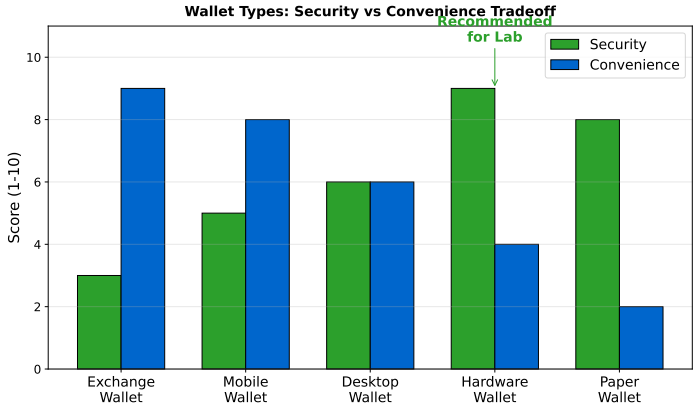
What We Need

- Cryptographic proof of ownership without intermediaries
- User-controlled key management system
- Secure backup mechanism for asset recovery

The Cryptoeconomics Question
How do private keys align economic incentives with security requirements?

Today's lab: Hands-on experience with self-custody wallet creation and key management

How Do Wallet Types Balance Security and Convenience?



Hardware wallets offer best security; MetaMask provides good balance for learning

What is MetaMask?

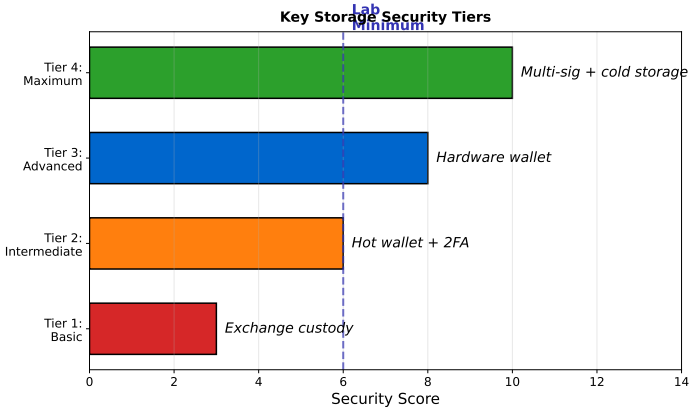
Overview:

- Browser extension and mobile app cryptocurrency wallet
- Supports Ethereum and EVM-compatible blockchains
- Non-custodial: you control private keys
- Most popular Ethereum wallet (30 million users)

Key Features:

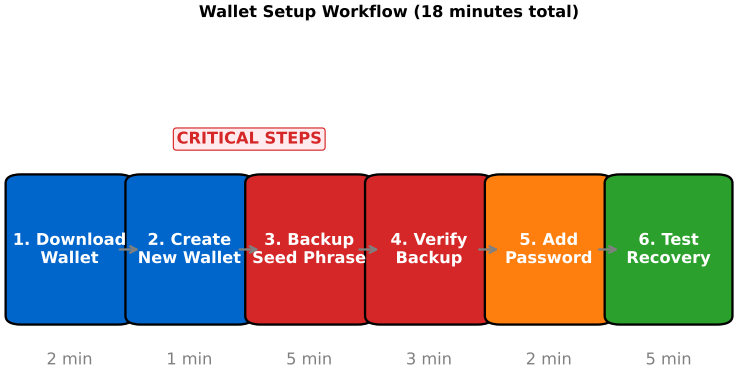
- Send and receive ETH and ERC-20 tokens
- Interact with decentralized applications (dApps) – apps running on blockchain instead of company servers
- Multiple account management
- Network switching (Mainnet, testnets, custom networks)

How Do Security Levels Differ for Key Storage?



For this lab, Tier 2 (hot wallet + 2FA) is the minimum acceptable level

What Are the Steps in Wallet Setup?



Seed phrase backup (steps 3-4) is the most critical part of wallet setup

How Do You Install MetaMask Safely?

Installation Steps:

1. Visit official website: `https://metamask.io`
2. Click "Download" and select your browser
3. Install extension from official browser store
4. Pin extension to browser toolbar
5. Click MetaMask icon to launch setup wizard

Security Warning:

- Only install from official sources
- Beware of phishing sites (check URL carefully)
- Fake extensions exist in browser stores

How Do You Create a Secure Wallet?

Setup Wizard Steps:

1. Click “Create a new wallet”
2. Set a strong password (8+ characters)
3. Reveal and record your 12-word seed phrase
4. Confirm seed phrase by selecting words in correct order

Critical: Seed Phrase vs. Password

- Seed phrase = master backup (recovers wallet on any device)
- Password = local device protection (cannot recover wallet)
- **Lose seed phrase -¿ lose wallet permanently**

How Do You Connect to the Sepolia Testnet?

Why Use Testnets?

- Practice without risking real money
- Free testnet ETH available from faucets
- Identical functionality to mainnet

Adding Sepolia Network:

1. Click network selector (top-right dropdown)
2. Settings -¿ Advanced -¿ Show test networks (enable)
3. Select “Sepolia test network”

Sepolia Faucets:

- Alchemy: `https://sepoliafaucet.com`
- Infura: `https://www.infura.io/faucet/sepolia`

How Do You Send Your First Transaction?

Transaction Steps:

1. Ensure you have Sepolia ETH (from faucet)
2. Click "Send" button in MetaMask
3. Enter recipient address (create second account or use classmate's)
4. Enter amount (e.g., 0.1 Sepolia ETH)
5. Review transaction details (gas fee, total)
6. Click "Confirm"
7. View in Activity tab

Understanding Gas Fees:

- Fee = gas units $\times$ gas price (in gwei)
- Gwei = 0.000000001 ETH (1 billionth of an ETH, or 10^{-9} ETH)
- Sepolia: fees are negligible (testnet)

What Security Best Practices Should You Follow?

Critical Security Rules:

1. **Seed Phrase:** Never share, never store digitally
2. **Phishing Protection:** Verify URLs, bookmark trusted sites
3. **Network Verification:** Confirm correct network before transacting
4. **Transaction Approval:** Review recipient and amounts carefully

Common Threats:

- Phishing websites requesting seed phrase
- Malicious dApps with unlimited token approvals
- Clipboard malware replacing copied addresses
- Fake support scams via DM

What Should You Submit for This Lab?

Submit the following:

1. **Screenshot Collection:**
   - MetaMask wallet showing Sepolia network
   - Transaction details from Activity tab
   - Etherscan transaction page (confirmed)
2. **Lab Report (1-2 pages):**
   - Your Sepolia address
   - Transaction hash of sent transaction
   - Reflection on seed phrase security

Submission Deadline: One week from lab session

Problem Solved? Self-Custody Trade-offs

The Original Problem

How to control digital assets without trusted intermediaries?

How Wallet Security Solves It

- Private keys provide cryptographic proof of ownership (ECDSA signatures)
- Seed phrases enable deterministic recovery across devices (BIP-39/HD wallets)
- Self-custody eliminates counterparty risk and censorship

Remaining Limitations

- User bears full responsibility for key security (no "forgot password" option)
- Lost seed phrase = permanent loss of funds (irreversible)
- Phishing and social engineering attacks target users directly

The Economic Trade-off

- Benefit: Full control, no intermediary fees, censorship resistance
- Cost: Security burden shifts to user (requires technical knowledge)

Self-custody solves intermediary risk but introduces user responsibility risk

(c) Joerg Osterrieder 2025

The Economics of Wallet Security

Incentive Structure

- **Core Problem:** Coordinating without trusted intermediaries
- **Why act honestly?** Participants verify rather than trust
- **Value Flow:** Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Wallet Security

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Wallet Security

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Seed phrase horror stories

[COMIC: A four-panel strip showing seed phrase disasters: (1) written on a napkin thrown away, (2) stored in a notes app that got hacked, (3) tattooed on arm now visible in beach photos, (4) memorized perfectly but forgotten after vacation]

Secure Backup Is Non-Negotiable

- $140 billion in Bitcoin estimated permanently lost due to lost keys
- Never store digitally, never share, never photograph
- Metal backup plates survive fire and flood—paper does not

James Howells lost 7,500 BTC in a landfill—worth over $500 million today

Key Takeaways

- MetaMask is a non-custodial wallet (you control private keys)
- Seed phrase is the master backup for all accounts
- Testnets provide safe environment for learning
- Gas fees vary by network congestion
- Blockchain transactions are irreversible
- Security requires vigilance against phishing and scams

Next Lesson: L09 – Proof of Stake

Quiz Questions - Part 1

Q1. What type of wallet is MetaMask?
A) Custodial wallet B) Non-custodial wallet C) Hardware wallet D) Paper wallet
Answer: B – MetaMask is non-custodial, meaning you control your private keys.

Q2. How many words are typically in a MetaMask seed phrase?
A) 6 words B) 12 words C) 24 words D) 32 words
Answer: B – MetaMask uses a 12-word seed phrase (BIP-39 standard).

Q3. What is the primary purpose of a seed phrase?
A) Login password B) Wallet recovery C) Transaction signing D) Network selection
Answer: B – Seed phrase is the master backup to recover your wallet on any device.

Q4. Which wallet type offers the highest security?
A) Mobile wallet B) Browser extension C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep private keys offline in secure hardware.

Q5. What happens if you lose your MetaMask password?
A) Wallet is lost forever B) Contact support C) Use seed phrase to recover D) Reset via email
Answer: C – Password is local; seed phrase recovers the wallet.

Quiz Questions - Part 2

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network identification D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. Can two people have the same Ethereum public address?
A) Yes, if on different networks B) Yes, addresses are reused C) No, addresses are unique D) Only on testnets
Answer: C – Addresses are cryptographically unique (collision probability negligible).

Q8. What is the purpose of using Sepolia testnet?
A) Faster transactions B) Lower fees C) Practice without risk D) Access exclusive dApps
Answer: C – Testnets allow safe practice with free testnet ETH.

Q9. How should you store your seed phrase?
A) Screenshot on phone B) Email to yourself C) Written on paper offline D) Cloud storage
Answer: C – Physical offline storage prevents digital theft or hacking.

Q10. What does "non-custodial" mean for wallets?
A) No fees B) You control keys C) Company holds keys D) No backups needed
Answer: B – Non-custodial means you (not a third party) control private keys.

Quiz Questions - Part 3

Q11. Which of these is a phishing attack vector?
A) Official MetaMask.io B) Fake site requesting seed phrase C) Hardware wallet D) Testnet faucets
Answer: B – Phishing sites impersonate legitimate services to steal seed phrases.

Q12. What is gas in Ethereum transactions?
A) Fuel for cars B) Computational work fee C) Token symbol D) Network name
Answer: B – Gas measures computational work; users pay miners/validators in ETH.

Q13. Can you reverse a confirmed blockchain transaction?
A) Yes, within 24 hours B) Yes, contact support C) No, transactions are irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q14. What information is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is meant to be shared for receiving funds.

Q15. How many accounts can you create from one seed phrase?
A) Only 1 B) Up to 5 C) Up to 100 D) Unlimited
Answer: D – HD wallets derive unlimited accounts from one seed phrase.

Quiz Questions - Part 4

Q16. What does MetaMask's password protect?
A) Seed phrase access B) Only local device access C) Network connections D) Transaction history
Answer: B – Password encrypts local storage; doesn't recover wallet without seed.

Q17. Which is NOT a recommended security practice?
A) Bookmark trusted sites B) Verify URLs carefully C) Share seed phrase with support D) Review transactions before confirming
Answer: C – Never share seed phrase; legitimate support never asks for it.

Q18. What is a hardware wallet example?
A) MetaMask B) Ledger Nano C) MyEtherWallet D) Trust Wallet
Answer: B – Ledger Nano is a hardware wallet; others are software wallets.

Q19. Where can you obtain Sepolia testnet ETH?
A) Exchanges B) Mining C) Faucets D) Purchase with credit card
Answer: C – Faucets distribute free testnet ETH for development/learning.

Q20. What does a transaction hash provide?
A) Sender's private key B) Unique transaction identifier C) Wallet password D) Gas price
Answer: B – Transaction hash (txhash) uniquely identifies transactions on blockchain.

Lab: Wallet Setup – Mini-Lecture

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab, you will be able to:

- Install and configure MetaMask wallet extension
- Secure your wallet with proper seed phrase backup
- Connect to Sepolia testnet and obtain free test ETH
- Send your first testnet transaction

Estimated time: 60 minutes hands-on practice

(c) Joerg Osterrieder 2025

What is a Crypto Wallet?

Key Concepts:

- Software or hardware that stores your private keys
- Non-custodial: YOU control access (not a company)
- Your "account number" = public address (safe to share)
- Your "password" = private key (NEVER share)

MetaMask:

- Browser extension wallet for Ethereum/EVM chains
- Over 30 million active users worldwide
- Free to install from `https://metamask.io`

Non-custodial means you have full responsibility for key security

Wallet Types: Security vs Convenience

Type	Security	Convenience	Example
Hardware wallet	High	Low	Ledger Nano, Trezor
Desktop wallet	Medium	Medium	Exodus, Electrum
Browser extension	Medium	High	**MetaMask**, Rabby
Mobile wallet	Medium	High	Trust Wallet
Web wallet	Low	High	Exchange wallets

For this lab: MetaMask provides the best balance for learning dApp interaction.

Hardware wallets keep private keys offline; never expose to internet

Exercise 1: Installing MetaMask

Step-by-Step:

1. Go to `https://metamask.io` (verify URL carefully!)
2. Click "Download" and select your browser
3. Install from official browser extension store
4. Pin the MetaMask fox icon to your toolbar

Security Warning:

- Only install from official sources
- Fake MetaMask extensions exist – check download count
- Phishing sites mimic the official site

Verify: Chrome Web Store shows "Offered by metamask.io"

Exercise 2: Creating Your Wallet

Setup Steps:

1. Click "Create a new wallet"
2. Set a strong password (8+ characters, used locally)
3. **Write down your 12-word seed phrase on paper**
4. Confirm seed phrase by clicking words in order

Critical Distinction:

- **Seed phrase** = master backup (recovers wallet anywhere)
- **Password** = local encryption (only for this device)
- Lose seed phrase = lose wallet forever

NEVER store seed phrase digitally (no photos, no cloud, no email)

Exercise 3: Connect to Sepolia Testnet

Why Testnets?

- Practice without real money risk
- Same functionality as mainnet
- Free ETH from "faucets"

Enable Sepolia:

1. Click network dropdown (top-right)
2. Settings → Advanced → Show test networks: ON
3. Select "Sepolia test network"

Get Free ETH:

- Alchemy Faucet: `https://sepoliafaucet.com`
- Infura Faucet: `https://www.infura.io/faucet/sepolia`

Faucets may require login; request 0.5 ETH for lab exercises

Exercise 4: Send Your First Transaction

Transaction Steps:

1. Verify you have Sepolia ETH in wallet
2. Click "Send" button
3. Create a second account OR use classmate's address
4. Enter amount: 0.1 Sepolia ETH
5. Review gas fee and confirm

Understanding Gas:

- Fee = Gas units $\times$ Gas price (gwei)
- Sepolia fees are negligible (free testnet)
- Mainnet: fees vary by network congestion

View your transaction on sepolia.etherscan.io using the tx hash

Security Best Practices

The 4 Golden Rules:

1. **Seed Phrase:** Never share, never store digitally
2. **Verify URLs:** Bookmark trusted sites, check before entering
3. **Review Transactions:** Check recipient and amount before signing
4. **Check Network:** Confirm you are on correct network (mainnet vs testnet)

Common Threats:

- Phishing sites requesting seed phrase
- Clipboard malware swapping addresses
- Fake support DMs asking for keys

Legitimate support will NEVER ask for your seed phrase

Wallet Security in Practice

Digital wallet concept

Mobile payment interface

Security protection

Images: Unsplash (CC0). Wallet security requires both technical and behavioral measures.

Key Takeaways

- MetaMask is a non-custodial wallet (you control private keys)
- Seed phrase (12 words) is your master backup – protect offline
- Password only protects local device; cannot recover wallet
- Testnets (Sepolia) provide safe practice environment
- Gas fees pay for computational work on the network
- Blockchain transactions are irreversible – verify before confirming

Lab deliverable: Screenshot of confirmed Sepolia transaction on Etherscan

Quiz Questions – Part 1

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – You control the private keys, not a third party.

Q2. What is the purpose of the seed phrase?
A) Local login B) Wallet recovery C) Transaction signing D) Network ID
Answer: B – Seed phrase recovers your wallet on any device.

Q3. What happens if you lose your seed phrase?
A) Reset via email B) Contact support C) Use password D) Wallet lost forever
Answer: D – No central authority can recover non-custodial wallets.

Q4. Where should you store your seed phrase?
A) Cloud storage B) Email draft C) Written on paper offline D) Screenshot
Answer: C – Physical offline storage prevents digital theft.

Q5. What is gas in Ethereum?
A) Token name B) Network type C) Computational fee D) Wallet feature
Answer: C – Gas pays for computational work on the blockchain.

(c) Joerg Osterrieder 2025

Quiz Questions – Part 2

Q6. Why use Sepolia testnet for this lab?
A) Faster speed B) Lower fees C) Practice without risk D) More features
Answer: C – Free testnet ETH allows safe experimentation.

Q7. What information is safe to share publicly?
A) Seed phrase B) Private key C) Password D) Public address
Answer: D – Public address is designed for receiving funds.

Q8. Can blockchain transactions be reversed?
A) Within 1 hour B) By support request C) No, irreversible D) Only on testnet
Answer: C – Blockchain immutability means no reversals.

Q9. What is a faucet in crypto?
A) Hardware device B) Security tool C) Free testnet ETH source D) Wallet type
Answer: C – Faucets distribute free test tokens for development.

Q10. Which wallet type offers highest security?
A) Browser extension B) Mobile wallet C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep keys offline in secure hardware.

L08: Lab – Wallet Setup and First Transaction

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

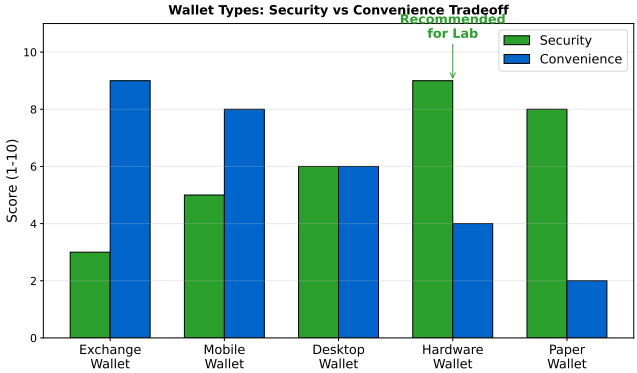
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Install and configure MetaMask wallet
- Understand seed phrase security and backup procedures
- Connect to Ethereum testnets (Sepolia)
- Send and receive testnet transactions

Wallet Types: Security vs Convenience



Key Trade-off: Hardware wallets offer best security; MetaMask provides good balance for learning.

What is MetaMask?

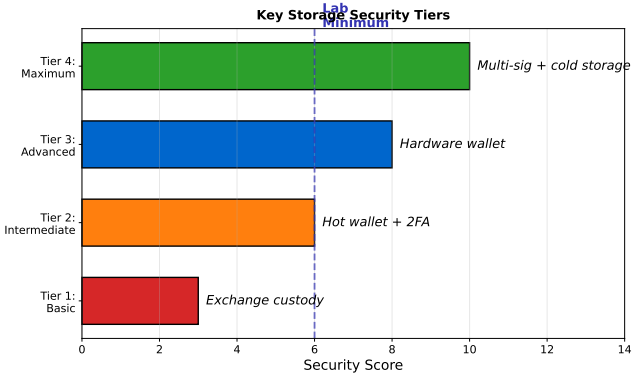
Overview:

- Browser extension and mobile cryptocurrency wallet
- Non-custodial: you control private keys
- Most popular Ethereum wallet (30 million users)

Key Features:

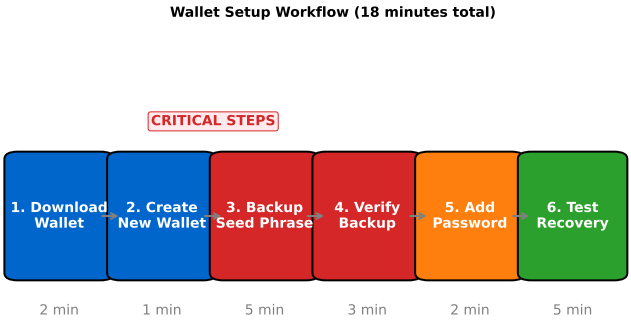
- Send/receive ETH and ERC-20 tokens
- Interact with decentralized applications (dApps)
- Network switching (Mainnet, testnets, custom networks)

Security Levels for Key Storage



Minimum for this lab: Tier 2 (hot wallet + 2FA) is acceptable for learning.

Wallet Setup Workflow



Critical: Seed phrase backup (steps 3-4) is the most important part.

Critical: Seed Phrase vs. Password

Seed Phrase (12 words):

- Master backup – recovers wallet on any device
- NEVER share, NEVER store digitally
- Lose seed phrase = lose wallet permanently

Password:

- Local device protection only
- Cannot recover wallet without seed phrase
- Can be reset if you have seed phrase

Rule: Write seed phrase on paper, store offline.

Using Testnets: Practice Without Risk

Why Testnets?

- Practice without risking real money
- Free testnet ETH from faucets
- Identical functionality to mainnet

Sepolia Faucets (2025):

- Alchemy: sepoliafaucet.com
- Infura: infura.io/faucet/sepolia
- Google Cloud: cloud.google.com/web3/faucet

Note: Most faucets require authentication to prevent abuse.

Security Best Practices

Critical Rules:

1. Never share seed phrase (support NEVER asks for it)
2. Verify URLs carefully – bookmark trusted sites
3. Confirm correct network before transacting
4. Review recipient address and amounts

Common Threats:

- Phishing websites requesting seed phrase
- Malicious dApps with unlimited token approvals
- Clipboard malware replacing copied addresses

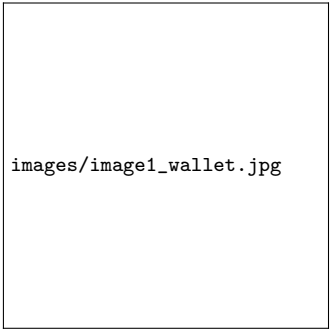
(c) Joerg Osterrieder 2025

Key Takeaways

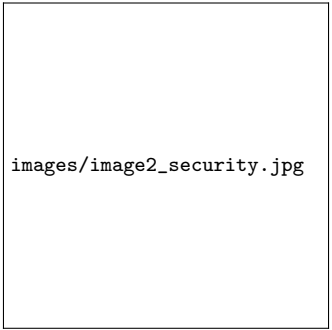
1. **Non-custodial:** You control private keys, you bear responsibility
2. **Seed Phrase:** Master backup – offline storage only
3. **Testnets:** Safe environment for learning (no real value)
4. **Security:** Vigilance against phishing is critical
5. **Irreversibility:** Blockchain transactions cannot be reversed

Lab Goal: Complete wallet setup, obtain testnet ETH, send first transaction.

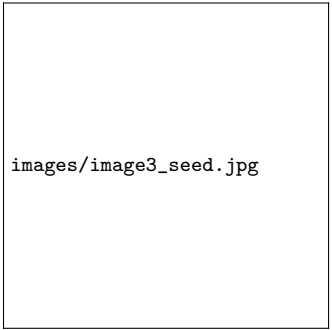
Wallet Setup in Practice



Digital Wallet



Security Layers



Seed Phrase Backup

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper

Quiz (1/2)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – You control your private keys, not a third party.

Q2. How many words are in a MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32

Quiz (1/2)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – You control your private keys, not a third party.

Q2. How many words are in a MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses BIP-39 standard 12-word seed phrases.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password

Quiz (1/2)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – You control your private keys, not a third party.

Q2. How many words are in a MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses BIP-39 standard 12-word seed phrases.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password
Answer: C – No seed phrase = no recovery. It's the master backup.

Q4. Which wallet type offers highest security?
A) Mobile wallet B) Browser extension C) Hardware wallet D) Web wallet

Quiz (1/2)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – You control your private keys, not a third party.

Q2. How many words are in a MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses BIP-39 standard 12-word seed phrases.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password
Answer: C – No seed phrase = no recovery. It's the master backup.

Q4. Which wallet type offers highest security?
A) Mobile wallet B) Browser extension C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep keys offline in secure hardware.

Q5. What is the purpose of a testnet?
A) Faster transactions B) Lower fees C) Practice without risk D) Access exclusive dApps

(c) Joerg Osterrieder 2025

Quiz (1/2)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – You control your private keys, not a third party.

Q2. How many words are in a MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses BIP-39 standard 12-word seed phrases.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password
Answer: C – No seed phrase = no recovery. It's the master backup.

Q4. Which wallet type offers highest security?
A) Mobile wallet B) Browser extension C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep keys offline in secure hardware.

Q5. What is the purpose of a testnet?
A) Faster transactions B) Lower fees C) Practice without risk D) Access exclusive dApps
Answer: C – Testnets allow safe practice with free testnet ETH.

Quiz (2/2)

Q6. What is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password

Quiz (2/2)

Q6. What is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is for receiving funds; share freely.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Cloud storage D) Written on paper offline

Quiz (2/2)

Q6. What is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is for receiving funds; share freely.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Cloud storage D) Written on paper offline
Answer: D – Physical offline storage prevents digital theft.

Q8. Can confirmed blockchain transactions be reversed?
A) Yes, within 24 hours B) Yes, contact support C) No, irreversible D) Only on testnets

Quiz (2/2)

Q6. What is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is for receiving funds; share freely.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Cloud storage D) Written on paper offline
Answer: D – Physical offline storage prevents digital theft.

Q8. Can confirmed blockchain transactions be reversed?
A) Yes, within 24 hours B) Yes, contact support C) No, irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q9. What does "gas" pay for on Ethereum?
A) Token purchases B) Computational work C) Wallet creation D) Network membership

Quiz (2/2)

Q6. What is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is for receiving funds; share freely.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Cloud storage D) Written on paper offline
Answer: D – Physical offline storage prevents digital theft.

Q8. Can confirmed blockchain transactions be reversed?
A) Yes, within 24 hours B) Yes, contact support C) No, irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q9. What does "gas" pay for on Ethereum?
A) Token purchases B) Computational work C) Wallet creation D) Network membership
Answer: B – Gas pays validators for computational resources.

Q10. How many accounts can one seed phrase generate?
A) 1 B) 5 C) 100 D) Unlimited

Quiz (2/2)

Q6. What is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is for receiving funds; share freely.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Cloud storage D) Written on paper offline
Answer: D – Physical offline storage prevents digital theft.

Q8. Can confirmed blockchain transactions be reversed?
A) Yes, within 24 hours B) Yes, contact support C) No, irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q9. What does "gas" pay for on Ethereum?
A) Token purchases B) Computational work C) Wallet creation D) Network membership
Answer: B – Gas pays validators for computational resources.

Q10. How many accounts can one seed phrase generate?
A) 1 B) 5 C) 100 D) Unlimited
Answer: D – HD wallets derive unlimited accounts from one seed.

Thank you

Questions?

Next: L09 – Proof of Stake Consensus

Quiz: Lab Wallet Setup

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper

Quiz (1–5)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – MetaMask is non-custodial: you control your private keys.

Q2. How many words are in a standard MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – MetaMask is non-custodial: you control your private keys.

Q2. How many words are in a standard MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses 12-word BIP-39 seed phrases by default.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password

Quiz (1–5)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – MetaMask is non-custodial: you control your private keys.

Q2. How many words are in a standard MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses 12-word BIP-39 seed phrases by default.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password
Answer: C – No seed phrase = no recovery. It is the master backup.

Q4. Which wallet type offers the highest security?
A) Mobile app B) Browser extension C) Hardware wallet D) Web wallet

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – MetaMask is non-custodial: you control your private keys.

Q2. How many words are in a standard MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses 12-word BIP-39 seed phrases by default.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password
Answer: C – No seed phrase = no recovery. It is the master backup.

Q4. Which wallet type offers the highest security?
A) Mobile app B) Browser extension C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep keys offline in secure hardware.

Q5. What is the purpose of using Sepolia testnet?
A) Faster transactions B) Lower fees C) Practice without risk D) Better security

Quiz (1–5)

Q1. What type of wallet is MetaMask?
A) Custodial B) Non-custodial C) Hardware D) Paper
Answer: B – MetaMask is non-custodial: you control your private keys.

Q2. How many words are in a standard MetaMask seed phrase?
A) 6 B) 12 C) 24 D) 32
Answer: B – MetaMask uses 12-word BIP-39 seed phrases by default.

Q3. What happens if you lose your seed phrase?
A) Contact support B) Reset via email C) Wallet lost forever D) Use password
Answer: C – No seed phrase = no recovery. It is the master backup.

Q4. Which wallet type offers the highest security?
A) Mobile app B) Browser extension C) Hardware wallet D) Web wallet
Answer: C – Hardware wallets keep keys offline in secure hardware.

Q5. What is the purpose of using Sepolia testnet?
A) Faster transactions B) Lower fees C) Practice without risk D) Better security
Answer: C – Testnets allow safe practice with free testnet ETH.

Quiz (6–10)

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network ID D) Gas estimation

Quiz (6–10)

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network ID D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Written on paper offline D) Cloud storage

Quiz (6–10)

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network ID D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Written on paper offline D) Cloud storage
Answer: C – Physical offline storage prevents digital theft.

Q8. Can you reverse a confirmed blockchain transaction?
A) Within 24 hours B) Contact support C) No, irreversible D) Only on testnets

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network ID D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Written on paper offline D) Cloud storage
Answer: C – Physical offline storage prevents digital theft.

Q8. Can you reverse a confirmed blockchain transaction?
A) Within 24 hours B) Contact support C) No, irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q9. What information is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password

Quiz (6–10)

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network ID D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Written on paper offline D) Cloud storage
Answer: C – Physical offline storage prevents digital theft.

Q8. Can you reverse a confirmed blockchain transaction?
A) Within 24 hours B) Contact support C) No, irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q9. What information is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is meant to be shared for receiving funds.

Q10. What does "non-custodial" mean?
A) No fees B) You control keys C) Exchange holds keys D) No backup needed

Quiz (6–10)

Q6. What is a private key used for?
A) Receiving funds B) Signing transactions C) Network ID D) Gas estimation
Answer: B – Private key cryptographically signs transactions to prove ownership.

Q7. How should you store your seed phrase?
A) Screenshot B) Email C) Written on paper offline D) Cloud storage
Answer: C – Physical offline storage prevents digital theft.

Q8. Can you reverse a confirmed blockchain transaction?
A) Within 24 hours B) Contact support C) No, irreversible D) Only on testnets
Answer: C – Blockchain transactions are immutable once confirmed.

Q9. What information is safe to share publicly?
A) Private key B) Seed phrase C) Public address D) Password
Answer: C – Public address is meant to be shared for receiving funds.

Q10. What does "non-custodial" mean?
A) No fees B) You control keys C) Exchange holds keys D) No backup needed
Answer: B – Non-custodial means you (not a third party) control private keys.

(c) Joerg Osterrieder 2025

Proof of Stake Consensus

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the proof-of-stake consensus mechanism
- Describe validator responsibilities: staking, attestation, block proposal
- Describe slashing conditions and economic penalties
- Analyze Ethereum's Beacon Chain architecture
- Distinguish between justification and finality
- Calculate staking rewards and economics
- Evaluate centralization risks in proof-of-stake systems

(c) Joerg Osterrieder 2025

The Problem: Can we secure networks without wasting energy?

The Challenge
Can we secure a blockchain network with economic stake instead of energy expenditure? How do we prevent attacks when validation doesn't require external resource costs?

Why It Matters

- Proof-of-Work criticized for consuming electricity of entire countries (Bitcoin ∼120 TWh/year)
- Environmental concerns threaten blockchain adoption by institutions and governments
- Ethereum's PoW consumed energy equivalent to Finland (2021-2022)

What We Need

- Economic alignment of actors
- Security guarantees from capital at risk, not energy burn
- Ability to penalize malicious behavior economically
- Finality mechanism without computational competition

The Cryptoeconomics Question
Aligning individual and collective interests

Today's lesson: How Proof of Stake addresses this challenge

Proof of Work vs. Proof of Stake

Proof of Work

- Security via computational cost
- Miners compete by hash power
- Energy-intensive
- Hardware requirements (ASICs)
- Block rewards + transaction fees
- 51% attack requires hash rate majority

Proof of Stake

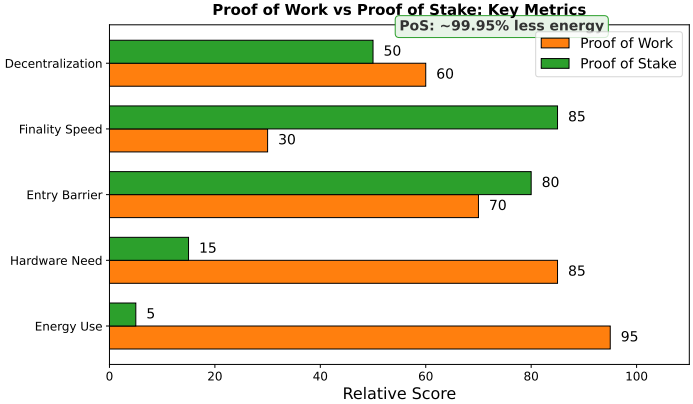
- Security via economic stake
- Validators selected by stake weight
- Energy-efficient (99% reduction)
- Capital requirements (staking)
- Transaction fees only (or low issuance)
- 51% attack requires token majority

Core Difference:

- PoW: external resource (electricity) $\rightarrow$ security
- PoS: internal resource (staked tokens) $\rightarrow$ security

(c) Joerg Osterrieder 2025

PoW vs PoS: Quantitative Comparison



PoS dramatically reduces energy while improving finality time and throughput.

The Nothing-at-Stake Problem

Theoretical Vulnerability:

In case of blockchain fork:

- PoW miners must choose one fork (cannot mine both simultaneously)
- PoS validators can vote on multiple forks simultaneously (no cost)
- Rational strategy: vote on all forks to maximize rewards

Solutions:

1. **Slashing:** Detect and penalize validators voting on conflicting blocks
2. **Finality Gadgets:** Checkpoint mechanisms (Casper FFG) prevent reversals

Practical Observation:

- Well-designed PoS systems have never experienced nothing-at-stake attacks
- Slashing and economic incentives effectively mitigate the threat

Ethereum's Transition to Proof of Stake

The Merge (September 15, 2022):

- Ethereum transitioned from PoW to PoS
- Beacon Chain (PoS) launched December 2020, ran parallel 21 months
- No downtime, seamless transition

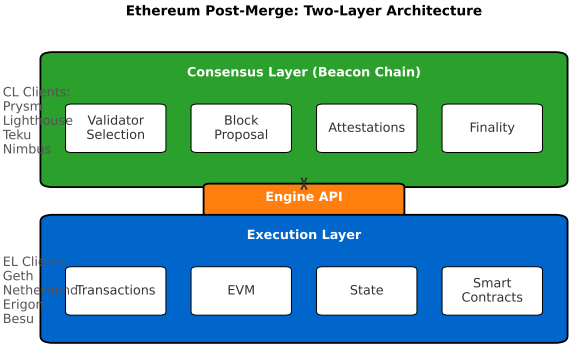
Impact:

- Energy consumption reduced by $\sim$99.95%
- ETH issuance reduced by $\sim$90% (13,000 $\rightarrow$ 1,600 ETH/day)
- Block time: $\sim$13s $\rightarrow$ $\sim$12s

Misconceptions Cleared:

- Did NOT reduce gas fees (addressed by Layer 2s)
- Did NOT increase throughput (scalability via sharding planned later)
- Changed consensus mechanism only

Ethereum Beacon Chain Architecture



The Merge unified execution and consensus layers under PoS.

Beacon Chain: Two-Layer Design

Execution Layer (EL):

- Processes transactions & smart contracts
- Maintains EVM and account state

Consensus Layer (Beacon Chain):

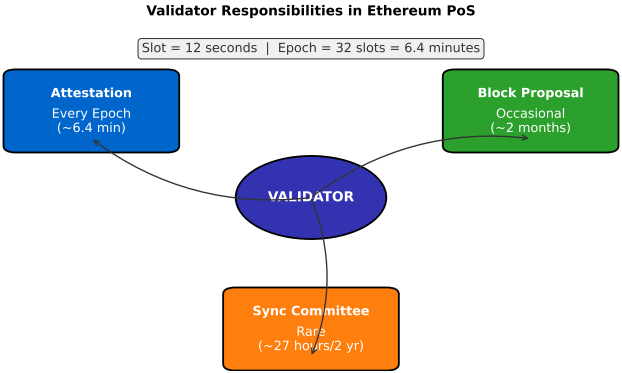
- Selects block proposers, coordinates validators
- Manages staking, slashing, finalization

Client Diversity:

- EL: Geth, Nethermind, Erigon, Besu
- CL: Prysm, Lighthouse, Teku, Nimbus
- Engine API connects layers

Multiple client implementations prevent single points of failure.

Validator Responsibilities



Validators perform multiple duties with varying frequencies and reward structures.

Validator Duties Explained

1. **Attestation (every epoch):**
   - Vote on chain head + checkpoints
   - Aggregated into blocks for efficiency
2. **Block Proposal (occasionally):**
   - Selected pseudo-randomly by stake
   - Earn transaction fees + block reward
3. **Sync Committee (rarely):**
   - Rotating $\sim$27 hour service period
   - Helps light clients sync

Timing:

- Slot = 12 seconds
- Epoch = 32 slots = 6.4 minutes

(c) Joerg Osterrieder 2025

Staking Requirements and Process

Minimum Stake: 32 ETH per validator

Staking Process:

1. Generate validator keys (BLS12-381)
2. Deposit 32 ETH to contract
3. Run validator client
4. Wait for activation, start attesting

Hardware Requirements:

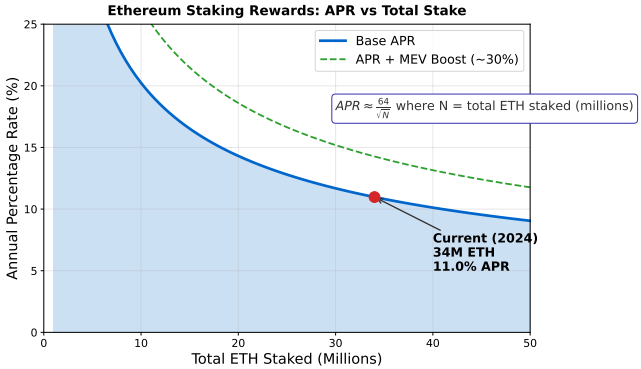
- CPU: 4+ cores — RAM: 16+ GB
- Storage: 2+ TB SSD
- 99%+ uptime — $50-200/month

Alternatives:

- Pools: Lido, Rocket Pool
- Exchanges: Coinbase, Kraken

(c) Joerg Osterrieder 2025

Staking Rewards: APR Curve



More stakers = lower APR due to reward dilution. MEV adds 30%+ boost.

Validator Rewards Breakdown

Reward Components:

1. **Attestation Rewards:** Earned for timely, correct attestations
2. **Block Proposal Rewards:** Transaction fees + attestation inclusion
3. **Sync Committee Rewards:** Small bonus for participation

Annual Percentage Rate (APR):

$$\text{APR} \approx \frac{64}{\sqrt{N}}$$

where N = total ETH staked (in millions)

Current State (2024-2025):

- 34M+ ETH staked: APR $\approx$ 3.2-3.5%
- Over 1 million active validators
- MEV-Boost adds 30-50% to base rewards

Penalties and Inactivity Leaks

Missed Attestation Penalty:

- Equal to reward you would have earned
- Validator balance decreases (linear, no compounding)

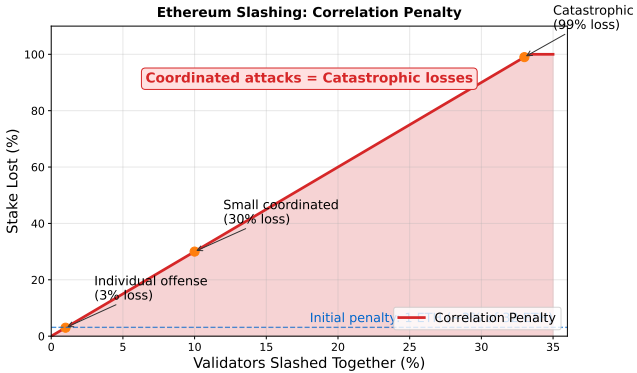
Inactivity Leak:

- Activated when chain fails to finalize (> 4 epochs)
- Offline validators lose stake at increasing rate (quadratic)
- Purpose: eject offline validators to restore finality

Example Scenario:

- Network partition: 40% validators offline
- Chain cannot finalize (requires 67% participation)
- Inactivity leak begins, offline validators lose stake rapidly
- Eventually chain resumes finalization with remaining validators

Slashing: Correlation Penalty



Coordinated attacks result in catastrophic losses – strong deterrent against collusion.

Slashable Offenses

Three Types:

1. **Double Proposal:** Proposing two blocks for same slot
2. **Surround Vote:** Attesting to conflicting checkpoint votes
3. **Double Vote:** Attesting to two different blocks in same epoch

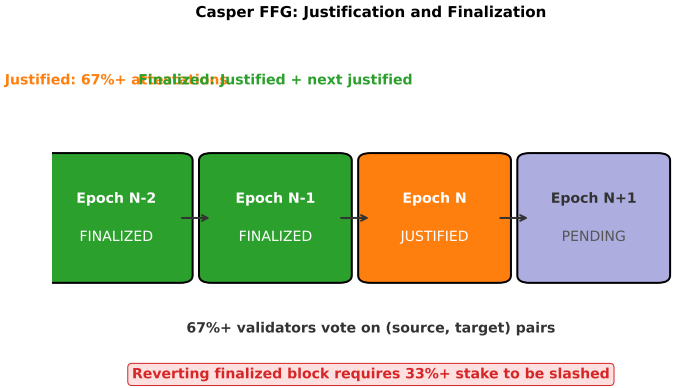
Slashing Penalties:

- **Initial penalty:** 1 ETH (immediate)
- **Correlation penalty:** Stake $\times$ 3 $\times$ (slashed/total validators)
- **Forced exit:** validator ejected from active set
- **Withdrawal delay:** 36 days before funds withdrawable

Penalty Examples:

- 1% slashed together: lose $\sim$3% of stake
- 33% slashed together: lose $\sim$99% of stake (catastrophic)

Casper FFG: Finality Mechanism



Finalized blocks cannot be reverted without 33%+ stake being slashed.

Casper FFG Explained

Purpose:

- Provide economic finality
- Prevent long-range reorganizations

Checkpoint Voting:

- Checkpoint = first block of epoch
- Validators vote: (source, target) pairs

Justification vs Finalization:

- **Justified:** 67%+ votes (can revert)
- **Finalized:** Justified + next epoch justified
- Takes $\sim$12.8 minutes (2 epochs)

Accountable Safety:
Conflicting checkpoints cannot finalize — attacker loses stake.

LMD GHOST: Fork Choice Rule

Purpose: Determine canonical chain head before finalization

LMD GHOST (Latest Message Driven Greedy Heaviest Observed SubTree):

1. Start at last finalized checkpoint
2. At each fork, choose subtree with most validator attestations
3. Recursively descend until leaf (chain head)

Example:

- Block A: 100 attestations — Block B: 150 attestations
- LMD GHOST selects Block B as canonical

Combination with Casper FFG:

- LMD GHOST: determines head (short-term)
- Casper FFG: determines finality (long-term)
- Together: fast confirmation + eventual certainty

(c) Joerg Osterrieder 2025

Validator Lifecycle

States:

1. **Deposited:** 32 ETH deposited, waiting in activation queue
2. **Active:** Attesting and proposing, earning rewards/penalties
3. **Exiting:** Voluntary exit initiated, still active for $\sim$1 day
4. **Exited:** No longer active, funds locked for 27 hours
5. **Withdrawable:** Funds available (auto-withdrawal after Shanghai)

Forced Exit:

- Triggered by slashing or balance $<$ 16 ETH
- Validator ejected automatically

Staking Economics: Risks and Rewards

Rewards (4-8% APR):

- Base APR: 3-5% (by total staked)
- Transaction fees: 0.5-2%
- MEV-Boost: 0.5-1% additional

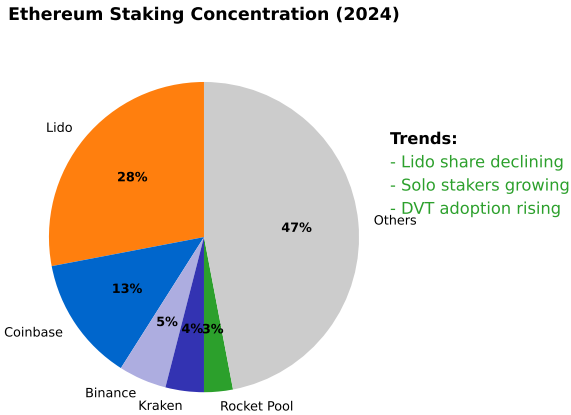
Risks:

- Slashing (malicious behavior/bugs)
- Inactivity penalties (offline)
- Locked capital (36-day exit)
- Technical/price risk

Net returns depend on uptime, MEV, and ETH price volatility.

(c) Joerg Osterrieder 2025

Centralization Risks: Stake Distribution



Top 5 entities: ~53% of staked ETH

33% threshold = finality blocking power

Top 5 entities control ∼53% of staked ETH – 33% threshold gives finality blocking power.

Centralization Concerns

Key Risks:

1. **Wealth Concentration:** Rich get richer (compound rewards), high 32 ETH barrier
2. **Exchange Dominance:** Lido $\sim$28%, Coinbase $\sim$13%, top 5 $\sim$55%
3. **Staking Pool Centralization:** Pool operators control validators
4. **Client Diversity:** Prysm $\sim$40% creates systemic risk

Mitigation Efforts:

- Promote client diversity (incentives for minority clients)
- Decentralized pools (Rocket Pool, DVT)
- Community norms against $>$33% concentration
- Lido share declining, solo stakers growing

MEV (Maximal Extractable Value)

Definition: Additional profit from reordering, inserting, or censoring transactions

How it Works:

1. Searchers find opportunities (arbitrage, liquidations)
2. Submit bundles to block builders
3. Builders construct MEV-optimized blocks
4. Validators select highest-paying block (MEV-Boost)

MEV-Boost: Used by $\sim$90% of validators, increases rewards 50-100%

Concerns:

- Centralizes block production (few builders dominate)
- Censorship risk (builders can exclude transactions)
- Users pay hidden costs (sandwich attacks)

2024-2025 Milestones

Network Growth:

- 34M+ ETH staked (28% of total supply)
- 1+ million active validators
- Network securing $400B+ in value

Protocol Upgrades:

- **Dencun (March 2024):** Proto-danksharding (EIP-4844), L2 fees down 90%+
- **July 2024:** Spot Ethereum ETFs approved by SEC
- Institutional staking products expanding

Restaking (EigenLayer):

- $15B+ in restaked ETH
- Validators secure additional networks
- Liquid restaking tokens (LRTs) proliferate

Problem Solved? Proof of Stake

The Original Problem

Can we secure networks without wasting energy?

How Proof of Stake Solves It

- Validators stake 32 ETH as collateral; slashing penalizes misbehavior (up to 99% stake loss for coordinated attacks)
- Beacon Chain coordinates validator committees via pseudo-random selection weighted by stake
- Casper FFG provides economic finality through checkpoint voting (67%+ attestations required)
- Ethereum reduced energy consumption by 99.95% after The Merge (Sept 2022)

Remaining Limitations

- "Rich get richer" centralization risk: staking rewards compound, 32 ETH barrier excludes smaller holders
- Nothing-at-stake problem solved by slashing, but still requires careful protocol design
- Lido controls 28% of stake, top 5 entities control 53% – approaching dangerous 33% finality blocking threshold

Open Questions

- Long-term security without external resource anchor (PoW uses electricity, PoS uses internal capital)
- Risk: Incentive misalignment, free-rider problems if staking rewards decline

Proof of Stake solves energy waste but introduces new trade-offs in wealth concentration and capital requirements

(c) Joerg Osterrieder 2025

Key Takeaways

- Proof-of-stake replaces computational work with economic stake
- Validators attest to blocks and occasionally propose new blocks
- Slashing penalizes malicious behavior, aligning incentives
- Casper FFG provides economic finality through checkpoint voting
- Ethereum's Beacon Chain reduced energy consumption by 99.95%
- Staking requires 32 ETH and generates 4-8% annual returns
- Centralization risks remain (exchanges, pools, client diversity)

Core Insight:
Proof-of-stake shifts blockchain security from external resources (energy) to internal resources (staked capital). Attackers must own and risk a significant portion of the network's value.

(c) Joerg Osterrieder 2025

Discussion Questions

1. How does slashing solve the nothing-at-stake problem?
2. Why is client diversity critical for proof-of-stake security?
3. What are the trade-offs between solo staking and using a staking pool?
4. How does the inactivity leak mechanism help restore finality?
5. Is proof-of-stake more or less centralized than proof-of-work?
6. What role does MEV play in validator economics?
7. How would a 33% attack differ from a 51% attack in PoS?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L10 Consensus Mechanism Comparison

Topics to be covered:

- Comprehensive comparison: PoW vs PoS vs DPoS vs PBFT
- Security models and assumptions
- Scalability and throughput trade-offs
- Energy consumption and sustainability
- Decentralization metrics
- Finality and confirmation times

Preparation:

- Review proof-of-work (Lesson 7) and proof-of-stake (Lesson 9)
- Read about Delegated Proof of Stake (DPoS) used in EOS, Tron
- Explore BFT consensus in Hyperledger, Cosmos

Quiz: Questions 1-5

Q1. What is the minimum amount of ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which of the following is NOT a slashable offense in Ethereum proof-of-stake?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations result in penalties but not slashing; only malicious behaviors are slashable.

Q3. What percentage of energy reduction did Ethereum achieve after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The transition from PoW to PoS reduced energy consumption by approximately 99.95%.

Q4. In Ethereum's PoS, how long is one epoch?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes
Answer: C – One epoch = 32 slots at 12 seconds each = 6.4 minutes.

Q5. What is the primary solution to the nothing-at-stake problem?
A) Higher staking rewards B) Slashing penalties C) Faster block times D) Lower barriers to entry
Answer: B – Slashing detects and penalizes validators who vote on conflicting blocks, eliminating costless voting.

Quiz: Questions 6-10

Q6. Which component manages validator selection and finalization in Ethereum?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain (Consensus Layer) coordinates validators, staking, and finalization.

Q7. What percentage of validator attestations is required for checkpoint justification?
A) 51% B) 67% C) 75% D) 100%
Answer: B – Casper FFG requires 67%+ attestations for a checkpoint to become justified.

Q8. When does the inactivity leak mechanism activate?
A) When a validator misses one attestation B) When gas fees are high
C) When the chain fails to finalize for more than 4 epochs D) During network upgrades
Answer: C – Inactivity leak activates when finalization stalls, penalizing offline validators to restore consensus.

Q9. What happens if 33% of validators are slashed together?
A) Each loses 1 ETH B) Each loses approximately 3% of stake
C) Each loses approximately 99% of stake D) No additional penalty beyond 1 ETH
Answer: C – Correlation penalty scales quadratically; 33% slashed together triggers catastrophic losses.

Q10. Which best describes validator delegation in Ethereum PoS?
A) Validators can delegate their voting power B) Users can delegate ETH to staking pools
C) The protocol randomly delegates validators to committees D) Delegation is not possible
Answer: B – Users can delegate ETH to pools like Lido or Rocket Pool; validators themselves do not delegate.

Quiz: Questions 11-15

Q11. What was the date of Ethereum's Merge to proof-of-stake?
A) December 1, 2020 B) September 15, 2022 C) March 13, 2024 D) January 10, 2024
Answer: B – The Merge occurred on September 15, 2022, transitioning Ethereum to PoS.

Q12. Approximately what APR do validators earn with 34M+ ETH staked (base rewards)?
A) 1-2% B) 3.2-3.5% C) 8-10% D) 15-20%
Answer: B – With 34M+ ETH staked, base APR is approximately 3.2-3.5%; MEV adds 30-50% more.

Q13. What is LMD GHOST used for in Ethereum PoS?
A) Slashing malicious validators B) Determining the canonical chain head
C) Calculating staking rewards D) Managing validator activation queue
Answer: B – LMD GHOST is the fork choice rule that selects the chain head before finalization.

Q14. How long does it typically take for a block to become finalized in Ethereum?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days
Answer: C – Finalization occurs after 2 epochs (approximately 12.8 minutes) via Casper FFG.

Q15. Which entity currently controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH, the largest single pool.

Quiz: Questions 16-20

Q16. What is the initial slashing penalty for a single slashable offense?
A) 0.1 ETH B) 1 ETH C) 5 ETH D) All 32 ETH
Answer: B – The initial penalty is 1 ETH; correlation penalties apply if many validators are slashed together.

Q17. What is MEV-Boost?
A) A protocol upgrade that increased block size B) A system allowing validators to select highest-paying blocks
C) A mechanism to reduce gas fees D) A new consensus algorithm
Answer: B – MEV-Boost lets validators access MEV-optimized blocks from builders, increasing rewards 50-100%.

Q18. At what balance is a validator automatically forced to exit?
A) Below 30 ETH B) Below 24 ETH C) Below 16 ETH D) Below 8 ETH
Answer: C – Validators with balance below 16 ETH are automatically ejected from the active set.

Q19. How does proof-of-stake fundamentally differ from proof-of-work in security?
A) PoS uses external resources (electricity) B) PoS uses internal resources (staked tokens)
C) PoS requires specialized hardware D) PoS has no security mechanism
Answer: B – PoS secures the network via internal economic stake, not external computational resources.

Q20. What percentage of validators must participate for finalization to occur?
A) 33% B) 51% C) 67% D) 100%
Answer: C – Casper FFG requires 67%+ validator participation for checkpoint finalization.

Proof of Stake Consensus

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

How Does Staking Work as a Security Deposit?

[COMIC: A validator nervously depositing 32 ETH into a giant vault labeled "Beacon Chain Security Deposit," while a stern protocol guardian holds a stamp reading "SLASHABLE" ready to mark any misbehavior]

Skin in the Game

- PoW: burn electricity to prove commitment (external cost)
- PoS: lock capital to prove commitment (internal cost)
- Misbehave? Your 32 ETH deposit gets slashed—up to 100% loss

32 ETH = $75,000+ at current prices—a serious commitment

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the proof-of-stake consensus mechanism
- Describe validator responsibilities: staking, attestation, block proposal
- Describe slashing conditions and economic penalties
- Analyze Ethereum's Beacon Chain architecture
- Distinguish between justification and finality
- Calculate staking rewards and economics
- Evaluate centralization risks in proof-of-stake systems

Building on L08: Lab: Wallet Setup

The Problem: Can we secure networks without wasting energy?

The Challenge
Can we secure a blockchain network with economic stake instead of energy expenditure? How do we prevent attacks when validation doesn't require external resource costs?

Why It Matters

- Proof-of-Work criticized for consuming electricity of entire countries (Bitcoin ∼120 TWh/year)
- Environmental concerns threaten blockchain adoption by institutions and governments
- Ethereum's PoW consumed energy equivalent to Finland (2021-2022)

What We Need

- Economic alignment of actors
- Security guarantees from capital at risk, not energy burn
- Ability to penalize malicious behavior economically
- Finality mechanism without computational competition

The Cryptoeconomics Question
Aligning individual and collective interests

Today's lesson: How Proof of Stake addresses this challenge

How Does Proof-of-Stake Differ from Proof-of-Work?

Proof of Work

- Security via computational cost
- Miners compete by hash power
- Energy-intensive
- Hardware requirements (ASICs)
- Block rewards + transaction fees
- 51% attack requires hash rate majority

Proof of Stake

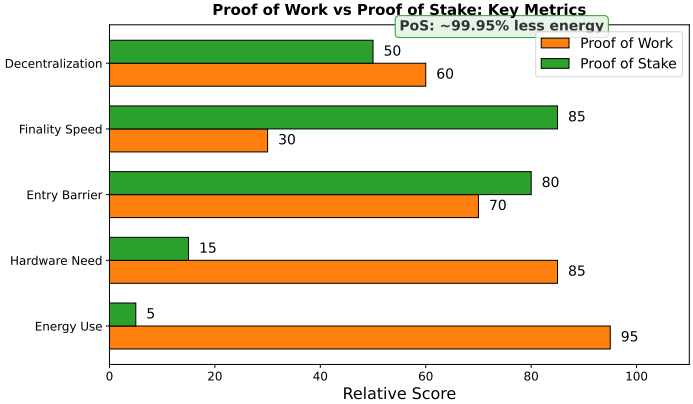
- Security via economic stake
- Validators selected by stake weight
- Energy-efficient (99% reduction)
- Capital requirements (staking)
- Transaction fees only (or low issuance)
- 51% attack requires token majority

Core Difference:

- PoW: external resource (electricity) $\rightarrow$ security
- PoS: internal resource (staked tokens) $\rightarrow$ security

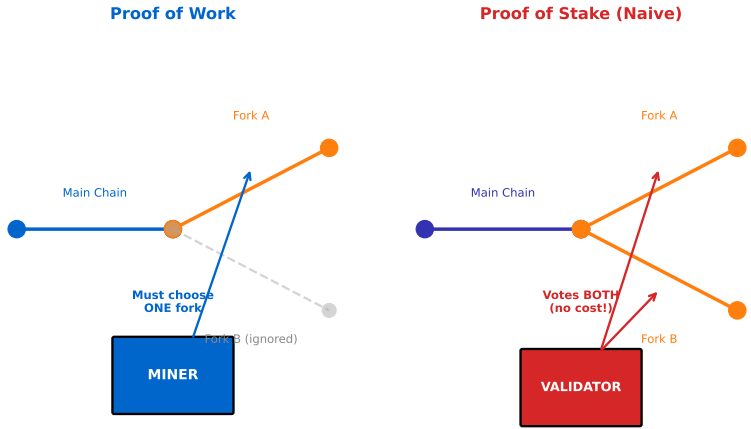
$\rightarrow$ *Problem: Can we secure networks without wasting... — Proof of Work vs. Proof of Stake: PoS replaces energy expenditure with economic stake while maintaining security guarantees*

PoW vs PoS: Quantitative Comparison



PoS dramatically reduces energy while improving finality time and throughput.

The Nothing-at-Stake Problem: Visualized



Solution: SLASHING detects double-voting and penalizes validators

Without slashing, validators have no cost to voting on every fork – a critical design flaw.

What is the Nothing-at-Stake Problem?

Theoretical Vulnerability:

In case of blockchain fork:

- PoW miners must choose one fork (cannot mine both simultaneously)
- PoS validators can vote on multiple forks simultaneously (no cost)
- Rational strategy: vote on all forks to maximize rewards

Solutions:

1. **Slashing:** Detect and penalize validators voting on conflicting blocks
2. **Finality Gadgets:** Checkpoint mechanisms (Casper FFG) prevent reversals

Practical Observation:

- Well-designed PoS systems have never experienced nothing-at-stake attacks
- Slashing and economic incentives effectively mitigate the threat

How Did Ethereum Transition to Proof-of-Stake?

The Merge (September 15, 2022):

- Ethereum transitioned from PoW to PoS
- Beacon Chain launched Dec 2020, ran parallel 21 months
- No downtime, seamless transition

Impact:

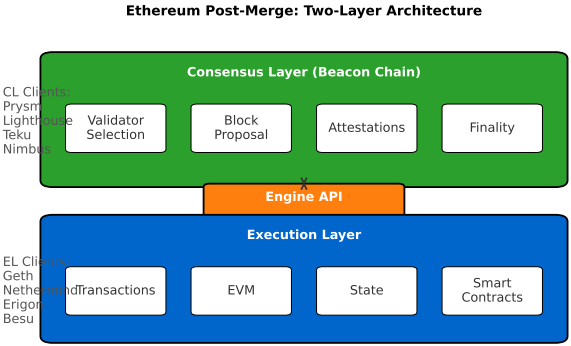
- Energy reduced by $\sim$99.95%
- ETH issuance $-$90% (13k $\rightarrow$ 1.6k ETH/day)
- Block time: $\sim$13s $\rightarrow$ $\sim$12s

Misconceptions Cleared:

- Did NOT reduce gas fees (Layer 2s)
- Did NOT increase throughput (sharding later)
- Changed consensus mechanism only

The Merge was the largest live protocol upgrade in blockchain history

Ethereum Beacon Chain Architecture



The Merge unified execution and consensus layers under PoS.

How Does the Beacon Chain's Two-Layer Design Work?

Execution Layer (EL):

- Processes transactions & smart contracts
- Maintains EVM and account state

Consensus Layer (Beacon Chain):

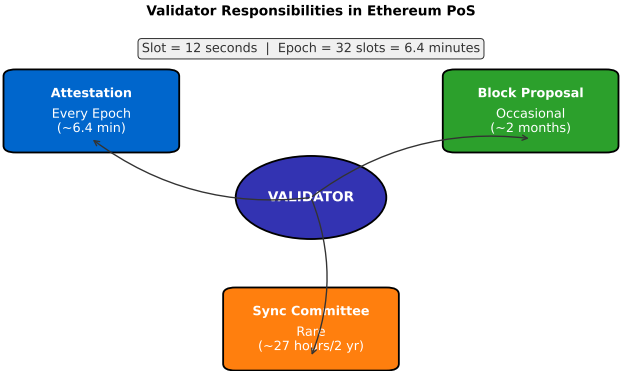
- Selects block proposers, coordinates validators
- Manages staking, slashing, finalization

Client Diversity:

- EL: Geth, Nethermind, Erigon, Besu
- CL: Prysm, Lighthouse, Teku, Nimbus
- Engine API connects layers

Multiple client implementations prevent single points of failure. | → Problem: Can we secure networks without wasting... — Beacon Chain: Two-Layer Design: The beacon chain coordinates validators using economic incentives instead of computational competition

Validator Responsibilities



Validators perform multiple duties with varying frequencies and reward structures.

What Are the Core Duties of Validators?

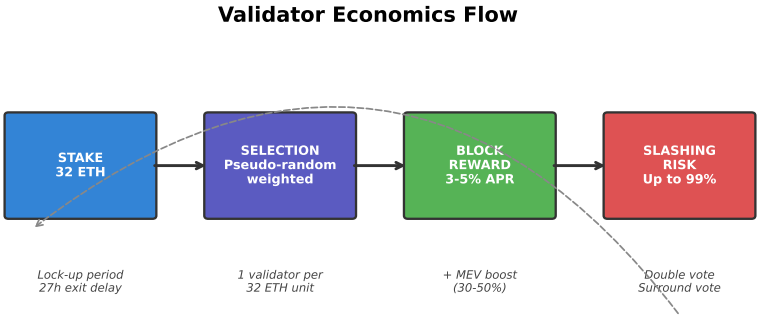
1. **Attestation (every epoch):**
   - Vote on chain head + checkpoints
   - Aggregated into blocks for efficiency
2. **Block Proposal (occasionally):**
   - Selected pseudo-randomly by stake
   - Earn transaction fees + block reward
3. **Sync Committee (rarely):**
   - Rotating $\sim$27 hour service period
   - Helps light clients sync

Timing:

- Slot = 12 seconds
- Epoch = 32 slots = 6.4 minutes

(c) Joerg Osterrieder 2025

Validator Economics: The Complete Picture



Honest behavior: Rewards compound, stake grows

Malicious behavior: Slashed, forced exit, capital lost

Economic incentives align validator behavior: stake at risk ensures honest participation.

What Do You Need to Become a Validator?

Minimum Stake: 32 ETH per validator

Staking Process:

1. Generate validator keys (BLS12-381)
2. Deposit 32 ETH to contract
3. Run validator client
4. Wait for activation, start attesting

Hardware Requirements:

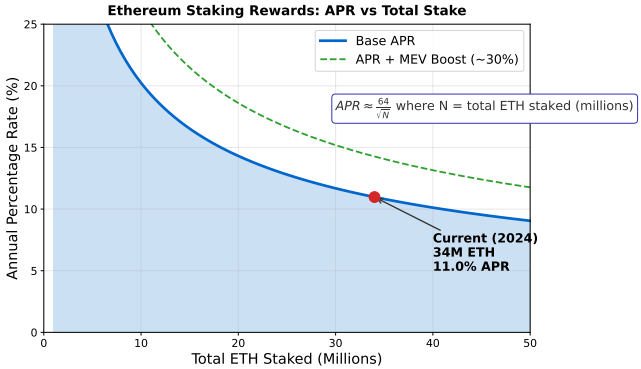
- CPU: 4+ cores — RAM: 16+ GB
- Storage: 2+ TB SSD
- 99%+ uptime — $50-200/month

Alternatives:

- Pools: Lido, Rocket Pool
- Exchanges: Coinbase, Kraken

(c) Joerg Osterrieder 2025

Staking Rewards: APR Curve



More stakers = lower APR due to reward dilution. MEV adds 30%+ boost.

How Are Validators Rewarded?

Reward Components:

1. **Attestation Rewards:** Earned for timely, correct attestations
2. **Block Proposal Rewards:** Transaction fees + attestation inclusion
3. **Sync Committee Rewards:** Small bonus for participation

Annual Percentage Rate (APR):

$$\text{APR} \approx \frac{64}{\sqrt{N}}$$

where N = total ETH staked (in millions)

Current State (2024-2025):

- 34M+ ETH staked: APR $\approx$ 3.2-3.5%
- Over 1 million active validators
- MEV-Boost adds 30-50% to base rewards

What Happens When Validators Go Offline?

Missed Attestation Penalty:

- Equal to reward you would have earned
- Balance decreases (linear, no compounding)

Inactivity Leak:

- Activated when finalization fails (> 4 epochs)
- Offline validators lose stake (quadratic rate)
- Purpose: eject offline to restore finality

Example Scenario:

- Network partition: 40% validators offline
- Cannot finalize (requires 67%)
- Inactivity leak begins, stake drains rapidly
- Chain resumes with remaining validators

→ Problem: Can we secure networks without wasting... — Penalties and Inactivity Leaks: Slashing and inactivity penalties ensure validators stay honest and online without wasting energy

Problem Check-In: Proof of Stake

Recall Our Problem

Can we secure networks without wasting energy?

What We've Learned So Far

- Validators stake 32 ETH as collateral, replacing computational work with economic stake
- Slashing penalizes double-voting and surround votes, making attacks costly
- Economic penalties replace energy expenditure while maintaining security guarantees

Still to Address

- Finality mechanism and checkpoint voting for irreversible transactions
- How do we prevent stake centralization in liquid staking pools?

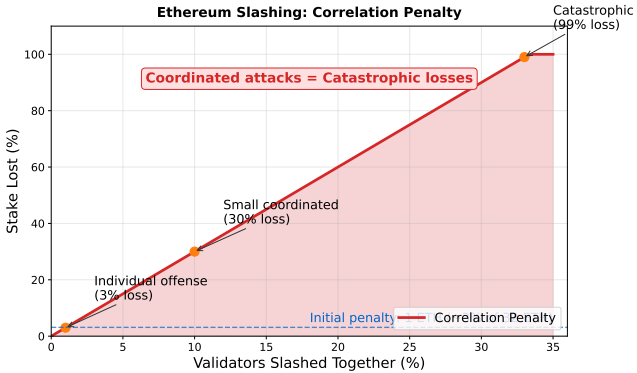
Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "Can we secure networks without wasting..."?

(c) Joerg Osterrieder 2025

Slashing: Correlation Penalty



Coordinated attacks result in catastrophic losses – strong deterrent against collusion.

What Actions Trigger Slashing?

Three Slashable Offenses:

1. **Double Proposal:** Two blocks for same slot
2. **Surround Vote:** Conflicting checkpoint votes
3. **Double Vote:** Two attestations in same epoch

Penalty Examples:

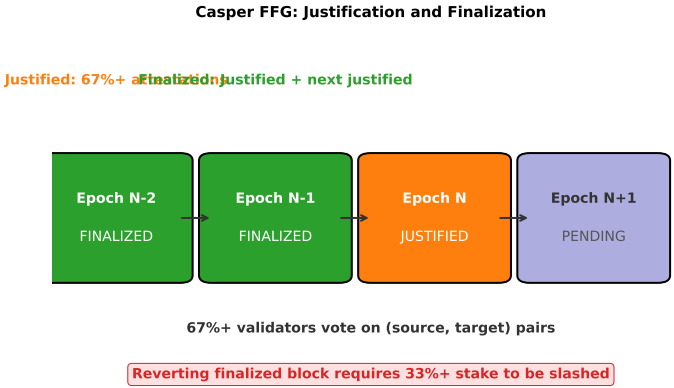
- 1% slashed together: lose $\sim$3%
- 33% slashed together: lose $\sim$99%

Slashing Penalties:

- **Initial:** 1 ETH (immediate)
- **Correlation:** Stake $\times$ 3 $\times$ (slashed/total)
- **Forced exit:** ejected from active set
- **Withdrawal delay:** 36 days

Correlation penalty makes coordinated attacks catastrophically expensive

Casper FFG: Finality Mechanism



Finalized blocks cannot be reverted without 33%+ stake being slashed.

How Does Casper FFG Provide Finality?

Purpose:

- Provide economic finality
- Prevent long-range reorganizations

Checkpoint Voting:

- Checkpoint = first block of epoch
- Validators vote: (source, target) pairs

Justification vs Finalization:

- **Justified:** 67%+ votes (can revert)
- **Finalized:** Justified + next epoch justified
- Takes ∼12.8 minutes (2 epochs)

Accountable Safety:
Conflicting checkpoints cannot finalize — attacker loses stake.

Finalized blocks cannot be reverted without 33%+ stake being slashed

How Does LMD GHOST Choose the Canonical Chain?

Purpose: Determine canonical chain head before finalization

LMD GHOST (Latest Message Driven Greedy Heaviest Observed SubTree):

1. Start at last finalized checkpoint
2. At each fork, choose subtree with most validator attestations
3. Recursively descend until leaf (chain head)

Example:

- Block A: 100 attestations — Block B: 150 attestations
- LMD GHOST selects Block B as canonical

Combination with Casper FFG:

- LMD GHOST: determines head (short-term)
- Casper FFG: determines finality (long-term)
- Together: fast confirmation + eventual certainty

What Are the Stages of a Validator's Lifecycle?

States:

1. **Deposited:** 32 ETH deposited, waiting in activation queue
2. **Active:** Attesting and proposing, earning rewards/penalties
3. **Exiting:** Voluntary exit initiated, still active for $\sim$1 day
4. **Exited:** No longer active, funds locked for 27 hours
5. **Withdrawable:** Funds available (auto-withdrawal after Shanghai)

Forced Exit:

- Triggered by slashing or balance $<$ 16 ETH
- Validator ejected automatically

$\rightarrow$ *Problem: Can we secure networks without wasting... — Validator Lifecycle: The validator lifecycle ensures orderly entry and exit while maintaining network security*

What Are the Risks and Rewards of Staking?

Rewards (4-8% APR):

- Base APR: 3-5% (by total staked)
- Transaction fees: 0.5-2%
- MEV-Boost: 0.5-1% additional

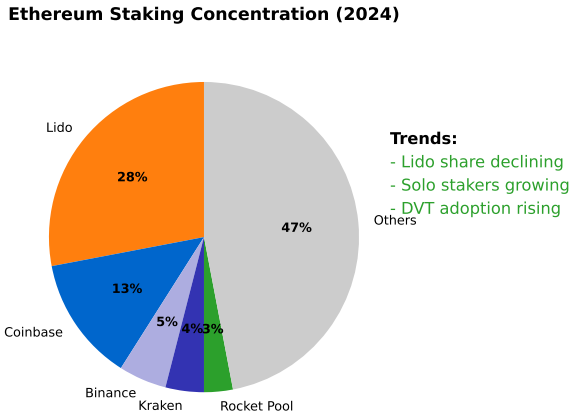
Risks:

- Slashing (malicious behavior/bugs)
- Inactivity penalties (offline)
- Locked capital (36-day exit)
- Technical/price risk

Net returns depend on uptime, MEV, and ETH price volatility.

(c) Joerg Osterrieder 2025

Centralization Risks: Stake Distribution



Top 5 entities: ~53% of staked ETH

33% threshold = finality blocking power

Top 5 entities control ∼53% of staked ETH – 33% threshold gives finality blocking power.

What Centralization Risks Does Proof of Stake Face?

Key Risks:

1. **Wealth Concentration:** Rich get richer, 32 ETH barrier
2. **Exchange Dominance:** Lido $\sim$28%, top 5 $\sim$55%
3. **Pool Centralization:** Operators control validators
4. **Client Diversity:** Prysm $\sim$40% systemic risk

Mitigation Efforts:

- Incentives for minority clients
- Decentralized pools (Rocket Pool, DVT)
- Community norms against $>$33%
- Lido declining, solo stakers growing

Centralization threatens PoS: 33% stake gives finality blocking power

How Do Validators Extract MEV?

How it Works:

1. Searchers find opportunities (arbitrage, liquidations)
2. Submit bundles to block builders
3. Builders construct MEV-optimized blocks
4. Validators select highest-paying block

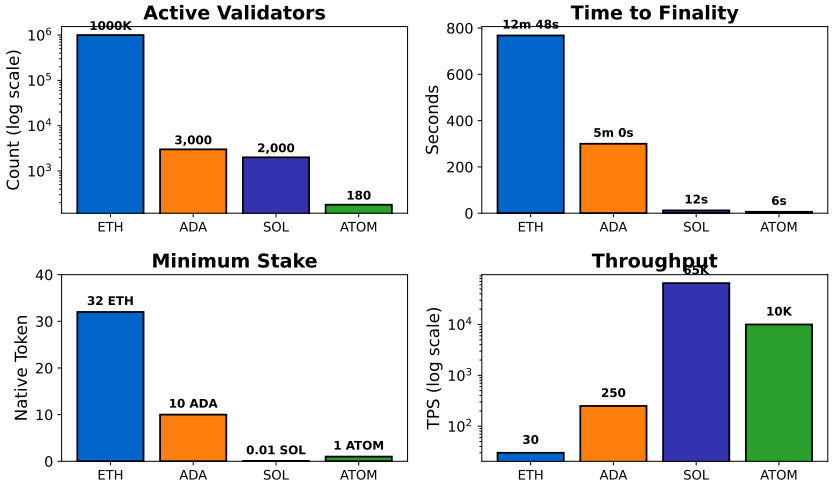
MEV-Boost: Used by $\sim$90% of validators, +50-100% rewards

Concerns:

- Centralizes block production (few builders)
- Censorship risk (exclude transactions)
- Users pay hidden costs (sandwich attacks)

MEV is additional profit from transaction ordering – a double-edged sword for validator economics

PoS Variants: Protocol Comparison



Each PoS variant optimizes different trade-offs: decentralization vs. throughput vs. finality speed.

What Happened in Ethereum PoS (2024-2025)?

Network Growth:

- 34M+ ETH staked (28% of supply)
- 1M+ active validators
- Securing $400B+ in value

Protocol Upgrades:

- **Dencun (Mar 2024):** EIP-4844, L2 fees $-90\%+$
- **Jul 2024:** Spot ETH ETFs approved
- Institutional staking expanding

Restaking (EigenLayer):

- $15B+ in restaked ETH
- Validators secure additional networks
- Liquid restaking tokens (LRTs) proliferate

Ethereum PoS matured rapidly: 34M+ ETH staked, institutional adoption accelerating

Problem Solved? Proof of Stake

The Original Problem

Can we secure networks without wasting energy?

How Proof of Stake Solves It

- Validators stake 32 ETH as collateral; slashing penalizes misbehavior (up to 99% stake loss for coordinated attacks)
- Beacon Chain coordinates validator committees via pseudo-random selection weighted by stake
- Casper FFG provides economic finality through checkpoint voting (67%+ attestations required)
- Ethereum reduced energy consumption by 99.95% after The Merge (Sept 2022)

Remaining Limitations

- "Rich get richer" centralization risk: staking rewards compound, 32 ETH barrier excludes smaller holders
- Nothing-at-stake problem solved by slashing, but still requires careful protocol design
- Lido controls 28% of stake, top 5 entities control 53% – approaching dangerous 33% finality blocking threshold

Open Questions

- Long-term security without external resource anchor (PoW uses electricity, PoS uses internal capital)
- Risk: Incentive misalignment, free-rider problems if staking rewards decline

Proof of Stake solves energy waste but introduces new trade-offs in wealth concentration and capital requirements

(c) Joerg Osterrieder 2025

The Economics of Proof of Stake

Incentive Structure

- **Core Problem:** Aligning individual and collective interests
- **Why act honestly?** Rewards for honest behavior, penalties for cheating
- **Value Flow:** Protocol gains security, participants earn rewards

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Protocol gains security, participants earn rewards

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Proof of Stake

Alternatives Considered

1. **Chosen Design:** Reward curves, slashing conditions
2. **Alternative:** Alternative reward mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Proof of Stake

Critical Failure Mode

- **What breaks:** Incentive misalignment, free-rider problems
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Nothing-at-stake problem

[COMIC: A validator character smugly betting on every horse in a race (each fork of the chain), saying "I'll vote for ALL of them!"—until a slashing sword descends from above labeled "Caught double-voting"]

Why Slashing Exists

- Without penalties, validators could vote on every fork (costless)
- Slashing creates real economic consequences for equivocation
- Coordinated attacks: up to 99% stake loss via correlation penalty

Nothing-at-stake was the #1 theoretical objection to PoS—slashing solved it

Key Takeaways

- Proof-of-stake replaces computational work with economic stake
- Validators attest to blocks and occasionally propose new blocks
- Slashing penalizes malicious behavior, aligning incentives
- Casper FFG provides economic finality through checkpoint voting
- Ethereum's Beacon Chain reduced energy consumption by 99.95%
- Staking requires 32 ETH and generates 4-8% annual returns
- Centralization risks remain (exchanges, pools, client diversity)

Core Insight:
Proof-of-stake shifts blockchain security from external resources (energy) to internal resources (staked capital). Attackers must own and risk a significant portion of the network's value.

Next Lesson: L10 – Consensus Comparison

(c) Joerg Osterrieder 2025

Discussion Questions

1. How does slashing solve the nothing-at-stake problem?
2. Why is client diversity critical for proof-of-stake security?
3. What are the trade-offs between solo staking and using a staking pool?
4. How does the inactivity leak mechanism help restore finality?
5. Is proof-of-stake more or less centralized than proof-of-work?
6. What role does MEV play in validator economics?
7. How would a 33% attack differ from a 51% attack in PoS?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L10 Consensus Mechanism Comparison

Topics to be covered:

- Comprehensive comparison: PoW vs PoS vs DPoS vs PBFT
- Security models and assumptions
- Scalability and throughput trade-offs
- Energy consumption and sustainability
- Decentralization metrics
- Finality and confirmation times

Preparation:

- Review proof-of-work (Lesson 7) and proof-of-stake (Lesson 9)
- Read about Delegated Proof of Stake (DPoS) used in EOS, Tron
- Explore BFT consensus in Hyperledger, Cosmos

Quiz: Questions 1-5

Q1. What is the minimum amount of ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which of the following is NOT a slashable offense in Ethereum proof-of-stake?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations result in penalties but not slashing; only malicious behaviors are slashable.

Q3. What percentage of energy reduction did Ethereum achieve after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The transition from PoW to PoS reduced energy consumption by approximately 99.95%.

Q4. In Ethereum's PoS, how long is one epoch?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes
Answer: C – One epoch = 32 slots at 12 seconds each = 6.4 minutes.

Q5. What is the primary solution to the nothing-at-stake problem?
A) Higher staking rewards B) Slashing penalties C) Faster block times D) Lower barriers to entry
Answer: B – Slashing detects and penalizes validators who vote on conflicting blocks, eliminating costless voting.

Quiz: Questions 6-10

Q6. Which component manages validator selection and finalization in Ethereum?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain (Consensus Layer) coordinates validators, staking, and finalization.

Q7. What percentage of validator attestations is required for checkpoint justification?
A) 51% B) 67% C) 75% D) 100%
Answer: B – Casper FFG requires 67%+ attestations for a checkpoint to become justified.

Q8. When does the inactivity leak mechanism activate?
A) When a validator misses one attestation B) When gas fees are high
C) When the chain fails to finalize for more than 4 epochs D) During network upgrades
Answer: C – Inactivity leak activates when finalization stalls, penalizing offline validators to restore consensus.

Q9. What happens if 33% of validators are slashed together?
A) Each loses 1 ETH B) Each loses approximately 3% of stake
C) Each loses approximately 99% of stake D) No additional penalty beyond 1 ETH
Answer: C – Correlation penalty scales quadratically; 33% slashed together triggers catastrophic losses.

Q10. Which best describes validator delegation in Ethereum PoS?
A) Validators can delegate their voting power B) Users can delegate ETH to staking pools
C) The protocol randomly delegates validators to committees D) Delegation is not possible
Answer: B – Users can delegate ETH to pools like Lido or Rocket Pool; validators themselves do not delegate.

Quiz: Questions 11-15

Q11. What was the date of Ethereum's Merge to proof-of-stake?
A) December 1, 2020 B) September 15, 2022 C) March 13, 2024 D) January 10, 2024
Answer: B – The Merge occurred on September 15, 2022, transitioning Ethereum to PoS.

Q12. Approximately what APR do validators earn with 34M+ ETH staked (base rewards)?
A) 1-2% B) 3.2-3.5% C) 8-10% D) 15-20%
Answer: B – With 34M+ ETH staked, base APR is approximately 3.2-3.5%; MEV adds 30-50% more.

Q13. What is LMD GHOST used for in Ethereum PoS?
A) Slashing malicious validators B) Determining the canonical chain head
C) Calculating staking rewards D) Managing validator activation queue
Answer: B – LMD GHOST is the fork choice rule that selects the chain head before finalization.

Q14. How long does it typically take for a block to become finalized in Ethereum?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days
Answer: C – Finalization occurs after 2 epochs (approximately 12.8 minutes) via Casper FFG.

Q15. Which entity currently controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH, the largest single pool.

Quiz: Questions 16-20

Q16. What is the initial slashing penalty for a single slashable offense?
A) 0.1 ETH B) 1 ETH C) 5 ETH D) All 32 ETH
Answer: B – The initial penalty is 1 ETH; correlation penalties apply if many validators are slashed together.

Q17. What is MEV-Boost?
A) A protocol upgrade that increased block size B) A system allowing validators to select highest-paying blocks
C) A mechanism to reduce gas fees D) A new consensus algorithm
Answer: B – MEV-Boost lets validators access MEV-optimized blocks from builders, increasing rewards 50-100%.

Q18. At what balance is a validator automatically forced to exit?
A) Below 30 ETH B) Below 24 ETH C) Below 16 ETH D) Below 8 ETH
Answer: C – Validators with balance below 16 ETH are automatically ejected from the active set.

Q19. How does proof-of-stake fundamentally differ from proof-of-work in security?
A) PoS uses external resources (electricity) B) PoS uses internal resources (staked tokens)
C) PoS requires specialized hardware D) PoS has no security mechanism
Answer: B – PoS secures the network via internal economic stake, not external computational resources.

Q20. What percentage of validators must participate for finalization to occur?
A) 33% B) 51% C) 67% D) 100%
Answer: C – Casper FFG requires 67%+ validator participation for checkpoint finalization.

L09: Proof of Stake Consensus

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

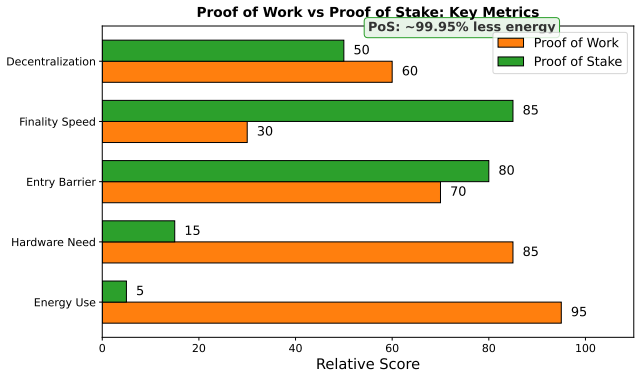
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

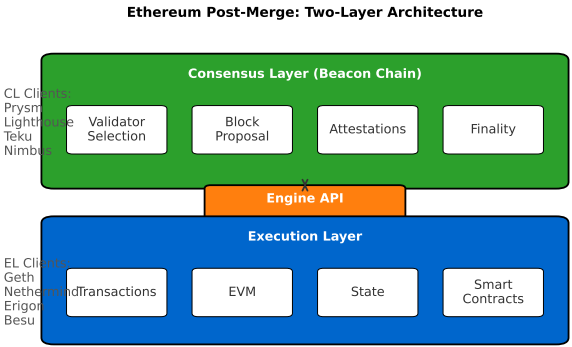
- Explain the proof-of-stake consensus mechanism
- Describe validator responsibilities and slashing
- Understand Ethereum's Beacon Chain architecture
- Analyze staking economics and centralization risks

PoW vs PoS: Comparison



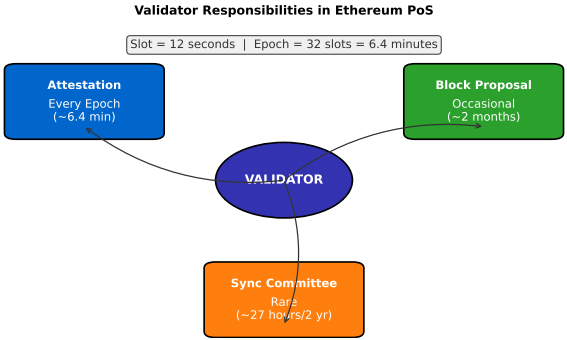
Core Difference: PoW uses external resources (energy); PoS uses internal resources (staked tokens).

Ethereum Beacon Chain Architecture



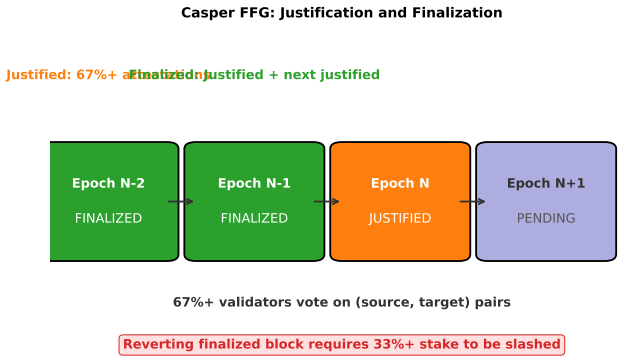
The Merge (Sept 15, 2022): 99.95% energy reduction, 90% lower issuance.

Validator Responsibilities



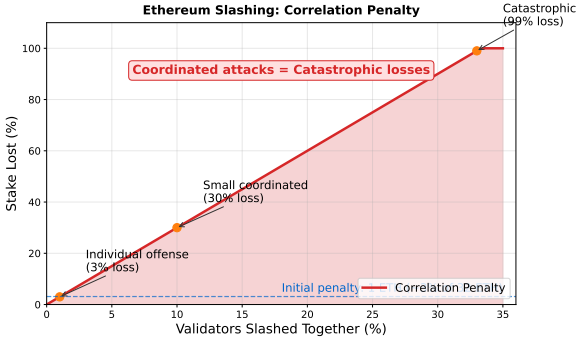
Timing: Slot = 12 seconds — Epoch = 32 slots = 6.4 minutes.

Casper FFG: Finality Mechanism



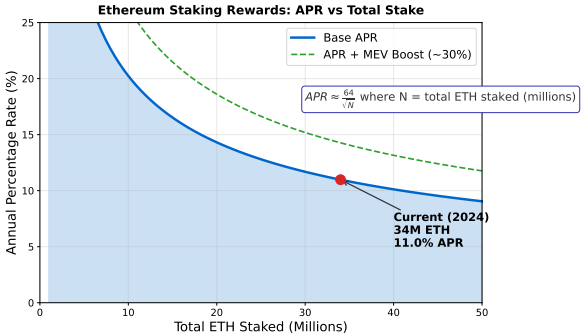
Justification: 67%+ attestations — **Finalization:** 12.8 minutes (2 epochs).

Slashing: Economic Security



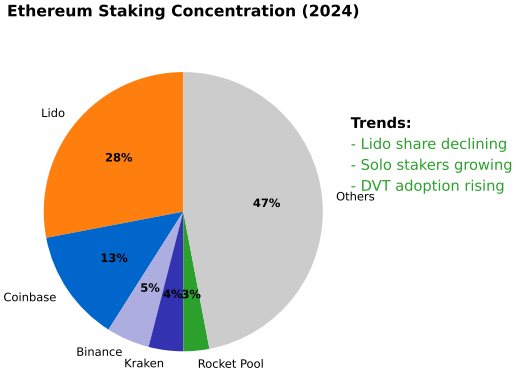
Slashable offenses: Double proposal, surround vote, double vote.
33% slashed together: Lose 99% of stake (catastrophic penalty).

Staking Rewards and Economics



Current State (2024-2025): 34M+ ETH staked, 1M+ validators, 3.5% base APR + MEV.

Centralization Risks



Top 5 entities: ~53% of staked ETH

33% threshold = finality blocking power

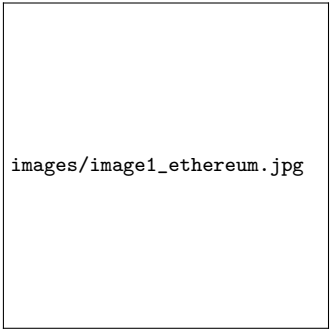
Concerns: Lido 28%, top 5 entities 55% — 33% threshold = finality blocking power.
Mitigations: Client diversity, DVT, solo staking growth.

Key Takeaways

1. **PoS:** Replaces computational work with economic stake
2. **Validators:** Attest to blocks, occasionally propose, earn rewards/penalties
3. **Slashing:** Penalizes malicious behavior – coordinated attacks lose 99%
4. **Finality:** Casper FFG provides economic finality in 12.8 minutes
5. **Staking:** 32 ETH minimum, 4-8% annual returns with MEV

Core Insight: PoS shifts security from external resources (energy) to internal resources (staked capital). Attackers must own and risk significant network value.

Proof of Stake in Practice



Ethereum Network

Staking Capital

Validators

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the minimum ETH required to run a validator?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH

Quiz (1/2)

Q1. What is the minimum ETH required to run a validator?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement.

Q2. Which is NOT a slashable offense?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote

Quiz (1/2)

Q1. What is the minimum ETH required to run a validator?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement.

Q2. Which is NOT a slashable offense?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations cause penalties but not slashing.

Q3. What energy reduction did The Merge achieve?
A) 50% B) 75% C) 90% D) 99.95%

Quiz (1/2)

Q1. What is the minimum ETH required to run a validator?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement.

Q2. Which is NOT a slashable offense?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations cause penalties but not slashing.

Q3. What energy reduction did The Merge achieve?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – Transition from PoW to PoS reduced energy by 99.95%.

Q4. How long is one epoch in Ethereum?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes

Quiz (1/2)

Q1. What is the minimum ETH required to run a validator?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement.

Q2. Which is NOT a slashable offense?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations cause penalties but not slashing.

Q3. What energy reduction did The Merge achieve?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – Transition from PoW to PoS reduced energy by 99.95%.

Q4. How long is one epoch in Ethereum?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes
Answer: C – One epoch = 32 slots at 12 seconds each = 6.4 minutes.

Q5. What percentage of attestations required for checkpoint justification?
A) 51% B) 67% C) 75% D) 100%

Quiz (1/2)

Q1. What is the minimum ETH required to run a validator?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement.

Q2. Which is NOT a slashable offense?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations cause penalties but not slashing.

Q3. What energy reduction did The Merge achieve?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – Transition from PoW to PoS reduced energy by 99.95%.

Q4. How long is one epoch in Ethereum?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes
Answer: C – One epoch = 32 slots at 12 seconds each = 6.4 minutes.

Q5. What percentage of attestations required for checkpoint justification?
A) 51% B) 67% C) 75% D) 100%
Answer: B – Casper FFG requires 67%+ for justification.

Quiz (2/2)

Q6. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024

Quiz (2/2)

Q6. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred September 15, 2022.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH B) Lose 3% of stake C) Lose 99% of stake D) No penalty

Quiz (2/2)

Q6. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred September 15, 2022.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH B) Lose 3% of stake C) Lose 99% of stake D) No penalty
Answer: C – Correlation penalty triggers catastrophic 99% loss.

Q8. Which pool controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool

Quiz (2/2)

Q6. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred September 15, 2022.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH B) Lose 3% of stake C) Lose 99% of stake D) No penalty
Answer: C – Correlation penalty triggers catastrophic 99% loss.

Q8. Which pool controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH.

Q9. How long does finalization typically take?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days

Quiz (2/2)

Q6. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred September 15, 2022.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH B) Lose 3% of stake C) Lose 99% of stake D) No penalty
Answer: C – Correlation penalty triggers catastrophic 99% loss.

Q8. Which pool controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH.

Q9. How long does finalization typically take?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days
Answer: C – Finalization occurs after 2 epochs (12.8 minutes).

Q10. What is MEV-Boost used by 90% of validators for?
A) Reduce gas fees B) Select highest-paying blocks C) Speed up finality D) Run multiple validators

Quiz (2/2)

Q6. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred September 15, 2022.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH B) Lose 3% of stake C) Lose 99% of stake D) No penalty
Answer: C – Correlation penalty triggers catastrophic 99% loss.

Q8. Which pool controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH.

Q9. How long does finalization typically take?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days
Answer: C – Finalization occurs after 2 epochs (12.8 minutes).

Q10. What is MEV-Boost used by 90% of validators for?
A) Reduce gas fees B) Select highest-paying blocks C) Speed up finality D) Run multiple validators
Answer: B – MEV-Boost lets validators access MEV-optimized blocks.

Thank you

Questions?

Next: L10 – Consensus Mechanism Comparison

Quiz: Proof of Stake

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the minimum ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH

Quiz (1–5)

Q1. What is the minimum ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which is NOT a slashable offense in Ethereum PoS?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote

Quiz (1–5)

Q1. What is the minimum ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which is NOT a slashable offense in Ethereum PoS?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations incur penalties but not slashing.

Q3. What energy reduction did Ethereum achieve after The Merge?
A) 50% B) 75% C) 90% D) 99.95%

Quiz (1–5)

Q1. What is the minimum ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which is NOT a slashable offense in Ethereum PoS?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations incur penalties but not slashing.

Q3. What energy reduction did Ethereum achieve after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – PoS reduced energy consumption by approximately 99.95%.

Q4. How long is one epoch in Ethereum PoS?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the minimum ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which is NOT a slashable offense in Ethereum PoS?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations incur penalties but not slashing.

Q3. What energy reduction did Ethereum achieve after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – PoS reduced energy consumption by approximately 99.95%.

Q4. How long is one epoch in Ethereum PoS?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes
Answer: C – One epoch = 32 slots at 12 seconds each = 6.4 minutes.

Q5. What percentage of attestations is required for checkpoint justification?
A) 51% B) 67% C) 75% D) 100%

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the minimum ETH required to run a single validator on Ethereum?
A) 16 ETH B) 24 ETH C) 32 ETH D) 64 ETH
Answer: C – 32 ETH is the all-or-nothing activation requirement per validator.

Q2. Which is NOT a slashable offense in Ethereum PoS?
A) Double proposal B) Missed attestation C) Surround vote D) Double vote
Answer: B – Missed attestations incur penalties but not slashing.

Q3. What energy reduction did Ethereum achieve after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – PoS reduced energy consumption by approximately 99.95%.

Q4. How long is one epoch in Ethereum PoS?
A) 12 seconds B) 32 seconds C) 6.4 minutes D) 12.8 minutes
Answer: C – One epoch = 32 slots at 12 seconds each = 6.4 minutes.

Q5. What percentage of attestations is required for checkpoint justification?
A) 51% B) 67% C) 75% D) 100%
Answer: B – Casper FFG requires 67%+ attestations for justification.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which component manages validator selection and finalization?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism

Quiz (6–10)

Q6. Which component manages validator selection and finalization?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain coordinates validators, staking, and finalization.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH each B) Lose $\sim$3% C) Lose $\sim$99% D) No additional penalty

Quiz (6–10)

Q6. Which component manages validator selection and finalization?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain coordinates validators, staking, and finalization.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH each B) Lose $\sim$3% C) Lose $\sim$99% D) No additional penalty
Answer: C – Correlation penalty scales quadratically; 33% triggers catastrophic losses.

Q8. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which component manages validator selection and finalization?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain coordinates validators, staking, and finalization.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH each B) Lose $\sim$3% C) Lose $\sim$99% D) No additional penalty
Answer: C – Correlation penalty scales quadratically; 33% triggers catastrophic losses.

Q8. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred on September 15, 2022.

Q9. Which entity controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool

Quiz (6–10)

Q6. Which component manages validator selection and finalization?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain coordinates validators, staking, and finalization.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH each B) Lose $\sim$3% C) Lose $\sim$99% D) No additional penalty
Answer: C – Correlation penalty scales quadratically; 33% triggers catastrophic losses.

Q8. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred on September 15, 2022.

Q9. Which entity controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH.

Q10. How long does it typically take for a block to become finalized?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which component manages validator selection and finalization?
A) Execution Layer B) Beacon Chain C) EVM D) Gas mechanism
Answer: B – The Beacon Chain coordinates validators, staking, and finalization.

Q7. What happens if 33% of validators are slashed together?
A) Lose 1 ETH each B) Lose ∼3% C) Lose ∼99% D) No additional penalty
Answer: C – Correlation penalty scales quadratically; 33% triggers catastrophic losses.

Q8. When was Ethereum's Merge to proof-of-stake?
A) December 2020 B) September 2022 C) March 2024 D) January 2024
Answer: B – The Merge occurred on September 15, 2022.

Q9. Which entity controls the largest share of staked ETH?
A) Coinbase B) Binance C) Lido D) Rocket Pool
Answer: C – Lido controls approximately 28% of staked ETH.

Q10. How long does it typically take for a block to become finalized?
A) 12 seconds B) 6.4 minutes C) 12.8 minutes D) 36 days
Answer: C – Finalization occurs after 2 epochs (∼12.8 minutes) via Casper FFG.

(c) Joerg Osterrieder 2025

Consensus Mechanism Comparison

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Compare proof-of-work, proof-of-stake, delegated proof-of-stake, and PBFT
- Evaluate security models and threat assumptions
- Analyze scalability and throughput trade-offs
- Assess energy consumption and environmental impact
- Measure decentralization across consensus protocols
- Understand finality and confirmation time differences
- Select appropriate consensus mechanism for specific use cases

The Problem: Why can't we have fast, secure, AND decentralized?

The Challenge
Why can't we have fast, secure, AND decentralized consensus simultaneously? Every blockchain must make fundamental trade-offs between these three properties.

Why It Matters

- Every blockchain makes trade-offs between speed, security, and openness
- Bitcoin chose security over speed; Solana chose speed over decentralization

What We Need

- Understanding design constraints
- Framework to evaluate consensus trade-offs across different mechanisms

The Cryptoeconomics Question
Optimizing multiple competing goals

Today's lesson: How Consensus Comparison addresses this challenge

Consensus Mechanisms Overview

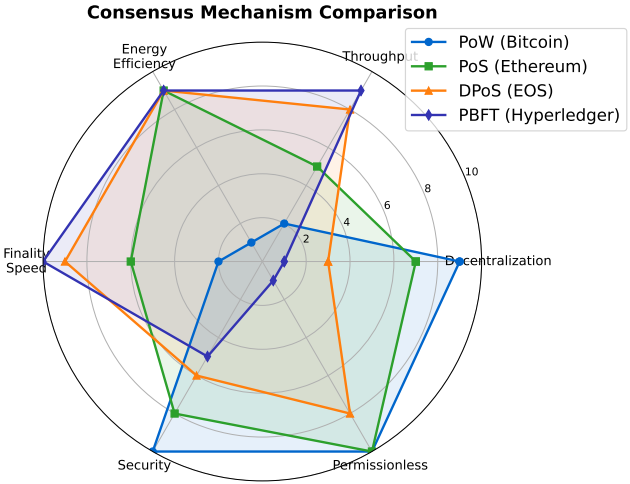
What is Consensus?

- Agreement among distributed nodes on shared state
- Ensures all participants have same transaction history
- Prevents double-spending and conflicting updates

Major Consensus Families:

1. **Proof-of-Work (PoW):** Bitcoin, Litecoin, Dogecoin
2. **Proof-of-Stake (PoS):** Ethereum, Cardano, Polkadot
3. **Delegated Proof-of-Stake (DPoS):** EOS, Tron, Cosmos
4. **Practical BFT (PBFT):** Hyperledger Fabric, Zilliqa
5. **Hybrid Models:** Decred (PoW + PoS), Algorand (Pure PoS + VRF)

Consensus Mechanism Comparison



No single mechanism excels in all dimensions – trade-offs are fundamental.

Proof of Work: Deep Dive

Mechanism:

- Miners compete to find valid block hash (difficulty target)
- First to find valid hash broadcasts block

Security Model:

- Honest majority: $> 50\%$ hash rate honest
- Attack cost proportional to hash rate
- Probabilistic finality (deeper blocks = safer)

Advantages:

- Proven security (Bitcoin: 15+ years, no successful attack)
- No trusted setup, permissionless, external security

Disadvantages:

- High energy (150 TWh/year for Bitcoin)
- Low throughput (7 TPS), slow finality (1 hour)

Proof of Stake: Deep Dive

Mechanism:

- Validators stake tokens as collateral
- Weighted random selection for proposals
- Slashing for misbehavior

Security Model:

- 67%+ honest stake for finality
- Attack cost = price $\times$ stake

Advantages:

- 99% energy reduction vs PoW
- Faster finality (12 min ETH)
- Attackers lose stake

Disadvantages:

- Wealth concentration
- Centralization via pools

(c) Joerg Osterrieder 2025

Delegated Proof of Stake (DPoS)

Mechanism:

- Token holders vote for delegates (block producers)
- Top N delegates (21 in EOS, 27 in Tron) produce blocks in rotation
- Delegates share rewards with voters

Security Model:

- Honest majority: $> 50\%$ of delegates honest
- Reputation-based trust (delegates have identities)

Advantages:

- High throughput (4,000 TPS for EOS)
- Fast finality (1-3 seconds), energy-efficient

Disadvantages:

- High centralization (only 21-100 block producers)
- Voter apathy, plutocracy, cartel risk

Practical Byzantine Fault Tolerance (PBFT)

Mechanism:

- Pre-selected committee of validators
- Three-phase consensus: pre-prepare, prepare, commit
- 2/3+ agreement required to finalize block

Security Model:

- BFT: tolerates $< 1/3$ malicious nodes
- Known validator set (permissioned)

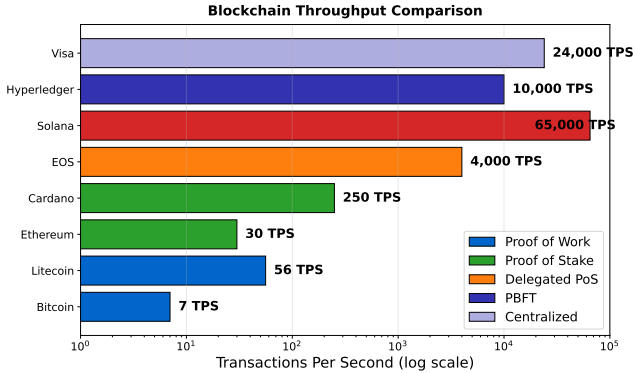
Advantages:

- Instant finality (no probabilistic confirmation)
- High throughput (1,000-10,000 TPS), energy-efficient

Disadvantages:

- Requires permissioned network
- Poor scalability ($O(N^2)$ communication)
- Centralized, not censorship-resistant

Throughput Comparison



Higher throughput typically requires sacrificing decentralization.

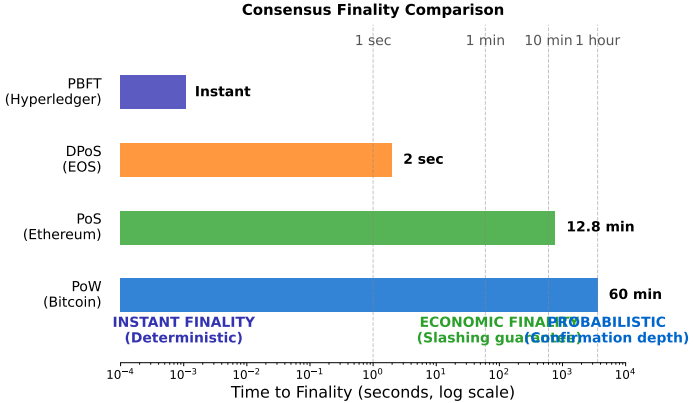
Consensus Comparison Table

Property	PoW	PoS	DPoS	PBFT
Throughput	7-15 TPS	30-100 TPS	1,000-4,000	1,000-10,000
Finality	Probabilistic	10-15 min	1-3 sec	Instant
Energy	Very High	Very Low	Very Low	Very Low
Decentralization	High	Medium	Low	Very Low
Permissionless	Yes	Yes	Yes	No
Attack Cost	Hash rate	Stake value	Vote buying	Compromise 1/3

Key Insight:

- No consensus mechanism is universally superior
- Trade-offs exist between decentralization, scalability, and finality
- Choice depends on use case requirements

Finality Comparison



Finality type affects settlement guarantees and application design.

Security Analysis: Attack Vectors

Proof of Work:

- **51% Attack:** control $> 50\%$ hash rate
- Cost: hardware + electricity (billions for Bitcoin)

Proof of Stake:

- **33% Attack (liveness):** prevent finality with 33% stake
- **67% Attack (safety):** finalize conflicting blocks
- Mitigation: slashing destroys attacker's stake

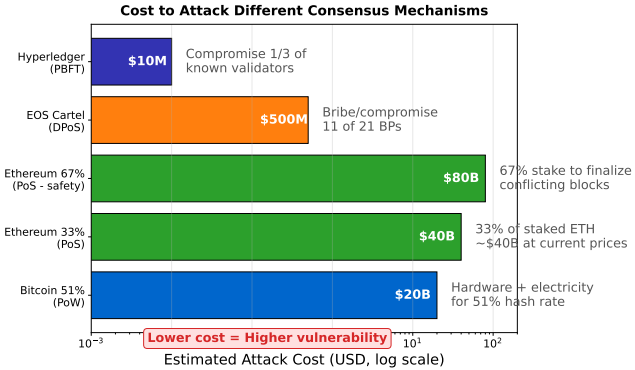
Delegated Proof of Stake:

- **Delegate Cartel:** majority of delegates collude
- **Vote Buying:** bribe token holders for votes

PBFT:

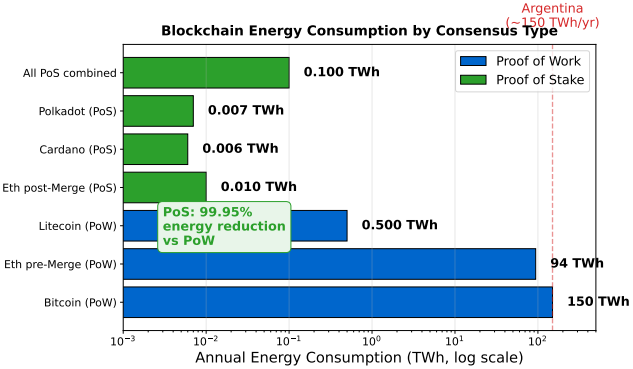
- **Byzantine Generals:** $> 1/3$ validators malicious
- Cost depends on permission model (regulatory/legal)

Attack Cost Comparison



Economic security varies dramatically across consensus mechanisms.

Energy Consumption Analysis



The Merge reduced Ethereum's energy by 99.95% – from Argentina's usage to negligible.

Energy and Environmental Context

Bitcoin Energy Usage:

- 150 TWh/year – comparable to Argentina
- 70 Mt CO2/year carbon footprint

PoS Reduction:

- Ethereum post-Merge: 0.01 TWh/year (99.95% reduction)
- All PoS chains combined: < 0.1 TWh/year

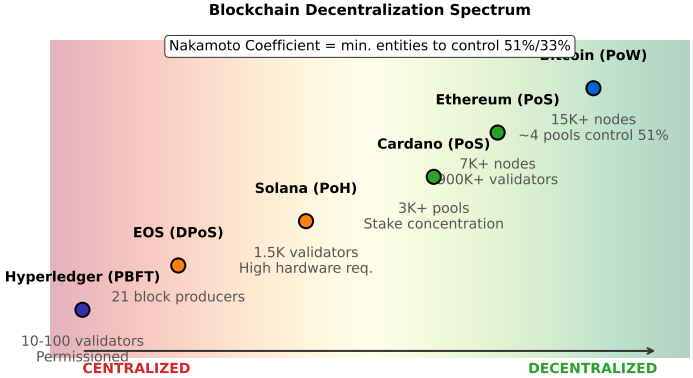
Context:

- Traditional banking: $\sim$260 TWh/year (estimated)
- Data centers globally: $\sim$200-300 TWh/year

Environmental Debate:

- PoW advocates: energy secures network, incentivizes renewables
- Critics: wasteful expenditure for limited throughput
- Industry trend: shift toward PoS driven by environmental concerns

Decentralization Spectrum



Nakamoto coefficient measures minimum entities to control 51%/33% of the network.

Decentralization Metrics

1. **Nakamoto Coefficient:**
   - Entities to control 51%/33%
   - BTC pools: 4 — ETH: 1000+
2. **Node Distribution:**
   - Bitcoin: 15K — Ethereum: 7K
   - Permissioned: 10-100 nodes
3. **Client Diversity:**
   - Multiple implementations reduce risk
   - ETH: 5+ clients vs mono: 1
4. **Wealth Distribution:**
   - Gini coefficient for tokens
   - PoS: wealth = power

(c) Joerg Osterrieder 2025

Use Case Selection Matrix

Proof of Work:

- Maximum decentralization, censorship resistance critical
- Examples: digital gold (Bitcoin), privacy coins (Monero)

Proof of Stake:

- Balance decentralization and scalability, environmental sustainability
- Examples: DeFi platforms (Ethereum), general-purpose chains

Delegated Proof of Stake:

- High throughput, fast finality essential
- Examples: gaming, social media dApps (EOS, Steemit)

PBFT:

- Permissioned acceptable, enterprise/consortium use
- Examples: supply chain (Hyperledger), interbank settlement

Emerging Consensus Mechanisms

Proof of History (Solana):

- Verifiable delay function creates timestamp proof
- Enables parallel processing, 65,000 TPS
- Concern: hardware requirements, network outages

Pure Proof of Stake (Algorand):

- VRF for leader selection, instant finality
- Low barrier (any amount stakeable)

Proof of Authority (PoA):

- Validators approved by reputation/identity
- Used in testnets (Goerli, Sepolia)

Hybrid Models:

- Decred (PoW + PoS), Tendermint (BFT + PoS)
- Mitigate weaknesses of individual mechanisms

Governance and Upgradability

PoW Governance:

- Off-chain (BIPs, rough consensus)
- Hard forks contentious (Bitcoin Cash, SV splits)

PoS Governance:

- On-chain potential (Tezos, Polkadot)
- Stake-weighted voting on protocol upgrades

DPoS Governance:

- Delegates propose and vote on changes
- Rapid upgrades possible, risk of centralized decisions

PBFT Governance:

- Consortium governance among known entities
- Fastest upgrade cycles

(c) Joerg Osterrieder 2025

Problem Solved? Consensus Comparison

The Original Problem

Why can't we have fast, secure, AND decentralized?

How Consensus Comparison Solves It

- PoW provides strong security guarantees at energy cost
- PoS provides efficiency with different trust assumptions (67% honest stake)
- Each mechanism optimizes different dimensions of the trilemma

Remaining Limitations

- No perfect solution – must choose trade-off profile for specific use case
- High throughput (DPoS/PBFT) requires sacrificing decentralization

Open Questions

- Can new mechanisms (DAGs, sharding) escape the trilemma constraints?
- Risk: Over-optimization for single metric (e.g., TPS) ignores security

Consensus Comparison partially solves "Why can't we have fast, secure, AND decentralized" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Key Takeaways

- Consensus mechanisms trade off decentralization, scalability, and finality
- PoW: maximum decentralization, high energy, low throughput
- PoS: balanced approach, energy-efficient, moderate throughput
- DPoS: high throughput, fast finality, lower decentralization
- PBFT: instant finality, permissioned, centralized
- No single consensus is optimal for all use cases
- Selection depends on application requirements: security, speed, openness

Design Philosophy:
Choose consensus based on priorities: censorship resistance (PoW), sustainability (PoS), throughput (DPoS), enterprise needs (PBFT). Understand trade-offs explicitly.

Discussion Questions

1. Why does PBFT achieve instant finality while PoW only offers probabilistic finality?
2. How does energy consumption relate to security in proof-of-work systems?
3. What are the risks of delegating block production to a small set of validators?
4. Can a highly scalable blockchain also be highly decentralized?
5. How might quantum computing impact different consensus mechanisms?
6. What role does governance play in consensus mechanism selection?

Next Lesson Preview: L11 Blockchain Scalability Trilemma

Topics to be covered:

- The scalability trilemma: security, decentralization, scalability
- Layer 1 scalability limits (block size, block time, state growth)
- Throughput comparisons (TPS benchmarks)
- Vertical vs. horizontal scaling approaches
- Emerging solutions: sharding, Layer 2, sidechains

Preparation:

- Review consensus mechanism trade-offs from this lesson
- Explore current blockchain TPS statistics (L2Beat)
- Consider why traditional databases achieve millions of TPS

Quiz: Questions 1-5

Q1. What is the primary security assumption for Proof-of-Work consensus?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee agreement
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus mechanism achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT provides deterministic finality after 2/3+ validators commit.

Q3. What percentage of energy did Ethereum save after The Merge to Proof-of-Stake?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The Merge reduced Ethereum's energy consumption by 99.95%.

Q4. In Proof-of-Stake, what is the minimum stake percentage needed to prevent finality?
A) 10% B) 33% C) 51% D) 67%
Answer: B – 33% stake can halt finality (liveness attack) in PoS systems.

Q5. What is the typical throughput range for DPoS systems like EOS?
A) 7-15 TPS B) 30-100 TPS C) 1,000-4,000 TPS D) 10,000+ TPS
Answer: C – DPoS achieves 1,000-4,000 TPS by limiting block producers.

Quiz: Questions 6-10

Q6. What is the Nakamoto Coefficient measuring?
A) Total network nodes B) Mining difficulty C) Minimum entities to control network D) Token price volatility
Answer: C – Nakamoto Coefficient is the minimum entities needed to control 51%/33%.

Q7. Which attack vector is specific to Delegated Proof-of-Stake?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS is vulnerable to vote buying to elect malicious delegates.

Q8. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes approximately 150 TWh/year, comparable to Argentina.

Q9. In PBFT, what fraction of validators can be malicious while maintaining safety?
A) $<1/4$ B) $<1/3$ C) $<1/2$ D) $<2/3$
Answer: B – PBFT tolerates $<1/3$ Byzantine (malicious) validators.

Q10. What is the typical finality time for Ethereum Proof-of-Stake?
A) 1 second B) 1 minute C) 12 minutes D) 1 hour
Answer: C – Ethereum PoS achieves finality in approximately 12 minutes (2 epochs).

Quiz: Questions 11-15

Q11. Which consensus mechanism requires a permissioned network?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT requires a known, permissioned validator set.

Q12. What is the primary disadvantage of PoW compared to PoS?
A) Lower security B) Slower finality C) High energy consumption D) Centralization
Answer: C – PoW's massive energy consumption is its main disadvantage versus PoS.

Q13. How many block producers does EOS use in its DPoS system?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers (delegates).

Q14. What is the security mechanism that penalizes misbehavior in Proof-of-Stake?
A) Hash difficulty B) Slashing C) Vote removal D) Block orphaning
Answer: B – Slashing destroys staked tokens of validators who misbehave.

Q15. Which consensus offers probabilistic rather than deterministic finality?
A) PBFT B) DPoS C) Proof-of-Work D) Proof-of-Authority
Answer: C – PoW provides probabilistic finality (deeper blocks = higher confidence).

Quiz: Questions 16-20

Q16. What percentage of stake is needed to finalize conflicting blocks in Ethereum PoS?
A) 33% B) 51% C) 67% D) 75%
Answer: C – 67% stake can execute a safety attack and finalize conflicting blocks.

Q17. Which consensus mechanism has the lowest decentralization?
A) Proof-of-Work B) Proof-of-Stake C) DPoS D) PBFT
Answer: D – PBFT is highly centralized with a small permissioned validator set.

Q18. What is the typical Bitcoin finality time for high-value transactions?
A) 10 minutes B) 30 minutes C) 1 hour D) 6 hours
Answer: C – Bitcoin typically requires 6 confirmations (1 hour) for finality.

Q19. Which emerging consensus uses Verifiable Delay Functions for timestamps?
A) Algorand B) Solana (Proof of History) C) Polkadot D) Cardano
Answer: B – Solana's Proof of History uses VDFs to create verifiable timestamps.

Q20. What is the main trade-off when increasing blockchain throughput?
A) Higher energy B) Reduced decentralization C) Slower finality D) Higher costs
Answer: B – Higher throughput typically requires sacrificing decentralization.

Consensus Mechanism Comparison

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Voting methods chaos

[COMIC: A chaotic town hall meeting where different groups are trying to reach consensus: one group mining with pickaxes (PoW), another holding up stacks of coins (PoS), a small elite committee in suits (PBFT), and delegates waving voter ID cards (DPoS)—all shouting at once]

Many Ways to Agree

- PoW: "I spent more electricity, so I decide"
- PoS: "I have more skin in the game, so I decide"
- PBFT: "We're the designated committee, so we decide"
- Each solves the same problem differently—with different trade-offs

The Byzantine Generals Problem has many solutions—none perfect

Learning Objectives

By the end of this lesson, you will be able to:

- Compare proof-of-work, proof-of-stake, delegated proof-of-stake, and PBFT
- Evaluate security models and threat assumptions
- Analyze scalability and throughput trade-offs
- Assess energy consumption and environmental impact
- Measure decentralization across consensus protocols
- Understand finality and confirmation time differences
- Select appropriate consensus mechanism for specific use cases

Building on L09: Proof of Stake

The Problem: Why can't we have fast, secure, AND decentralized?

The Challenge
Why can't we have fast, secure, AND decentralized consensus simultaneously? Every blockchain must make fundamental trade-offs between these three properties.

Why It Matters

- Every blockchain makes trade-offs between speed, security, and openness
- Bitcoin chose security over speed; Solana chose speed over decentralization

What We Need

- Understanding design constraints
- Framework to evaluate consensus trade-offs across different mechanisms

The Cryptoeconomics Question
Optimizing multiple competing goals

Today's lesson: How Consensus Comparison addresses this challenge

What Are the Main Consensus Mechanisms?

What is Consensus?

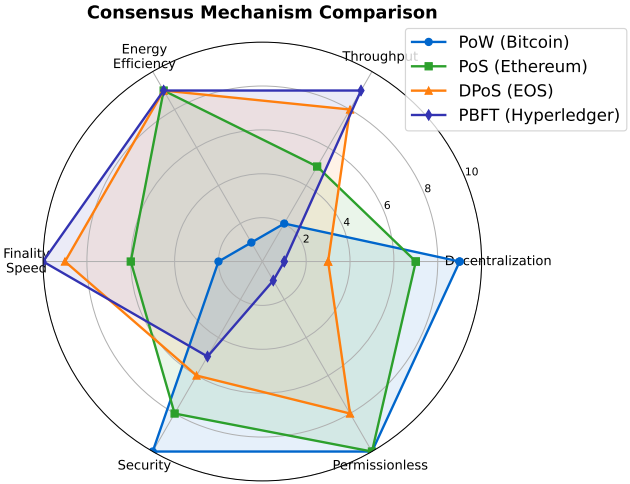
- Agreement among distributed nodes on shared state
- Ensures same transaction history
- Prevents double-spending

Major Consensus Families:

1. **PoW:** Bitcoin, Litecoin, Dogecoin
2. **PoS:** Ethereum, Cardano, Polkadot
3. **DPoS:** EOS, Tron, Cosmos
4. **PBFT:** Hyperledger Fabric, Zilliqa
5. **Hybrid:** Decred, Algorand (VRF)

→ *Problem: Why can't we have fast, secure, AND... — What Are the Main Consensus Mechanisms? — Different consensus mechanisms represent different trade-off choices on the security-decentralization-speed triangle*

How Do Different Consensus Mechanisms Compare?



No single mechanism excels in all dimensions – trade-offs are fundamental.

How Does Proof of Work Function?

Mechanism:

- Miners compete to find valid block hash
- First valid hash broadcasts block

Security Model:

- Honest majority: $> 50\%$ hash rate
- Attack cost proportional to hash rate
- Probabilistic finality (deeper = safer)

Advantages:

- Proven security (15+ years, no attack)
- No trusted setup, permissionless

Disadvantages:

- High energy (150 TWh/year)
- Low throughput (7 TPS), slow finality

PoW trades energy consumption for the strongest decentralization and censorship resistance

How Does Proof of Stake Function?

Mechanism:

- Validators stake tokens as collateral
- Weighted random selection for proposals
- Slashing for misbehavior

Security Model:

- 67%+ honest stake for finality
- Attack cost = price $\times$ stake

Advantages:

- 99% energy reduction vs PoW
- Faster finality (12 min ETH)
- Attackers lose stake

Disadvantages:

- Wealth concentration
- Centralization via pools

How Does Delegated Proof of Stake Function?

Mechanism:

- Token holders vote for delegates
- Top N delegates (21 EOS, 27 Tron) rotate
- Delegates share rewards with voters

Security Model:

- $>$ 50% of delegates must be honest
- Reputation-based trust (known identities)

Advantages:

- High throughput (4,000 TPS for EOS)
- Fast finality (1–3 seconds), energy-efficient

Disadvantages:

- High centralization (21–100 producers)
- Voter apathy, plutocracy, cartel risk

→ *Problem: Why can't we have fast, secure, AND... — How Does Delegated Proof of Stake Function? — DPoS trades decentralization for speed – voters delegate to professional validators who can run fast hardware*

How Does Practical Byzantine Fault Tolerance Function?

Mechanism:

- Pre-selected committee of validators
- Three-phase: pre-prepare, prepare, commit
- $2/3+$ agreement to finalize block

Security Model:

- Tolerates $< 1/3$ malicious nodes
- Known validator set (permissioned)

Advantages:

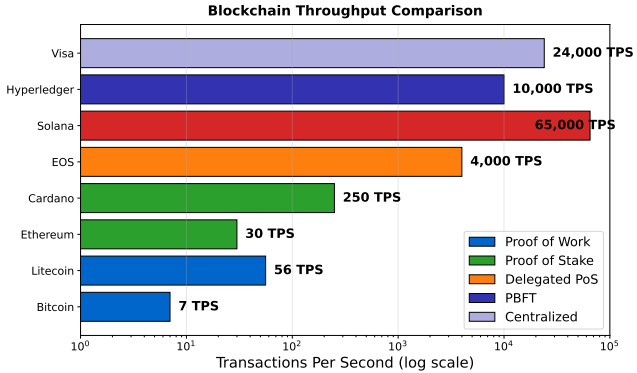
- Instant finality (deterministic)
- 1,000–10,000 TPS, energy-efficient

Disadvantages:

- Requires permissioned network
- Poor scalability ($O(N^2)$ messages)
- Centralized, not censorship-resistant

PBFT achieves instant finality but sacrifices openness and scalability

How Does Throughput Differ Across Mechanisms?



Higher throughput typically requires sacrificing decentralization.

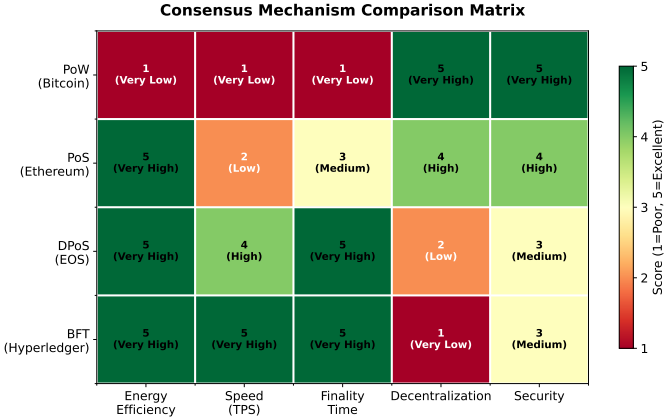
What Are the Key Differences Between Mechanisms?

Property	PoW	PoS	DPoS	PBFT
Throughput	7-15 TPS	30-100 TPS	1,000-4,000	1,000-10,000
Finality	Probabilistic	10-15 min	1-3 sec	Instant
Energy	Very High	Very Low	Very Low	Very Low
Decentralization	High	Medium	Low	Very Low
Permissionless	Yes	Yes	Yes	No
Attack Cost	Hash rate	Stake value	Vote buying	Compromise 1/3

Key Insight:

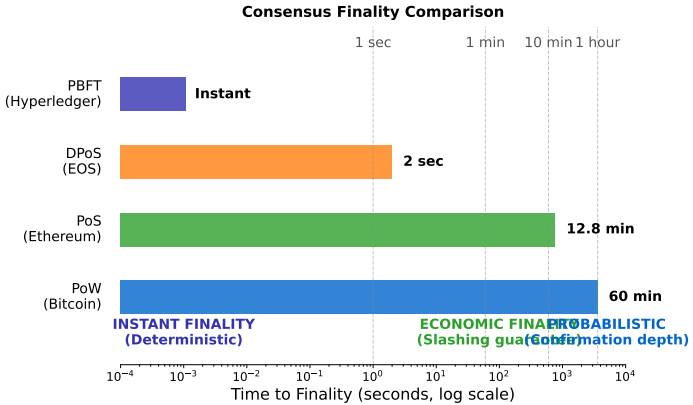
- No consensus mechanism is universally superior
- Trade-offs exist between decentralization, scalability, and finality
- Choice depends on use case requirements

Where Do Mechanisms Excel and Struggle?



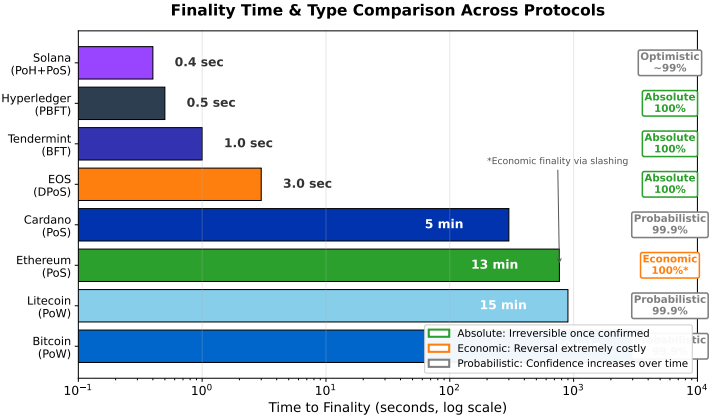
Green = strength, Red = weakness. No mechanism excels in all dimensions.

How Does Finality Time Vary Across Mechanisms?



Finality type affects settlement guarantees and application design.

What Are the Types of Finality?



Absolute finality (BFT) is instant; probabilistic (PoW) requires multiple confirmations.

Problem Check-In: Consensus Comparison

Recall Our Problem

Why can't we have fast, secure, AND decentralized?

What We've Learned So Far

- Consensus mechanisms differ in how they achieve agreement (PoW uses energy, PoS uses stake, DPoS uses delegation, PBFT uses voting rounds)
- Each mechanism makes different trade-offs: PoW maximizes decentralization, PBFT maximizes speed, DPoS balances both
- No single mechanism achieves fast, secure, AND decentralized – understanding trade-offs helps choose the right one

Still to Address

- Quantifying decentralization (Nakamoto coefficient) and real-world attack costs across mechanisms
- Which consensus mechanism best fits our specific use case requirements?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "Why can't we have fast, secure, AND..."?

What Are the Attack Vectors for Each Mechanism?

Proof of Work:

- **51% Attack:** control $>$ 50% hash rate
- Cost: hardware + electricity (billions)

Proof of Stake:

- **33% Attack:** prevent finality
- **67% Attack:** finalize conflicts
- Mitigation: slashing destroys stake

Delegated Proof of Stake:

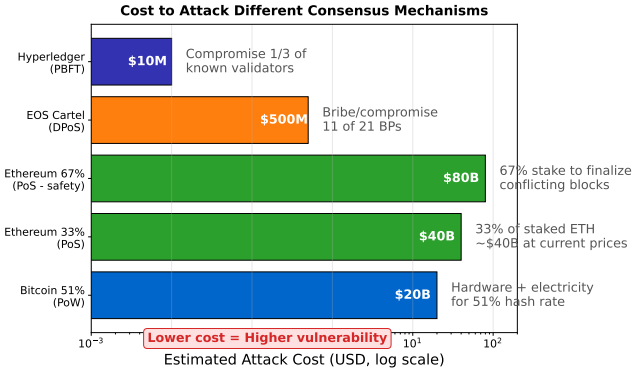
- **Delegate Cartel:** majority collude
- **Vote Buying:** bribe token holders

PBFT:

- **Byzantine:** $>$ 1/3 validators malicious
- Cost depends on permission model

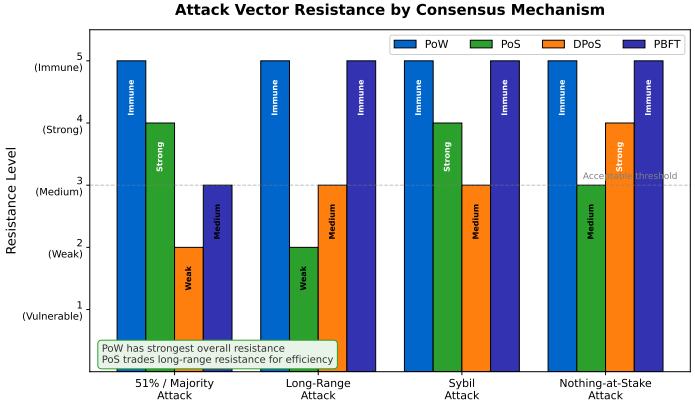
→ Problem: Why can't we have fast, secure, AND... — What Are the Attack Vectors for Each Mechanism? — Attack costs differ by mechanism: PoW requires hardware, PoS requires capital, PBFT requires corrupting known validators

How Do Attack Costs Compare Across Mechanisms?



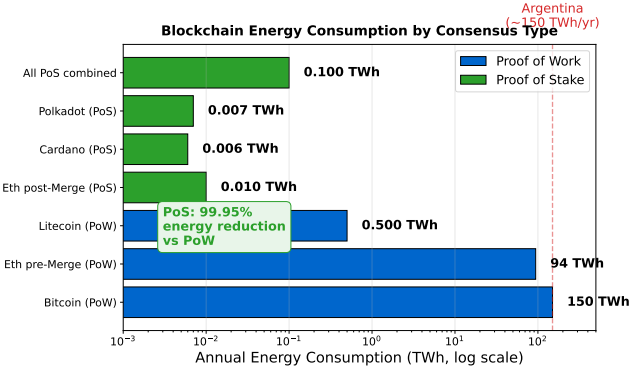
Economic security varies dramatically across consensus mechanisms.

How Resistant Are Mechanisms to Different Attacks?



PoW provides strongest overall security; PoS vulnerable to long-range attacks without checkpoints.

How Does Energy Consumption Differ Across Mechanisms?



The Merge reduced Ethereum's energy by 99.95% – from Argentina's usage to negligible.

What Is the Environmental Impact of Each Mechanism?

Bitcoin (PoW):

- 150 TWh/year (comparable to Argentina)
- 70 Mt CO2/year carbon footprint

PoS Reduction:

- Ethereum post-Merge: 0.01 TWh/year
- 99.95% energy reduction
- All PoS chains: < 0.1 TWh/year

Context:

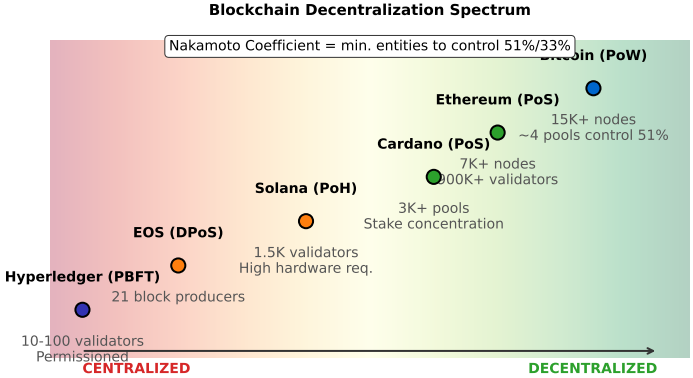
- Traditional banking: $\sim$260 TWh/year
- Data centers globally: $\sim$200–300 TWh/year

Environmental Debate:

- PoW: secures network, incentivizes renewables
- Critics: wasteful for limited throughput
- Trend: shift toward PoS

PoW's energy use is a feature (security) and a bug (sustainability) depending on perspective

How Decentralized Is Each Mechanism?



Nakamoto coefficient measures minimum entities to control 51%/33% of the network. | → *Problem: Why can't we have fast, secure, AND...* — *How Decentralized Is Each Mechanism?* — *Nakamoto coefficient measures decentralization – higher means more entities needed to attack the network*

How Do We Measure Decentralization?

1. **Nakamoto Coefficient:**
   - Entities to control 51%/33%
   - BTC pools: 4 — ETH: 1000+
2. **Node Distribution:**
   - Bitcoin: 15K — Ethereum: 7K
   - Permissioned: 10-100 nodes
3. **Client Diversity:**
   - Multiple implementations reduce risk
   - ETH: 5+ clients vs mono: 1
4. **Wealth Distribution:**
   - Gini coefficient for tokens
   - PoS: wealth = power

(c) Joerg Osterrieder 2025

Which Consensus Mechanism Fits Your Use Case?

Proof of Work:

- Max decentralization, censorship resistance
- Examples: Bitcoin, Monero

Proof of Stake:

- Balance decentralization + scalability
- Examples: Ethereum, Cardano

Delegated Proof of Stake:

- High throughput, fast finality
- Examples: EOS, Steemit

PBFT:

- Enterprise/consortium use
- Examples: Hyperledger, interbank

Match consensus to priorities: censorship resistance (PoW), sustainability (PoS), speed (DPoS), enterprise (PBFT)

What New Consensus Mechanisms Are Emerging?

Proof of History (Solana):

- VDF creates timestamp proof
- 65,000 TPS, parallel processing
- Concern: outages, hardware cost

Pure PoS (Algorand):

- VRF for leader selection
- Instant finality, low barrier

Proof of Authority (PoA):

- Validators by reputation/identity
- Used in testnets (Sepolia)

Hybrid Models:

- Decred (PoW + PoS)
- Tendermint (BFT + PoS)
- Mitigate individual weaknesses

Innovation continues: hybrid models and novel approaches seek to escape the trilemma

How Do Governance Models Differ Across Mechanisms?

PoW Governance:

- Off-chain (BIPs, rough consensus)
- Hard forks contentious (BCH, BSV)

PoS Governance:

- On-chain potential (Tezos, Polkadot)
- Stake-weighted voting on upgrades

DPoS Governance:

- Delegates propose and vote
- Rapid upgrades, centralization risk

PBFT Governance:

- Consortium among known entities
- Fastest upgrade cycles

Governance reflects consensus: PoW is conservative, PoS enables on-chain voting, PBFT is corporate

Problem Solved? Consensus Comparison

The Original Problem

Why can't we have fast, secure, AND decentralized?

How Consensus Comparison Solves It

- PoW provides strong security guarantees at energy cost
- PoS provides efficiency with different trust assumptions (67% honest stake)
- Each mechanism optimizes different dimensions of the trilemma

Remaining Limitations

- No perfect solution – must choose trade-off profile for specific use case
- High throughput (DPoS/PBFT) requires sacrificing decentralization

Open Questions

- Can new mechanisms (DAGs, sharding) escape the trilemma constraints?
- Risk: Over-optimization for single metric (e.g., TPS) ignores security

Consensus Comparison partially solves "Why can't we have fast, secure, AND decentralized" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Consensus Comparison

Incentive Structure

- **Core Problem:** Optimizing multiple competing goals
- **Why act honestly?** Choose based on use case requirements
- **Value Flow:** Gain in one dimension, sacrifice in another

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Gain in one dimension, sacrifice in another

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Consensus Comparison

Alternatives Considered

1. **Chosen Design:** Different points on trade-off frontier
2. **Alternative:** Layer 2 solutions, hybrid approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Consensus Comparison

Critical Failure Mode

- **What breaks:** Over-optimization for single metric
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Which consensus? decision paralysis

[COMIC: A blockchain architect standing at a crossroads with signposts pointing to "PoW: Secure but slow," "PoS: Efficient but centralized?," "DPoS: Fast but 21 validators," "PBFT: Instant but permissioned"—sweating profusely as stakeholders shout conflicting requirements]

No Perfect Choice

- Bitcoin: maximum decentralization (7 TPS)
- Solana: maximum speed (65,000 TPS, frequent outages)
- Ethereum: balanced approach (30 TPS base + L2 for scale)
- Your use case determines the right trade-off profile

The trilemma is real: pick two of three (decentralization, security, scalability)

Key Takeaways

- Consensus mechanisms trade off decentralization, scalability, and finality
- PoW: maximum decentralization, high energy, low throughput
- PoS: balanced approach, energy-efficient, moderate throughput
- DPoS: high throughput, fast finality, lower decentralization
- PBFT: instant finality, permissioned, centralized
- No single consensus is optimal for all use cases
- Selection depends on application requirements: security, speed, openness

Design Philosophy:
Choose consensus based on priorities: censorship resistance (PoW), sustainability (PoS), throughput (DPoS), enterprise needs (PBFT). Understand trade-offs explicitly.

Next Lesson: L11 – Scalability Trilemma

Discussion Questions

1. Why does PBFT achieve instant finality while PoW only offers probabilistic finality?
2. How does energy consumption relate to security in proof-of-work systems?
3. What are the risks of delegating block production to a small set of validators?
4. Can a highly scalable blockchain also be highly decentralized?
5. How might quantum computing impact different consensus mechanisms?
6. What role does governance play in consensus mechanism selection?

Next Lesson Preview: L11 Blockchain Scalability Trilemma

Topics to be covered:

- The scalability trilemma: security, decentralization, scalability
- Layer 1 scalability limits (block size, block time, state growth)
- Throughput comparisons (TPS benchmarks)
- Vertical vs. horizontal scaling approaches
- Emerging solutions: sharding, Layer 2, sidechains

Preparation:

- Review consensus mechanism trade-offs from this lesson
- Explore current blockchain TPS statistics (L2Beat)
- Consider why traditional databases achieve millions of TPS

Quiz: Questions 1-5

Q1. What is the primary security assumption for Proof-of-Work consensus?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee agreement
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus mechanism achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT provides deterministic finality after 2/3+ validators commit.

Q3. What percentage of energy did Ethereum save after The Merge to Proof-of-Stake?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The Merge reduced Ethereum's energy consumption by 99.95%.

Q4. In Proof-of-Stake, what is the minimum stake percentage needed to prevent finality?
A) 10% B) 33% C) 51% D) 67%
Answer: B – 33% stake can halt finality (liveness attack) in PoS systems.

Q5. What is the typical throughput range for DPoS systems like EOS?
A) 7-15 TPS B) 30-100 TPS C) 1,000-4,000 TPS D) 10,000+ TPS
Answer: C – DPoS achieves 1,000-4,000 TPS by limiting block producers.

Quiz: Questions 6-10

Q6. What is the Nakamoto Coefficient measuring?
A) Total network nodes B) Mining difficulty C) Minimum entities to control network D) Token price volatility
Answer: C – Nakamoto Coefficient is the minimum entities needed to control 51%/33%.

Q7. Which attack vector is specific to Delegated Proof-of-Stake?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS is vulnerable to vote buying to elect malicious delegates.

Q8. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes approximately 150 TWh/year, comparable to Argentina.

Q9. In PBFT, what fraction of validators can be malicious while maintaining safety?
A) $<1/4$ B) $<1/3$ C) $<1/2$ D) $<2/3$
Answer: B – PBFT tolerates $<1/3$ Byzantine (malicious) validators.

Q10. What is the typical finality time for Ethereum Proof-of-Stake?
A) 1 second B) 1 minute C) 12 minutes D) 1 hour
Answer: C – Ethereum PoS achieves finality in approximately 12 minutes (2 epochs).

Quiz: Questions 11-15

Q11. Which consensus mechanism requires a permissioned network?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT requires a known, permissioned validator set.

Q12. What is the primary disadvantage of PoW compared to PoS?
A) Lower security B) Slower finality C) High energy consumption D) Centralization
Answer: C – PoW's massive energy consumption is its main disadvantage versus PoS.

Q13. How many block producers does EOS use in its DPoS system?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers (delegates).

Q14. What is the security mechanism that penalizes misbehavior in Proof-of-Stake?
A) Hash difficulty B) Slashing C) Vote removal D) Block orphaning
Answer: B – Slashing destroys staked tokens of validators who misbehave.

Q15. Which consensus offers probabilistic rather than deterministic finality?
A) PBFT B) DPoS C) Proof-of-Work D) Proof-of-Authority
Answer: C – PoW provides probabilistic finality (deeper blocks = higher confidence).

Quiz: Questions 16-20

Q16. What percentage of stake is needed to finalize conflicting blocks in Ethereum PoS?
A) 33% B) 51% C) 67% D) 75%
Answer: C – 67% stake can execute a safety attack and finalize conflicting blocks.

Q17. Which consensus mechanism has the lowest decentralization?
A) Proof-of-Work B) Proof-of-Stake C) DPoS D) PBFT
Answer: D – PBFT is highly centralized with a small permissioned validator set.

Q18. What is the typical Bitcoin finality time for high-value transactions?
A) 10 minutes B) 30 minutes C) 1 hour D) 6 hours
Answer: C – Bitcoin typically requires 6 confirmations (1 hour) for finality.

Q19. Which emerging consensus uses Verifiable Delay Functions for timestamps?
A) Algorand B) Solana (Proof of History) C) Polkadot D) Cardano
Answer: B – Solana's Proof of History uses VDFs to create verifiable timestamps.

Q20. What is the main trade-off when increasing blockchain throughput?
A) Higher energy B) Reduced decentralization C) Slower finality D) Higher costs
Answer: B – Higher throughput typically requires sacrificing decentralization.

L10: Consensus Mechanism Comparison

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

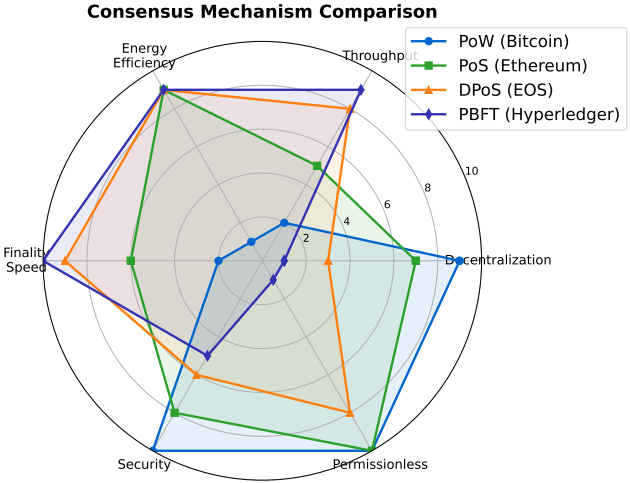
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

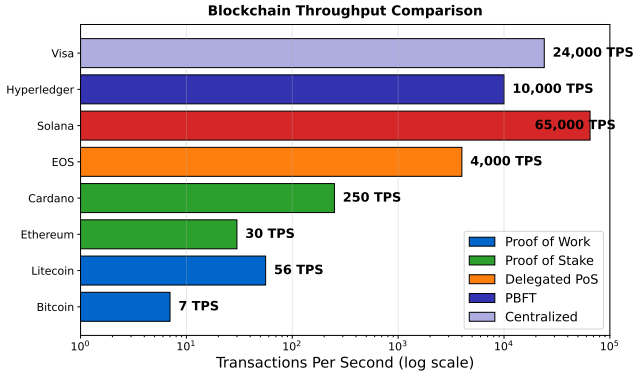
- Compare PoW, PoS, DPoS, and PBFT consensus mechanisms
- Evaluate security models and attack vectors
- Analyze trade-offs: throughput, finality, decentralization
- Select appropriate consensus for specific use cases

Consensus Mechanism Comparison



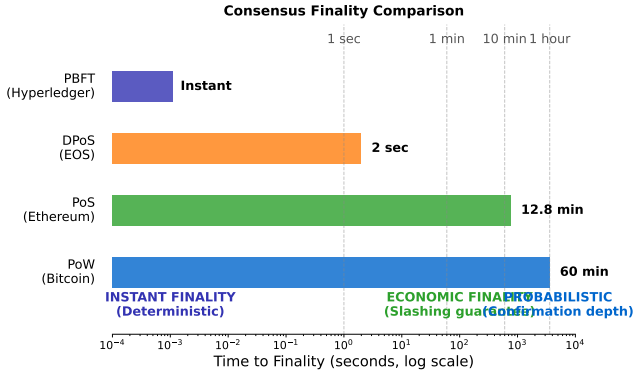
Key Insight: No single mechanism excels in all dimensions – trade-offs are fundamental.

Throughput Comparison



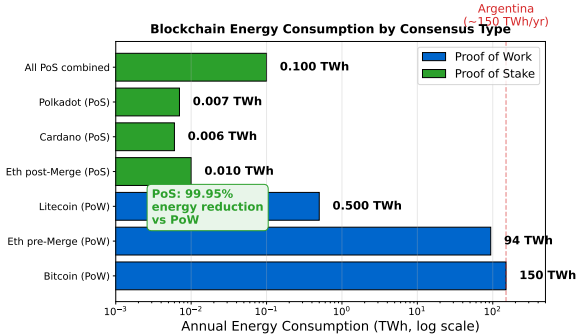
Inverse Correlation: Higher TPS generally means fewer nodes and lower decentralization.

Finality Comparison



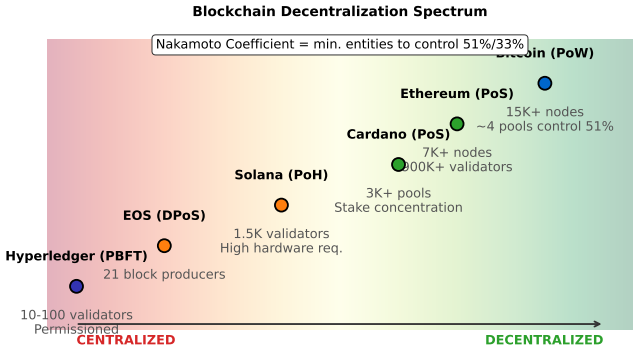
PoW: Probabilistic (1 hour) — **PoS:** Economic (12 min) — **PBFT:** Instant

Energy Consumption



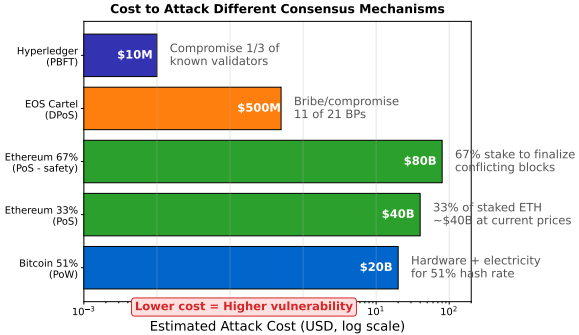
Bitcoin: 150 TWh/year — **Ethereum post-Merge:** 0.01 TWh (99.95% reduction)

Decentralization Spectrum



Nakamoto Coefficient: Minimum entities to control 51%/33% of network.

Attack Cost Comparison



PoW: Hash rate — **PoS:** Stake value — **DPoS:** Vote buying — **PBFT:** Compromise 1/3

Quick Comparison

Property	PoW	PoS	DPoS	PBFT
Throughput	7-15 TPS	30-100 TPS	1-4K TPS	1-10K TPS
Finality	1 hour	12 min	1-3 sec	Instant
Energy	Very High	Very Low	Very Low	Very Low
Decentralization	High	Medium	Low	Very Low

Use Case Selection:

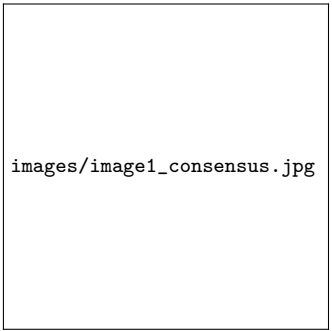
- **PoW:** Maximum censorship resistance (Bitcoin)
- **PoS:** Balance decentralization + sustainability (Ethereum)
- **DPoS:** High throughput apps (gaming, social)
- **PBFT:** Enterprise/consortium (Hyperledger)

Key Takeaways

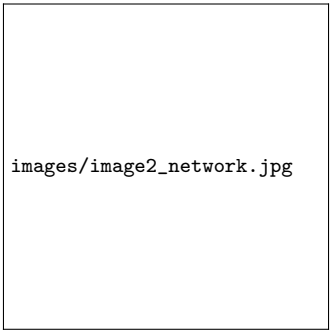
1. **Trade-offs:** No consensus optimizes decentralization, security, AND scalability
2. **PoW:** Maximum decentralization, high energy, 7 TPS, 1 hour finality
3. **PoS:** Balanced approach, 99% less energy, 12 min finality
4. **DPoS:** High throughput (4K TPS), fast finality, centralized (21 producers)
5. **PBFT:** Instant finality, permissioned, enterprise use

Design Philosophy: Choose consensus based on priorities: censorship resistance (PoW), sustainability (PoS), throughput (DPoS), enterprise needs (PBFT).

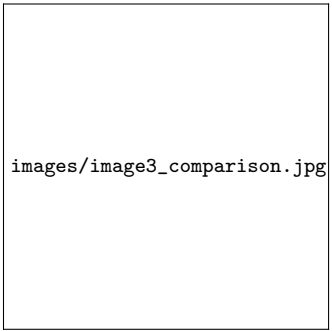
Consensus Mechanisms in Action



Consensus Protocol



Distributed Network



Trade-off Analysis

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is PoW's primary security assumption?
A) ¿33% stake honest B) ¿50% hash rate honest C) ¡1/3 validators malicious D) 2/3+ agreement

Quiz (1/2)

Q1. What is PoW's primary security assumption?
A) ¿33% stake honest B) ¿50% hash rate honest C) ¡1/3 validators malicious D) 2/3+ agreement
Answer: B – PoW requires ¿50% honest hash rate.

Q2. Which consensus achieves instant finality?
A) PoW B) PoS C) PBFT D) DPoS

Quiz (1/2)

Q1. What is PoW's primary security assumption?
A) ¿33% stake honest B) ¿50% hash rate honest C) ¡1/3 validators malicious D) 2/3+ agreement
Answer: B – PoW requires ¿50% honest hash rate.

Q2. Which consensus achieves instant finality?
A) PoW B) PoS C) PBFT D) DPoS
Answer: C – PBFT provides deterministic finality after 2/3+ commit.

Q3. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh

Quiz (1/2)

Q1. What is PoW's primary security assumption?
A) ¿33% stake honest B) ¿50% hash rate honest C) ¡1/3 validators malicious D) 2/3+ agreement
Answer: B – PoW requires ¿50% honest hash rate.

Q2. Which consensus achieves instant finality?
A) PoW B) PoS C) PBFT D) DPoS
Answer: C – PBFT provides deterministic finality after 2/3+ commit.

Q3. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes 150 TWh/year.

Q4. In PoS, what stake percentage can prevent finality?
A) 10% B) 33% C) 51% D) 67%

Quiz (1/2)

Q1. What is PoW's primary security assumption?
A) ¿33% stake honest B) ¿50% hash rate honest C) ¡1/3 validators malicious D) 2/3+ agreement
Answer: B – PoW requires ¿50% honest hash rate.

Q2. Which consensus achieves instant finality?
A) PoW B) PoS C) PBFT D) DPoS
Answer: C – PBFT provides deterministic finality after 2/3+ commit.

Q3. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes 150 TWh/year.

Q4. In PoS, what stake percentage can prevent finality?
A) 10% B) 33% C) 51% D) 67%
Answer: B – 33% can halt finality (liveness attack).

Q5. What is the typical TPS range for DPoS (EOS)?
A) 7-15 B) 30-100 C) 1,000-4,000 D) 10,000+

Quiz (1/2)

Q1. What is PoW's primary security assumption?
A) ¿33% stake honest B) ¿50% hash rate honest C) ¡1/3 validators malicious D) 2/3+ agreement
Answer: B – PoW requires ¿50% honest hash rate.

Q2. Which consensus achieves instant finality?
A) PoW B) PoS C) PBFT D) DPoS
Answer: C – PBFT provides deterministic finality after 2/3+ commit.

Q3. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes 150 TWh/year.

Q4. In PoS, what stake percentage can prevent finality?
A) 10% B) 33% C) 51% D) 67%
Answer: B – 33% can halt finality (liveness attack).

Q5. What is the typical TPS range for DPoS (EOS)?
A) 7-15 B) 30-100 C) 1,000-4,000 D) 10,000+
Answer: C – DPoS achieves 1,000-4,000 TPS.

Quiz (2/2)

Q6. What does Nakamoto Coefficient measure?
A) Total nodes B) Mining difficulty C) Min entities to control network D) Token price

Quiz (2/2)

Q6. What does Nakamoto Coefficient measure?
A) Total nodes B) Mining difficulty C) Min entities to control network D) Token price
Answer: C – Minimum entities to control 51%/33%.

Q7. Which attack vector is specific to DPoS?
A) 51% attack B) Double-spending C) Vote buying D) Selfish mining

Quiz (2/2)

Q6. What does Nakamoto Coefficient measure?
A) Total nodes B) Mining difficulty C) Min entities to control network D) Token price
Answer: C – Minimum entities to control 51%/33%.

Q7. Which attack vector is specific to DPoS?
A) 51% attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS vulnerable to vote buying for delegates.

Q8. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000

Quiz (2/2)

Q6. What does Nakamoto Coefficient measure?
A) Total nodes B) Mining difficulty C) Min entities to control network D) Token price
Answer: C – Minimum entities to control 51%/33%.

Q7. Which attack vector is specific to DPoS?
A) 51% attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS vulnerable to vote buying for delegates.

Q8. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers.

Q9. What is Ethereum's typical finality time (PoS)?
A) 1 second B) 1 minute C) 12 minutes D) 1 hour

Quiz (2/2)

Q6. What does Nakamoto Coefficient measure?
A) Total nodes B) Mining difficulty C) Min entities to control network D) Token price
Answer: C – Minimum entities to control 51%/33%.

Q7. Which attack vector is specific to DPoS?
A) 51% attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS vulnerable to vote buying for delegates.

Q8. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers.

Q9. What is Ethereum's typical finality time (PoS)?
A) 1 second B) 1 minute C) 12 minutes D) 1 hour
Answer: C – Ethereum PoS achieves finality in 12 minutes.

Q10. Which consensus has lowest decentralization?
A) PoW B) PoS C) DPoS D) PBFT

Quiz (2/2)

Q6. What does Nakamoto Coefficient measure?
A) Total nodes B) Mining difficulty C) Min entities to control network D) Token price
Answer: C – Minimum entities to control 51%/33%.

Q7. Which attack vector is specific to DPoS?
A) 51% attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS vulnerable to vote buying for delegates.

Q8. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers.

Q9. What is Ethereum's typical finality time (PoS)?
A) 1 second B) 1 minute C) 12 minutes D) 1 hour
Answer: C – Ethereum PoS achieves finality in 12 minutes.

Q10. Which consensus has lowest decentralization?
A) PoW B) PoS C) DPoS D) PBFT
Answer: D – PBFT is highly centralized with permissioned validators.

Thank you

Questions?

Next: L11 – Blockchain Scalability Trilemma

Quiz: Consensus Comparison

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary security assumption for Proof-of-Work?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee

Quiz (1–5)

Q1. What is the primary security assumption for Proof-of-Work?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake

Quiz (1–5)

Q1. What is the primary security assumption for Proof-of-Work?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT provides deterministic finality after 2/3+ validators commit.

Q3. What percentage of energy did Ethereum save after The Merge?
A) 50% B) 75% C) 90% D) 99.95%

Quiz (1–5)

Q1. What is the primary security assumption for Proof-of-Work?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT provides deterministic finality after 2/3+ validators commit.

Q3. What percentage of energy did Ethereum save after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The Merge reduced Ethereum's energy by 99.95%.

Q4. In PoS, what stake percentage can halt finality?
A) 10% B) 33% C) 51% D) 67%

Quiz (1–5)

Q1. What is the primary security assumption for Proof-of-Work?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT provides deterministic finality after 2/3+ validators commit.

Q3. What percentage of energy did Ethereum save after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The Merge reduced Ethereum's energy by 99.95%.

Q4. In PoS, what stake percentage can halt finality?
A) 10% B) 33% C) 51% D) 67%
Answer: B – 33% stake can execute a liveness attack.

Q5. What is typical DPoS throughput (EOS)?
A) 7-15 TPS B) 30-100 TPS C) 1,000-4,000 TPS D) 10,000+ TPS

Quiz (1–5)

Q1. What is the primary security assumption for Proof-of-Work?
A) >33% stake honest B) >50% hash rate honest C) <1/3 validators malicious D) 2/3+ committee
Answer: B – PoW requires >50% honest hash rate to prevent 51% attacks.

Q2. Which consensus achieves instant finality?
A) Proof-of-Work B) Proof-of-Stake C) PBFT D) Delegated Proof-of-Stake
Answer: C – PBFT provides deterministic finality after 2/3+ validators commit.

Q3. What percentage of energy did Ethereum save after The Merge?
A) 50% B) 75% C) 90% D) 99.95%
Answer: D – The Merge reduced Ethereum's energy by 99.95%.

Q4. In PoS, what stake percentage can halt finality?
A) 10% B) 33% C) 51% D) 67%
Answer: B – 33% stake can execute a liveness attack.

Q5. What is typical DPoS throughput (EOS)?
A) 7-15 TPS B) 30-100 TPS C) 1,000-4,000 TPS D) 10,000+ TPS
Answer: C – DPoS achieves 1,000-4,000 TPS by limiting block producers.

Quiz (6–10)

Q6. What does the Nakamoto Coefficient measure?
A) Network nodes B) Mining difficulty C) Minimum entities to control network D) Token volatility

Quiz (6–10)

Q6. What does the Nakamoto Coefficient measure?
A) Network nodes B) Mining difficulty C) Minimum entities to control network D) Token volatility
Answer: C – Minimum entities to control 51%/33% of the network.

Q7. Which attack vector is specific to DPoS?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining

Quiz (6–10)

Q6. What does the Nakamoto Coefficient measure?
A) Network nodes B) Mining difficulty C) Minimum entities to control network D) Token volatility
Answer: C – Minimum entities to control 51%/33% of the network.

Q7. Which attack vector is specific to DPoS?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS is vulnerable to vote buying to elect malicious delegates.

Q8. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh

Quiz (6–10)

Q6. What does the Nakamoto Coefficient measure?
A) Network nodes B) Mining difficulty C) Minimum entities to control network D) Token volatility
Answer: C – Minimum entities to control 51%/33% of the network.

Q7. Which attack vector is specific to DPoS?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS is vulnerable to vote buying to elect malicious delegates.

Q8. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes approximately 150 TWh/year.

Q9. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000

Quiz (6–10)

Q6. What does the Nakamoto Coefficient measure?
A) Network nodes B) Mining difficulty C) Minimum entities to control network D) Token volatility
Answer: C – Minimum entities to control 51%/33% of the network.

Q7. Which attack vector is specific to DPoS?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS is vulnerable to vote buying to elect malicious delegates.

Q8. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes approximately 150 TWh/year.

Q9. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers.

Q10. What penalizes misbehavior in Proof-of-Stake?
A) Hash difficulty B) Slashing C) Vote removal D) Block orphaning

Quiz (6–10)

Q6. What does the Nakamoto Coefficient measure?
A) Network nodes B) Mining difficulty C) Minimum entities to control network D) Token volatility
Answer: C – Minimum entities to control 51%/33% of the network.

Q7. Which attack vector is specific to DPoS?
A) 51% hash attack B) Double-spending C) Vote buying D) Selfish mining
Answer: C – DPoS is vulnerable to vote buying to elect malicious delegates.

Q8. What is Bitcoin's annual energy consumption?
A) 15 TWh B) 50 TWh C) 150 TWh D) 500 TWh
Answer: C – Bitcoin consumes approximately 150 TWh/year.

Q9. How many block producers does EOS use?
A) 7 B) 21 C) 100 D) 1,000
Answer: B – EOS uses 21 elected block producers.

Q10. What penalizes misbehavior in Proof-of-Stake?
A) Hash difficulty B) Slashing C) Vote removal D) Block orphaning
Answer: B – Slashing destroys staked tokens of misbehaving validators.

Blockchain Scalability Trilemma

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the blockchain scalability trilemma
- Analyze trade-offs between security, decentralization, and scalability
- Understand Layer 1 scalability bottlenecks
- Compare throughput limitations across blockchains
- Evaluate vertical vs. horizontal scaling approaches
- Recognize emerging scalability solutions

(c) Joerg Osterrieder 2025

The Problem: How do we scale blockchains?

The Challenge
Blockchains face a fundamental limitation: achieving global-scale transaction throughput while preserving decentralization and security. Bitcoin processes 7 TPS while Ethereum handles 15 TPS—far below the requirements for mass adoption or competition with traditional payment systems.

Why It Matters

- Bitcoin: 7 TPS vs. Visa: 65,000 TPS—blockchains cannot serve billions of users
- Ethereum's 2017 CryptoKitties congestion halted the network, with gas prices spiking 1000%

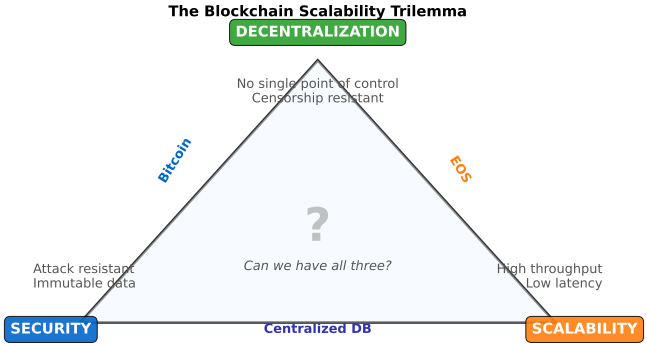
What We Need

- Understanding design constraints
- Scale to handle global transaction volumes without sacrificing decentralization or security

The Cryptoeconomics Question
How do we optimize for competing goals: throughput, decentralization, and security?

Today's lesson: How the Scalability Trilemma framework addresses this challenge

The Scalability Trilemma



Coined by Vitalik Buterin: a blockchain can achieve at most two of three properties.

Understanding the Trilemma

Three Properties:

- **Decentralization:** No single controller
- **Security:** Attack resistant
- **Scalability:** High TPS, low latency

Trade-Offs:

- BTC: Decentral + Secure = 7 TPS
- EOS: Scale + Secure = 21 nodes
- DB: Scale + Secure = centralized

Core Challenges:

- Large blocks = fewer validators
- Fewer validators = faster consensus
- Optimizing one degrades others

Key Insight:
No free lunch - trade-offs are fundamental

(c) Joerg Osterrieder 2025

Why Each Property Matters

Decentralization

- Censorship resistance
- Fault tolerance
- Trustlessness
- No single point of failure

Security

- Immutability
- Double-spend prevention
- Attack resistance
- Data integrity

Scalability

- High throughput (TPS)
- Low latency (finality)
- Low transaction costs
- Mass adoption support

Why Blockchain Needs All Three:

- DeFi applications need high throughput AND security
- Mass adoption requires scalability without sacrificing decentralization
- Competition with traditional payment systems (Visa: 24,000 TPS)

Layer 1 Bottlenecks

Block Size:

- Larger = more TXs, slower propagation
- BTC: 1-4 MB — ETH: gas limit

Block Time:

- Faster = more orphans/forks
- BTC: 10m — ETH: 12s — SOL: 0.4s

State Growth:

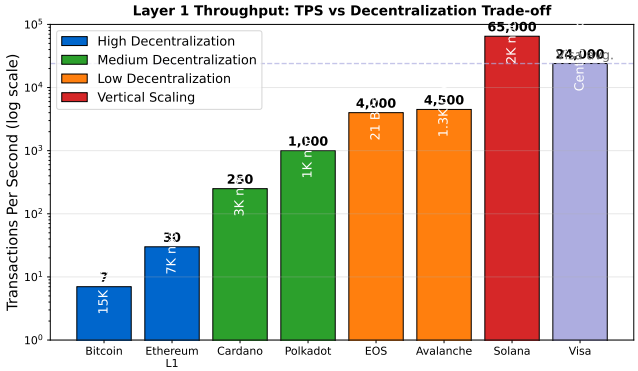
- BTC: 500 GB — ETH: 1 TB
- Full nodes need storage

Computation:

- Every node verifies all TXs
- Smart contracts expensive

(c) Joerg Osterrieder 2025

Layer 1 Throughput Comparison



Inverse correlation: higher TPS generally means fewer nodes and lower decentralization.

The Block Size Debate: Bitcoin Case Study

Big Block Camp:

- Increase to 8+ MB
- Higher throughput, low fees
- Risk: centralization

Small Block Camp:

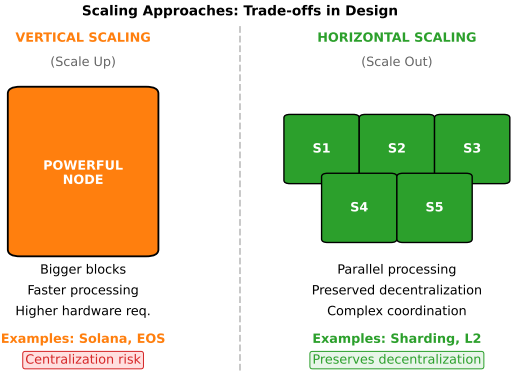
- Preserve decentralization
- Scale via Layer 2
- Accept higher on-chain fees

Outcome (2017):

- BCH fork: 8 MB blocks
- BTC: SegWit (1-4 MB)
- Market: BTC ¿ BCH

Lesson:
Decentralization prioritized; Layer 2 for scale

Vertical vs. Horizontal Scaling



Most major blockchains pursue horizontal scaling to preserve decentralization.

Scaling Approaches Explained

Vertical Scaling (Scale Up)

- Increase capacity of individual nodes
- Require more powerful hardware
- Examples: Solana, EOS

Advantages:

- Simpler implementation
- Immediate throughput gains

Disadvantages:

- Raises barrier to run nodes
- Centralization risk
- Hits physical limits

Horizontal Scaling (Scale Out)

- Distribute load across many nodes
- Parallel processing
- Examples: Sharding, Layer 2, Rollups

Advantages:

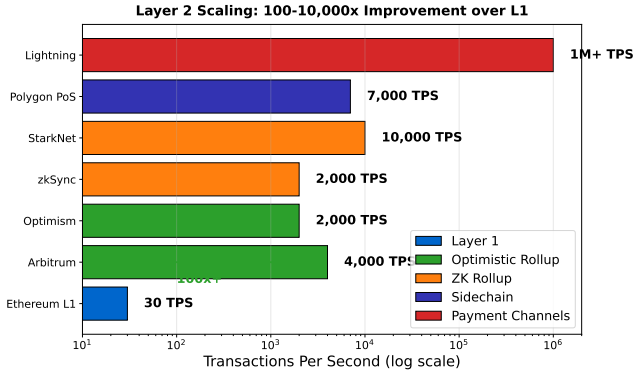
- Preserves decentralization
- Theoretically unbounded scaling

Disadvantages:

- Complex implementation
- Cross-shard communication overhead
- Longer development timelines

(c) Joerg Osterrieder 2025

Layer 2 Scaling Solutions



Layer 2 achieves 100-10,000x improvement while inheriting L1 security.

Layer 2 Types

Payment Channels:

- Lightning Network
- 1 on-chain, unlimited off-chain
- Micropayments

Rollups:

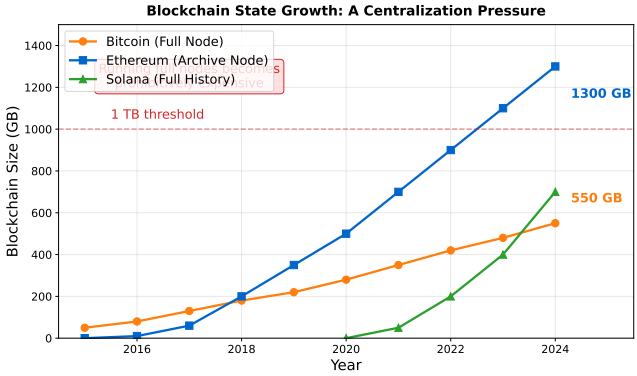
- Bundle 100s of TXs
- Optimistic: fraud proofs
- ZK: validity proofs

Sidechains:

- Independent chain
- Own consensus
- Weaker security

Adoption: Ethereum L2 TVL \$54B+ (Dec 2024, 205% YoY)

State Growth Problem



Running full nodes becomes prohibitively expensive as state grows.

State Growth Solutions

Challenge:

- Unbounded growth
- ETH state: 100 GB
- Sync takes days/weeks
- Centralization pressure

Solutions:

- **State Expiry:** evict inactive, proof to recover
- **Pruning:** keep recent blocks only
- **Rent:** pay to store (Cosmos, EOS)

Sharding: Horizontal Scaling at Layer 1

Concept:

- Split into parallel shards
- Each processes subset of TXs
- Total TPS = shards x per-shard

Ethereum Roadmap:

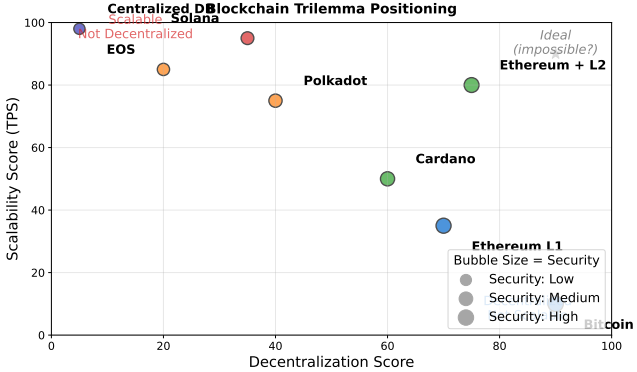
- Danksharding for DA
- EIP-4844 (March 2024)
- Target: 100K+ TPS

Challenges:

- Cross-shard complexity
- Shard takeover attacks
- State management

Other Chains:
Zilliqa, NEAR, Elrond

Trilemma Positioning



Ethereum + L2 approaches the "ideal" corner without sacrificing security.

Breaking the Trilemma: Possible?

Optimistic:

- L2 separates layers
- Rollups keep security
- ZK compresses compute

Pessimistic:

- L2 adds trust
- More complexity
- DA bandwidth limits

Consensus:

- Mitigate, not solve
- Modular design
- L1 security, L2 scale

Navigate the trilemma intelligently rather than "solve" it

Problem Solved? Scalability Trilemma

The Original Problem

How do we scale blockchains to handle global transaction volume?

How Scalability Solutions Address It

- **Layer 2 solutions (rollups, state channels):** Move computation off-chain, achieve 100-10,000x throughput improvement while inheriting L1 security
- **Sharding:** Split state across parallel chains, enabling horizontal scaling to theoretically unbounded throughput
- **Modular design:** Separate consensus, data availability, and execution layers to optimize each independently

Remaining Limitations

- **Layer 2 introduces new trust assumptions:** Sequencer centralization, bridge security risks, and withdrawal delays
- **Trade-off made:** Increased complexity and fragmented liquidity in exchange for higher throughput

Open Questions

- Will rollups or sharding dominate as the long-term scaling solution?
- Risk: Over-optimization for single metric

Scalability Trilemma framework helps navigate trade-offs but doesn't eliminate fundamental constraints

(c) Joerg Osterrieder 2025

Key Takeaways

Trilemma:

- Cannot maximize all three
- L1: block size, time, state
- Vertical = centralization
- Horizontal = decentralization

Solutions:

- L2: 100-1000x throughput
- State growth = risk
- Real TPS ¡ theoretical

Philosophy:
BTC: decentral — SOL: scale — ETH: L2 balance

(c) Joerg Osterrieder 2025

Discussion Questions

1. Why cannot a blockchain simply increase block size indefinitely?
2. How do Layer 2 solutions differ from sidechains in terms of security?
3. What are the implications of state growth for decentralization?
4. Can the trilemma be "solved" or only mitigated?
5. How does sharding introduce new security challenges?
6. Why do most blockchains have lower actual TPS than theoretical TPS?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L12 Lab - Block Explorer Analysis

Lab Activities:

- Navigate Etherscan, Blockstream
- Analyze TX details
- Trace mempool to confirmation
- Examine block structure
- Forensic analysis

Preparation:

- Review L6 TX structure
- Access Etherscan.io
- Access Blockstream.info

(c) Joerg Osterrieder 2025

Quiz Questions (1/4)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability
C) The trade-off between speed and cost D) The conflict between miners and validators

Answer: B – The trilemma states a blockchain can optimize at most two of three properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks
C) It makes attacks easier D) It decreases transaction fees

Answer: B – Larger blocks require more bandwidth and storage, raising barriers to running full nodes.

Q3. Bitcoin processes approximately how many transactions per second (TPS)?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS

Answer: B – Bitcoin's design prioritizes decentralization and security over throughput.

Q4. What is vertical scaling in blockchain context?
A) Adding more nodes to the network B) Increasing capacity of individual nodes
C) Creating Layer 2 solutions D) Implementing sharding

Answer: B – Vertical scaling means requiring more powerful hardware per node.

Q5. Which blockchain outcome resulted from the 2017 block size debate?
A) Ethereum Classic fork B) Bitcoin Cash fork with larger blocks
C) Bitcoin unlimited blocks D) Complete consensus on 8 MB blocks

Answer: B – Bitcoin Cash forked with 8 MB blocks while Bitcoin implemented SegWit.

Quiz Questions (2/4)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security
C) Lower hardware requirements D) Simpler code implementation

Answer: B – Layer 2 achieves 100-10,000x scalability while settling to secure Layer 1.

Q7. How does horizontal scaling differ from vertical scaling?
A) It uses better hardware B) It distributes load across many nodes/shards
C) It reduces security D) It eliminates the need for consensus

Answer: B – Horizontal scaling parallelizes processing to preserve decentralization.

Q8. What is sharding?
A) Compressing blockchain data B) Splitting blockchain into parallel processing shards
C) Encrypting transactions D) A type of consensus algorithm

Answer: B – Sharding divides the network to process transactions in parallel.

Q9. Which Layer 2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains

Answer: C – Optimistic Rollups assume validity and allow challenges via fraud proofs.

Q10. What is the state growth problem?
A) Blockchain size growing unbounded over time B) Decreasing transaction volume
C) Fewer validators joining D) Rising energy consumption

Answer: A – As blockchain accumulates data, storage requirements create centralization pressure.

Quiz Questions (3/4)

Q11. How do ZK-Rollups validate transactions?
A) Through fraud proofs B) Using cryptographic validity proofs
C) By running full nodes D) Through validator voting

Answer: B – ZK-Rollups use zero-knowledge proofs to guarantee transaction validity.

Q12. What was Ethereum's EIP-4844 proto-danksharding (March 2024)?
A) Full execution sharding B) Data availability sharding to reduce L2 costs
C) Transition to PoS D) Gas fee elimination

Answer: B – Proto-danksharding adds blob transactions for cheaper L2 data availability.

Q13. Which property does Bitcoin prioritize over scalability?
A) Speed and cost B) Decentralization and security
C) Smart contract flexibility D) Energy efficiency

Answer: B – Bitcoin's design maintains decentralization and security at the cost of throughput.

Q14. What is the main security concern with sidechains?
A) They are too slow B) They have separate validator sets (weaker security)
C) They cannot process smart contracts D) They require PoW consensus

Answer: B – Sidechains do not inherit L1 security guarantees like rollups do.

Q15. How does the Lightning Network achieve high throughput?
A) Larger blocks B) Off-chain transactions in payment channels
C) Faster block times D) More miners

Answer: B – Lightning opens channels with one on-chain TX, then unlimited off-chain payments.

Quiz Questions (4/4)

Q16. What is state expiry in Ethereum's roadmap?
A) Deleting old transactions B) Evicting inactive state, requiring proofs to re-activate
C) Eliminating smart contracts D) Reducing gas fees to zero

Answer: B – State expiry removes inactive data to limit state growth while allowing recovery.

Q17. Why is cross-shard communication challenging?
A) It requires complex coordination between shards B) It eliminates security
C) It is impossible to implement D) It reduces decentralization

Answer: A – Transactions spanning shards need atomic execution and additional overhead.

Q18. Which blockchain has approximately 65,000 theoretical TPS?
A) Bitcoin B) Ethereum C) Solana D) Cardano

Answer: C – Solana uses vertical scaling with high hardware requirements to achieve high TPS.

Q19. What is the Total Value Locked (TVL) in Ethereum Layer 2 solutions as of late 2024?
A) $5 billion B) $50+ billion C) $200 billion D) $500 billion

Answer: B – Ethereum L2 TVL reached $54B by Dec 2024 (205% YoY growth).

Q20. Can the scalability trilemma be fully "solved"?
A) Yes, with sharding B) Yes, with Layer 2 C) No, only mitigated through trade-offs
D) Yes, Solana solved it

Answer: C – The trilemma represents fundamental trade-offs; solutions mitigate but don't eliminate them.

Blockchain Scalability Trilemma

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Pick any two tradeoff

[COMIC: A blockchain engineer at a carnival game with three prizes behind glass labeled "Decentralization," "Security," and "Scalability." Sign reads: "WIN ANY TWO! (Sorry, three is physically impossible)"—the engineer looks frustrated while holding only two tickets]

The Fundamental Constraint

- Bitcoin chose decentralization + security = 7 TPS
- EOS chose security + scalability = 21 block producers
- Traditional databases chose scalability + security = single point of failure
- Can we escape this constraint? Layer 2 and sharding try...

Vitalik Buterin coined "scalability trilemma" in 2017—still no one has solved it

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the blockchain scalability trilemma
- Analyze trade-offs between security, decentralization, and scalability
- Understand Layer 1 scalability bottlenecks
- Compare throughput limitations across blockchains
- Evaluate vertical vs. horizontal scaling approaches
- Recognize emerging scalability solutions

Building on L10: Consensus Comparison

The Problem: How do we scale blockchains?

The Challenge
Blockchains face a fundamental limitation: achieving global-scale transaction throughput while preserving decentralization and security. Bitcoin processes 7 TPS while Ethereum handles 15 TPS—far below the requirements for mass adoption or competition with traditional payment systems.

Why It Matters

- Bitcoin: 7 TPS vs. Visa: 65,000 TPS—blockchains cannot serve billions of users
- Ethereum's 2017 CryptoKitties congestion halted the network, with gas prices spiking 1000%

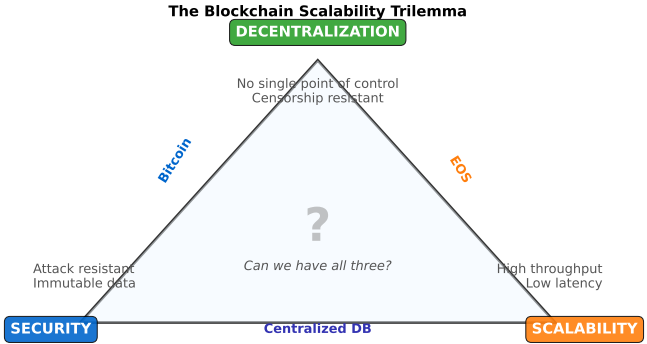
What We Need

- Understanding design constraints
- Scale to handle global transaction volumes without sacrificing decentralization or security

The Cryptoeconomics Question
How do we optimize for competing goals: throughput, decentralization, and security?

Today's lesson: How the Scalability Trilemma framework addresses this challenge

What is the Scalability Trilemma?



Coined by Vitalik Buterin: a blockchain can achieve at most two of three properties. | → *Problem: How do we scale blockchains? — The trilemma is a fundamental constraint – every blockchain project must choose which properties to optimize*

Why Can't Blockchains Have It All?

Three Properties:

- **Decentralization:** No single controller
- **Security:** Attack resistant
- **Scalability:** High TPS, low latency

Trade-Offs:

- BTC: Decentral + Secure = 7 TPS
- EOS: Scale + Secure = 21 nodes
- DB: Scale + Secure = centralized

Core Challenges:

- Large blocks = fewer validators
- Fewer validators = faster consensus
- Optimizing one degrades others

Key Insight:
No free lunch - trade-offs are fundamental

(c) Joerg Osterrieder 2025

Why Do These Three Properties Matter?

Decentralization

- Censorship resistance
- Fault tolerance
- Trustlessness
- No single point of failure

Security

- Immutability
- Double-spend prevention
- Attack resistance
- Data integrity

Scalability

- High throughput (TPS)
- Low latency (finality)
- Low transaction costs
- Mass adoption support

Why Blockchain Needs All Three:

- DeFi applications need high throughput AND security
- Mass adoption requires scalability without sacrificing decentralization
- Competition with traditional payment systems (Visa: 24,000 TPS)

What Limits Layer 1 Throughput?

Block Size:

- Larger = more TXs, slower propagation
- BTC: 1-4 MB — ETH: gas limit

Block Time:

- Faster = more orphans/forks
- BTC: 10m — ETH: 12s — SOL: 0.4s

State Growth:

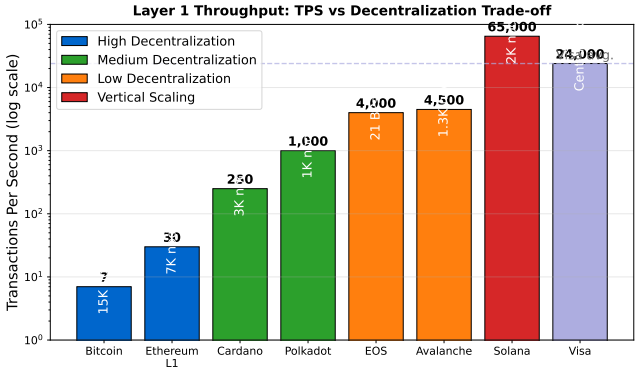
- BTC: 500 GB — ETH: 1 TB
- Full nodes need storage

Computation:

- Every node verifies all TXs
- Smart contracts expensive

→ *Problem: How do we scale blockchains? — Bitcoin's 7 TPS limit comes from 1MB blocks every 10 minutes – a deliberate security choice, not a technical limitation*

Layer 1 Throughput Comparison



Inverse correlation: higher TPS generally means fewer nodes and lower decentralization.

Should Bitcoin Increase Block Size?

Big Block Camp:

- Increase to 8+ MB
- Higher throughput, low fees
- Risk: centralization

Small Block Camp:

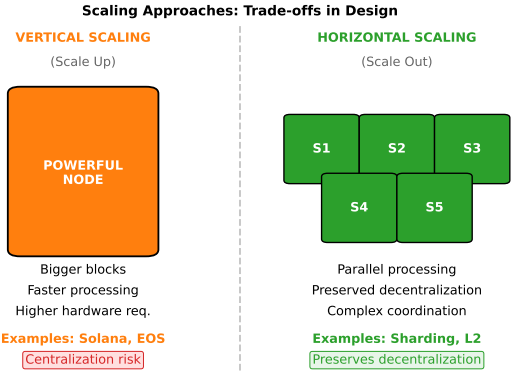
- Preserve decentralization
- Scale via Layer 2
- Accept higher on-chain fees

Outcome (2017):

- BCH fork: 8 MB blocks
- BTC: SegWit (1-4 MB)
- Market: BTC ¿ BCH

Lesson:
Decentralization prioritized; Layer 2 for scale

Vertical vs. Horizontal Scaling



Most major blockchains pursue horizontal scaling to preserve decentralization.

How Should We Scale: Up or Out?

Vertical Scaling (Scale Up)

- Increase capacity of individual nodes
- Require more powerful hardware
- Examples: Solana, EOS

Advantages:

- Simpler implementation
- Immediate throughput gains

Disadvantages:

- Raises barrier to run nodes
- Centralization risk
- Hits physical limits

Horizontal Scaling (Scale Out)

- Distribute load across many nodes
- Parallel processing
- Examples: Sharding, Layer 2, Rollups

Advantages:

- Preserves decentralization
- Theoretically unbounded scaling

Disadvantages:

- Complex implementation
- Cross-shard communication overhead
- Longer development timelines

→ *Problem: How do we scale blockchains? — Vertical scaling (bigger blocks) centralizes; horizontal scaling (sharding, L2) preserves decentralization*

Problem Check-In: Scalability Trilemma

Recall Our Problem

How do we scale blockchains?

What We've Learned So Far

- The scalability trilemma states blockchains can optimize only 2 of 3 properties: decentralization, security, scalability
- Layer 1 bottlenecks include block size, block time, state growth, and computation limits
- Bitcoin chose security/decentralization (7 TPS); Solana chose speed/security (65k TPS but 33 validators)

Still to Address

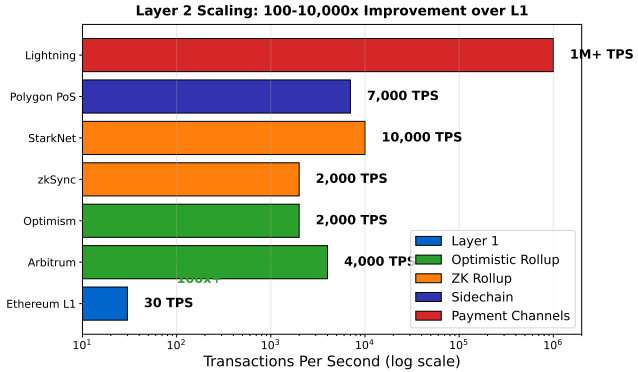
- Layer 2 solutions (rollups) and sharding as approaches to escape the trilemma
- Can we achieve 10,000+ TPS without sacrificing decentralization?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we scale blockchains?"?

Layer 2 Scaling Solutions



Layer 2 achieves 100-10,000x improvement while inheriting L1 security.

What Layer 2 Solutions Exist?

Payment Channels:

- Lightning Network
- 1 on-chain, unlimited off-chain
- Micropayments

Rollups:

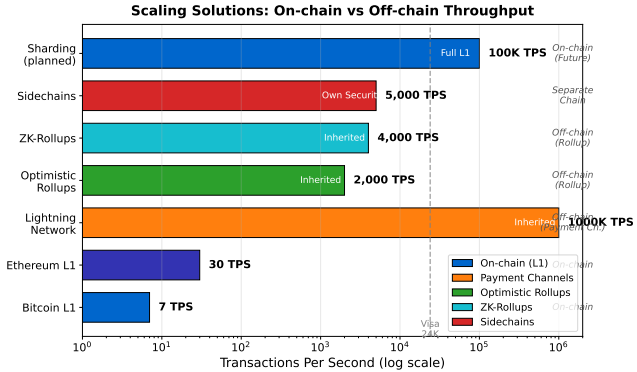
- Bundle 100s of TXs off-chain
- Optimistic: fraud proofs (7-day challenge window)
- ZK: validity proofs (instant cryptographic verification)

Sidechains:

- Independent chain
- Own consensus
- Weaker security

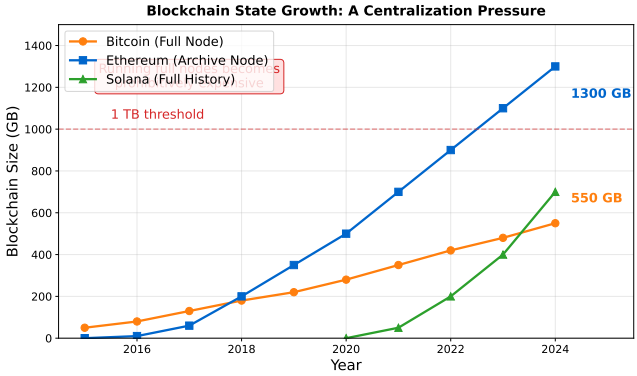
Adoption: Ethereum L2 TVL $54B+ (Dec 2024, 205% YoY)

Scaling Solutions Comparison



On-chain solutions inherit full L1 security; off-chain achieves higher TPS with varying trust assumptions.

State Growth Problem



Running full nodes becomes prohibitively expensive as state grows.

How Do We Control State Growth?

Challenge:

- Unbounded growth
- ETH state: 100 GB
- Sync takes days/weeks
- Centralization pressure

Solutions:

- **State Expiry:** evict inactive, proof to recover
- **Pruning:** keep recent blocks only
- **Rent:** pay to store (Cosmos, EOS)

→ *Problem: How do we scale blockchains? — State growth is blockchain's hidden scaling problem – Ethereum's state grows 60GB/year, pricing out home validators*

How Does Sharding Scale at Layer 1?

Concept:

- Split into parallel shards
- Each processes subset of TXs
- Total TPS = shards x per-shard

Ethereum Roadmap:

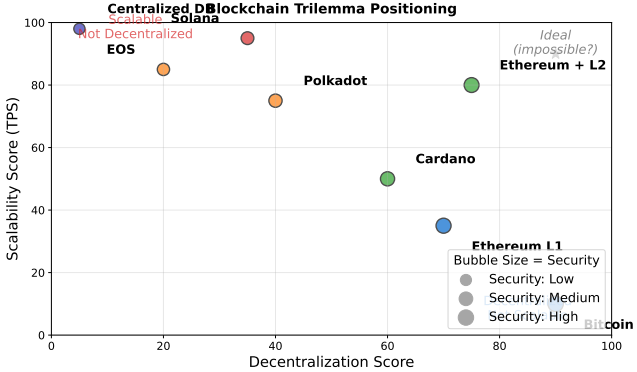
- Danksharding (Ethereum's data availability approach using temporary "blobs" for cheap rollup data) for DA (Data Availability – the guarantee that transaction data is published and accessible)
- EIP-4844 (March 2024)
- Target: 100K+ TPS

Challenges:

- Cross-shard complexity
- Shard takeover attacks
- State management

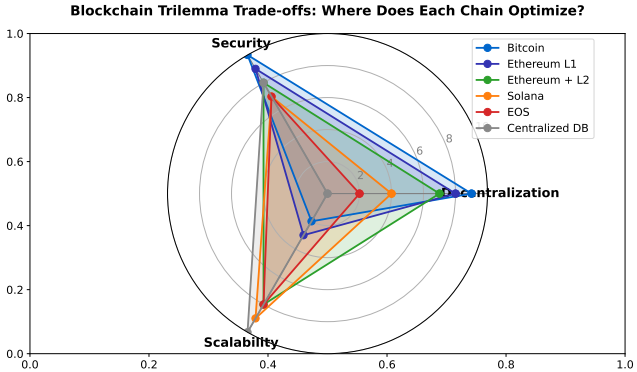
Other Chains:
Zilliqa, NEAR, Elrond

Trilemma Positioning



Ethereum + L2 approaches the "ideal" corner without sacrificing security.

Trilemma Trade-offs by Blockchain



Radar chart shows each blockchain's optimization choices. Bitcoin maximizes security/decentralization; Solana prioritizes scalability.

Can We Break the Trilemma?

Optimistic:

- L2 separates layers
- Rollups keep security
- ZK compresses compute

Pessimistic:

- L2 adds trust
- More complexity
- DA (Data Availability) bandwidth limits

Consensus:

- Mitigate, not solve
- Modular design
- L1 security, L2 scale

Navigate the trilemma intelligently rather than "solve" it

Problem Solved? Scalability Trilemma

The Original Problem

How do we scale blockchains to handle global transaction volume?

How Scalability Solutions Address It

- **Layer 2 solutions (rollups, state channels):** Move computation off-chain, achieve 100-10,000x throughput improvement while inheriting L1 security
- **Sharding:** Split state across parallel chains, enabling horizontal scaling to theoretically unbounded throughput
- **Modular design:** Separate consensus, data availability, and execution layers to optimize each independently

Remaining Limitations

- **Layer 2 introduces new trust assumptions:** Sequencer centralization, bridge security risks, and withdrawal delays
- **Trade-off made:** Increased complexity and fragmented liquidity in exchange for higher throughput

Open Questions

- Will rollups or sharding dominate as the long-term scaling solution?
- Risk: Over-optimization for single metric

Scalability Trilemma framework helps navigate trade-offs but doesn't eliminate fundamental constraints

(c) Joerg Osterrieder 2025

The Economics of Scalability Trilemma

Incentive Structure

- **Core Problem:** Optimizing multiple competing goals
- **Why act honestly?** Choose based on use case requirements
- **Value Flow:** Gain in one dimension, sacrifice in another

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Gain in one dimension, sacrifice in another

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Scalability Trilemma

Alternatives Considered

1. **Chosen Design:** Different points on trade-off frontier
2. **Alternative:** Layer 2 solutions, hybrid approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Scalability Trilemma

Critical Failure Mode

- **What breaks:** Over-optimization for single metric
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Blockchain throughput traffic jam

[COMIC: A massive traffic jam on a single-lane road (Bitcoin at 7 TPS) while parallel roads (Layer 2) and multi-lane highways (sharding) show alternative routes—some cars taking the toll road labeled "Roll up: $0.01 fee, 1000x faster"]

Scaling Without Compromise

- Layer 1: the secure but congested main highway (7-30 TPS)
- Layer 2 rollups: toll roads that inherit L1 security (1000+ TPS)
- Ethereum's strategy: L1 for settlement, L2 for execution
- Result: $54B TVL on L2s, 90%+ fee reduction post-EIP-4844

CryptoKitties 2017: gas fees hit $100—today's L2s: same tx for $0.01

Key Takeaways

Trilemma:

- Cannot maximize all three
- L1: block size, time, state
- Vertical = centralization
- Horizontal = decentralization

Next Lesson: L12 – Lab: Block Explorer

Solutions:

- L2: 100-1000x throughput
- State growth = risk
- Real TPS ¡ theoretical

Philosophy:
BTC: decentral — SOL: scale — ETH: L2 balance

Discussion Questions

1. Why cannot a blockchain simply increase block size indefinitely?
2. How do Layer 2 solutions differ from sidechains in terms of security?
3. What are the implications of state growth for decentralization?
4. Can the trilemma be "solved" or only mitigated?
5. How does sharding introduce new security challenges?
6. Why do most blockchains have lower actual TPS than theoretical TPS?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L12 Lab - Block Explorer Analysis

Lab Activities:

- Navigate Etherscan, Blockstream
- Analyze TX details
- Trace mempool to confirmation
- Examine block structure
- Forensic analysis

Preparation:

- Review L6 TX structure
- Access Etherscan.io
- Access Blockstream.info

(c) Joerg Osterrieder 2025

Quiz Questions (1/4)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability
C) The trade-off between speed and cost D) The conflict between miners and validators

Answer: B – The trilemma states a blockchain can optimize at most two of three properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks
C) It makes attacks easier D) It decreases transaction fees

Answer: B – Larger blocks require more bandwidth and storage, raising barriers to running full nodes.

Q3. Bitcoin processes approximately how many transactions per second (TPS)?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS

Answer: B – Bitcoin's design prioritizes decentralization and security over throughput.

Q4. What is vertical scaling in blockchain context?
A) Adding more nodes to the network B) Increasing capacity of individual nodes
C) Creating Layer 2 solutions D) Implementing sharding

Answer: B – Vertical scaling means requiring more powerful hardware per node.

Q5. Which blockchain outcome resulted from the 2017 block size debate?
A) Ethereum Classic fork B) Bitcoin Cash fork with larger blocks
C) Bitcoin unlimited blocks D) Complete consensus on 8 MB blocks

Answer: B – Bitcoin Cash forked with 8 MB blocks while Bitcoin implemented SegWit.

Quiz Questions (2/4)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security
C) Lower hardware requirements D) Simpler code implementation

Answer: B – Layer 2 achieves 100-10,000x scalability while settling to secure Layer 1.

Q7. How does horizontal scaling differ from vertical scaling?
A) It uses better hardware B) It distributes load across many nodes/shards
C) It reduces security D) It eliminates the need for consensus

Answer: B – Horizontal scaling parallelizes processing to preserve decentralization.

Q8. What is sharding?
A) Compressing blockchain data B) Splitting blockchain into parallel processing shards
C) Encrypting transactions D) A type of consensus algorithm

Answer: B – Sharding divides the network to process transactions in parallel.

Q9. Which Layer 2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains

Answer: C – Optimistic Rollups assume validity and allow challenges via fraud proofs.

Q10. What is the state growth problem?
A) Blockchain size growing unbounded over time B) Decreasing transaction volume
C) Fewer validators joining D) Rising energy consumption

Answer: A – As blockchain accumulates data, storage requirements create centralization pressure.

Quiz Questions (3/4)

Q11. How do ZK-Rollups validate transactions?
A) Through fraud proofs B) Using cryptographic validity proofs
C) By running full nodes D) Through validator voting

Answer: B – ZK-Rollups use zero-knowledge proofs to guarantee transaction validity.

Q12. What was Ethereum's EIP-4844 proto-danksharding (March 2024)?
A) Full execution sharding B) Data availability sharding to reduce L2 costs
C) Transition to PoS D) Gas fee elimination

Answer: B – Proto-danksharding adds blob transactions for cheaper L2 data availability.

Q13. Which property does Bitcoin prioritize over scalability?
A) Speed and cost B) Decentralization and security
C) Smart contract flexibility D) Energy efficiency

Answer: B – Bitcoin's design maintains decentralization and security at the cost of throughput.

Q14. What is the main security concern with sidechains?
A) They are too slow B) They have separate validator sets (weaker security)
C) They cannot process smart contracts D) They require PoW consensus

Answer: B – Sidechains do not inherit L1 security guarantees like rollups do.

Q15. How does the Lightning Network achieve high throughput?
A) Larger blocks B) Off-chain transactions in payment channels
C) Faster block times D) More miners

Answer: B – Lightning opens channels with one on-chain TX, then unlimited off-chain payments.

Quiz Questions (4/4)

Q16. What is state expiry in Ethereum's roadmap?
A) Deleting old transactions B) Evicting inactive state, requiring proofs to re-activate
C) Eliminating smart contracts D) Reducing gas fees to zero

Answer: B – State expiry removes inactive data to limit state growth while allowing recovery.

Q17. Why is cross-shard communication challenging?
A) It requires complex coordination between shards B) It eliminates security
C) It is impossible to implement D) It reduces decentralization

Answer: A – Transactions spanning shards need atomic execution and additional overhead.

Q18. Which blockchain has approximately 65,000 theoretical TPS?
A) Bitcoin B) Ethereum C) Solana D) Cardano

Answer: C – Solana uses vertical scaling with high hardware requirements to achieve high TPS.

Q19. What is the Total Value Locked (TVL) in Ethereum Layer 2 solutions as of late 2024?
A) $5 billion B) $50+ billion C) $200 billion D) $500 billion

Answer: B – Ethereum L2 TVL reached $54B by Dec 2024 (205% YoY growth).

Q20. Can the scalability trilemma be fully "solved"?
A) Yes, with sharding B) Yes, with Layer 2 C) No, only mitigated through trade-offs
D) Yes, Solana solved it

Answer: C – The trilemma represents fundamental trade-offs; solutions mitigate but don't eliminate them.

Blockchain Scalability Trilemma

BSc Blockchain, Crypto Economy & NFTs – Condensed Version

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

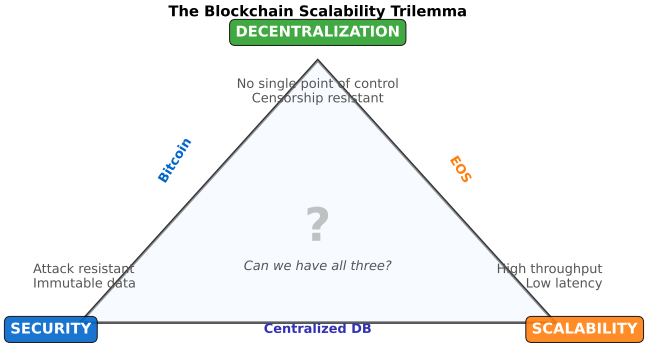
Learning Objectives

By the end of this lesson, you will be able to:

- Explain the blockchain scalability trilemma
- Analyze trade-offs between security, decentralization, and scalability
- Compare throughput limitations across blockchains
- Evaluate vertical vs. horizontal scaling approaches

(c) Joerg Osterrieder 2025

The Scalability Trilemma



Coined by Vitalik Buterin: a blockchain can achieve at most two of three properties.

Understanding the Trilemma

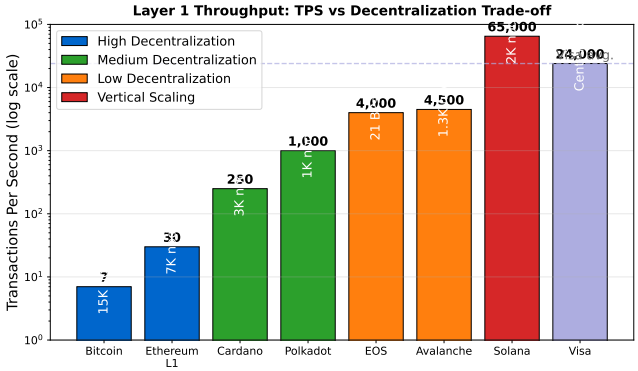
The Three Properties:

1. **Decentralization:** No single entity controls the network
2. **Security:** Resistant to attacks, ensures data integrity
3. **Scalability:** High transaction throughput and low latency

Trade-Off Examples:

- Bitcoin: Decentralized + Secure $\rightarrow$ Low Scalability (7 TPS)
- EOS: Scalable + Secure $\rightarrow$ Low Decentralization (21 block producers)
- No free lunch: optimizing one property often degrades another

Layer 1 Throughput Comparison



Inverse correlation: higher TPS generally means fewer nodes and lower decentralization.

Layer 1 Bottlenecks

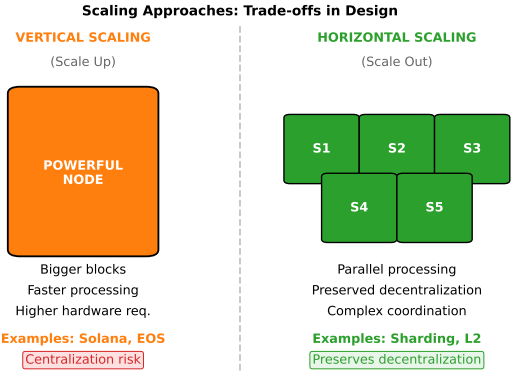
Fundamental Constraints:

1. **Block Size:** Larger blocks = more TXs, but slower propagation
2. **Block Time:** Faster blocks = higher throughput, but more orphans
3. **State Growth:** Bitcoin ∼500 GB, Ethereum ∼1 TB (archive)
4. **Computational Overhead:** Every node verifies every transaction

Example Block Times:

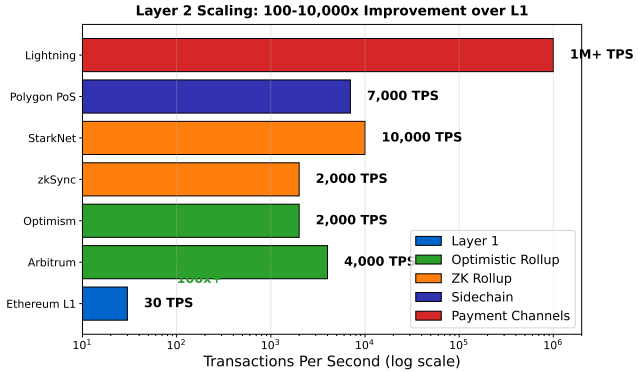
- Bitcoin: 10 min — Ethereum: 12 sec — Solana: 0.4 sec

Vertical vs. Horizontal Scaling



Most major blockchains pursue horizontal scaling to preserve decentralization.

Layer 2 Scaling Solutions

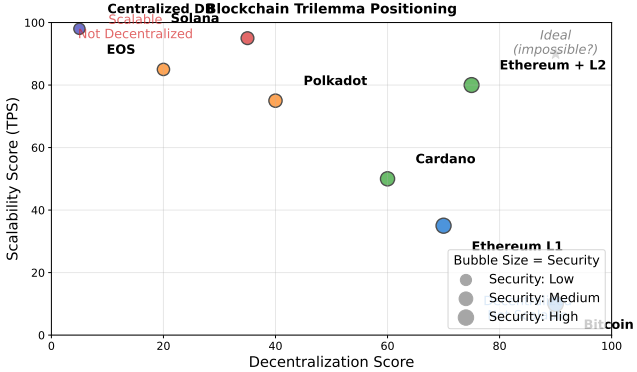


Layer 2 achieves 100-10,000x improvement while inheriting L1 security.

Layer 2 Types

1. **Payment Channels (Lightning Network):**
   - Open channel with on-chain TX, unlimited off-chain TXs
   - Use case: micropayments, instant transfers
2. **Rollups (Optimistic, ZK):**
   - Bundle hundreds of transactions into one
   - Optimistic: assume valid, fraud proofs challenge
   - ZK: cryptographic validity proofs
3. **Sidechains (Polygon):**
   - Independent blockchain with bridge to main chain
   - Weaker security than rollups (separate validator set)

Trilemma Positioning



Ethereum + L2 approaches the "ideal" corner without sacrificing security.

Key Takeaways

- Scalability trilemma: cannot maximize decentralization, security, and scalability simultaneously
- Layer 1 bottlenecks: block size, block time, state growth
- Vertical scaling (bigger nodes) increases centralization
- Horizontal scaling (sharding, Layer 2) preserves decentralization
- Layer 2 solutions achieve 100-1000x throughput improvement

Design Philosophy:
Accept that trade-offs exist. Bitcoin prioritizes decentralization/security. Solana prioritizes scalability. Ethereum aims for balance via Layer 2.

Visual Concepts

Balance & Trade-offs

Network Scaling

Decision Points

Images: Unsplash (CC0 License)

Quiz Questions (1/2)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability
C) The trade-off between speed and cost D) The conflict between miners and validators

Answer: B – The trilemma states a blockchain can optimize at most two of three properties.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks
C) It makes attacks easier D) It decreases transaction fees

Answer: B – Larger blocks require more bandwidth and storage, raising barriers to running full nodes.

Q3. Bitcoin processes approximately how many transactions per second (TPS)?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS

Answer: B – Bitcoin's design prioritizes decentralization and security over throughput.

Quiz Questions (2/2)

Q4. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security
C) Lower hardware requirements D) Simpler code implementation

Answer: B – Layer 2 achieves 100-10,000x scalability while settling to secure Layer 1.

Q5. How does horizontal scaling differ from vertical scaling?
A) It uses better hardware B) It distributes load across many nodes/shards
C) It reduces security D) It eliminates the need for consensus

Answer: B – Horizontal scaling parallelizes processing to preserve decentralization.

Q6. Which Layer 2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains

Answer: C – Optimistic Rollups assume validity and allow challenges via fraud proofs.

L11: Blockchain Scalability Trilemma

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

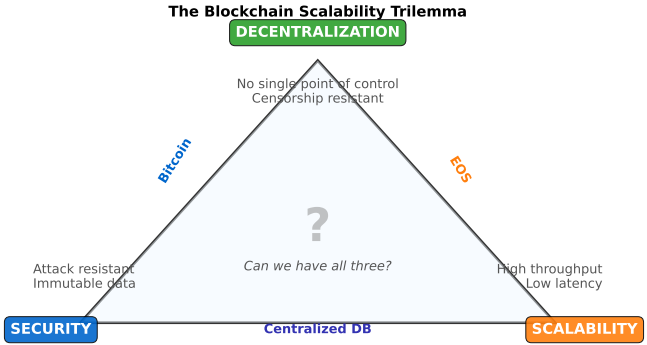
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

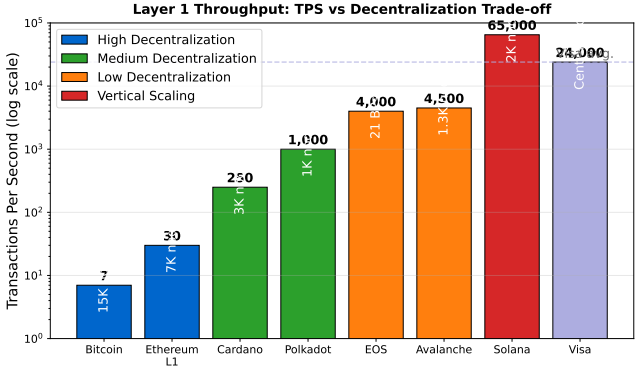
- Explain the blockchain scalability trilemma
- Analyze trade-offs: security, decentralization, scalability
- Understand Layer 1 bottlenecks and Layer 2 solutions
- Evaluate vertical vs horizontal scaling approaches

The Scalability Trilemma



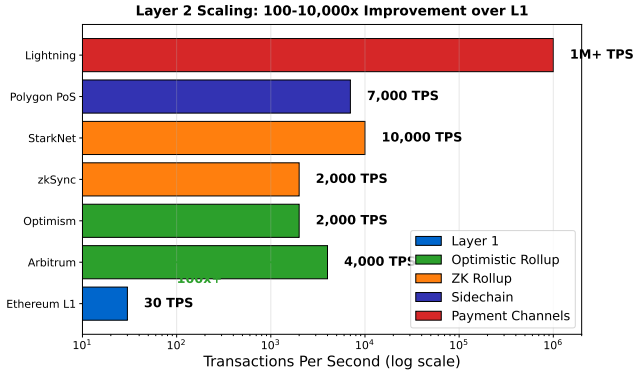
Vitalik Buterin: A blockchain can achieve at most two of three properties simultaneously.

Layer 1 Throughput Comparison



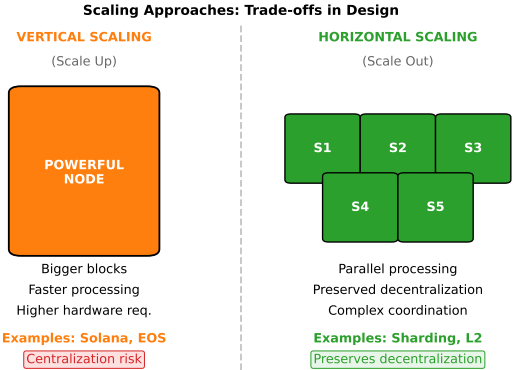
Inverse Correlation: Higher TPS generally requires sacrificing decentralization.

Layer 2 Scaling Solutions



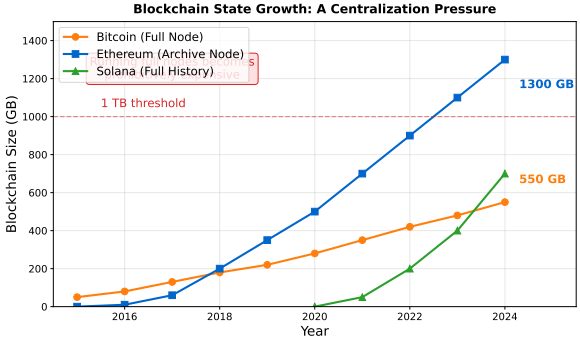
100-10,000x improvement while inheriting L1 security. L2 TVL: \$54B+ (Dec 2024).

Vertical vs Horizontal Scaling



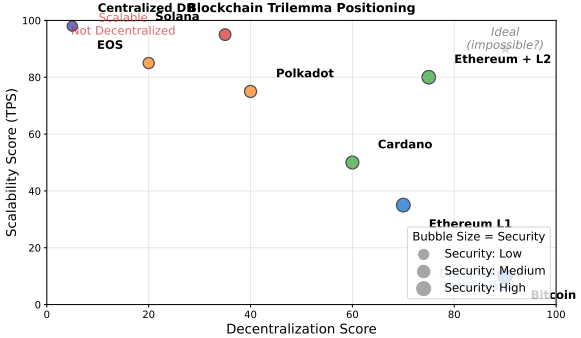
Vertical: Bigger nodes (Solana) — **Horizontal:** Sharding, L2 (Ethereum)

State Growth Problem



Challenge: Blockchain size grows unbounded; syncing new nodes takes days/weeks.

Blockchain Trilemma Positioning



Ethereum + L2: Approaches ideal corner without sacrificing security.

Layer 2 Solutions Explained

1. **Payment Channels (Lightning):**
   - One on-chain TX opens channel, unlimited off-chain transfers
   - Use case: micropayments, instant transfers

2. **Rollups (Optimistic, ZK):**
   - Bundle 100s of transactions into one
   - Optimistic: fraud proofs — ZK: validity proofs
   - Use case: DeFi, NFTs, general computation

3. **Sidechains (Polygon):**
   - Independent chain with bridge to L1
   - Weaker security (separate validator set)

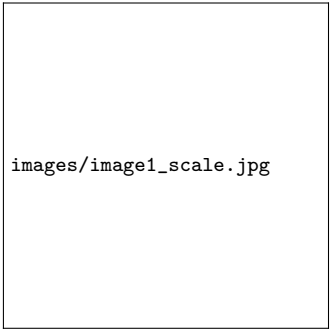
(c) Joerg Osterrieder 2025

Key Takeaways

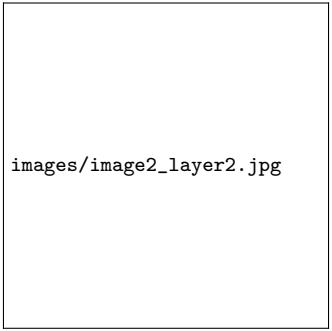
1. **Trilemma:** Cannot maximize decentralization, security, AND scalability
2. **L1 Bottlenecks:** Block size, block time, state growth
3. **Vertical Scaling:** Bigger nodes = centralization (Solana: 65K TPS)
4. **Horizontal Scaling:** Sharding, L2 preserves decentralization
5. **Layer 2:** Achieves 100-1000x throughput improvement

Design Philosophy: Accept trade-offs exist. Bitcoin prioritizes decentralization/security. Ethereum balances via L2. No free lunch.

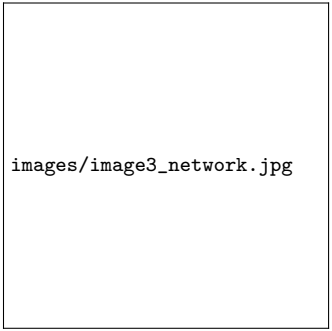
Blockchain Scaling in Action



Scaling Challenge



Layer 2 Solutions



Network Growth

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) PoW vs PoS vs DPoS B) Only two of: decentralization, security, scalability C) Speed vs cost D) Miners vs validators

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) PoW vs PoS vs DPoS B) Only two of: decentralization, security, scalability C) Speed vs cost D) Miners vs validators
Answer: B – Can optimize at most two properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) Reduces rewards B) Fewer nodes can store/propagate C) Makes attacks easier D) Decreases fees

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) PoW vs PoS vs DPoS B) Only two of: decentralization, security, scalability C) Speed vs cost D) Miners vs validators
Answer: B – Can optimize at most two properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) Reduces rewards B) Fewer nodes can store/propagate C) Makes attacks easier D) Decreases fees
Answer: B – Larger blocks require more bandwidth and storage.

Q3. Bitcoin processes approximately how many TPS?
A) 3 B) 7 C) 30 D) 100

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) PoW vs PoS vs DPoS B) Only two of: decentralization, security, scalability C) Speed vs cost D) Miners vs validators
Answer: B – Can optimize at most two properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) Reduces rewards B) Fewer nodes can store/propagate C) Makes attacks easier D) Decreases fees
Answer: B – Larger blocks require more bandwidth and storage.

Q3. Bitcoin processes approximately how many TPS?
A) 3 B) 7 C) 30 D) 100
Answer: B – Bitcoin prioritizes decentralization over throughput.

Q4. What is vertical scaling?
A) Adding more nodes B) Increasing capacity of individual nodes C) Layer 2 D) Sharding

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) PoW vs PoS vs DPoS B) Only two of: decentralization, security, scalability C) Speed vs cost D) Miners vs validators
Answer: B – Can optimize at most two properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) Reduces rewards B) Fewer nodes can store/propagate C) Makes attacks easier D) Decreases fees
Answer: B – Larger blocks require more bandwidth and storage.

Q3. Bitcoin processes approximately how many TPS?
A) 3 B) 7 C) 30 D) 100
Answer: B – Bitcoin prioritizes decentralization over throughput.

Q4. What is vertical scaling?
A) Adding more nodes B) Increasing capacity of individual nodes C) Layer 2 D) Sharding
Answer: B – Requiring more powerful hardware per node.

Q5. Which L2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) PoW vs PoS vs DPoS B) Only two of: decentralization, security, scalability C) Speed vs cost D) Miners vs validators
Answer: B – Can optimize at most two properties simultaneously.

Q2. Why does increasing block size lead to centralization?
A) Reduces rewards B) Fewer nodes can store/propagate C) Makes attacks easier D) Decreases fees
Answer: B – Larger blocks require more bandwidth and storage.

Q3. Bitcoin processes approximately how many TPS?
A) 3 B) 7 C) 30 D) 100
Answer: B – Bitcoin prioritizes decentralization over throughput.

Q4. What is vertical scaling?
A) Adding more nodes B) Increasing capacity of individual nodes C) Layer 2 D) Sharding
Answer: B – Requiring more powerful hardware per node.

Q5. Which L2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains
Answer: C – Optimistic Rollups assume validity, allow challenges.

Quiz (2/2)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware D) Simpler code

Quiz (2/2)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware D) Simpler code
Answer: B – 100-10,000x scalability while settling to secure L1.

Q7. What was EIP-4844 proto-danksharding (March 2024)?
A) Full sharding B) Data availability to reduce L2 costs C) PoS transition D) Gas elimination

Quiz (2/2)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware D) Simpler code
Answer: B – 100-10,000x scalability while settling to secure L1.

Q7. What was EIP-4844 proto-danksharding (March 2024)?
A) Full sharding B) Data availability to reduce L2 costs C) PoS transition D) Gas elimination
Answer: B – Adds blob transactions for cheaper L2 data availability.

Q8. Which blockchain has 65,000 theoretical TPS?
A) Bitcoin B) Ethereum C) Solana D) Cardano

Quiz (2/2)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware D) Simpler code
Answer: B – 100-10,000x scalability while settling to secure L1.

Q7. What was EIP-4844 proto-danksharding (March 2024)?
A) Full sharding B) Data availability to reduce L2 costs C) PoS transition D) Gas elimination
Answer: B – Adds blob transactions for cheaper L2 data availability.

Q8. Which blockchain has 65,000 theoretical TPS?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: C – Solana uses vertical scaling with high hardware requirements.

Q9. What is the L2 TVL on Ethereum as of late 2024?
A) $5B B) $54B+ C) $200B D) $500B

Quiz (2/2)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware D) Simpler code
Answer: B – 100-10,000x scalability while settling to secure L1.

Q7. What was EIP-4844 proto-danksharding (March 2024)?
A) Full sharding B) Data availability to reduce L2 costs C) PoS transition D) Gas elimination
Answer: B – Adds blob transactions for cheaper L2 data availability.

Q8. Which blockchain has 65,000 theoretical TPS?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: C – Solana uses vertical scaling with high hardware requirements.

Q9. What is the L2 TVL on Ethereum as of late 2024?
A) $5B B) $54B+ C) $200B D) $500B
Answer: B – $54B+ (205% YoY growth).

Q10. Can the scalability trilemma be fully solved?
A) Yes with sharding B) Yes with L2 C) No, only mitigated D) Solana solved it

Quiz (2/2)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware D) Simpler code
Answer: B – 100-10,000x scalability while settling to secure L1.

Q7. What was EIP-4844 proto-danksharding (March 2024)?
A) Full sharding B) Data availability to reduce L2 costs C) PoS transition D) Gas elimination
Answer: B – Adds blob transactions for cheaper L2 data availability.

Q8. Which blockchain has 65,000 theoretical TPS?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: C – Solana uses vertical scaling with high hardware requirements.

Q9. What is the L2 TVL on Ethereum as of late 2024?
A) $5B B) $54B+ C) $200B D) $500B
Answer: B – $54B+ (205% YoY growth).

Q10. Can the scalability trilemma be fully solved?
A) Yes with sharding B) Yes with L2 C) No, only mitigated D) Solana solved it
Answer: C – Fundamental trade-offs; solutions mitigate but don't eliminate.

Thank you

Questions?

Next: L12 Lab – Block Explorer Analysis

Quiz: Scalability Trilemma

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability C) The trade-off between speed and cost D) The conflict between miners and validators

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability C) The trade-off between speed and cost D) The conflict between miners and validators
Answer: B – A blockchain can optimize at most two of three properties.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks C) It makes attacks easier D) It decreases transaction fees

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability C) The trade-off between speed and cost D) The conflict between miners and validators
Answer: B – A blockchain can optimize at most two of three properties.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks C) It makes attacks easier D) It decreases transaction fees
Answer: B – Larger blocks require more bandwidth/storage, raising node barriers.

Q3. Bitcoin processes approximately how many TPS?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability C) The trade-off between speed and cost D) The conflict between miners and validators
Answer: B – A blockchain can optimize at most two of three properties.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks C) It makes attacks easier D) It decreases transaction fees
Answer: B – Larger blocks require more bandwidth/storage, raising node barriers.

Q3. Bitcoin processes approximately how many TPS?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS
Answer: B – Bitcoin prioritizes decentralization and security over throughput.

Q4. What is vertical scaling?
A) Adding more nodes B) Increasing individual node capacity C) Layer 2 solutions D) Sharding

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability C) The trade-off between speed and cost D) The conflict between miners and validators
Answer: B – A blockchain can optimize at most two of three properties.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks C) It makes attacks easier D) It decreases transaction fees
Answer: B – Larger blocks require more bandwidth/storage, raising node barriers.

Q3. Bitcoin processes approximately how many TPS?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS
Answer: B – Bitcoin prioritizes decentralization and security over throughput.

Q4. What is vertical scaling?
A) Adding more nodes B) Increasing individual node capacity C) Layer 2 solutions D) Sharding
Answer: B – Vertical scaling means more powerful hardware per node.

Q5. Which Layer 2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) The choice between PoW, PoS, and DPoS B) Achieving only two of: decentralization, security, scalability C) The trade-off between speed and cost D) The conflict between miners and validators
Answer: B – A blockchain can optimize at most two of three properties.

Q2. Why does increasing block size lead to centralization?
A) It reduces miner rewards B) Fewer nodes can store/propagate large blocks C) It makes attacks easier D) It decreases transaction fees
Answer: B – Larger blocks require more bandwidth/storage, raising node barriers.

Q3. Bitcoin processes approximately how many TPS?
A) 3 TPS B) 7 TPS C) 30 TPS D) 100 TPS
Answer: B – Bitcoin prioritizes decentralization and security over throughput.

Q4. What is vertical scaling?
A) Adding more nodes B) Increasing individual node capacity C) Layer 2 solutions D) Sharding
Answer: B – Vertical scaling means more powerful hardware per node.

Q5. Which Layer 2 solution uses fraud proofs?
A) ZK-Rollups B) Payment channels C) Optimistic Rollups D) Sidechains
Answer: C – Optimistic Rollups assume validity and allow fraud proof challenges.

Quiz (6–10)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware requirements
D) Simpler implementation

Quiz (6–10)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware requirements
D) Simpler implementation
Answer: B – L2 achieves 100-10,000x scalability while settling to secure L1.

Q7. What is sharding?
A) Compressing data B) Splitting blockchain into parallel shards C) Encrypting TXs D) A consensus type

Quiz (6–10)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware requirements D) Simpler implementation
Answer: B – L2 achieves 100-10,000x scalability while settling to secure L1.

Q7. What is sharding?
A) Compressing data B) Splitting blockchain into parallel shards C) Encrypting TXs D) A consensus type
Answer: B – Sharding divides the network to process transactions in parallel.

Q8. What was the 2017 block size debate outcome?
A) Ethereum Classic fork B) Bitcoin Cash fork (8 MB blocks) C) Bitcoin unlimited blocks D) Complete consensus on 8 MB

Quiz (6–10)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware requirements D) Simpler implementation
Answer: B – L2 achieves 100-10,000x scalability while settling to secure L1.

Q7. What is sharding?
A) Compressing data B) Splitting blockchain into parallel shards C) Encrypting TXs D) A consensus type
Answer: B – Sharding divides the network to process transactions in parallel.

Q8. What was the 2017 block size debate outcome?
A) Ethereum Classic fork B) Bitcoin Cash fork (8 MB blocks) C) Bitcoin unlimited blocks D) Complete consensus on 8 MB
Answer: B – BCH forked with larger blocks; BTC implemented SegWit.

Q9. Which property does Bitcoin prioritize over scalability?
A) Speed and cost B) Decentralization and security C) Smart contracts D) Energy efficiency

Quiz (6–10)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware requirements D) Simpler implementation
Answer: B – L2 achieves 100-10,000x scalability while settling to secure L1.

Q7. What is sharding?
A) Compressing data B) Splitting blockchain into parallel shards C) Encrypting TXs D) A consensus type
Answer: B – Sharding divides the network to process transactions in parallel.

Q8. What was the 2017 block size debate outcome?
A) Ethereum Classic fork B) Bitcoin Cash fork (8 MB blocks) C) Bitcoin unlimited blocks D) Complete consensus on 8 MB
Answer: B – BCH forked with larger blocks; BTC implemented SegWit.

Q9. Which property does Bitcoin prioritize over scalability?
A) Speed and cost B) Decentralization and security C) Smart contracts D) Energy efficiency
Answer: B – Bitcoin maintains decentralization/security at cost of throughput.

Q10. Can the scalability trilemma be fully solved?
A) Yes, with sharding B) Yes, with L2 C) No, only mitigated D) Yes, Solana solved it

Quiz (6–10)

Q6. What is the primary advantage of Layer 2 solutions?
A) Complete decentralization B) Higher throughput while inheriting L1 security C) Lower hardware requirements D) Simpler implementation
Answer: B – L2 achieves 100-10,000x scalability while settling to secure L1.

Q7. What is sharding?
A) Compressing data B) Splitting blockchain into parallel shards C) Encrypting TXs D) A consensus type
Answer: B – Sharding divides the network to process transactions in parallel.

Q8. What was the 2017 block size debate outcome?
A) Ethereum Classic fork B) Bitcoin Cash fork (8 MB blocks) C) Bitcoin unlimited blocks D) Complete consensus on 8 MB
Answer: B – BCH forked with larger blocks; BTC implemented SegWit.

Q9. Which property does Bitcoin prioritize over scalability?
A) Speed and cost B) Decentralization and security C) Smart contracts D) Energy efficiency
Answer: B – Bitcoin maintains decentralization/security at cost of throughput.

Q10. Can the scalability trilemma be fully solved?
A) Yes, with sharding B) Yes, with L2 C) No, only mitigated D) Yes, Solana solved it
Answer: C – The trilemma represents fundamental trade-offs; solutions mitigate but don't eliminate.

(c) Joerg Osterrieder 2025

Lab Session: Block Explorer Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Navigate Etherscan and Blockstream block explorers
- Analyze transaction details: inputs, outputs, fees
- Trace transaction lifecycle from broadcast to confirmation
- Examine block structure and validator information
- Investigate address activity and transaction history
- Conduct basic blockchain forensic analysis

The Problem: Hands-on Blockchain Analysis

The Challenge
How do users verify blockchain transactions without running a full node? Raw blockchain data is complex (hex addresses, gas units, block headers) and requires specialized infrastructure to query and interpret.

Why It Matters

- Without accessible data tools, users must trust centralized exchanges to report balances
- Investigative journalists and auditors need transparent access to on-chain activity

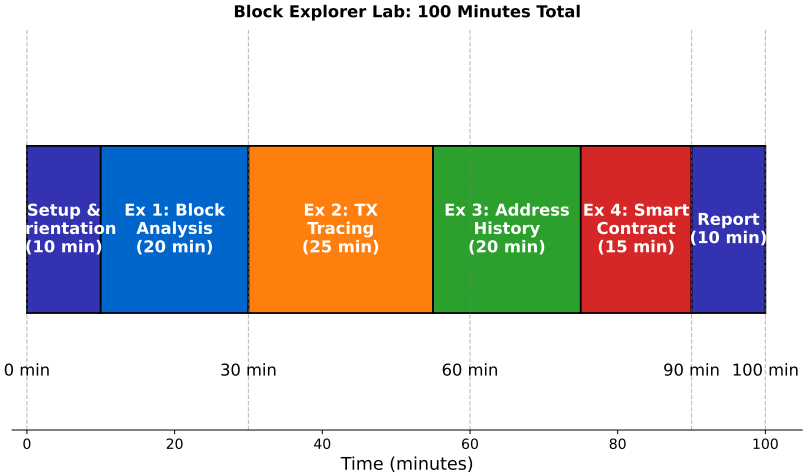
What We Need

- Trustless verification mechanism
- Human-readable interfaces to blockchain data without running costly infrastructure

The Cryptoeconomics Question
How do block explorers enable transparency while remaining economically sustainable?

Today's lesson: How block explorers solve the blockchain data accessibility challenge

Lab Session Structure



Total duration: 100 minutes with 4 main exercises

What is a Block Explorer?

Definition:

- Web-based interface to query blockchain data
- Provides human-readable view of blocks, transactions, addresses
- Free and publicly accessible

Major Block Explorers:

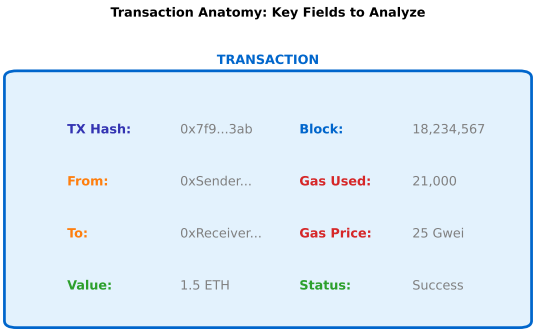
Bitcoin:

- Blockstream.info
- Blockchain.com
- Mempool.space

Ethereum:

- Etherscan.io
- Blockscout.com
- Ethplorer.io

Transaction Anatomy



Understanding these fields is essential for analyzing any blockchain transaction

Exercise 1: Analyzing Bitcoin Transactions

Instructions:

1. Visit: `https://blockstream.info`
2. Search for the first-ever Bitcoin transaction:
   `f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16`
3. Examine: inputs, outputs, fee, block number, confirmations

Key Observations:

- **Inputs:** Reference to previous transaction output
- **Outputs:** New UTXOs with amounts and addresses
- **Fee:** Difference between input sum and output sum
- **Confirmations:** Blocks built on top of this transaction

Exercise 2: Analyzing Ethereum Transactions

Instructions:

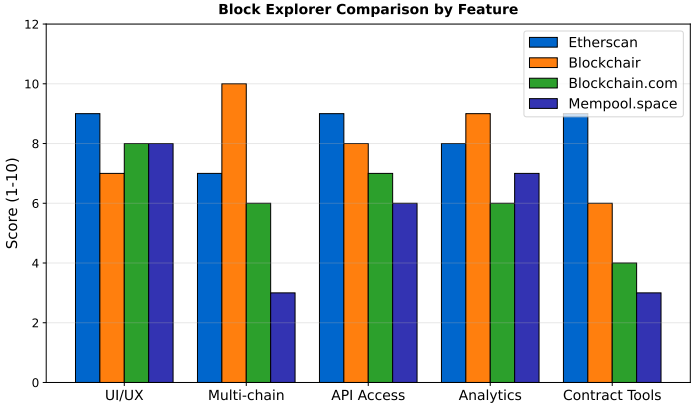
1. Visit: `https://etherscan.io`
2. Select a recent transaction from homepage
3. Examine: hash, status, block, from, to, value, gas

Gas Mechanics:

- Gas Limit: Maximum gas user willing to pay
- Gas Used: Actual gas consumed
- Gas Price: Price per unit (in gwei)
- Transaction Fee: Gas Used $\times$ Gas Price

Example: 21,000 gas $\times$ 32 gwei $=$ 0.000672 ETH

Block Explorer Comparison



Etherscan excels for Ethereum; Blockchair for multi-chain research

Exercise 3: Address Investigation

Entity Types to Analyze:

1. **Exchange Address:** High volume, large balances, labeled
2. **Smart Contract:** "Contract" label, receives interactions
3. **Individual User:** Low volume, smaller balances

Sample Addresses:

- Binance: `0x28C6c06298d514Db089934071355E5743bf21d60`
- Uniswap: `0xE592427A0AEce92De3Edee1F18E0157C05861564`
- Your MetaMask address (from Lab 8)

Exercise 4: Forensic Case Study

Scenario: Tracking fund flows

Investigation Steps:

1. Confirm source transaction
2. Click on destination address
3. View subsequent transactions
4. Follow the chain of transfers
5. Document path with transaction hashes

Privacy Techniques to Recognize:

- Mixers/Tumblers (e.g., Tornado Cash)
- CoinJoin transactions
- Exchange deposits (off-chain after deposit)

Lab Deliverables

Submit the following:

1. **Transaction Analysis Report (2-3 pages):**
   - Bitcoin transaction: hash, inputs/outputs, fee
   - Ethereum transaction: hash, gas breakdown
   - Three addresses with entity type identification
2. **Screenshots:**
   - Bitcoin and Ethereum transaction details
   - Block details page
   - Address activity page

Submission Deadline: One week from lab session

Problem Solved? Block Explorers

The Original Problem

How do users verify blockchain data without running expensive infrastructure?

How Block Explorers Solve It

- Run full nodes and index all historical data for instant queries
- Translate raw blockchain data into human-readable formats (addresses, timestamps, gas)
- Provide free public APIs for programmatic access

Remaining Limitations

- Centralization risk: Users trust explorer's data presentation (could censor or manipulate)
- Privacy loss: IP addresses linked to address lookups

Open Questions

- How do explorers monetize while keeping data access free? (Ads, premium APIs, analytics tools)
- Risk: Centralized explorers could be pressured to comply with government censorship

Block explorers enable transparency at the cost of introducing new trust assumptions

Key Takeaways

- Block explorers provide transparency into all blockchain activity
- Bitcoin uses UTXO model; Ethereum uses account model
- Gas fees vary based on network congestion
- Addresses can be identified by transaction patterns
- Blockchain forensics is powerful but faces privacy challenges
- Verified smart contracts allow code auditing

Real-World Applications:

- Auditing and compliance
- Fraud investigation
- Market analysis (whale watching)

Quiz Questions 1-5

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable interfaces to query and view blockchain data.

Q2. On Etherscan, what does the "Gas Used" field represent?
A) Maximum gas limit B) Gas price in gwei C) Actual gas consumed D) Total transaction value
Answer: C – Gas Used shows the actual computational resources consumed by the transaction.

Q3. How is the transaction fee calculated on Ethereum?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Block size $\times$ Fee rate D) Value transferred $\times$ 1%
Answer: B – Transaction fee = Gas Used $\times$ Gas Price (measured in wei/gwei).

Q4. What information can you find in a Bitcoin transaction's input field?
A) Destination address B) Reference to previous UTXO C) Transaction fee D) Block timestamp
Answer: B – Bitcoin inputs reference previous transaction outputs (UTXOs) being spent.

Q5. Which block explorer is most commonly used for Ethereum?
A) Blockstream.info B) Blockchain.com C) Etherscan.io D) Mempool.space
Answer: C – Etherscan.io is the dominant block explorer for Ethereum network.

Quiz Questions 6-10

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) Low fee C) High security/finality D) Large value transfer
Answer: C – More confirmations = more blocks built on top = higher security and finality.

Q7. On a block explorer, what distinguishes a smart contract address from a regular wallet?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions
Answer: B – Contract addresses display a "Contract" label and have associated bytecode.

Q8. How is the Bitcoin transaction fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum minus output sum D) Gas price $\times$ gas used
Answer: C – Bitcoin fee = total inputs - total outputs (the difference goes to miners).

Q9. What does "Internal Transactions" tab on Etherscan show?
A) Failed transactions B) Contract-to-contract calls C) Pending transactions D) Gas refunds
Answer: B – Internal transactions show ETH transfers triggered by smart contract execution.

Q10. Which address type typically shows the highest transaction volume?
A) Individual users B) Smart contracts C) Exchange hot wallets D) Mining pools
Answer: C – Exchange hot wallets handle deposits/withdrawals, resulting in very high volume.

Quiz Questions 11-15

Q11. What information is displayed in the "Block" section of a transaction?
A) Transaction hash only B) Block height, timestamp, miner C) Gas price D) Sender address
Answer: B – Block section shows block number, timestamp, validator/miner, and other block-level data.

Q12. What does "Nonce" represent in an Ethereum transaction?
A) Random number B) Gas price C) Transaction sequence number D) Block difficulty
Answer: C – Nonce is the transaction count from the sender's address, ensuring correct ordering.

Q13. On Etherscan, what does a green checkmark next to "Contract" indicate?
A) High balance B) Verified source code C) Active contract D) Low gas usage
Answer: B – Green checkmark means the contract's source code has been verified and published.

Q14. What is the typical gas limit for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas (protocol minimum).

Q15. Which privacy technique makes transaction tracing difficult?
A) Higher gas fees B) Multiple confirmations C) Mixers/CoinJoin D) Verified contracts
Answer: C – Mixers (e.g., Tornado Cash) and CoinJoin break the on-chain transaction trail.

Quiz Questions 16-20

Q16. What does "Txn Type: 2 (EIP-1559)" indicate on Etherscan?
A) Failed transaction B) Token transfer C) Modern fee market transaction D) Contract creation
Answer: C – Type 2 transactions use EIP-1559 fee market with base fee + priority fee.

Q17. How can you identify if a transaction failed on Etherscan?
A) High gas price B) Red "Fail" status badge C) Zero confirmations D) No input data
Answer: B – Failed transactions show a red badge with "Fail" or error message.

Q18. What does the "Read Contract" tab allow you to do?
A) Modify contract state B) View function outputs without gas C) Deploy new contracts D) Send transactions
Answer: B – "Read Contract" calls view functions that don't modify state or cost gas.

Q19. On Bitcoin block explorers, what is a UTXO?
A) Transaction fee B) Unspent Transaction Output C) Validated block D) Mining reward
Answer: B – UTXO = Unspent Transaction Output, the fundamental unit in Bitcoin's model.

Q20. What can you learn from an address's "Token Holdings" tab on Etherscan?
A) ETH balance only B) Gas usage history C) ERC-20/ERC-721 tokens owned D) Mining rewards
Answer: C – Token Holdings shows all ERC-20, ERC-721, and ERC-1155 tokens held by the address.

Lab Session: Block Explorer Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module A: Blockchain Foundations

(c) Joerg Osterrieder 2025

Where did my transaction go?

[COMIC: A person frantically searching through a maze of hexadecimal strings and block numbers, while another person calmly points at Etherscan on their laptop saying "Just paste the tx hash here"]

The Transparency Window

- Blockchain = public ledger, but raw data is incomprehensible
- Block explorers: human-readable interfaces to on-chain data
- Track any transaction, verify any balance, audit any contract
- Today: you become a blockchain detective

Every Bitcoin and Ethereum transaction ever made is publicly viewable

Learning Objectives

By the end of this lab session, you will be able to:

- Navigate Etherscan and Blockstream block explorers
- Analyze transaction details: inputs, outputs, fees
- Trace transaction lifecycle from broadcast to confirmation
- Examine block structure and validator information
- Investigate address activity and transaction history
- Conduct basic blockchain forensic analysis

Building on L11: Scalability Trilemma

The Problem: Hands-on Blockchain Analysis

The Challenge
How do users verify blockchain transactions without running a full node? Raw blockchain data is complex (hex addresses, gas units, block headers) and requires specialized infrastructure to query and interpret.

Why It Matters

- Without accessible data tools, users must trust centralized exchanges to report balances
- Investigative journalists and auditors need transparent access to on-chain activity

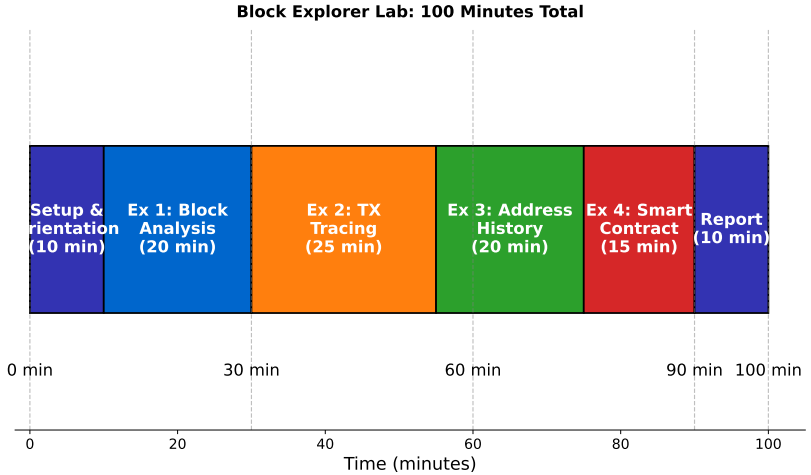
What We Need

- Trustless verification mechanism
- Human-readable interfaces to blockchain data without running costly infrastructure

The Cryptoeconomics Question
How do block explorers enable transparency while remaining economically sustainable?

Today's lesson: How block explorers solve the blockchain data accessibility challenge

How Is This Lab Session Structured?



Total duration: 100 minutes with 4 main exercises

What is a Block Explorer?

Definition:

- Web-based interface to query blockchain data
- Provides human-readable view of blocks, transactions, addresses
- Free and publicly accessible

Major Block Explorers:

Bitcoin:

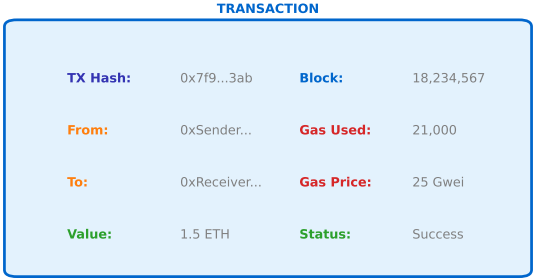
- Blockstream.info
- Blockchain.com
- Mempool.space

Ethereum:

- Etherscan.io
- Blockscout.com
- Ethplorer.io

What Are the Essential Components of a Transaction?

Transaction Anatomy: Key Fields to Analyze



Understanding these fields is essential for analyzing any blockchain transaction

Exercise 1: Analyzing Bitcoin Transactions

Instructions:

1. Visit: `https://blockstream.info`
2. Search for the first-ever Bitcoin transaction:
   `f4184fc596403b9d638783cf57adfe4c75c605f6356fbc91338530e9831e9e16`
3. Examine: inputs, outputs, fee, block number, confirmations

Key Observations:

- **Inputs:** Reference to previous transaction output
- **Outputs:** New UTXOs with amounts and addresses
- **Fee:** Difference between input sum and output sum
- **Confirmations:** Blocks built on top of this transaction

Exercise 2: Analyzing Ethereum Transactions

Instructions:

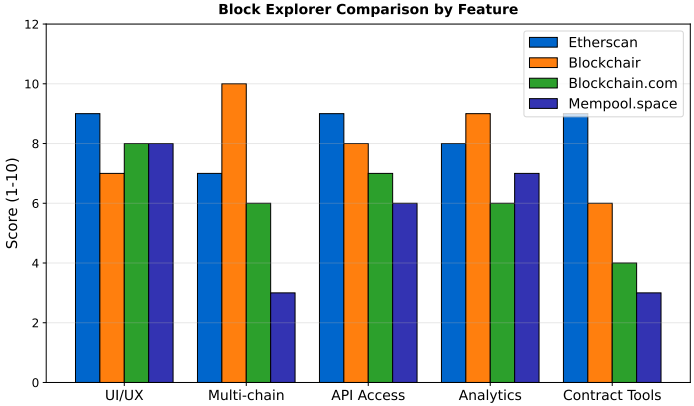
1. Visit: `https://etherscan.io`
2. Select a recent transaction from homepage
3. Examine: hash, status, block, from, to, value, gas

Gas Mechanics:

- Gas Limit: Maximum gas user willing to pay
- Gas Used: Actual gas consumed
- Gas Price: Price per unit (in gwei)
- Transaction Fee: Gas Used $\times$ Gas Price

Example: 21,000 gas $\times$ 32 gwei $=$ 0.000672 ETH

How Do Block Explorers Differ Across Platforms?



Etherscan excels for Ethereum; Blockchair for multi-chain research

Exercise 3: Address Investigation

Entity Types to Analyze:

1. **Exchange Address:** High volume, large balances, labeled
2. **Smart Contract:** "Contract" label, receives interactions
3. **Individual User:** Low volume, smaller balances

Sample Addresses:

- Binance: `0x28C6c06298d514Db089934071355E5743bf21d60`
- Uniswap: `0xE592427A0AEce92De3Edee1F18E0157C05861564`
- Your MetaMask address (from Lab 8)

Exercise 4: Forensic Case Study

Scenario: Tracking fund flows

Investigation Steps:

1. Confirm source transaction
2. Click on destination address
3. View subsequent transactions
4. Follow the chain of transfers
5. Document path with transaction hashes

Privacy Techniques to Recognize:

- Mixers/Tumblers (e.g., Tornado Cash)
- CoinJoin transactions
- Exchange deposits (off-chain after deposit)

Lab Deliverables

Submit the following:

1. **Transaction Analysis Report (2-3 pages):**
   - Bitcoin transaction: hash, inputs/outputs, fee
   - Ethereum transaction: hash, gas breakdown
   - Three addresses with entity type identification
2. **Screenshots:**
   - Bitcoin and Ethereum transaction details
   - Block details page
   - Address activity page

Submission Deadline: One week from lab session

Problem Solved? Block Explorers

The Original Problem

How do users verify blockchain data without running expensive infrastructure?

How Block Explorers Solve It

- Run full nodes and index all historical data for instant queries
- Translate raw blockchain data into human-readable formats (addresses, timestamps, gas)
- Provide free public APIs for programmatic access

Remaining Limitations

- Centralization risk: Users trust explorer's data presentation (could censor or manipulate)
- Privacy loss: IP addresses linked to address lookups

Open Questions

- How do explorers monetize while keeping data access free? (Ads, premium APIs, analytics tools)
- Risk: Centralized explorers could be pressured to comply with government censorship

Block explorers enable transparency at the cost of introducing new trust assumptions

The Economics of Block Explorers

Incentive Structure

- **Core Problem:** Coordinating without trusted intermediaries
- **Why act honestly?** Participants verify rather than trust
- **Value Flow:** Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Block Explorers

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Block Explorers

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Why Do Some Transactions Confirm Faster Than Others?

[COMIC: A crowded hospital waiting room labeled "Mempool," with transactions sitting in chairs holding numbered tickets. A rich transaction in a suit (high gas) gets called immediately, while low-fee transactions have been waiting for hours with cobwebs forming]

Transaction Priority Economics

- Mempool: unconfirmed transactions waiting for block inclusion
- Higher fee = higher priority = faster confirmation
- During congestion: low-fee txs can wait hours or get dropped
- Pro tip: check mempool.space before setting gas prices

During NFT mints, gas fees can spike 100x in minutes—watch the mempool

Key Takeaways

- Block explorers provide transparency into all blockchain activity
- Bitcoin uses UTXO model; Ethereum uses account model
- Gas fees vary based on network congestion
- Addresses can be identified by transaction patterns
- Blockchain forensics is powerful but faces privacy challenges
- Verified smart contracts allow code auditing

Real-World Applications:

- Auditing and compliance
- Fraud investigation
- Market analysis (whale watching)

Next Lesson: L13 – Ethereum Architecture

Quiz Questions 1-5

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable interfaces to query and view blockchain data.

Q2. On Etherscan, what does the "Gas Used" field represent?
A) Maximum gas limit B) Gas price in gwei C) Actual gas consumed D) Total transaction value
Answer: C – Gas Used shows the actual computational resources consumed by the transaction.

Q3. How is the transaction fee calculated on Ethereum?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Block size $\times$ Fee rate D) Value transferred $\times$ 1%
Answer: B – Transaction fee = Gas Used $\times$ Gas Price (measured in wei/gwei).

Q4. What information can you find in a Bitcoin transaction's input field?
A) Destination address B) Reference to previous UTXO C) Transaction fee D) Block timestamp
Answer: B – Bitcoin inputs reference previous transaction outputs (UTXOs) being spent.

Q5. Which block explorer is most commonly used for Ethereum?
A) Blockstream.info B) Blockchain.com C) Etherscan.io D) Mempool.space
Answer: C – Etherscan.io is the dominant block explorer for Ethereum network.

Quiz Questions 6-10

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) Low fee C) High security/finality D) Large value transfer
Answer: C – More confirmations = more blocks built on top = higher security and finality.

Q7. On a block explorer, what distinguishes a smart contract address from a regular wallet?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions
Answer: B – Contract addresses display a "Contract" label and have associated bytecode.

Q8. How is the Bitcoin transaction fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum minus output sum D) Gas price $\times$ gas used
Answer: C – Bitcoin fee = total inputs - total outputs (the difference goes to miners).

Q9. What does "Internal Transactions" tab on Etherscan show?
A) Failed transactions B) Contract-to-contract calls C) Pending transactions D) Gas refunds
Answer: B – Internal transactions show ETH transfers triggered by smart contract execution.

Q10. Which address type typically shows the highest transaction volume?
A) Individual users B) Smart contracts C) Exchange hot wallets D) Mining pools
Answer: C – Exchange hot wallets handle deposits/withdrawals, resulting in very high volume.

Quiz Questions 11-15

Q11. What information is displayed in the "Block" section of a transaction?
A) Transaction hash only B) Block height, timestamp, miner C) Gas price D) Sender address
Answer: B – Block section shows block number, timestamp, validator/miner, and other block-level data.

Q12. What does "Nonce" represent in an Ethereum transaction?
A) Random number B) Gas price C) Transaction sequence number D) Block difficulty
Answer: C – Nonce is the transaction count from the sender's address, ensuring correct ordering.

Q13. On Etherscan, what does a green checkmark next to "Contract" indicate?
A) High balance B) Verified source code C) Active contract D) Low gas usage
Answer: B – Green checkmark means the contract's source code has been verified and published.

Q14. What is the typical gas limit for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas (protocol minimum).

Q15. Which privacy technique makes transaction tracing difficult?
A) Higher gas fees B) Multiple confirmations C) Mixers/CoinJoin D) Verified contracts
Answer: C – Mixers (e.g., Tornado Cash) and CoinJoin break the on-chain transaction trail.

Quiz Questions 16-20

Q16. What does "Txn Type: 2 (EIP-1559)" indicate on Etherscan?
A) Failed transaction B) Token transfer C) Modern fee market transaction D) Contract creation
Answer: C – Type 2 transactions use EIP-1559 fee market with base fee + priority fee.

Q17. How can you identify if a transaction failed on Etherscan?
A) High gas price B) Red "Fail" status badge C) Zero confirmations D) No input data
Answer: B – Failed transactions show a red badge with "Fail" or error message.

Q18. What does the "Read Contract" tab allow you to do?
A) Modify contract state B) View function outputs without gas C) Deploy new contracts D) Send transactions
Answer: B – "Read Contract" calls view functions that don't modify state or cost gas.

Q19. On Bitcoin block explorers, what is a UTXO?
A) Transaction fee B) Unspent Transaction Output C) Validated block D) Mining reward
Answer: B – UTXO = Unspent Transaction Output, the fundamental unit in Bitcoin's model.

Q20. What can you learn from an address's "Token Holdings" tab on Etherscan?
A) ETH balance only B) Gas usage history C) ERC-20/ERC-721 tokens owned D) Mining rewards
Answer: C – Token Holdings shows all ERC-20, ERC-721, and ERC-1155 tokens held by the address.

L12: Lab – Block Explorer Analysis

Mini-Lecture – Module A: Blockchain Foundations

Blockchain & Cryptocurrency Course

January 2026

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Navigate Etherscan and Blockstream block explorers
- Analyze transaction details: inputs, outputs, fees, gas
- Trace transaction lifecycle from broadcast to confirmation
- Conduct basic blockchain forensic analysis

What is a Block Explorer?

Definition: Web-based interface to query blockchain data

- Provides human-readable view of blocks, transactions, addresses
- Free and publicly accessible
- Essential tool for blockchain transparency

Major Explorers:

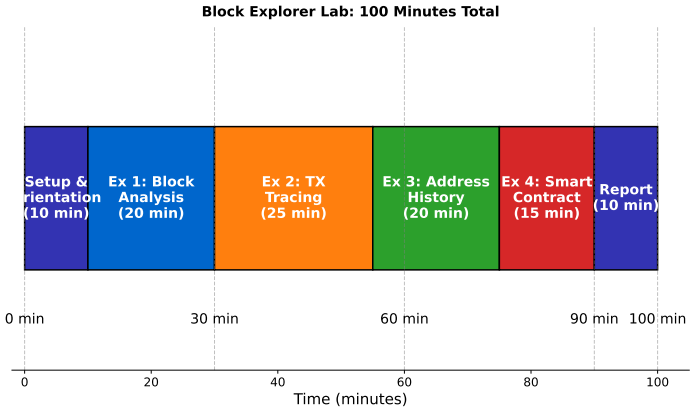
Bitcoin:

- Blockstream.info
- Mempool.space

Ethereum:

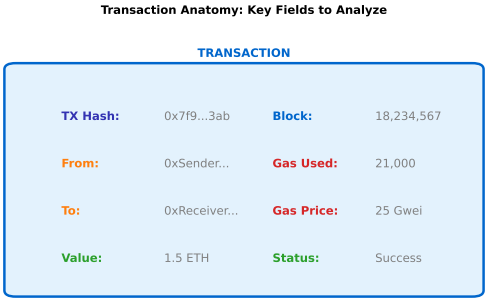
- Etherscan.io
- Blockscout.com

Lab Session Structure



Focus: Transaction analysis, address investigation, basic forensics.

Transaction Anatomy



Key Fields: Hash, status, block, from, to, value, gas used, fee.

Bitcoin vs Ethereum Transactions

Bitcoin (UTXO Model):

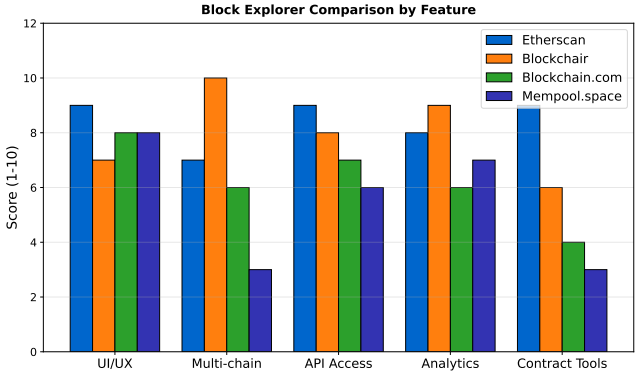
- Inputs: Reference to previous transaction outputs
- Outputs: New UTXOs with amounts and addresses
- Fee = Sum of inputs - Sum of outputs

Ethereum (Account Model):

- From/To: Account addresses
- Gas Limit: Maximum gas willing to pay
- Gas Used: Actual gas consumed
- Fee = Gas Used $\times$ Gas Price (in gwei)

Example: 21,000 gas $\times$ 32 gwei = 0.000672 ETH

Block Explorer Comparison



Etherscan: Best for Ethereum — **Blockchair:** Multi-chain research

Address Investigation

Entity Types:

1. **Exchange:** High volume, large balances, labeled (e.g., "Binance")
2. **Smart Contract:** "Contract" label, receives interactions
3. **Individual:** Low volume, smaller balances, unlabeled

Key Indicators:

- Transaction frequency and volume
- Token holdings (ERC-20, ERC-721)
- Contract verification status (green checkmark)

Fund Tracing Steps:

1. Confirm source transaction
2. Click destination address
3. View subsequent transactions
4. Follow the chain of transfers
5. Document path with transaction hashes

Privacy Techniques to Recognize:

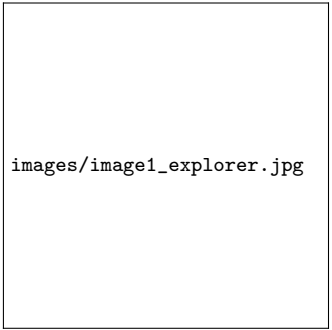
- Mixers/Tumblers (e.g., Tornado Cash – sanctioned)
- CoinJoin transactions
- Exchange deposits (funds go off-chain)

Key Takeaways

1. **Transparency:** Block explorers provide public audit of all activity
2. **Two Models:** Bitcoin uses UTXO; Ethereum uses account model
3. **Gas Fees:** Ethereum fees = Gas Used $\times$ Gas Price
4. **Confirmations:** More confirmations = higher security/finality
5. **Forensics:** Transaction tracing possible but privacy tools exist

Real-World Use: Auditing, fraud investigation, whale watching.

Block Explorer Analysis in Practice



Block Explorer

Transaction View

Forensic Analysis

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the primary purpose of a block explorer?
A) Mining blocks B) Querying blockchain data C) Creating wallets D) Validating transactions

Quiz (1/2)

Q1. What is the primary purpose of a block explorer?
A) Mining blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable blockchain queries.

Q2. How is Ethereum transaction fee calculated?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Value $\times$ 1% D) Block size

Quiz (1/2)

Q1. What is the primary purpose of a block explorer?
A) Mining blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable blockchain queries.

Q2. How is Ethereum transaction fee calculated?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Value $\times$ 1% D) Block size
Answer: B – Fee = Gas Used $\times$ Gas Price (in wei/gwei).

Q3. What is standard gas for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000

Quiz (1/2)

Q1. What is the primary purpose of a block explorer?
A) Mining blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable blockchain queries.

Q2. How is Ethereum transaction fee calculated?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Value $\times$ 1% D) Block size
Answer: B – Fee = Gas Used $\times$ Gas Price (in wei/gwei).

Q3. What is standard gas for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas.

Q4. What does high confirmation count indicate?
A) Fast transaction B) Low fee C) High security/finality D) Large value

Quiz (1/2)

Q1. What is the primary purpose of a block explorer?
A) Mining blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable blockchain queries.

Q2. How is Ethereum transaction fee calculated?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Value $\times$ 1% D) Block size
Answer: B – Fee = Gas Used $\times$ Gas Price (in wei/gwei).

Q3. What is standard gas for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas.

Q4. What does high confirmation count indicate?
A) Fast transaction B) Low fee C) High security/finality D) Large value
Answer: C – More confirmations = more blocks on top = more secure.

Q5. Which explorer is best for Ethereum?
A) Blockstream B) Mempool.space C) Etherscan D) Blockchain.com

Quiz (1/2)

Q1. What is the primary purpose of a block explorer?
A) Mining blocks B) Querying blockchain data C) Creating wallets D) Validating transactions
Answer: B – Block explorers provide human-readable blockchain queries.

Q2. How is Ethereum transaction fee calculated?
A) Fixed 0.01 ETH B) Gas Used $\times$ Gas Price C) Value $\times$ 1% D) Block size
Answer: B – Fee = Gas Used $\times$ Gas Price (in wei/gwei).

Q3. What is standard gas for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas.

Q4. What does high confirmation count indicate?
A) Fast transaction B) Low fee C) High security/finality D) Large value
Answer: C – More confirmations = more blocks on top = more secure.

Q5. Which explorer is best for Ethereum?
A) Blockstream B) Mempool.space C) Etherscan D) Blockchain.com
Answer: C – Etherscan.io is the dominant Ethereum explorer.

Quiz (2/2)

Q6. How is Bitcoin fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Gas $\times$ Price

Quiz (2/2)

Q6. How is Bitcoin fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Gas $\times$ Price
Answer: C – Bitcoin fee = total inputs - total outputs.

Q7. What does "Contract" label on Etherscan indicate?
A) Exchange address B) Smart contract address C) Whale wallet D) Mining pool

Quiz (2/2)

Q6. How is Bitcoin fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Gas $\times$ Price
Answer: C – Bitcoin fee = total inputs - total outputs.

Q7. What does "Contract" label on Etherscan indicate?
A) Exchange address B) Smart contract address C) Whale wallet D) Mining pool
Answer: B – Contract addresses have bytecode and "Contract" label.

Q8. What is a UTXO?
A) Transaction fee B) Unspent Transaction Output C) Validated block D) Gas unit

Quiz (2/2)

Q6. How is Bitcoin fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Gas $\times$ Price
Answer: C – Bitcoin fee = total inputs - total outputs.

Q7. What does "Contract" label on Etherscan indicate?
A) Exchange address B) Smart contract address C) Whale wallet D) Mining pool
Answer: B – Contract addresses have bytecode and "Contract" label.

Q8. What is a UTXO?
A) Transaction fee B) Unspent Transaction Output C) Validated block D) Gas unit
Answer: B – UTXO = Unspent Transaction Output (Bitcoin model).

Q9. What does green checkmark on contract indicate?
A) High balance B) Verified source code C) Active status D) Low gas

Quiz (2/2)

Q6. How is Bitcoin fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Gas $\times$ Price
Answer: C – Bitcoin fee = total inputs - total outputs.

Q7. What does "Contract" label on Etherscan indicate?
A) Exchange address B) Smart contract address C) Whale wallet D) Mining pool
Answer: B – Contract addresses have bytecode and "Contract" label.

Q8. What is a UTXO?
A) Transaction fee B) Unspent Transaction Output C) Validated block D) Gas unit
Answer: B – UTXO = Unspent Transaction Output (Bitcoin model).

Q9. What does green checkmark on contract indicate?
A) High balance B) Verified source code C) Active status D) Low gas
Answer: B – Green checkmark means verified, auditable source code.

Q10. Which technique makes transaction tracing difficult?
A) Higher gas B) More confirmations C) Mixers/CoinJoin D) Verified contracts

Quiz (2/2)

Q6. How is Bitcoin fee determined?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Gas $\times$ Price
Answer: C – Bitcoin fee = total inputs - total outputs.

Q7. What does "Contract" label on Etherscan indicate?
A) Exchange address B) Smart contract address C) Whale wallet D) Mining pool
Answer: B – Contract addresses have bytecode and "Contract" label.

Q8. What is a UTXO?
A) Transaction fee B) Unspent Transaction Output C) Validated block D) Gas unit
Answer: B – UTXO = Unspent Transaction Output (Bitcoin model).

Q9. What does green checkmark on contract indicate?
A) High balance B) Verified source code C) Active status D) Low gas
Answer: B – Green checkmark means verified, auditable source code.

Q10. Which technique makes transaction tracing difficult?
A) Higher gas B) More confirmations C) Mixers/CoinJoin D) Verified contracts
Answer: C – Mixers and CoinJoin break the on-chain transaction trail.

Thank you

Questions?

Next: L13 – Ethereum Architecture

Quiz: Lab Block Explorer

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating nodes

Quiz (1–5)

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating nodes
Answer: B – Block explorers query and display blockchain data in human-readable format.

Q2. How is the Bitcoin transaction fee calculated?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Block size

Quiz (1–5)

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating nodes
Answer: B – Block explorers query and display blockchain data in human-readable format.

Q2. How is the Bitcoin transaction fee calculated?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Block size
Answer: C – Fee equals total inputs minus total outputs; difference goes to miners.

Q3. What is the typical gas limit for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000

Quiz (1–5)

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating nodes
Answer: B – Block explorers query and display blockchain data in human-readable format.

Q2. How is the Bitcoin transaction fee calculated?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Block size
Answer: C – Fee equals total inputs minus total outputs; difference goes to miners.

Q3. What is the typical gas limit for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas (protocol minimum).

Q4. What does a green checkmark next to "Contract" on Etherscan indicate?
A) High balance B) Verified source code C) Active contract D) Low gas usage

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating nodes
Answer: B – Block explorers query and display blockchain data in human-readable format.

Q2. How is the Bitcoin transaction fee calculated?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Block size
Answer: C – Fee equals total inputs minus total outputs; difference goes to miners.

Q3. What is the typical gas limit for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas (protocol minimum).

Q4. What does a green checkmark next to "Contract" on Etherscan indicate?
A) High balance B) Verified source code C) Active contract D) Low gas usage
Answer: B – Green checkmark means source code is verified and publicly readable.

Q5. Which address type typically shows the highest transaction volume?
A) Individual users B) Smart contracts C) Exchange hot wallets D) Mining pools

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of a blockchain block explorer?
A) Mining new blocks B) Querying blockchain data C) Creating wallets D) Validating nodes
Answer: B – Block explorers query and display blockchain data in human-readable format.

Q2. How is the Bitcoin transaction fee calculated?
A) Fixed by protocol B) Percentage of value C) Input sum - Output sum D) Block size
Answer: C – Fee equals total inputs minus total outputs; difference goes to miners.

Q3. What is the typical gas limit for a simple ETH transfer?
A) 10,000 B) 21,000 C) 50,000 D) 100,000
Answer: B – Simple ETH transfers require exactly 21,000 gas (protocol minimum).

Q4. What does a green checkmark next to "Contract" on Etherscan indicate?
A) High balance B) Verified source code C) Active contract D) Low gas usage
Answer: B – Green checkmark means source code is verified and publicly readable.

Q5. Which address type typically shows the highest transaction volume?
A) Individual users B) Smart contracts C) Exchange hot wallets D) Mining pools
Answer: C – Exchange hot wallets process deposits/withdrawals constantly.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) High security/finality C) Large value transfer D) Low fees

Quiz (6–10)

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) High security/finality C) Large value transfer D) Low fees
Answer: B – More confirmations = more blocks built on top = higher security.

Q7. What distinguishes a smart contract address from a wallet on Etherscan?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions

Quiz (6–10)

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) High security/finality C) Large value transfer D) Low fees
Answer: B – More confirmations = more blocks built on top = higher security.

Q7. What distinguishes a smart contract address from a wallet on Etherscan?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions
Answer: B – Contract addresses display a "Contract" label and associated bytecode.

Q8. What is a UTXO in Bitcoin?
A) Transaction fee B) Unspent Transaction Output C) Mining reward D) Block hash

Quiz (6–10)

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) High security/finality C) Large value transfer D) Low fees
Answer: B – More confirmations = more blocks built on top = higher security.

Q7. What distinguishes a smart contract address from a wallet on Etherscan?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions
Answer: B – Contract addresses display a "Contract" label and associated bytecode.

Q8. What is a UTXO in Bitcoin?
A) Transaction fee B) Unspent Transaction Output C) Mining reward D) Block hash
Answer: B – UTXO = Unspent Transaction Output, Bitcoin's fundamental accounting unit.

Q9. Which privacy technique makes transaction tracing difficult?
A) Higher gas fees B) Multiple confirmations C) Mixers/CoinJoin D) Verified contracts

Quiz (6–10)

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) High security/finality C) Large value transfer D) Low fees
Answer: B – More confirmations = more blocks built on top = higher security.

Q7. What distinguishes a smart contract address from a wallet on Etherscan?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions
Answer: B – Contract addresses display a "Contract" label and associated bytecode.

Q8. What is a UTXO in Bitcoin?
A) Transaction fee B) Unspent Transaction Output C) Mining reward D) Block hash
Answer: B – UTXO = Unspent Transaction Output, Bitcoin's fundamental accounting unit.

Q9. Which privacy technique makes transaction tracing difficult?
A) Higher gas fees B) Multiple confirmations C) Mixers/CoinJoin D) Verified contracts
Answer: C – Mixers and CoinJoin break the on-chain transaction trail.

Q10. What does "Nonce" represent in an Ethereum transaction?
A) Random number B) Gas price C) Transaction sequence number D) Block difficulty

Quiz (6–10)

Q6. What does a high number of confirmations indicate?
A) Fast transaction B) High security/finality C) Large value transfer D) Low fees
Answer: B – More confirmations = more blocks built on top = higher security.

Q7. What distinguishes a smart contract address from a wallet on Etherscan?
A) Higher balance B) "Contract" label and bytecode C) Longer address D) More transactions
Answer: B – Contract addresses display a "Contract" label and associated bytecode.

Q8. What is a UTXO in Bitcoin?
A) Transaction fee B) Unspent Transaction Output C) Mining reward D) Block hash
Answer: B – UTXO = Unspent Transaction Output, Bitcoin's fundamental accounting unit.

Q9. Which privacy technique makes transaction tracing difficult?
A) Higher gas fees B) Multiple confirmations C) Mixers/CoinJoin D) Verified contracts
Answer: C – Mixers and CoinJoin break the on-chain transaction trail.

Q10. What does "Nonce" represent in an Ethereum transaction?
A) Random number B) Gas price C) Transaction sequence number D) Block difficulty
Answer: C – Nonce is the sender's transaction count, ensuring correct ordering.

(c) Joerg Osterrieder 2025

L13: Ethereum Architecture

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the Ethereum Virtual Machine (EVM) architecture
- Distinguish between Externally Owned Accounts (EOA) and Contract Accounts
- Describe Ethereum as a state machine and explain the world state concept
- Explain the Merkle Patricia Trie data structure
- Compare Ethereum's account model to Bitcoin's UTXO model

The Problem: How do we make money programmable?

The Challenge
How do we create a blockchain system that can execute arbitrary code with value at stake, where code execution is deterministic and verifiable across all nodes?

Why It Matters

- Bitcoin's scripting language only allows simple operations (send, verify signatures)
- Complex financial logic (lending, options, DAOs) requires Turing-complete computation
- Vitalik's 2013 whitepaper proposed "world computer"; Ethereum launched 2015; The DAO hack 2016 revealed execution risks

What We Need

- System design principles
- A virtual machine where all nodes execute code identically and reach consensus on state changes

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How Ethereum Architecture addresses this challenge

What is Ethereum?

Key Characteristics:

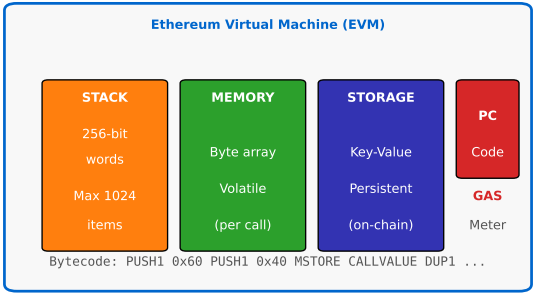
- Decentralized computation platform
- Turing-complete blockchain
- Smart contract support
- Native cryptocurrency: Ether (ETH)
- Launched July 30, 2015

Beyond Bitcoin:

- Bitcoin: Digital gold, value transfer
- Ethereum: World computer, programmable logic
- Enables decentralized applications (dApps)
- Foundation for DeFi, NFTs, DAOs

Ethereum Virtual Machine (EVM)

EVM: Stack-Based Virtual Machine



Deterministic | Isolated | Gas-metered | 256-bit word size

The EVM is a quasi-Turing complete, stack-based virtual machine with gas metering.

EVM: Technical Details

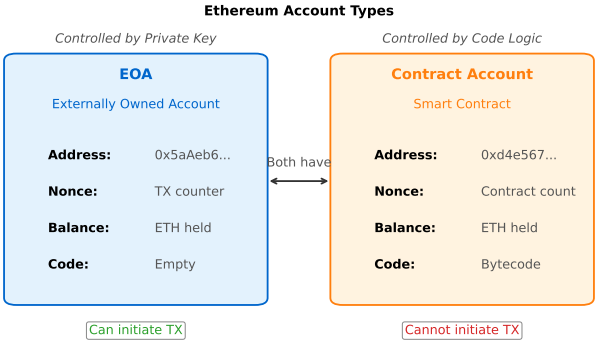
The EVM is a quasi-Turing complete state machine:

- Stack-based virtual machine (256-bit word size)
- Executes bytecode compiled from Solidity, Vyper
- Deterministic: same input always produces same output
- Gas metering prevents infinite loops
- Isolated: no network, filesystem, or process access

EVM Components:

- **Stack:** LIFO, max 1024 items, 256-bit each
- **Memory:** Byte array, volatile (per call), linear cost
- **Storage:** Key-value, persistent (on-chain), expensive
- **Program Counter:** Current bytecode position
- **Gas Counter:** Remaining computation budget

Account Types: EOA vs Contract



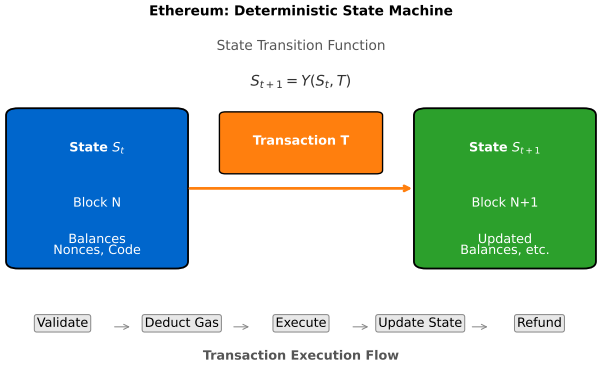
EOAs are controlled by private keys; contracts are controlled by code.

Account State Components

Every account (EOA or Contract) has four fields:

1. **Nonce:**
   - EOA: Counter of transactions sent
   - Contract: Counter of contracts created
   - Prevents replay attacks
2. **Balance:**
   - Amount of Wei (10^{-18} ETH) owned
   - 1 ETH = 1,000,000,000,000,000,000 Wei
3. **StorageRoot:**
   - Hash of account's storage trie root
   - Empty for EOAs
4. **CodeHash:**
   - Hash of EVM bytecode
   - Empty for EOAs, immutable for contracts

Ethereum as a State Machine



State transitions are deterministic: given S_t and T, S_{t+1} is uniquely determined.

World State

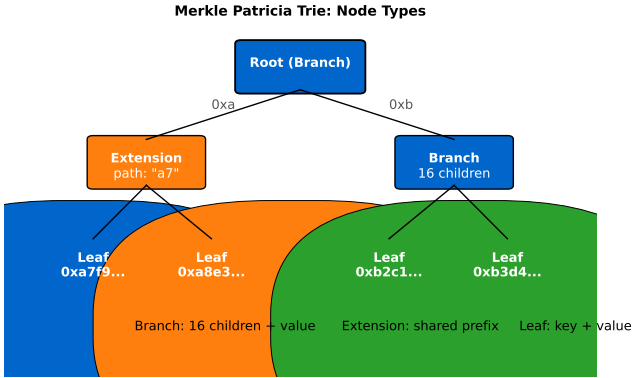
The World State is a mapping between addresses and account states:

- Maps 160-bit addresses to account states
- Stored as a Merkle Patricia Trie
- Root hash included in every block header
- Allows efficient verification of account state
- Enables light clients to verify data without full state

State Root:

- 256-bit hash representing entire world state
- Changes with every block
- Uniquely identifies state at a specific block height

Merkle Patricia Trie (MPT)



MPT combines Merkle verification, Patricia path compression, and radix optimization.

MPT Properties

Combines three data structures:

1. **Merkle Tree:** Cryptographic verification via hashes
2. **Patricia Trie:** Efficient key-value storage with shared prefixes
3. **Radix Trie:** Optimized path compression

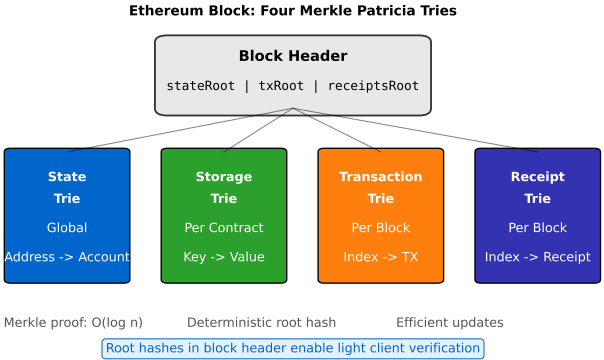
Key Properties:

- Deterministic: Same key-value pairs $\rightarrow$ same root hash
- Efficient verification: $O(\log n)$ proof size
- Efficient updates: Only modified paths need rehashing

Node Types:

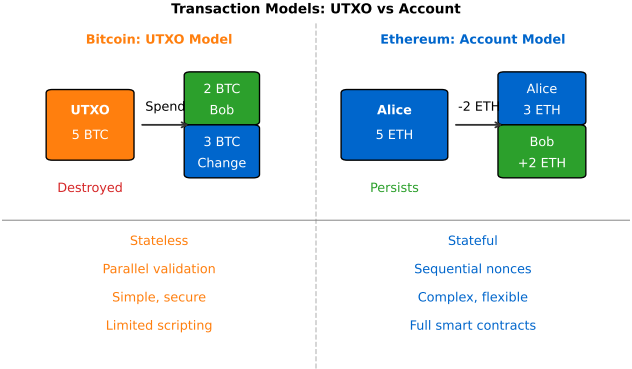
- **Branch:** 16 children (hex 0-F) + optional value
- **Extension:** Shared path prefix + next node pointer
- **Leaf:** Remaining key path + value

Four MPT Tries in Ethereum



Block header contains root hashes of all four tries for verification.

Ethereum vs Bitcoin: Account Model vs UTXO



Account model enables smart contracts but requires nonce tracking.

Account Model: Trade-offs

Advantages:

1. **Simplicity:** Intuitive balance model, easier wallets
2. **Space Efficiency:** No UTXO tracking overhead
3. **Fungibility:** All Ether equivalent, no dust
4. **Smart Contracts:** Natural fit for persistent storage

Challenges:

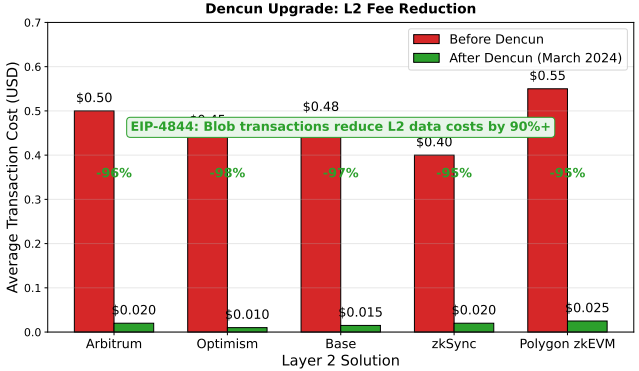
1. **Replay Prevention:** Requires nonce tracking
2. **State Growth:** All accounts stored indefinitely
3. **Privacy:** All activity linked to single address
4. **Parallelization:** Sequential nonces limit parallel validation

Block Structure

Ethereum block header contains:

- **parentHash:** Hash of parent block
- **beneficiary:** Address receiving block reward
- **stateRoot:** Root hash of state trie
- **transactionsRoot:** Root hash of transaction trie
- **receiptsRoot:** Root hash of receipt trie
- **logsBloom:** Bloom filter for efficient log lookup
- **number:** Block height
- **gasLimit / gasUsed:** Gas constraints
- **timestamp:** Unix timestamp
- **extraData:** Arbitrary data (max 32 bytes)

2024 Milestone: Dencun Upgrade



EIP-4844 blob transactions reduce L2 data costs by 90%+.

Dencun: Proto-Danksharding

Major Network Upgrade (March 13, 2024):

- **EIP-4844**: Introduces "blob" transactions for Layer 2 data
- **Problem**: L2 rollups pay expensive calldata for data availability
- **Solution**: New data type (blobs) with separate, cheaper gas market

How Blobs Work:

- Blobs: 128 KB data chunks, stored for $\sim$18 days
- Separate "blob gas" market (independent of execution gas)
- L2s post transaction batches as blobs instead of calldata

Impact:

- L2 transaction fees reduced by 90%+ (\$0.50 $\rightarrow$ \$0.01)
- Arbitrum, Optimism, Base adopted immediately
- Paves way for full Danksharding (future upgrade)

Problem Solved? Ethereum Architecture

The Original Problem

How do we make money programmable?

How Ethereum Architecture Solves It

- **EVM executes bytecode**: All nodes run identical stack-based VM, ensuring deterministic state transitions
- **Account-based model**: Persistent storage (vs UTXO) enables complex contract logic and state management
- **World state + MPT**: Cryptographic verification of all account states at every block

Remaining Limitations

- **Execution costs**: Gas fees make computation expensive; state bloat from permanent storage
- **Single-threaded**: Sequential transaction processing (nonce ordering) limits parallelization and throughput

Open Questions

- How to scale smart contract execution (10,000+ TPS) while maintaining decentralization and security?
- Risk: State growth, MEV exploitation, smart contract bugs with irreversible financial consequences

Ethereum Architecture solves programmable money but introduces scalability and cost trade-offs

Key Takeaways

1. **EVM:** Deterministic, stack-based VM enabling Turing-complete smart contracts
2. **Two Account Types:** EOAs (user-controlled) and Contracts (code-controlled)
3. **State Machine:** Ethereum transitions between states via transactions
4. **World State:** Mapping of addresses to accounts, stored as MPT
5. **MPT:** Efficient cryptographic data structure for state verification
6. **Account Model:** Simpler than UTXO but with privacy/parallelization trade-offs

Discussion Questions

1. Why is the EVM only “quasi”-Turing complete?
2. What security benefits does the nonce provide?
3. How does MPT enable light client verification?
4. When might Bitcoin's UTXO model be preferable?
5. How does state growth affect node operators?

Next Lesson Preview: L14 - Gas Mechanics

Coming up next:

- Understanding gas as a computational unit
- Gas price, gas limit, and transaction cost calculation
- EIP-1559: Base fee and priority fee mechanism
- Gas costs for different EVM operations
- Optimization techniques for reducing gas consumption

Preparation:

- Review basic Ethereum transaction structure
- Familiarize yourself with Wei/Gwei/ETH units
- Browse Etherscan to see gas usage in real transactions

Quiz Questions (1/4)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete" rather than fully Turing complete?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas metering prevents infinite loops, limiting true Turing completeness.

Q3. What is the maximum stack depth in the EVM?
A) 256 items B) 512 items C) 1024 items D) 2048 items
Answer: C – The EVM stack can hold a maximum of 1024 items.

Q4. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither type D) Externally Owned Accounts (EOA)
Answer: D – EOAs are controlled by private keys; contracts are controlled by code.

Q5. How many Wei are in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}
Answer: C – 1 ETH = 1,000,000,000,000,000,000 Wei (10^{18}).

Quiz Questions (2/4)

Q6. What does the nonce field track for an EOA?
A) Balance B) Transaction count sent C) Gas used D) Contract deployments
Answer: B – For EOAs, nonce counts transactions sent to prevent replay attacks.

Q7. Which field is empty for Externally Owned Accounts but populated for Contract Accounts?
A) Nonce B) Balance C) CodeHash D) All fields are populated
Answer: C – EOAs have no code, so CodeHash is empty; contracts store bytecode.

Q8. What data structure is used to store the Ethereum world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – The world state uses a Merkle Patricia Trie for efficient verification.

Q9. How many tries does an Ethereum block header reference?
A) One B) Two C) Three D) Four
Answer: D – State, transaction, receipt, and storage tries (four total).

Q10. What is the state root?
A) First block hash B) 256-bit hash of entire world state C) Genesis state D) Merkle tree root
Answer: B – The state root is a 256-bit hash representing the entire world state.

Quiz Questions (3/4)

Q11. Which node type in MPT has 16 children?
A) Leaf B) Extension C) Branch D) Root
Answer: C – Branch nodes have 16 children (hex 0-F) plus optional value.

Q12. What is the primary advantage of Ethereum's account model over Bitcoin's UTXO model?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state size
Answer: C – Account model is more natural for persistent contract storage.

Q13. What is Ethereum often called to distinguish it from Bitcoin?
A) Digital silver B) World computer C) Smart ledger D) Crypto platform
Answer: B – Ethereum is called a "world computer" for programmable logic.

Q14. When was Ethereum mainnet launched?
A) January 3, 2009 B) July 30, 2015 C) August 1, 2017 D) December 1, 2020
Answer: B – Ethereum launched July 30, 2015 (Bitcoin was 2009).

Q15. Which EVM memory type is persistent and stored on-chain?
A) Stack B) Memory C) Storage D) Cache
Answer: C – Storage is persistent on-chain (expensive); Memory is volatile per call.

Quiz Questions (4/4)

Q16. What does EIP-4844 (Dencun upgrade) introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding
Answer: B – EIP-4844 introduces blob transactions for cheaper L2 data availability.

Q17. By approximately how much did Dencun reduce Layer 2 transaction fees?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – L2 fees dropped 90%+ (e.g., \$0.50 to \$0.01) after Dencun.

Q18. What is the address size in Ethereum?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: B – Ethereum addresses are 160 bits (40 hex characters).

Q19. Which field in the account state prevents replay attacks?
A) Balance B) Nonce C) CodeHash D) StorageRoot
Answer: B – The nonce ensures each transaction is unique and sequential.

Q20. What challenge does Ethereum's account model face compared to UTXO?
A) Complexity B) Privacy limitations C) Higher storage D) No smart contracts
Answer: B – All activity is linked to a single address, reducing privacy vs UTXO.

L13: Ethereum Architecture

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

What Is the World Computer?

[COMIC: Developer announces "I'm building on the world computer!" while sitting at an actual laptop with 8GB RAM and a spinning fan. The Ethereum logo floats above looking majestic while the laptop displays "Low Memory Warning."]

Frame the Concept:

- The "world computer" executes code across thousands of nodes simultaneously
- Yet each node is just an ordinary machine running the same deterministic bytecode

Ethereum: Where your code runs everywhere, but somehow still costs more than AWS

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the Ethereum Virtual Machine (EVM) architecture
- Distinguish between Externally Owned Accounts (EOA) and Contract Accounts
- Describe Ethereum as a state machine and explain the world state concept
- Explain the Merkle Patricia Trie data structure
- Compare Ethereum's account model to Bitcoin's UTXO model

Building on L12: Lab: Block Explorer

The Problem: How do we make money programmable?

The Challenge
How do we create a blockchain system that can execute arbitrary code with value at stake, where code execution is deterministic and verifiable across all nodes?

Why It Matters

- Bitcoin's scripting language only allows simple operations (send, verify signatures)
- Complex financial logic (lending, options, DAOs) requires Turing-complete computation
- Vitalik's 2013 whitepaper proposed "world computer"; Ethereum launched 2015; The DAO hack 2016 revealed execution risks

What We Need

- System design principles
- A virtual machine where all nodes execute code identically and reach consensus on state changes

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How Ethereum Architecture addresses this challenge

How Is Ethereum Different from Bitcoin?

Key Characteristics:

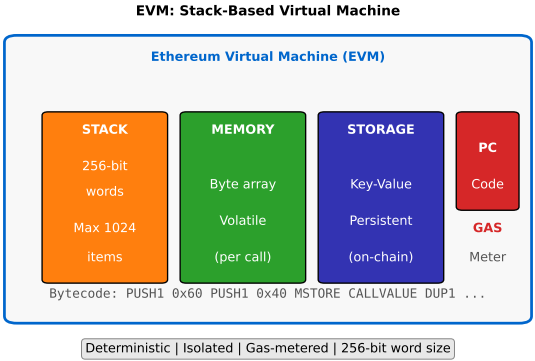
- Decentralized computation platform
- Turing-complete blockchain
- Smart contract support
- Native cryptocurrency: Ether (ETH)
- Launched July 30, 2015

Beyond Bitcoin:

- Bitcoin: Digital gold, value transfer
- Ethereum: World computer, programmable logic
- Enables decentralized applications (dApps)
- Foundation for DeFi, NFTs, DAOs

→ *Problem: How do we make money programmable? — What is Ethereum? Ethereum provides a global computer where code handles value, not just records it*

How Does the EVM Execute Smart Contracts?



The EVM is a quasi-Turing complete (can compute anything, but gas limits prevent infinite loops), stack-based (operations push/pop values from a last-in-first-out stack) virtual machine with gas metering.

What Are the Technical Details of the EVM?

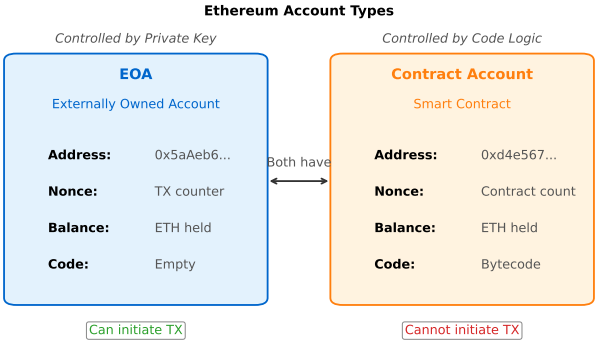
The EVM is a quasi-Turing complete state machine:

- Stack-based virtual machine (256-bit word size)
- Executes bytecode compiled from Solidity, Vyper
- Deterministic: same input always produces same output
- Gas metering prevents infinite loops
- Isolated: no network, filesystem, or process access

EVM Components:

- **Stack:** LIFO, max 1024 items, 256-bit each
- **Memory:** Byte array, volatile (per call), linear cost
- **Storage:** Key-value, persistent (on-chain), expensive
- **Program Counter:** Current bytecode position
- **Gas Counter:** Remaining computation budget

What Are the Two Types of Ethereum Accounts?



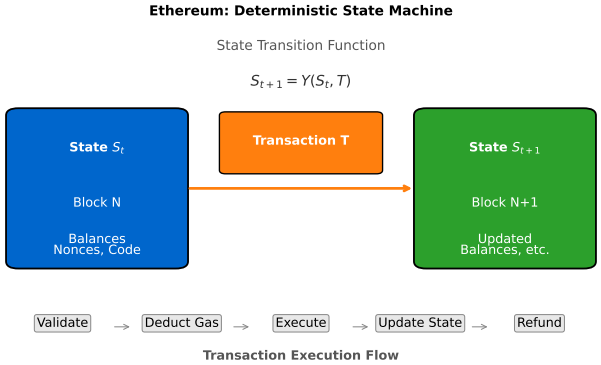
EOAs are controlled by private keys; contracts are controlled by code. | → Problem: How do we make money programmable? — Account Types: EOA vs Contract Contracts ARE the programmable money – code that controls value automatically

What Components Make Up Account State?

Every account (EOA or Contract) has four fields:

1. **Nonce:**
   - EOA: Counter of transactions sent
   - Contract: Counter of contracts created
   - Prevents replay attacks
2. **Balance:**
   - Amount of Wei (10^{-18} ETH) owned
   - 1 ETH = 1,000,000,000,000,000,000 Wei
3. **StorageRoot:**
   - Hash of account's storage trie root
   - Empty for EOAs
4. **CodeHash:**
   - Hash of EVM bytecode
   - Empty for EOAs, immutable for contracts

How Does Ethereum Track State Changes?



State transitions are deterministic: given S_t and T, S_{t+1} is uniquely determined.

What Is the World State?

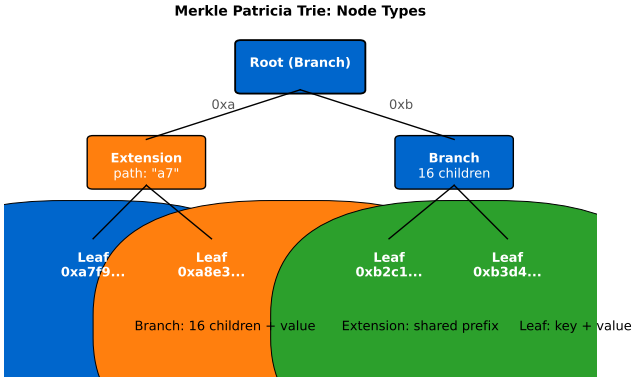
The World State is a mapping between addresses and account states:

- Maps 160-bit addresses to account states
- Stored as a Merkle Patricia Trie (from L02b: tree combining hash verification with key-value storage)
- Root hash included in every block header
- Allows efficient verification of account state
- Enables light clients to verify data without full state

State Root:

- 256-bit hash representing entire world state
- Changes with every block
- Uniquely identifies state at a specific block height

How Does Ethereum Efficiently Store State?



MPT combines Merkle verification, Patricia path compression, and radix optimization. | → Problem: How do we make money programmable? — Merkle Patricia Trie (MPT) MPT enables efficient verification of any account state – essential for light clients

Problem Check-In: Ethereum Architecture

Recall Our Problem

How do we make money programmable?

What We've Learned So Far

- The EVM executes bytecode deterministically across all nodes
- Two account types: EOAs (humans with keys) control contracts (autonomous code)
- Together they enable programmable money: code that controls value without intermediaries

Still to Address

- How do we verify state efficiently? (Merkle Patricia Trie) What trade-offs vs Bitcoin?
- How would YOU design a system to make money programmable?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we make money programmable?"?

What Properties Does the MPT Have?

Combines three data structures:

1. **Merkle Tree:** Cryptographic verification via hashes
2. **Patricia Trie:** Efficient key-value storage with shared prefixes
3. **Radix Trie:** Optimized path compression

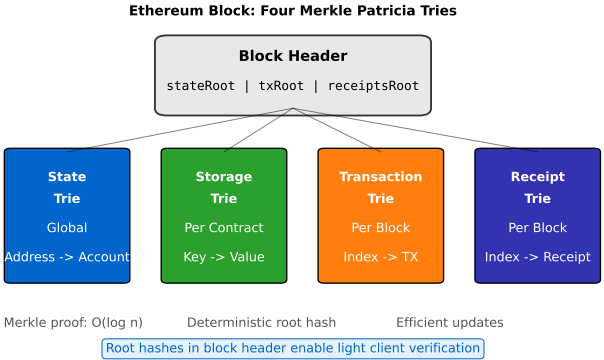
Key Properties:

- Deterministic: Same key-value pairs $\rightarrow$ same root hash
- Efficient verification: $O(\log n)$ proof size
- Efficient updates: Only modified paths need rehashing

Node Types:

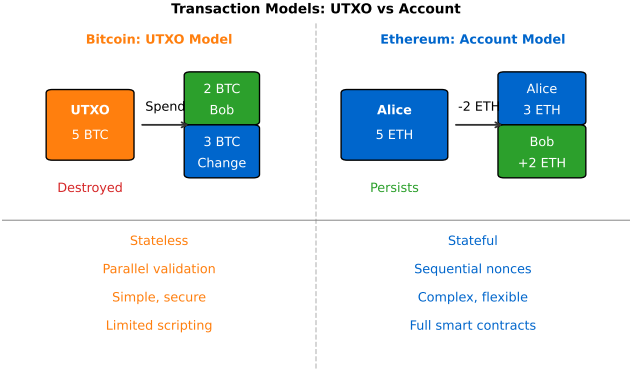
- **Branch:** 16 children (hex 0-F) + optional value
- **Extension:** Shared path prefix + next node pointer
- **Leaf:** Remaining key path + value

What Are the Four MPT Tries in Ethereum?



Block header contains root hashes of all four tries for verification.

Why Did Ethereum Choose Accounts Instead of UTXOs?



Account model enables smart contracts but requires nonce tracking.

What Are the Trade-offs of the Account Model?

Advantages:

1. **Simplicity:** Intuitive balance model, easier wallets
2. **Space Efficiency:** No UTXO tracking overhead
3. **Fungibility:** All Ether equivalent, no dust
4. **Smart Contracts:** Natural fit for persistent storage

Challenges:

1. **Replay Prevention:** Requires nonce tracking
2. **State Growth:** All accounts stored indefinitely
3. **Privacy:** All activity linked to single address
4. **Parallelization:** Sequential nonces limit parallel validation

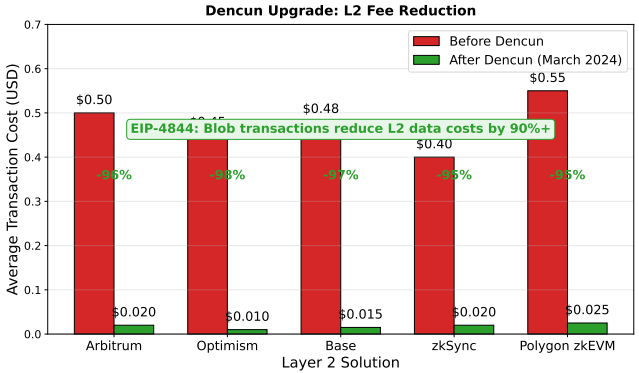
→ *Problem: How do we make money programmable? — Account Model: Trade-offs Account model enables smart contracts but sacrifices privacy and parallelization*

What Is Ethereum's Block Structure?

Ethereum block header contains:

- **parentHash:** Hash of parent block
- **beneficiary:** Address receiving block reward
- **stateRoot:** Root hash of state trie
- **transactionsRoot:** Root hash of transaction trie
- **receiptsRoot:** Root hash of receipt trie
- **logsBloom:** Bloom filter for efficient log lookup
- **number:** Block height
- **gasLimit / gasUsed:** Gas constraints
- **timestamp:** Unix timestamp
- **extraData:** Arbitrary data (max 32 bytes)

How Did the Dencun Upgrade Reduce L2 Costs?



EIP-4844 blob transactions reduce L2 data costs by 90%+.

What Is Proto-Danksharding in the Dencun Upgrade?

Major Network Upgrade (March 13, 2024):

- **EIP-4844**: Introduces "blob" transactions for Layer 2 data
- **Problem**: L2 rollups pay expensive calldata for data availability
- **Solution**: New data type (blobs) with separate, cheaper gas market

How Blobs Work:

- Blobs: 128 KB data chunks, stored for $\sim$18 days
- Separate "blob gas" market (independent of execution gas)
- L2s post transaction batches as blobs instead of calldata

Impact:

- L2 transaction fees reduced by 90%+ (\$0.50 $\rightarrow$ \$0.01)
- Arbitrum, Optimism, Base adopted immediately
- Paves way for full Danksharding (future upgrade)

Problem Solved? Ethereum Architecture

The Original Problem

How do we make money programmable?

How Ethereum Architecture Solves It

- **EVM executes bytecode**: All nodes run identical stack-based VM, ensuring deterministic state transitions
- **Account-based model**: Persistent storage (vs UTXO) enables complex contract logic and state management
- **World state + MPT**: Cryptographic verification of all account states at every block

Remaining Limitations

- **Execution costs**: Gas fees make computation expensive; state bloat from permanent storage
- **Single-threaded**: Sequential transaction processing (nonce ordering) limits parallelization and throughput

Open Questions

- How to scale smart contract execution (10,000+ TPS) while maintaining decentralization and security?
- Risk: State growth, MEV exploitation, smart contract bugs with irreversible financial consequences

Ethereum Architecture solves programmable money but introduces scalability and cost trade-offs

The Economics of Ethereum Architecture

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Ethereum Architecture

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Ethereum Architecture

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Why Is the EVM Like a Universal Calculator?

[COMIC: The EVM depicted as a giant vintage calculator with a tiny screen showing "256-bit math." Thousands of identical calculators around the world all display the same result. One calculator in the corner shows a different number and is being ejected from the network with a "CONSENSUS FAILED" stamp.]

Key Insight:

- The EVM's power lies in determinism: every node computes the same result, every time
- Disagreement means you are wrong—consensus is ruthless but reliable

10,000 calculators, one answer: that is the magic of deterministic computation

Key Takeaways

1. **EVM:** Deterministic, stack-based VM enabling Turing-complete smart contracts
2. **Two Account Types:** EOAs (user-controlled) and Contracts (code-controlled)
3. **State Machine:** Ethereum transitions between states via transactions
4. **World State:** Mapping of addresses to accounts, stored as MPT
5. **MPT:** Efficient cryptographic data structure for state verification
6. **Account Model:** Simpler than UTXO but with privacy/parallelization trade-offs

Next Lesson: L14 – Gas Mechanics

Discussion Questions

1. Why is the EVM only “quasi”-Turing complete?
2. What security benefits does the nonce provide?
3. How does MPT enable light client verification?
4. When might Bitcoin's UTXO model be preferable?
5. How does state growth affect node operators?

Next Lesson Preview: L14 - Gas Mechanics

Coming up next:

- Understanding gas as a computational unit
- Gas price, gas limit, and transaction cost calculation
- EIP-1559: Base fee and priority fee mechanism
- Gas costs for different EVM operations
- Optimization techniques for reducing gas consumption

Preparation:

- Review basic Ethereum transaction structure
- Familiarize yourself with Wei/Gwei/ETH units
- Browse Etherscan to see gas usage in real transactions

Quiz Questions (1/4)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete" rather than fully Turing complete?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas metering prevents infinite loops, limiting true Turing completeness.

Q3. What is the maximum stack depth in the EVM?
A) 256 items B) 512 items C) 1024 items D) 2048 items
Answer: C – The EVM stack can hold a maximum of 1024 items.

Q4. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither type D) Externally Owned Accounts (EOA)
Answer: D – EOAs are controlled by private keys; contracts are controlled by code.

Q5. How many Wei are in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}
Answer: C – 1 ETH = 1,000,000,000,000,000,000 Wei (10^{18}).

Quiz Questions (2/4)

Q6. What does the nonce field track for an EOA?
A) Balance B) Transaction count sent C) Gas used D) Contract deployments
Answer: B – For EOAs, nonce counts transactions sent to prevent replay attacks.

Q7. Which field is empty for Externally Owned Accounts but populated for Contract Accounts?
A) Nonce B) Balance C) CodeHash D) All fields are populated
Answer: C – EOAs have no code, so CodeHash is empty; contracts store bytecode.

Q8. What data structure is used to store the Ethereum world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – The world state uses a Merkle Patricia Trie for efficient verification.

Q9. How many tries does an Ethereum block header reference?
A) One B) Two C) Three D) Four
Answer: D – State, transaction, receipt, and storage tries (four total).

Q10. What is the state root?
A) First block hash B) 256-bit hash of entire world state C) Genesis state D) Merkle tree root
Answer: B – The state root is a 256-bit hash representing the entire world state.

Quiz Questions (3/4)

Q11. Which node type in MPT has 16 children?
A) Leaf B) Extension C) Branch D) Root
Answer: C – Branch nodes have 16 children (hex 0-F) plus optional value.

Q12. What is the primary advantage of Ethereum's account model over Bitcoin's UTXO model?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state size
Answer: C – Account model is more natural for persistent contract storage.

Q13. What is Ethereum often called to distinguish it from Bitcoin?
A) Digital silver B) World computer C) Smart ledger D) Crypto platform
Answer: B – Ethereum is called a "world computer" for programmable logic.

Q14. When was Ethereum mainnet launched?
A) January 3, 2009 B) July 30, 2015 C) August 1, 2017 D) December 1, 2020
Answer: B – Ethereum launched July 30, 2015 (Bitcoin was 2009).

Q15. Which EVM memory type is persistent and stored on-chain?
A) Stack B) Memory C) Storage D) Cache
Answer: C – Storage is persistent on-chain (expensive); Memory is volatile per call.

Quiz Questions (4/4)

Q16. What does EIP-4844 (Dencun upgrade) introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding
Answer: B – EIP-4844 introduces blob transactions for cheaper L2 data availability.

Q17. By approximately how much did Dencun reduce Layer 2 transaction fees?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – L2 fees dropped 90%+ (e.g., \$0.50 to \$0.01) after Dencun.

Q18. What is the address size in Ethereum?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: B – Ethereum addresses are 160 bits (40 hex characters).

Q19. Which field in the account state prevents replay attacks?
A) Balance B) Nonce C) CodeHash D) StorageRoot
Answer: B – The nonce ensures each transaction is unique and sequential.

Q20. What challenge does Ethereum's account model face compared to UTXO?
A) Complexity B) Privacy limitations C) Higher storage D) No smart contracts
Answer: B – All activity is linked to a single address, reducing privacy vs UTXO.

L13: Ethereum Architecture

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

January 2026

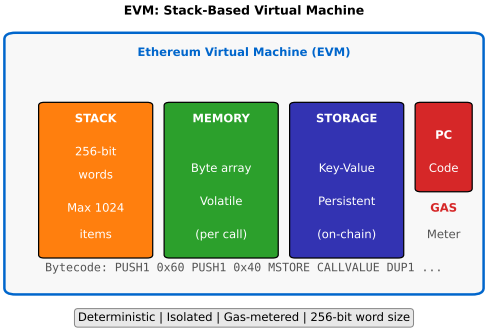
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

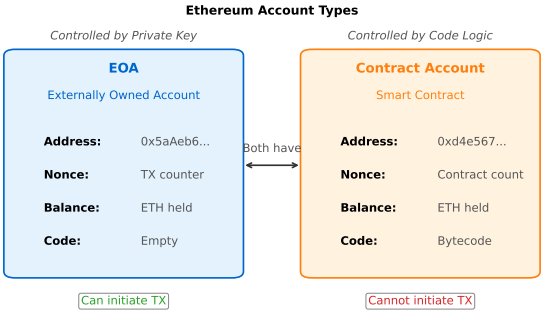
- Explain the Ethereum Virtual Machine (EVM) architecture
- Distinguish between EOA and Contract accounts
- Describe Ethereum as a state machine
- Compare Ethereum's account model to Bitcoin's UTXO

Ethereum Virtual Machine (EVM)



Key: Stack-based VM, 256-bit words, gas metering prevents infinite loops.

Account Types: EOA vs Contract



EOAs: Controlled by private keys — **Contracts:** Controlled by code

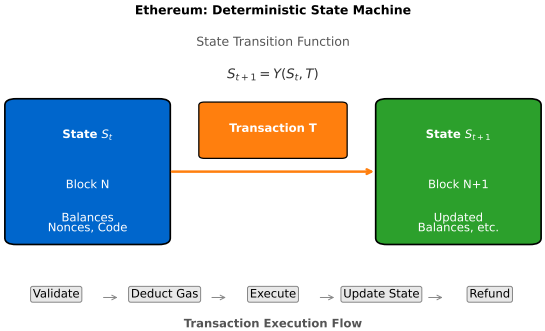
Account State Components

Every account has four fields:

1. **Nonce:** Transaction count (EOA) or contracts created (Contract)
2. **Balance:** Wei owned (1 ETH $= 10^{18}$ Wei)
3. **StorageRoot:** Hash of account's storage trie (empty for EOA)
4. **CodeHash:** Hash of EVM bytecode (empty for EOA)

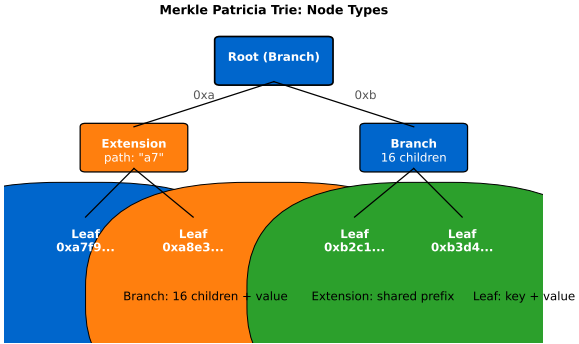
Key Insight: Nonce prevents replay attacks by ensuring sequential transactions.

Ethereum as a State Machine



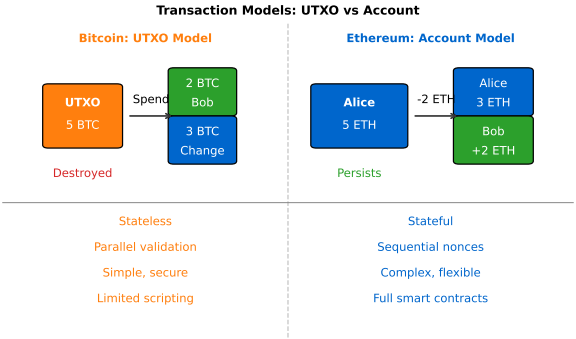
Deterministic: Given state S_t and transaction T, next state S_{t+1} is uniquely determined.

Merkle Patricia Trie (MPT)



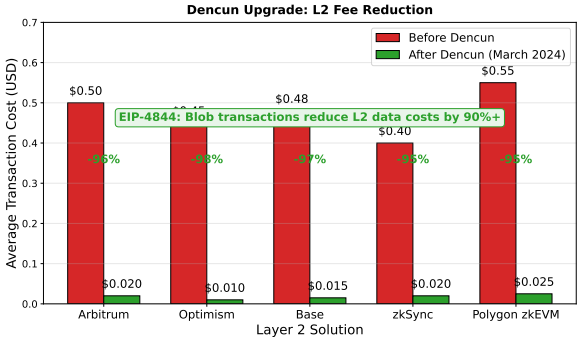
Properties: Efficient verification $O(\log n)$, deterministic root hash, path compression.

Account Model vs UTXO



Trade-off: Account model simpler for smart contracts but has privacy limitations.

2024 Milestone: Dencun Upgrade



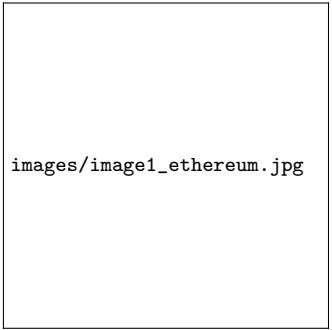
EIP-4844 (March 13, 2024): Blob transactions reduce L2 costs by 90%+.

Key Takeaways

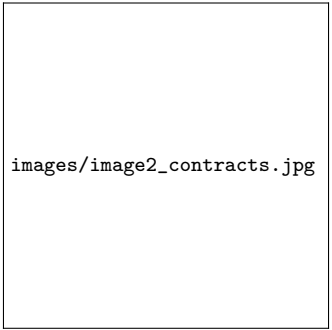
1. **EVM:** Deterministic, stack-based VM enabling smart contracts
2. **Account Types:** EOAs (user-controlled) vs Contracts (code-controlled)
3. **State Machine:** Transactions transition between deterministic states
4. **MPT:** Efficient cryptographic data structure for state verification
5. **Dencun:** EIP-4844 blobs reduced L2 fees by 90%+ (March 2024)

Core Insight: Ethereum extends Bitcoin from value transfer to programmable logic.

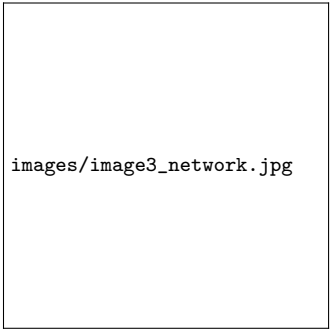
Ethereum Architecture in Practice



Ethereum Network



Smart Contracts



Global State

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits

Quiz (1/2)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – EVM uses 256-bit words for all stack operations.

Q2. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither D) Externally Owned Accounts

Quiz (1/2)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – EVM uses 256-bit words for all stack operations.

Q2. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither D) Externally Owned Accounts
Answer: D – EOAs are controlled by private keys; contracts by code.

Q3. How many Wei in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}

Quiz (1/2)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – EVM uses 256-bit words for all stack operations.

Q2. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither D) Externally Owned Accounts
Answer: D – EOAs are controlled by private keys; contracts by code.

Q3. How many Wei in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}
Answer: C – 1 ETH $= 10^{18}$ Wei.

Q4. What makes EVM "quasi"-Turing complete?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length

Quiz (1/2)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – EVM uses 256-bit words for all stack operations.

Q2. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither D) Externally Owned Accounts
Answer: D – EOAs are controlled by private keys; contracts by code.

Q3. How many Wei in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}
Answer: C – 1 ETH $= 10^{18}$ Wei.

Q4. What makes EVM "quasi"-Turing complete?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas metering prevents infinite loops.

Q5. When was Ethereum mainnet launched?
A) January 2009 B) July 2015 C) August 2017 D) December 2020

Quiz (1/2)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – EVM uses 256-bit words for all stack operations.

Q2. Which account type is controlled by private keys?
A) Contract accounts B) Both types C) Neither D) Externally Owned Accounts
Answer: D – EOAs are controlled by private keys; contracts by code.

Q3. How many Wei in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}
Answer: C – 1 ETH $= 10^{18}$ Wei.

Q4. What makes EVM "quasi"-Turing complete?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas metering prevents infinite loops.

Q5. When was Ethereum mainnet launched?
A) January 2009 B) July 2015 C) August 2017 D) December 2020
Answer: B – Ethereum launched July 30, 2015.

Quiz (2/2)

Q6. What data structure stores the world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter

Quiz (2/2)

Q6. What data structure stores the world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient state verification.

Q7. What does the nonce field prevent?
A) Double spending B) Replay attacks C) High gas costs D) Contract bugs

Quiz (2/2)

Q6. What data structure stores the world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient state verification.

Q7. What does the nonce field prevent?
A) Double spending B) Replay attacks C) High gas costs D) Contract bugs
Answer: B – Nonce ensures transaction uniqueness and ordering.

Q8. What is Ethereum's address size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits

Quiz (2/2)

Q6. What data structure stores the world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient state verification.

Q7. What does the nonce field prevent?
A) Double spending B) Replay attacks C) High gas costs D) Contract bugs
Answer: B – Nonce ensures transaction uniqueness and ordering.

Q8. What is Ethereum's address size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: B – 160 bits (40 hex characters).

Q9. What did EIP-4844 introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding

Quiz (2/2)

Q6. What data structure stores the world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient state verification.

Q7. What does the nonce field prevent?
A) Double spending B) Replay attacks C) High gas costs D) Contract bugs
Answer: B – Nonce ensures transaction uniqueness and ordering.

Q8. What is Ethereum's address size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: B – 160 bits (40 hex characters).

Q9. What did EIP-4844 introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding
Answer: B – Blob transactions for cheaper L2 data availability.

Q10. Account model advantage over UTXO?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state

Quiz (2/2)

Q6. What data structure stores the world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient state verification.

Q7. What does the nonce field prevent?
A) Double spending B) Replay attacks C) High gas costs D) Contract bugs
Answer: B – Nonce ensures transaction uniqueness and ordering.

Q8. What is Ethereum's address size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: B – 160 bits (40 hex characters).

Q9. What did EIP-4844 introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding
Answer: B – Blob transactions for cheaper L2 data availability.

Q10. Account model advantage over UTXO?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state
Answer: C – Account model is natural for persistent contract storage.

Thank you

Questions?

Next: L14 – Gas Mechanics

Quiz: Ethereum Architecture

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits

Quiz (1–5)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete"?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length

Quiz (1–5)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete"?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas prevents infinite loops, limiting true Turing completeness.

Q3. Which account type is controlled by private keys?
A) Contract B) Both types C) Neither D) EOA

Quiz (1–5)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete"?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas prevents infinite loops, limiting true Turing completeness.

Q3. Which account type is controlled by private keys?
A) Contract B) Both types C) Neither D) EOA
Answer: D – EOAs are controlled by private keys; contracts by code.

Q4. What data structure stores Ethereum's world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter

Quiz (1–5)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete"?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas prevents infinite loops, limiting true Turing completeness.

Q3. Which account type is controlled by private keys?
A) Contract B) Both types C) Neither D) EOA
Answer: D – EOAs are controlled by private keys; contracts by code.

Q4. What data structure stores Ethereum's world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient cryptographic verification.

Q5. How many Wei are in 1 ETH?
A) 10^{9} B) 10^{12} C) 10^{18} D) 10^{21}

Quiz (1–5)

Q1. What is the EVM's word size?
A) 128 bits B) 160 bits C) 256 bits D) 512 bits
Answer: C – The EVM uses 256-bit words for stack operations.

Q2. Which component makes the EVM "quasi-Turing complete"?
A) Stack limit B) Gas metering C) Memory size D) Bytecode length
Answer: B – Gas prevents infinite loops, limiting true Turing completeness.

Q3. Which account type is controlled by private keys?
A) Contract B) Both types C) Neither D) EOA
Answer: D – EOAs are controlled by private keys; contracts by code.

Q4. What data structure stores Ethereum's world state?
A) Hash table B) Binary tree C) Merkle Patricia Trie D) Bloom filter
Answer: C – MPT enables efficient cryptographic verification.

Q5. How many Wei are in 1 ETH?
A) 10^9 B) 10^{12} C) 10^{18} D) 10^{21}
Answer: C – 1 ETH = 10^{18} Wei.

Quiz (6–10)

Q6. What does the nonce field prevent?
A) Double spending B) Replay attacks C) Overflow D) Gas exhaustion

Quiz (6–10)

Q6. What does the nonce field prevent?
A) Double spending B) Replay attacks C) Overflow D) Gas exhaustion
Answer: B – Nonce ensures each transaction is unique and sequential.

Q7. Which MPT node type has 16 children?
A) Leaf B) Extension C) Branch D) Root

Quiz (6–10)

Q6. What does the nonce field prevent?
A) Double spending B) Replay attacks C) Overflow D) Gas exhaustion
Answer: B – Nonce ensures each transaction is unique and sequential.

Q7. Which MPT node type has 16 children?
A) Leaf B) Extension C) Branch D) Root
Answer: C – Branch nodes have 16 children (hex 0-F).

Q8. What advantage does Account model have over UTXO?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state

Quiz (6–10)

Q6. What does the nonce field prevent?
A) Double spending B) Replay attacks C) Overflow D) Gas exhaustion
Answer: B – Nonce ensures each transaction is unique and sequential.

Q7. Which MPT node type has 16 children?
A) Leaf B) Extension C) Branch D) Root
Answer: C – Branch nodes have 16 children (hex 0-F).

Q8. What advantage does Account model have over UTXO?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state
Answer: C – Account model is more natural for persistent contract storage.

Q9. What did EIP-4844 (Dencun) introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding

Quiz (6–10)

Q6. What does the nonce field prevent?
A) Double spending B) Replay attacks C) Overflow D) Gas exhaustion
Answer: B – Nonce ensures each transaction is unique and sequential.

Q7. Which MPT node type has 16 children?
A) Leaf B) Extension C) Branch D) Root
Answer: C – Branch nodes have 16 children (hex 0-F).

Q8. What advantage does Account model have over UTXO?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state
Answer: C – Account model is more natural for persistent contract storage.

Q9. What did EIP-4844 (Dencun) introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding
Answer: B – Blob transactions for cheaper L2 data availability.

Q10. By how much did Dencun reduce L2 fees?
A) 30% B) 50% C) 70% D) 90%+

Quiz (6–10)

Q6. What does the nonce field prevent?
A) Double spending B) Replay attacks C) Overflow D) Gas exhaustion
Answer: B – Nonce ensures each transaction is unique and sequential.

Q7. Which MPT node type has 16 children?
A) Leaf B) Extension C) Branch D) Root
Answer: C – Branch nodes have 16 children (hex 0-F).

Q8. What advantage does Account model have over UTXO?
A) Better privacy B) Easier parallelization C) Simpler for smart contracts D) Smaller state
Answer: C – Account model is more natural for persistent contract storage.

Q9. What did EIP-4844 (Dencun) introduce?
A) Proof of Stake B) Blob transactions C) Smart contracts D) Sharding
Answer: B – Blob transactions for cheaper L2 data availability.

Q10. By how much did Dencun reduce L2 fees?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – L2 fees dropped 90%+ after Dencun upgrade.

(c) Joerg Osterrieder 2025

L14: Gas Mechanics

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain what gas is and why Ethereum uses it
- Calculate transaction costs using gas price and gas limit
- Explain EIP-1559's base fee and priority fee mechanism
- Identify gas costs for different EVM operations
- Apply optimization techniques to reduce gas consumption
- Analyze real-world gas usage patterns

(c) Joerg Osterrieder 2025

The Problem: How do we price scarce computation fairly?

The Challenge
How do we price scarce computational resources on a public blockchain without enabling denial-of-service attacks? Ethereum's EVM must process transactions from anyone, but unlimited computation could halt the network.

Why It Matters

- Without gas limits, infinite loops could halt the entire network
- Historical example: EIP-1559 (August 2021) addressed fee market inefficiencies, but fee spikes still occur during high-demand events (e.g., NFT mints)

What We Need

- Value creation and capture
- Market-based pricing that reflects true computational cost without manual estimation

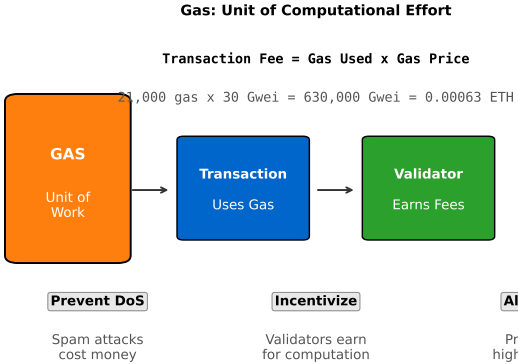
The Cryptoeconomics Question
Creating and distributing economic value

Today's lesson: How Gas Mechanics addresses this challenge

What is Gas?

Gas is a unit of computational effort in Ethereum:

- Measures the cost of executing operations on the EVM
- Prevents infinite loops and spam attacks
- Compensates validators for computation and storage



Why Gas Exists

Three Critical Functions:

1. **Prevent Denial-of-Service Attacks:**
   - Without gas, infinite loops could halt the network
   - Attackers would need to pay for computational resources
2. **Incentivize Validators:**
   - Validators earn transaction fees for including transactions
   - Higher gas price = higher priority in block inclusion
3. **Resource Allocation:**
   - Limited block gas limit (e.g., 30,000,000 gas per block)
   - Prioritizes transactions willing to pay more

Ether Denominations

Ether units from smallest to largest:

Unit	Wei Value	Typical Use
Wei	1	Smallest unit (like satoshi)
Gwei (Shannon)	10^9	Gas prices
Microether (Szabo)	10^{12}	-
Milliether (Finney)	10^{15}	-
Ether	10^{18}	Main unit

Most Common:

- **Gwei (Gigawei):** Standard unit for gas prices (1 Gwei = 10^9 Wei)
- **Ether:** User-facing unit (1 ETH = 10^{18} Wei)

Gas Calculation: Pre-EIP-1559

Legacy Transaction Fee Model (before August 2021):
Formula:

$$\text{Transaction Fee} = \text{Gas Used} \times \text{Gas Price}$$

Example:

- Gas Used: 21,000 (simple ETH transfer)
- Gas Price: 50 Gwei (user-specified)
- Transaction Fee: $21{,}000 \times 50 = 1{,}050{,}000$ Gwei $= 0.00105$ ETH

Challenges:

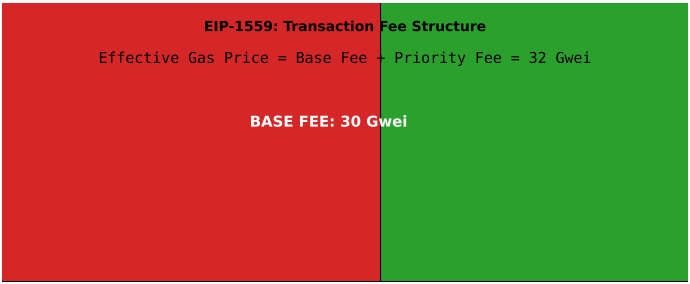
- Users had to manually estimate gas price
- Overpaying was common to ensure inclusion
- No refund if gas price was too high

EIP-1559: London Hard Fork (August 2021)

Major overhaul of gas fee mechanism:

- **Base Fee:** Algorithmically determined, burned (removed from circulation)
- **Priority Fee (Tip):** User-specified tip to validator for inclusion
- **Max Fee:** Maximum gas price user is willing to pay

EIP-1559 Fee Breakdown (August 2021)



EIP-1559 Fee Calculation

New Formula:

$$\text{Transaction Fee} = \text{Gas Used} \times (\text{Base Fee} + \text{Priority Fee})$$

With cap:

$$\text{Effective Gas Price} = \min(\text{Base Fee} + \text{Priority Fee}, \text{Max Fee})$$

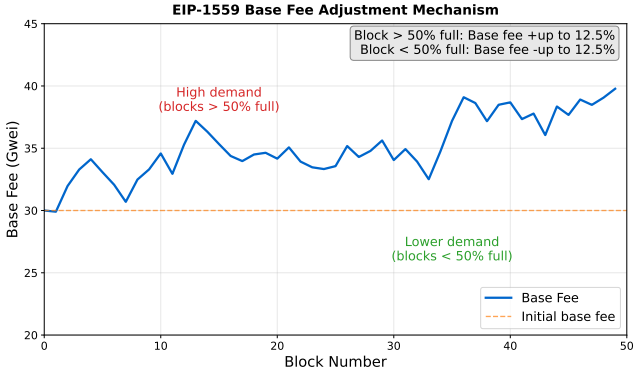
Example:

- Gas Used: 21,000
- Base Fee: 30 Gwei (set by protocol)
- Priority Fee: 2 Gwei (user tip)
- Effective Gas Price: $\min(30 + 2, 50) = 32$ Gwei
- Transaction Fee: $21{,}000 \times 32 = 672{,}000$ Gwei $= 0.000672$ ETH
- Burned: $21{,}000 \times 30 = 630{,}000$ Gwei

Base Fee Adjustment Mechanism

Dynamic base fee targets 50% full blocks:

- Target gas per block: 15,000,000 (50% of 30M limit)
- If block $>$ 50% full: Base fee increases by max 12.5%
- If block $<$ 50% full: Base fee decreases by max 12.5%



Gas Limit vs Gas Used

Understanding the difference:

Gas Limit:

- Maximum gas transaction may consume
- Set by user before sending transaction
- Acts as safety cap
- Unused gas is refunded

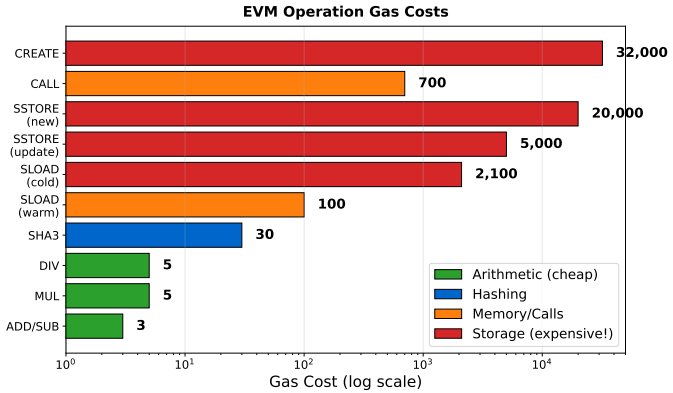
Gas Used:

- Actual gas consumed by transaction
- Determined by operations executed
- Used for fee calculation
- Visible on Etherscan

Common Values: Simple transfer: 21,000 — ERC-20 transfer: 45,000-65,000 — Complex contract: 100,000+

Gas Costs by Operation

Every EVM opcode has a fixed gas cost:



Key Insight: Storage operations (SSTORE, SLOAD) are by far the most expensive

Gas Costs by Operation (Table)

Operation	Description	Gas Cost
ADD, SUB, MUL	Arithmetic operations	3
DIV, MOD	Division/modulo	5
SHA3 (Keccak-256)	Hash function	30 + 6/word
SLOAD	Load from storage	100 (warm) / 2100 (cold)
SSTORE	Write to storage	20,000 (new) / 5,000 (update)
CALL	External contract call	700 + value transfer costs
CREATE	Deploy contract	32,000 + code size

Cold vs Warm Access (EIP-2929):

- **Cold:** First access to storage slot in transaction (expensive)
- **Warm:** Subsequent accesses to same slot (cheaper)

Storage: The Gas Guzzler

Why storage is expensive:

- Persists data across all nodes forever
- Requires disk I/O (slower than RAM)
- State bloat affects all future nodes

Storage Gas Costs (EIP-2929, EIP-2200):

- **SSTORE (set to non-zero from zero):** 20,000 gas
- **SSTORE (update non-zero):** 5,000 gas
- **SSTORE (set to zero):** 5,000 gas + 15,000 refund
- **SLOAD (cold access):** 2,100 gas (first access in transaction)
- **SLOAD (warm access):** 100 gas (subsequent accesses)

Example: Storing one 256-bit word (32 bytes) at 32 Gwei: 0.00064 ETH = $1.28 at $2000/ETH

Gas Optimization: Storage Patterns

Inefficient: Multiple SSTOREs

```
contract Inefficient {
    uint256 public value1;
    uint256 public value2;
    uint256 public value3;

    function updateAll(uint256 v1, uint256 v2, uint256 v3) public {
        value1 = v1;  // 20,000 gas (or 5,000 if updating)
        value2 = v2;  // 20,000 gas
        value3 = v3;  // 20,000 gas
    }
    // Total: 60,000 gas for 3 writes
}
```

Efficient: Packed Storage

```
contract Efficient {
    uint256 public packedValues;  // Pack 3 uint85 values in one slot

    function updateAll(uint85 v1, uint85 v2, uint85 v3) public {
        packedValues = uint256(v1) | (uint256(v2) << 85) | (uint256(v3) << 170);
    }
    // Total: 20,000 gas for single write (3x cheaper!)
}
```

Gas Optimization: Memory vs Storage

Use memory for temporary data:
Inefficient: Storage for Temporary Array

```
contract Inefficient {
    uint256[] public tempArray;  // Storage
    function processData(uint256[] calldata input) public {
        delete tempArray;
        for (uint i = 0; i < input.length; i++) {
            tempArray.push(input[i] * 2);  // SSTORE per iteration
        }
    }
}
```

Efficient: Memory Array

```
contract Efficient {
    function processData(uint256[] calldata input) public {
        uint256[] memory tempArray = new uint256[](input.length);
        for (uint i = 0; i < input.length; i++) {
            tempArray[i] = input[i] * 2;  // Memory write (cheap)
        }
    }
}
```

Gas Optimization: Short-Circuiting

Exploit boolean evaluation order:
Inefficient: Expensive Check First

```
function transfer(address to, uint256 amount) public {
    require(balances[msg.sender] >= amount && to != address(0), "Invalid");
    // If to == address(0), still loads balances[msg.sender] (2100 gas SLOAD)
}
```

Efficient: Cheap Check First

```
function transfer(address to, uint256 amount) public {
    require(to != address(0) && balances[msg.sender] >= amount, "Invalid");
    // If to == address(0), immediately fails (no SLOAD)
}
```

Principle: Place cheaper conditions first in logical AND (&&)
Savings: 2100 gas when early condition fails

Gas Optimization: Event Logs vs Storage

Events are much cheaper than storage:

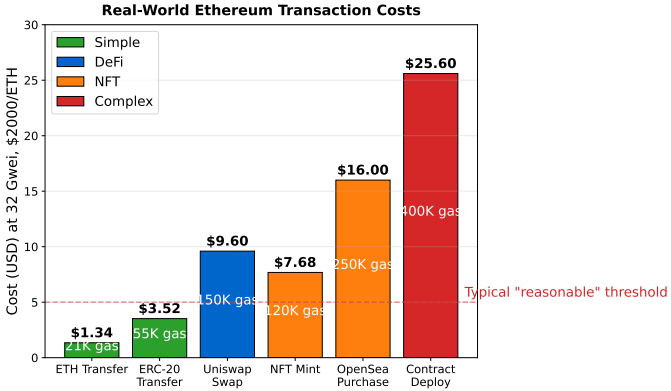
Storage: Accessible on-chain, 20,000 gas per new slot

Events: Not accessible on-chain, 375 gas + 8/byte

```
event Transfer(address indexed from, address indexed to, uint256 amount);

function transfer(address to, uint256 amount) public {
    balances[msg.sender] -= amount;
    balances[to] += amount;
    emit Transfer(msg.sender, to, amount);  // ~1500 gas vs 20,000+ for storage
}
```

Real-World Transaction Costs

Typical gas costs on Ethereum mainnet:



Note: Costs vary significantly based on network congestion and gas prices

Real-World Gas Usage (Table)

Transaction Type	Gas Used
Simple ETH transfer	21,000
ERC-20 token transfer	45,000 - 65,000
Uniswap V2 swap	100,000 - 150,000
Uniswap V3 swap	120,000 - 185,000
NFT mint (ERC-721)	80,000 - 150,000
OpenSea NFT purchase	150,000 - 300,000
Deploy simple contract	200,000 - 500,000

At 32 Gwei (30 base + 2 tip):

- Simple transfer: 0.000672 ETH ($1.34 at $2000/ETH)
- Uniswap swap: 0.004 ETH ($8 at $2000/ETH)
- Contract deploy: 0.016+ ETH ($32+ at $2000/ETH)

Gas Refunds

Refundable Actions:

- **SSTORE to zero:** 15,000 gas refund (after paying 5,000 to clear)
- **SELFDESTRUCT:** 24,000 gas refund (contract deletion)

Refund Cap (EIP-3529): Maximum refund: 20% of gas used (prevents exploitation)

```
function clearStorage() public {
    delete largeMapping[key1];  // 5,000 cost + 15,000 refund
    delete largeMapping[key2];  // 5,000 cost + 15,000 refund
    // Gas used: 10,000, Potential: 30,000 (capped at 2,000)
}
```

EIP-4844: Blob Gas Market (Dencun Upgrade, March 2024)

Ethereum now has TWO gas markets:

- **Execution gas**: Traditional EVM operations (existing market)
- **Blob gas**: Data availability for L2 rollups (new market)
- Markets operate independently with separate base fees

Blob Gas Mechanics:

- Target: 3 blobs per block (384 KB), Maximum: 6 blobs (768 KB)
- Blob gas price adjusts like EIP-1559 (targets 50% capacity)

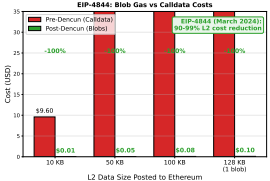
EIP-4844: Blob Gas Savings

Cost comparison for posting L2 data to Ethereum:

$122.88

$96.00

$48.00



Impact: 90-99% reduction in L2 transaction costs since Dencun upgrade

Problem Solved? Gas Mechanics

The Original Problem

How do we price scarce computation fairly?

How Gas Mechanics Solves It

- Gas units: Fixed costs per EVM operation
- EIP-1559: Dynamic base fee targets 50% blocks
- Base fee burning aligns incentives

Remaining Limitations

- Volatile fees during congestion (10x-100x spikes)
- MEV extraction undermines fairness

Open Questions

- Can fees be more predictable?
- Does it scale without L2 solutions?

Gas Mechanics partially solves fair pricing but introduces volatility and MEV trade-offs

(c) Joerg Osterrieder 2025

Key Takeaways

1. **Gas Purpose:** Prevents spam/DoS, compensates validators, allocates block space
2. **EIP-1559:** Base fee (burned) + priority fee (to validator) for predictable pricing
3. **Base Fee Dynamics:** Adjusts up to 12.5% per block to target 50% full blocks
4. **Storage is Expensive:** SSTORE costs 20,000 gas (new) or 5,000 gas (update)
5. **Optimization:** Pack storage, use memory for temp data, batch operations
6. **EIP-4844:** Blob gas market reduced L2 costs by 90-99%

Discussion Questions

1. Why does EIP-1559 burn the base fee instead of giving it to validators?
2. If Ethereum's block gas limit is 30M and average block time is 12 seconds, what is the theoretical maximum transactions per second for simple ETH transfers?
3. Under what circumstances might a user set a very high max fee per gas?
4. How do Layer 2 solutions (e.g., Optimism, Arbitrum) reduce gas costs?
5. What are the tradeoffs between storing data on-chain vs using events vs off-chain storage?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L15 - Solidity Fundamentals

Coming up next:

- Introduction to Solidity programming language
- Data types: uint, address, string, arrays, mappings
- Functions, visibility modifiers, state mutability
- Events and error handling
- Inheritance and interfaces

Preparation:

- Install MetaMask browser extension
- Familiarize yourself with Remix IDE (remix.ethereum.org)
- Review basic programming concepts (if-else, loops, functions)

Quiz Questions (1/4)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei = 10^9 Wei, 1 ETH = 10^{18} Wei.

Q3. In the pre-EIP-1559 model, what was the transaction fee formula?
A) Gas Used + Gas Price B) Gas Used × Gas Price
C) Gas Limit × Gas Price D) Base Fee + Priority Fee
Answer: B – Transaction Fee = Gas Used × Gas Price (legacy).

Q4. What happens to the base fee in EIP-1559 transactions?
A) Sent to validators B) Burned (removed from circulation)
C) Returned to users D) Stored in treasury
Answer: B – EIP-1559 burns base fees to reduce ETH supply.

Q5. If a block is more than 50% full, how does the base fee change?
A) Decreases by 12.5% B) Stays the same C) Increases by up to 12.5% D) Doubles
Answer: C – Base fee increases when blocks exceed 50% capacity.

Quiz Questions (2/4)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q8. What is the difference between gas limit and gas used?
A) No difference B) Gas limit is max allowed, gas used is actual consumed
C) Gas limit is for validators only D) Gas used includes refunds
Answer: B – Gas limit is user-set cap; gas used is actual. Unused refunded.

Q9. In EIP-1559, the priority fee goes to:
A) The Ethereum Foundation B) The user as refund C) Validators D) Burned
Answer: C – Priority fee (tip) incentivizes validators to include transaction.

Q10. What is the target gas per block in Ethereum's EIP-1559 mechanism?
A) 10,000,000 B) 15,000,000 C) 30,000,000 D) 60,000,000
Answer: B – Target is 15M gas (50% of 30M block limit).

Quiz Questions (3/4)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000
Answer: C – Clearing storage (SSTORE to zero) refunds 15,000 gas (after 5,000 cost).

Q13. What is the maximum gas refund cap introduced by EIP-3529?
A) 10% of gas used B) 20% of gas used C) 50% of gas used D) No cap
Answer: B – EIP-3529 caps refunds at 20% of gas used to prevent exploitation.

Q14. Which transaction type typically uses the most gas?
A) Simple ETH transfer B) ERC-20 transfer C) Uniswap swap D) Contract deployment
Answer: D – Deploying contracts costs 200k-500k+ gas, far exceeding other operations.

Q15. What is the advantage of using event logs instead of storage?
A) Events are faster B) Events cost much less gas (375 vs 20,000)
C) Events are on-chain accessible D) No advantage
Answer: B – Events cost 375 gas + 8/byte vs 20,000+ for storage.

Quiz Questions (4/4)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs
Answer: B – Target is 3 blobs/block (384 KB), max 6 blobs (768 KB).

Q18. What optimization technique reduces gas by packing multiple values in one storage slot?
A) Memory arrays B) Packed storage C) Short-circuiting D) Event logging
Answer: B – Packing multiple small values into one uint256 slot saves SSTORE costs.

Q19. In a require statement with AND logic, which condition should come first?
A) Most expensive B) Cheapest (to short-circuit and save gas)
C) Random order D) Order doesn't matter
Answer: B – Place cheap checks first; if they fail, expensive operations are skipped.

Q20. If base fee is 30 Gwei, priority fee is 2 Gwei, and max fee is 50 Gwei, what is the effective gas price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective gas price = min(base + priority, max) = min(30+2, 50) = 32 Gwei.

L14: Gas Mechanics

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Surprise Transaction Fees

[COMIC: User excitedly clicks "Swap 10 USDC" button. MetaMask popup appears with "Estimated Gas: 0.1 ETH ($200)." User's smile inverts to shock. Wallet balance shows exactly 0.09 ETH.]

Frame the Concept:

- Gas prices fluctuate based on network demand—high congestion means expensive transactions
- Understanding gas mechanics helps you time transactions and optimize contract code

The true cost of decentralization: paying $50 to swap $10

Learning Objectives

By the end of this lesson, you will be able to:

- Explain what gas is and why Ethereum uses it
- Calculate transaction costs using gas price and gas limit
- Explain EIP-1559's base fee and priority fee mechanism
- Identify gas costs for different EVM operations
- Apply optimization techniques to reduce gas consumption
- Analyze real-world gas usage patterns

Building on L13: Ethereum Architecture

(c) Joerg Osterrieder 2025

The Problem: How do we price scarce computation fairly?

The Challenge
How do we price scarce computational resources on a public blockchain without enabling denial-of-service attacks? Ethereum's EVM must process transactions from anyone, but unlimited computation could halt the network.

Why It Matters

- Without gas limits, infinite loops could halt the entire network
- Historical example: EIP-1559 (August 2021) addressed fee market inefficiencies, but fee spikes still occur during high-demand events (e.g., NFT mints)

What We Need

- Value creation and capture
- Market-based pricing that reflects true computational cost without manual estimation

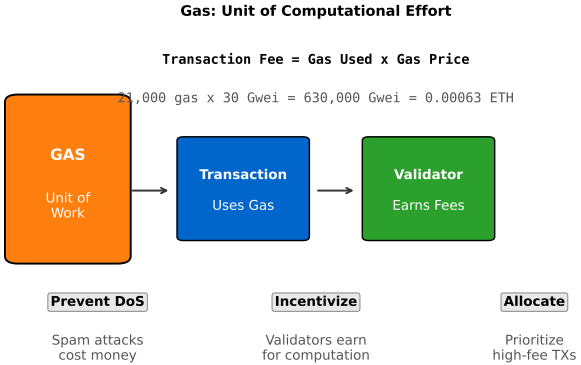
The Cryptoeconomics Question
Creating and distributing economic value

Today's lesson: How Gas Mechanics addresses this challenge

Why Does Ethereum Need Gas?

Gas is a unit of computational effort in Ethereum:

- Measures the cost of executing operations on the EVM
- Prevents infinite loops and spam attacks
- Compensates validators for computation and storage



→ **Problem: How do we price scarce computation... — What is Gas? Gas measures computational effort, preventing infinite loops and compensating validators**

Why Does Gas Exist?

Three Critical Functions:

1. **Prevent Denial-of-Service Attacks:**
   - Without gas, infinite loops could halt the network
   - Attackers would need to pay for computational resources
2. **Incentivize Validators:**
   - Validators earn transaction fees for including transactions
   - Higher gas price = higher priority in block inclusion
3. **Resource Allocation:**
   - Limited block gas limit (e.g., 30,000,000 gas per block)
   - Prioritizes transactions willing to pay more

What Are the Main Ether Denominations?

Ether units from smallest to largest:

Unit	Wei Value	Typical Use
Wei	1	Smallest unit (like satoshi)
Gwei (Shannon)	10^9	Gas prices (1 Gwei = 0.000000001 ETH)
Microether (Szabo)	10^{12}	-
Milliether (Finney)	10^{15}	-
Ether	10^{18}	Main unit

Most Common:

- **Gwei (Gigawei):** Standard unit for gas prices (1 Gwei = 10^9 Wei)
- **Ether:** User-facing unit (1 ETH = 10^{18} Wei)

How Were Gas Fees Calculated Before EIP-1559?

Legacy Transaction Fee Model (before August 2021):
Formula:

$$\text{Transaction Fee} = \text{Gas Used} \times \text{Gas Price}$$

Example:

- Gas Used: 21,000 (simple ETH transfer)
- Gas Price: 50 Gwei (user-specified)
- Transaction Fee: $21{,}000 \times 50 = 1{,}050{,}000$ Gwei $= 0.00105$ ETH

Challenges:

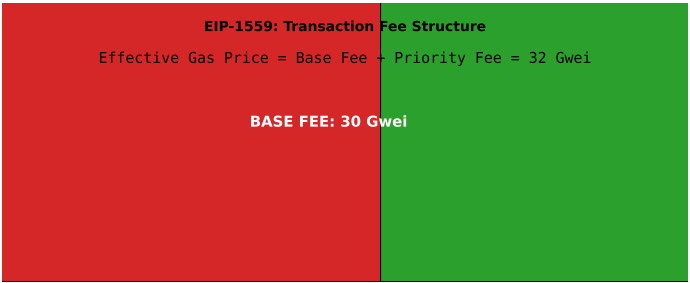
- Users had to manually estimate gas price
- Overpaying was common to ensure inclusion
- No refund if gas price was too high

What Did EIP-1559 Change About Gas Fees?

Major overhaul of gas fee mechanism:

- **Base Fee:** Algorithmically determined, burned (removed from circulation)
- **Priority Fee (Tip):** User-specified tip to validator for inclusion
- **Max Fee:** Maximum gas price user is willing to pay

EIP-1559 Fee Breakdown (August 2021)



Max Fee (user sets cap) >= Base Fee + Priority Fee
Unused Max Fee is refunded

How Do We Calculate Fees Under EIP-1559?

New Formula:

$$\text{Transaction Fee} = \text{Gas Used} \times (\text{Base Fee} + \text{Priority Fee})$$

With cap:

$$\text{Effective Gas Price} = \min(\text{Base Fee} + \text{Priority Fee}, \text{Max Fee})$$

Example:

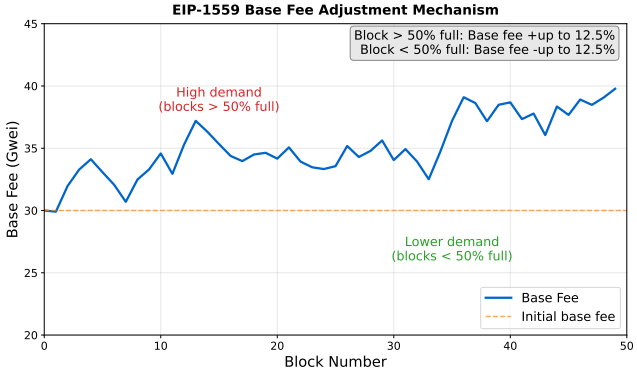
- Gas Used: 21,000
- Base Fee: 30 Gwei (set by protocol)
- Priority Fee: 2 Gwei (user tip)
- Effective Gas Price: $\min(30 + 2, 50) = 32$ Gwei
- Transaction Fee: $21{,}000 \times 32 = 672{,}000$ Gwei $= 0.000672$ ETH
- Burned: $21{,}000 \times 30 = 630{,}000$ Gwei

→ Problem: How do we price scarce computation... — EIP-1559 Fee Calculation EIP-1559 solves the estimation problem: base fee is algorithmic, priority fee is your tip

How Does the Base Fee Adjust Automatically?

Dynamic base fee targets 50% full blocks:

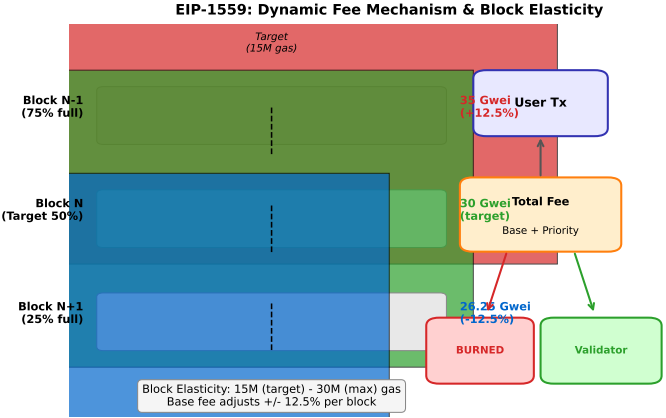
- Target gas per block: 15,000,000 (50% of 30M limit)
- If block $>$ 50% full: Base fee increases by max 12.5%
- If block $<$ 50% full: Base fee decreases by max 12.5%



How Do Block Elasticity and Fee Burning Work in EIP-1559?

Two key innovations:

- **Block Elasticity:** Blocks can expand from 15M (target) to 30M (max) gas
- **Fee Burning:** Base fee is permanently removed from ETH supply



Elasticity absorbs demand spikes; burning creates deflationary pressure during high activity

What's the Difference Between Gas Limit and Gas Used?

Understanding the difference:

Gas Limit:

- Maximum gas transaction may consume
- Set by user before sending transaction
- Acts as safety cap
- Unused gas is refunded

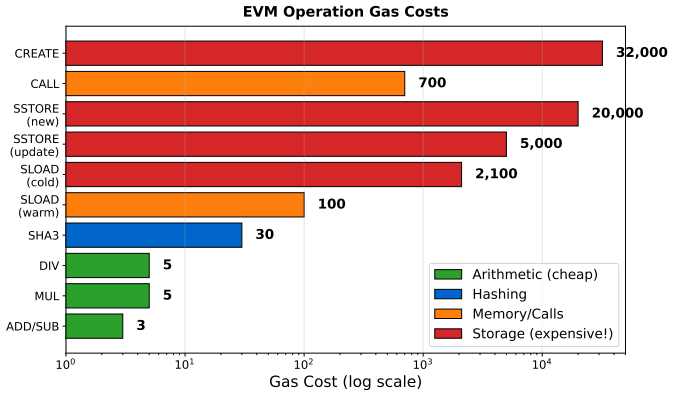
Gas Used:

- Actual gas consumed by transaction
- Determined by operations executed
- Used for fee calculation
- Visible on Etherscan

Common Values: Simple transfer: 21,000 — ERC-20 transfer: 45,000-65,000 — Complex contract: 100,000+

Why Do Different Operations Cost Different Gas?

Every EVM opcode has a fixed gas cost:



Key Insight: Storage operations (SSTORE, SLOAD) are by far the most expensive

How Much Gas Do Common Operations Cost?

Operation	Description	Gas Cost
ADD, SUB, MUL	Arithmetic operations	3
DIV, MOD	Division/modulo	5
SHA3 (Keccak-256)	Hash function	30 + 6/word
SLOAD	Load from storage	100 (warm) / 2100 (cold)
SSTORE	Write to storage	20,000 (new) / 5,000 (update)
CALL	External contract call	700 + value transfer costs
CREATE	Deploy contract	32,000 + code size

Cold vs Warm Access (EIP-2929):

- **Cold:** First access to storage slot in transaction (expensive)
- **Warm:** Subsequent accesses to same slot (cheaper)

Problem Check-In: Gas Mechanics

Recall Our Problem

How do we price scarce computation fairly?

What We've Learned So Far

- Gas units measure computational work (21,000 for simple transfer)
- EIP-1559 introduced base fee (burned) + priority fee (tip to validators)
- Base fee adjusts algorithmically to target 50% full blocks – fair pricing without estimation

Still to Address

- Why is storage so expensive? (SSTORE: 20,000 gas) How can developers optimize?
- How would YOU design a pricing system for scarce blockchain resources?

Think About

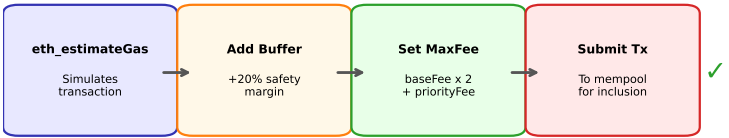
- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we price scarce computation..."?

How Does Gas Estimation Work?

How wallets estimate gas before sending:

Gas Estimation Flow: From Simulation to Submission



Example: Uniswap Swap

1. `eth_estimateGas` returns: 150,000 gas
2. Add 20% buffer: 150,000 x 1.2 = 180,000 gas limit
3. Current baseFee: 25 Gwei
4. MaxFeePerGas: 25 x 2 + 2 = 52 Gwei

Why Buffer?

- State may change
- Other txs in block
- Dynamic gas costs

Unused gas refunded!

Always add buffer – state changes between estimation and execution can increase gas needed

Why Is Storage So Expensive on Ethereum?

Why storage is expensive:

- Persists data across all nodes forever
- Requires disk I/O (slower than RAM)
- State bloat affects all future nodes

Storage Gas Costs (EIP-2929, EIP-2200):

- **SSTORE (set to non-zero from zero):** 20,000 gas
- **SSTORE (update non-zero):** 5,000 gas
- **SSTORE (set to zero):** 5,000 gas + 15,000 refund
- **SLOAD (cold access):** 2,100 gas (first access in transaction)
- **SLOAD (warm access):** 100 gas (subsequent accesses)

Example: Storing one 256-bit word (32 bytes) at 32 Gwei: 0.00064 ETH = $1.28 at $2000/ETH

→ **Problem: How do we price scarce computation... — Storage: The Gas Guzzler Storage is expensive because data persists forever across all nodes – pricing reflects true cost**

How Can We Optimize Storage Patterns?

Inefficient: Multiple SSTOREs

```
contract Inefficient {
    uint256 public value1;
    uint256 public value2;
    uint256 public value3;

    function updateAll(uint256 v1, uint256 v2, uint256 v3) public {
        value1 = v1;  // 20,000 gas (or 5,000 if updating)
        value2 = v2;  // 20,000 gas
        value3 = v3;  // 20,000 gas
    }
    // Total: 60,000 gas for 3 writes
}
```

Efficient: Packed Storage

```
contract Efficient {
    uint256 public packedValues;  // Pack 3 uint85 values in one slot

    function updateAll(uint85 v1, uint85 v2, uint85 v3) public {
        packedValues = uint256(v1) | (uint256(v2) << 85) | (uint256(v3) << 170);
    }
    // Total: 20,000 gas for single write (3x cheaper!)
}
```

When Should We Use Memory vs Storage?

Use memory for temporary data:
Inefficient: Storage for Temporary Array

```
contract Inefficient {
    uint256[] public tempArray;  // Storage
    function processData(uint256[] calldata input) public {
        delete tempArray;
        for (uint i = 0; i < input.length; i++) {
            tempArray.push(input[i] * 2);  // SSTORE per iteration
        }
    }
}
```

Efficient: Memory Array

```
contract Efficient {
    function processData(uint256[] calldata input) public {
        uint256[] memory tempArray = new uint256[](input.length);
        for (uint i = 0; i < input.length; i++) {
            tempArray[i] = input[i] * 2;  // Memory write (cheap)
        }
    }
}
```

How Does Short-Circuiting Save Gas?

Exploit boolean evaluation order:
Inefficient: Expensive Check First

```
function transfer(address to, uint256 amount) public {
    require(balances[msg.sender] >= amount && to != address(0), "Invalid");
    // If to == address(0), still loads balances[msg.sender] (2100 gas SLOAD)
}
```

Efficient: Cheap Check First

```
function transfer(address to, uint256 amount) public {
    require(to != address(0) && balances[msg.sender] >= amount, "Invalid");
    // If to == address(0), immediately fails (no SLOAD)
}
```

Principle: Place cheaper conditions first in logical AND (&&)
Savings: 2100 gas when early condition fails

Why Are Event Logs Cheaper Than Storage?

Events are much cheaper than storage:

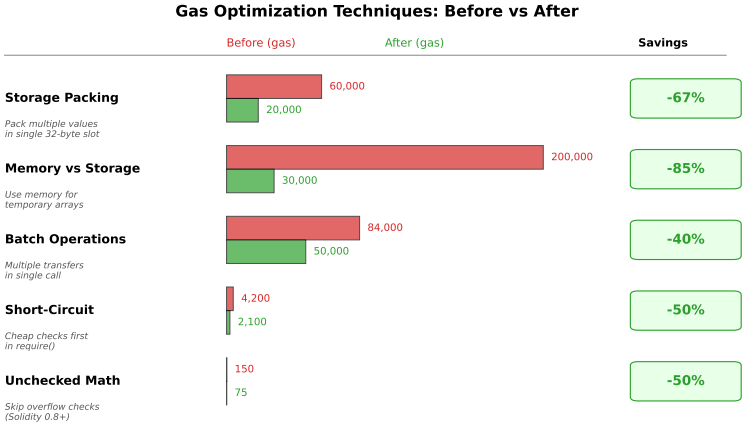
Storage: Accessible on-chain, 20,000 gas per new slot

Events: Not accessible on-chain, 375 gas + 8/byte

```
event Transfer(address indexed from, address indexed to, uint256 amount);

function transfer(address to, uint256 amount) public {
    balances[msg.sender] -= amount;
    balances[to] += amount;
    emit Transfer(msg.sender, to, amount);  // ~1500 gas vs 20,000+ for storage
}
```

How Much Can Optimization Techniques Save?

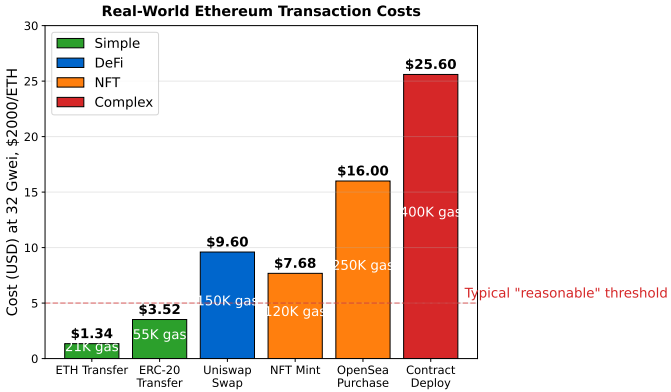
Impact of common optimization patterns:



Storage packing and memory usage provide the largest savings – always optimize storage first

How Much Do Real-World Transactions Cost?

Typical gas costs on Ethereum mainnet:



Note: Costs vary significantly based on network congestion and gas prices

→ **Problem: How do we price scarce computation... — Real-World Transaction Costs Real costs vary 10x-100x based on network congestion – gas pricing is volatile but fair**

How Much Gas Do Common Transactions Use?

Transaction Type	Gas Used
Simple ETH transfer	21,000
ERC-20 token transfer	45,000 - 65,000
Uniswap V2 swap	100,000 - 150,000
Uniswap V3 swap	120,000 - 185,000
NFT mint (ERC-721)	80,000 - 150,000
OpenSea NFT purchase	150,000 - 300,000
Deploy simple contract	200,000 - 500,000

At 32 Gwei (30 base + 2 tip):

- Simple transfer: 0.000672 ETH ($1.34 at $2000/ETH)
- Uniswap swap: 0.004 ETH ($8 at $2000/ETH)
- Contract deploy: 0.016+ ETH ($32+ at $2000/ETH)

How Do Gas Refunds Work?

Refundable Actions:

- **SSTORE to zero:** 15,000 gas refund (after paying 5,000 to clear)
- **SELFDESTRUCT:** 24,000 gas refund (contract deletion)

Refund Cap (EIP-3529): Maximum refund: 20% of gas used (prevents exploitation)

```
function clearStorage() public {
    delete largeMapping[key1];  // 5,000 cost + 15,000 refund
    delete largeMapping[key2];  // 5,000 cost + 15,000 refund
    // Gas used: 10,000, Potential: 30,000 (capped at 2,000)
}
```

How Does the Blob Gas Market Work?

Ethereum now has TWO gas markets:

- **Execution gas**: Traditional EVM operations (existing market)
- **Blob gas**: Data availability for L2 rollups (new market)
- Markets operate independently with separate base fees

Blob Gas Mechanics:

- Target: 3 blobs per block (384 KB), Maximum: 6 blobs (768 KB)
- Blob gas price adjusts like EIP-1559 (targets 50% capacity)

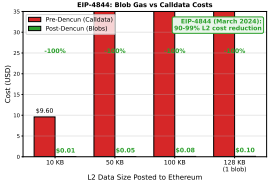
How Much Does EIP-4844 Save on Blob Gas?

Cost comparison for posting L2 data to Ethereum:

$122.88

$96.00

$48.00



Impact: 90-99% reduction in L2 transaction costs since Dencun upgrade

Problem Solved? Gas Mechanics

The Original Problem

How do we price scarce computation fairly?

How Gas Mechanics Solves It

- Gas units: Fixed costs per EVM operation
- EIP-1559: Dynamic base fee targets 50% blocks
- Base fee burning aligns incentives

Remaining Limitations

- Volatile fees during congestion (10x-100x spikes)
- MEV extraction undermines fairness

Open Questions

- Can fees be more predictable?
- Does it scale without L2 solutions?

Gas Mechanics partially solves fair pricing but introduces volatility and MEV trade-offs

(c) Joerg Osterrieder 2025

The Economics of Gas Mechanics

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Gas Mechanics

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Gas Mechanics

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

(c) Joerg Osterrieder 2025

Gas Estimation Gone Wrong

[COMIC: Developer confidently sets gas limit to "exactly what the estimator said." Transaction starts. Midway through, another user's transaction changes state. Original transaction reverts. Gas consumed anyway. Developer stares at "Out of Gas" error while $50 disappears. Caption: "The blockchain waits for no one."]

Key Insight:

- Gas estimation is a prediction, not a guarantee—state can change between estimation and execution
- Always add a buffer to gas limits; failed transactions still consume gas up to the failure point

In Web2, failed requests are free. In Web3, failure has a price.

Key Takeaways

1. **Gas Purpose:** Prevents spam/DoS, compensates validators, allocates block space
2. **EIP-1559:** Base fee (burned) + priority fee (to validator) for predictable pricing
3. **Base Fee Dynamics:** Adjusts up to 12.5% per block to target 50% full blocks
4. **Storage is Expensive:** SSTORE costs 20,000 gas (new) or 5,000 gas (update)
5. **Optimization:** Pack storage, use memory for temp data, batch operations
6. **EIP-4844:** Blob gas market reduced L2 costs by 90-99%

Next Lesson: L15 – Solidity Fundamentals

Discussion Questions

1. Why does EIP-1559 burn the base fee instead of giving it to validators?
2. If Ethereum's block gas limit is 30M and average block time is 12 seconds, what is the theoretical maximum transactions per second for simple ETH transfers?
3. Under what circumstances might a user set a very high max fee per gas?
4. How do Layer 2 solutions (e.g., Optimism, Arbitrum) reduce gas costs?
5. What are the tradeoffs between storing data on-chain vs using events vs off-chain storage?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L15 - Solidity Fundamentals

Coming up next:

- Introduction to Solidity programming language
- Data types: uint, address, string, arrays, mappings
- Functions, visibility modifiers, state mutability
- Events and error handling
- Inheritance and interfaces

Preparation:

- Install MetaMask browser extension
- Familiarize yourself with Remix IDE (remix.ethereum.org)
- Review basic programming concepts (if-else, loops, functions)

Quiz Questions (1/4)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei = 10^9 Wei, 1 ETH = 10^{18} Wei.

Q3. In the pre-EIP-1559 model, what was the transaction fee formula?
A) Gas Used + Gas Price B) Gas Used × Gas Price
C) Gas Limit × Gas Price D) Base Fee + Priority Fee
Answer: B – Transaction Fee = Gas Used × Gas Price (legacy).

Q4. What happens to the base fee in EIP-1559 transactions?
A) Sent to validators B) Burned (removed from circulation)
C) Returned to users D) Stored in treasury
Answer: B – EIP-1559 burns base fees to reduce ETH supply.

Q5. If a block is more than 50% full, how does the base fee change?
A) Decreases by 12.5% B) Stays the same C) Increases by up to 12.5% D) Doubles
Answer: C – Base fee increases when blocks exceed 50% capacity.

Quiz Questions (2/4)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q8. What is the difference between gas limit and gas used?
A) No difference B) Gas limit is max allowed, gas used is actual consumed
C) Gas limit is for validators only D) Gas used includes refunds
Answer: B – Gas limit is user-set cap; gas used is actual. Unused refunded.

Q9. In EIP-1559, the priority fee goes to:
A) The Ethereum Foundation B) The user as refund C) Validators D) Burned
Answer: C – Priority fee (tip) incentivizes validators to include transaction.

Q10. What is the target gas per block in Ethereum's EIP-1559 mechanism?
A) 10,000,000 B) 15,000,000 C) 30,000,000 D) 60,000,000
Answer: B – Target is 15M gas (50% of 30M block limit).

Quiz Questions (3/4)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000
Answer: C – Clearing storage (SSTORE to zero) refunds 15,000 gas (after 5,000 cost).

Q13. What is the maximum gas refund cap introduced by EIP-3529?
A) 10% of gas used B) 20% of gas used C) 50% of gas used D) No cap
Answer: B – EIP-3529 caps refunds at 20% of gas used to prevent exploitation.

Q14. Which transaction type typically uses the most gas?
A) Simple ETH transfer B) ERC-20 transfer C) Uniswap swap D) Contract deployment
Answer: D – Deploying contracts costs 200k-500k+ gas, far exceeding other operations.

Q15. What is the advantage of using event logs instead of storage?
A) Events are faster B) Events cost much less gas (375 vs 20,000)
C) Events are on-chain accessible D) No advantage
Answer: B – Events cost 375 gas + 8/byte vs 20,000+ for storage.

Quiz Questions (4/4)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs
Answer: B – Target is 3 blobs/block (384 KB), max 6 blobs (768 KB).

Q18. What optimization technique reduces gas by packing multiple values in one storage slot?
A) Memory arrays B) Packed storage C) Short-circuiting D) Event logging
Answer: B – Packing multiple small values into one uint256 slot saves SSTORE costs.

Q19. In a require statement with AND logic, which condition should come first?
A) Most expensive B) Cheapest (to short-circuit and save gas)
C) Random order D) Order doesn't matter
Answer: B – Place cheap checks first; if they fail, expensive operations are skipped.

Q20. If base fee is 30 Gwei, priority fee is 2 Gwei, and max fee is 50 Gwei, what is the effective gas price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective gas price = min(base + priority, max) = min(30+2, 50) = 32 Gwei.

L14: Gas Mechanics – Mini Lecture

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Explain what gas is and why Ethereum uses it
- Calculate transaction costs using gas price and gas limit
- Understand EIP-1559's base fee and priority fee mechanism
- Identify gas costs for different EVM operations

What is Gas?

Gas is a unit of computational effort in Ethereum:

- Measures the cost of executing operations on the EVM
- Prevents infinite loops and spam attacks
- Compensates validators for computation and storage

Three Critical Functions:

1. **Prevent DoS Attacks:** Without gas, infinite loops could halt the network
2. **Incentivize Validators:** Higher gas price = higher priority
3. **Resource Allocation:** Limited to 30M gas per block

Ether Denominations

Ether units from smallest to largest:

Unit	Wei Value	Typical Use
Wei	1	Smallest unit (like satoshi)
Gwei (Shannon)	10^9	Gas prices
Ether	10^{18}	Main unit

Key Relationship:

- 1 Gwei = 1,000,000,000 Wei (10^9)
- 1 ETH = 1,000,000,000,000,000,000 Wei (10^{18})
- Gas prices typically quoted in Gwei (e.g., 30 Gwei)

Gas Calculation: Pre-EIP-1559

Legacy Transaction Fee Model (before August 2021):
Formula:

$$\text{Transaction Fee} = \text{Gas Used} \times \text{Gas Price}$$

Example:

- Gas Used: 21,000 (simple ETH transfer)
- Gas Price: 50 Gwei (user-specified)
- Transaction Fee: $21{,}000 \times 50 = 1{,}050{,}000$ Gwei $= 0.00105$ ETH

Challenges:

- Users had to manually estimate gas price
- Overpaying was common to ensure inclusion

EIP-1559: London Hard Fork (August 2021)

Major overhaul of gas fee mechanism:

- **Base Fee:** Algorithmically determined, burned (removed from circulation)
- **Priority Fee (Tip):** User-specified tip to validator for inclusion
- **Max Fee:** Maximum gas price user is willing to pay

New Formula:

$$\text{Transaction Fee} = \text{Gas Used} \times (\text{Base Fee} + \text{Priority Fee})$$

Example: Gas 21,000 — Base 30 Gwei — Tip 2 Gwei

- Effective Price: 32 Gwei — Fee: 0.000672 ETH — Burned: 0.00063 ETH

Base Fee Adjustment Mechanism

Dynamic base fee targets 50% full blocks:

- Target gas per block: 15,000,000 (50% of 30M limit)
- If block $>$ 50% full: Base fee increases by max 12.5%
- If block $<$ 50% full: Base fee decreases by max 12.5%

Gas Limit vs Gas Used:

Gas Limit:

- Maximum gas transaction may consume
- Set by user, acts as safety cap
- Unused gas is refunded

Gas Used:

- Actual gas consumed
- Determined by operations executed
- Used for fee calculation

Gas Costs by Operation

Every EVM opcode has a fixed gas cost:

Operation	Description	Gas Cost
ADD, SUB, MUL	Arithmetic operations	3
SHA3 (Keccak-256)	Hash function	30 + 6/word
SLOAD (warm)	Load from storage	100
SLOAD (cold)	First access in tx	2,100
SSTORE (new)	Write to new slot	20,000
SSTORE (update)	Update existing	5,000

Key Insight: Storage operations (SSTORE, SLOAD) are by far the most expensive

Real-World Transaction Costs

Typical gas costs on Ethereum mainnet:

Transaction Type	Gas Used
Simple ETH transfer	21,000
ERC-20 token transfer	45,000 – 65,000
Uniswap V3 swap	120,000 – 185,000
NFT mint (ERC-721)	80,000 – 150,000
Deploy simple contract	200,000 – 500,000

At 32 Gwei (30 base + 2 tip) and $2000/ETH:

- Simple transfer: 0.000672 ETH ($1.34)
- Uniswap swap: 0.004 ETH ($8)
- Contract deploy: 0.016+ ETH ($32+)

EIP-4844: Blob Gas Market (Dencun Upgrade, March 2024)

Ethereum now has TWO gas markets:

- **Execution gas**: Traditional EVM operations (existing market)
- **Blob gas**: Data availability for L2 rollups (new market)
- Markets operate independently with separate base fees

Blob Gas Mechanics:

- Target: 3 blobs per block (384 KB), Maximum: 6 blobs (768 KB)
- Blob gas price adjusts like EIP-1559 (targets 50% capacity)

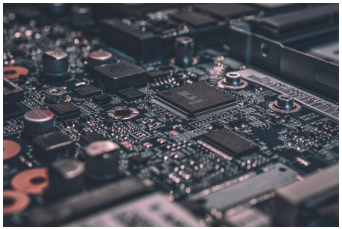
Impact: 90–99% reduction in L2 transaction costs since Dencun upgrade

Key Takeaways

1. **Gas Purpose:** Prevents spam/DoS, compensates validators, allocates block space
2. **EIP-1559:** Base fee (burned) + priority fee (to validator) for predictable pricing
3. **Base Fee Dynamics:** Adjusts up to 12.5% per block to target 50% full blocks
4. **Storage is Expensive:** SSTORE costs 20,000 gas (new) or 5,000 gas (update)
5. **EIP-4844:** Blob gas market reduced L2 costs by 90–99%

Image Credits

Fuel pump metaphor
Source: Unsplash (CC0)



Computational resources
Source: Unsplash (CC0)

Transaction costs
Source: Unsplash (CC0)

All images are CC0 licensed (public domain) from Unsplash.com

Quiz Questions (1/2)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei $= 10^9$ Wei, 1 ETH $= 10^{18}$ Wei.

Q3. What happens to the base fee in EIP-1559 transactions?
A) Sent to validators B) Burned (removed from circulation)
C) Returned to users D) Stored in treasury
Answer: B – EIP-1559 burns base fees to reduce ETH supply.

Q4. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Quiz Questions (2/2)

Q5. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q6. If a block is more than 50% full, how does the base fee change?
A) Decreases by 12.5% B) Stays the same C) Increases by up to 12.5% D) Doubles
Answer: C – Base fee increases when blocks exceed 50% capacity.

Q7. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

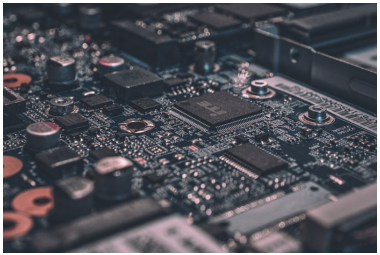
Q8. If base fee is 30 Gwei, priority fee is 2 Gwei, what is effective gas price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective gas price = base fee + priority fee = 30 + 2 = 32 Gwei.

L14: Gas Mechanics

Module B: Ethereum & Smart Contracts

Mini-Lecture — December 2025

Learning Objectives: Explain what gas is and why Ethereum uses it — Calculate transaction costs using gas price and gas limit — Understand EIP-1559's base fee and priority fee mechanism — Identify gas costs for different EVM operations



What is Gas?

Definition

Gas is a unit measuring computational effort required to execute operations on the Ethereum Virtual Machine (EVM).

Three Critical Functions:

1. **Prevent DoS Attacks:** Without gas, infinite loops halt network (attackers must pay)
2. **Incentivize Validators:** Higher gas price = higher priority (tip mechanism)
3. **Resource Allocation:** Limited to 30M gas per block (scarcity)

Gas decouples computation cost from ETH price volatility

(c) Joerg Osterrieder 2025

Ether Denominations and Fee Models

Ether Units:

Unit	Wei Value
Wei	1
Gwei	10^9 (gas prices)
Ether	10^{18}

Key: 1 ETH = 10^9 Gwei

Fee Evolution:

- **Pre-1559:** Gas × Price
- **EIP-1559:** Gas × (Base + Tip)

Legacy: 21,000 × 50 = 0.00105 ETH

EIP-1559: 21,000 × 32 = 0.000672 ETH

Gwei is the standard unit for gas prices – memorize this conversion

EIP-1559 Fee Components

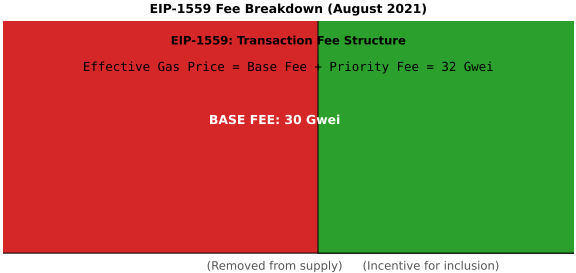
Three Components:

- **Base Fee:** Protocol-set, burned
- **Priority Fee:** User tip to validators
- **Max Fee:** Cap user will pay

Effective Price:

$$\min(\text{Base} + \text{Priority}, \text{Max})$$

Unused max fee is refunded



EIP-1559 burns base fee, making ETH potentially deflationary

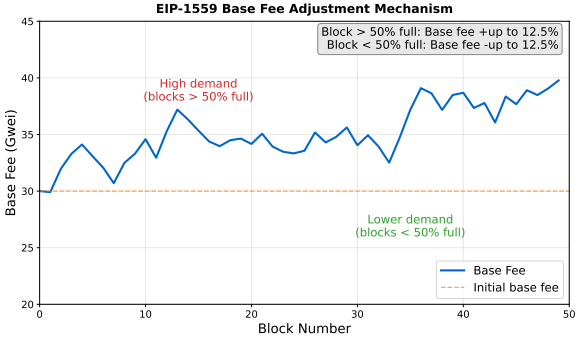
Base Fee Adjustment Mechanism

Dynamic Targeting:

- Target: 15M gas (50% of 30M)
- Block $>$ 50%: +12.5% max
- Block $<$ 50%: -12.5% max

Gas Limit vs Used:

- **Limit:** User-set max (refundable)
- **Used:** Actual consumption

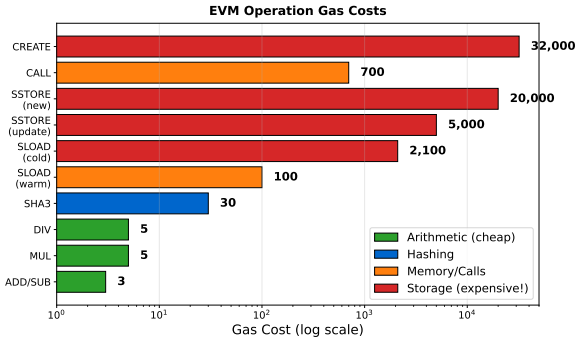


Base fee can 2x in about 20 blocks during high demand

Gas Costs by EVM Operation

Operation Costs:

Operation	Gas
ADD, SUB, MUL	3
SHA3 (Keccak)	30+
SLOAD (warm)	100
SLOAD (cold)	2,100
SSTORE (new)	20,000
SSTORE (update)	5,000



Storage is 6,600x more expensive than arithmetic – optimize storage first!

Real-World Costs and L2 Savings

Mainnet Gas Usage:

Transaction	Gas
ETH transfer	21,000
ERC-20 transfer	45-65K
Uniswap swap	120-185K
Contract deploy	200-500K

At 32 Gwei: transfer=$1.34, swap=$8

EIP-4844 Blob Gas (Mar 2024):

- Execution gas: EVM ops
- Blob gas: L2 data
- Target: 3 blobs/block

Impact: 90-99% L2 cost reduction

Optimism/Base now under $0.01

Dencun upgrade made L2s the practical choice for most users

Key Takeaways

1. **Gas Purpose:** Prevents spam/DoS, compensates validators, allocates scarce block space
2. **EIP-1559:** Base fee (burned) + priority fee (to validator) = predictable, deflationary
3. **Base Fee Dynamics:** Adjusts $\pm 12.5\%$/block targeting 50% full (15M of 30M gas)
4. **Storage Dominates Costs:** SSTORE at 20,000 gas is 6,600$\times$ arithmetic operations

Bottom Line: Gas is Ethereum's anti-spam mechanism that makes every computation cost-transparent – optimize storage operations for 90%+ of gas savings.

(c) Joerg Osterrieder 2025

Concrete Examples: Making It Real

Real Transaction (Dec 2025)

- Hash: `0x1a2b...f9e8`
- Gas Used: 21,000 (ETH transfer)
- Base Fee: 28.5 Gwei
- Priority Fee: 1.5 Gwei
- Total Cost: 0.00063 ETH ($1.26)

Uniswap Swap Example

- Gas Used: 152,847
- At 30 Gwei: 0.00458 ETH ($9.16)
- During congestion (100 Gwei): $30+

Storage Cost Comparison

- 1 SSTORE (new): 20,000 gas = $1.28
- 3 SSTOREs: 60,000 gas = $3.84
- Packed (1 slot): 20,000 gas = $1.28
- **Savings: 67%**

L2 Post-Dencun (Dec 2025)

- Optimism swap: $0.005
- Arbitrum transfer: $0.002
- Base transfer: $0.001

All data verified Dec 2025 — Sources: Etherscan, L2Beat, DefiLlama

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) Make transactions expensive B) Prevent spam and compensate validators
C) Create scarcity D) Replace Ether

Quiz Questions (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) Make transactions expensive B) Prevent spam and compensate validators
C) Create scarcity D) Replace Ether
Answer: B – Gas prevents DoS attacks and incentivizes validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}

Quiz Questions (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) Make transactions expensive B) Prevent spam and compensate validators
C) Create scarcity D) Replace Ether
Answer: B – Gas prevents DoS attacks and incentivizes validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 ETH = 10^9 Gwei = 10^{18} Wei.

Q3. What happens to the base fee in EIP-1559?
A) Sent to validators B) Burned C) Returned to users D) Treasury

Quiz Questions (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) Make transactions expensive B) Prevent spam and compensate validators
C) Create scarcity D) Replace Ether
Answer: B – Gas prevents DoS attacks and incentivizes validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 ETH = 10^9 Gwei = 10^{18} Wei.

Q3. What happens to the base fee in EIP-1559?
A) Sent to validators B) Burned C) Returned to users D) Treasury
Answer: B – Base fee is burned, reducing ETH supply.

Q4. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000

Quiz Questions (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) Make transactions expensive B) Prevent spam and compensate validators
C) Create scarcity D) Replace Ether
Answer: B – Gas prevents DoS attacks and incentivizes validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 ETH = 10^9 Gwei = 10^{18} Wei.

Q3. What happens to the base fee in EIP-1559?
A) Sent to validators B) Burned C) Returned to users D) Treasury
Answer: B – Base fee is burned, reducing ETH supply.

Q4. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple transfers cost exactly 21,000 gas.

Q5. Which EVM operation is most expensive?
A) ADD B) SHA3 C) SLOAD D) SSTORE

Quiz Questions (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) Make transactions expensive B) Prevent spam and compensate validators
C) Create scarcity D) Replace Ether
Answer: B – Gas prevents DoS attacks and incentivizes validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 ETH = 10^9 Gwei = 10^{18} Wei.

Q3. What happens to the base fee in EIP-1559?
A) Sent to validators B) Burned C) Returned to users D) Treasury
Answer: B – Base fee is burned, reducing ETH supply.

Q4. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple transfers cost exactly 21,000 gas.

Q5. Which EVM operation is most expensive?
A) ADD B) SHA3 C) SLOAD D) SSTORE
Answer: D – SSTORE costs 20,000 gas (new slot).

Quiz Questions (6–10)

Q6. If block is >50% full, base fee changes by:
A) -12.5% B) No change C) +12.5% max D) Doubles

Quiz Questions (6–10)

Q6. If block is >50% full, base fee changes by:
A) -12.5% B) No change C) +12.5% max D) Doubles
Answer: C – Base fee increases up to 12.5% per block.

Q7. What does EIP-4844 introduce?
A) Higher block limit B) Blob gas market C) Free txs D) PoW return

Quiz Questions (6–10)

Q6. If block is >50% full, base fee changes by:
A) -12.5% B) No change C) +12.5% max D) Doubles
Answer: C – Base fee increases up to 12.5% per block.

Q7. What does EIP-4844 introduce?
A) Higher block limit B) Blob gas market C) Free txs D) PoW return
Answer: B – EIP-4844 (Dencun) adds blob gas for L2 data.

Q8. Base fee 30 Gwei + priority 2 Gwei = effective price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei

Quiz Questions (6–10)

Q6. If block is >50% full, base fee changes by:
A) -12.5% B) No change C) +12.5% max D) Doubles
Answer: C – Base fee increases up to 12.5% per block.

Q7. What does EIP-4844 introduce?
A) Higher block limit B) Blob gas market C) Free txs D) PoW return
Answer: B – EIP-4844 (Dencun) adds blob gas for L2 data.

Q8. Base fee 30 Gwei + priority 2 Gwei = effective price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective = Base + Priority = 32 Gwei.

Q9. Cold SLOAD costs how much gas?
A) 100 B) 700 C) 2,100 D) 5,000

Quiz Questions (6–10)

Q6. If block is >50% full, base fee changes by:
A) -12.5% B) No change C) +12.5% max D) Doubles
Answer: C – Base fee increases up to 12.5% per block.

Q7. What does EIP-4844 introduce?
A) Higher block limit B) Blob gas market C) Free txs D) PoW return
Answer: B – EIP-4844 (Dencun) adds blob gas for L2 data.

Q8. Base fee 30 Gwei + priority 2 Gwei = effective price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective = Base + Priority = 32 Gwei.

Q9. Cold SLOAD costs how much gas?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – First access (cold) costs 2,100; subsequent (warm) 100.

Q10. Target gas per block in EIP-1559?
A) 10M B) 15M C) 30M D) 60M

Quiz Questions (6–10)

Q6. If block is >50% full, base fee changes by:
A) -12.5% B) No change C) +12.5% max D) Doubles
Answer: C – Base fee increases up to 12.5% per block.

Q7. What does EIP-4844 introduce?
A) Higher block limit B) Blob gas market C) Free txs D) PoW return
Answer: B – EIP-4844 (Dencun) adds blob gas for L2 data.

Q8. Base fee 30 Gwei + priority 2 Gwei = effective price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective = Base + Priority = 32 Gwei.

Q9. Cold SLOAD costs how much gas?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – First access (cold) costs 2,100; subsequent (warm) 100.

Q10. Target gas per block in EIP-1559?
A) 10M B) 15M C) 30M D) 60M
Answer: B – Target is 15M gas (50% of 30M block limit).

Next Steps and Resources

Explore Further:

- **Etherscan Gas Tracker:** Real-time gas prices and trends
- **L2Beat.com:** Compare L2 costs and security
- **EIP-1559 Visualization:** ultrasound.money (ETH burn tracking)

Practice:

- Check gas for your next transaction on Etherscan
- Compare mainnet vs L2 costs for same operation
- Watch base fee fluctuate during network congestion

Next Lesson: L15 Solidity Fundamentals – Learn to write gas-efficient smart contracts with proper storage patterns, packed variables, and optimization techniques.

(c) Joerg Osterrieder 2025

Quiz: Gas Mechanics

Instructions: Multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether

Quiz (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}

Quiz (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei $= 10^9$ Wei, 1 ETH $= 10^{18}$ Wei.

Q3. In the pre-EIP-1559 model, what was the transaction fee formula?
A) Gas Used + Gas Price B) Gas Used $\times$ Gas Price
C) Gas Limit $\times$ Gas Price D) Base Fee + Priority Fee

Quiz (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei $= 10^9$ Wei, 1 ETH $= 10^{18}$ Wei.

Q3. In the pre-EIP-1559 model, what was the transaction fee formula?
A) Gas Used + Gas Price B) Gas Used $\times$ Gas Price
C) Gas Limit $\times$ Gas Price D) Base Fee + Priority Fee
Answer: B – Transaction Fee = Gas Used $\times$ Gas Price (legacy).

Q4. What happens to the base fee in EIP-1559 transactions?
A) Sent to validators B) Burned (removed from circulation)
C) Returned to users D) Stored in treasury

Quiz (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei $= 10^9$ Wei, 1 ETH $= 10^{18}$ Wei.

Q3. In the pre-EIP-1559 model, what was the transaction fee formula?
A) Gas Used + Gas Price B) Gas Used $\times$ Gas Price
C) Gas Limit $\times$ Gas Price D) Base Fee + Priority Fee
Answer: B – Transaction Fee = Gas Used $\times$ Gas Price (legacy).

Q4. What happens to the base fee in EIP-1559 transactions?
A) Sent to validators B) Burned (removed from circulation)
C) Returned to users D) Stored in treasury
Answer: B – EIP-1559 burns base fees to reduce ETH supply.

Q5. If a block is more than 50% full, how does the base fee change?
A) Decreases by 12.5% B) Stays the same C) Increases by up to 12.5% D) Doubles

Quiz (1–5)

Q1. What is the primary purpose of gas in Ethereum?
A) To make transactions expensive B) To prevent spam and compensate validators
C) To create scarcity D) To replace Ether
Answer: B – Gas prevents DoS attacks and compensates validators.

Q2. How many Gwei are in 1 Ether?
A) 10^6 B) 10^9 C) 10^{12} D) 10^{18}
Answer: B – 1 Gwei $= 10^9$ Wei, 1 ETH $= 10^{18}$ Wei.

Q3. In the pre-EIP-1559 model, what was the transaction fee formula?
A) Gas Used + Gas Price B) Gas Used $\times$ Gas Price
C) Gas Limit $\times$ Gas Price D) Base Fee + Priority Fee
Answer: B – Transaction Fee = Gas Used $\times$ Gas Price (legacy).

Q4. What happens to the base fee in EIP-1559 transactions?
A) Sent to validators B) Burned (removed from circulation)
C) Returned to users D) Stored in treasury
Answer: B – EIP-1559 burns base fees to reduce ETH supply.

Q5. If a block is more than 50% full, how does the base fee change?
A) Decreases by 12.5% B) Stays the same C) Increases by up to 12.5% D) Doubles
Answer: C – Base fee increases when blocks exceed 50% capacity.

Quiz (6–10)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000

Quiz (6–10)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q8. What is the difference between gas limit and gas used?
A) No difference B) Gas limit is max allowed, gas used is actual consumed
C) Gas limit is for validators only D) Gas used includes refunds

Quiz (6–10)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q8. What is the difference between gas limit and gas used?
A) No difference B) Gas limit is max allowed, gas used is actual consumed
C) Gas limit is for validators only D) Gas used includes refunds
Answer: B – Gas limit is user-set cap; gas used is actual. Unused refunded.

Q9. In EIP-1559, the priority fee goes to:
A) The Ethereum Foundation B) The user as refund C) Validators D) Burned

Quiz (6–10)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q8. What is the difference between gas limit and gas used?
A) No difference B) Gas limit is max allowed, gas used is actual consumed
C) Gas limit is for validators only D) Gas used includes refunds
Answer: B – Gas limit is user-set cap; gas used is actual. Unused refunded.

Q9. In EIP-1559, the priority fee goes to:
A) The Ethereum Foundation B) The user as refund C) Validators D) Burned
Answer: C – Priority fee (tip) incentivizes validators to include transaction.

Q10. What is the target gas per block in Ethereum's EIP-1559 mechanism?
A) 10,000,000 B) 15,000,000 C) 30,000,000 D) 60,000,000

Quiz (6–10)

Q6. What is the gas cost for a simple ETH transfer?
A) 10,000 B) 21,000 C) 45,000 D) 100,000
Answer: B – Simple ETH transfers cost exactly 21,000 gas.

Q7. Which EVM operation is the most expensive?
A) ADD (arithmetic) B) SHA3 (hashing) C) SLOAD (read storage) D) SSTORE (write storage)
Answer: D – SSTORE costs 20,000 gas (new) or 5,000 gas (update).

Q8. What is the difference between gas limit and gas used?
A) No difference B) Gas limit is max allowed, gas used is actual consumed
C) Gas limit is for validators only D) Gas used includes refunds
Answer: B – Gas limit is user-set cap; gas used is actual. Unused refunded.

Q9. In EIP-1559, the priority fee goes to:
A) The Ethereum Foundation B) The user as refund C) Validators D) Burned
Answer: C – Priority fee (tip) incentivizes validators to include transaction.

Q10. What is the target gas per block in Ethereum's EIP-1559 mechanism?
A) 10,000,000 B) 15,000,000 C) 30,000,000 D) 60,000,000
Answer: B – Target is 15M gas (50% of 30M block limit).

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000

Quiz (11–15)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000

Quiz (11–15)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000
Answer: C – Clearing storage (SSTORE to zero) refunds 15,000 gas (after 5,000 cost).

Q13. What is the maximum gas refund cap introduced by EIP-3529?
A) 10% of gas used B) 20% of gas used C) 50% of gas used D) No cap

Quiz (11–15)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000
Answer: C – Clearing storage (SSTORE to zero) refunds 15,000 gas (after 5,000 cost).

Q13. What is the maximum gas refund cap introduced by EIP-3529?
A) 10% of gas used B) 20% of gas used C) 50% of gas used D) No cap
Answer: B – EIP-3529 caps refunds at 20% of gas used to prevent exploitation.

Q14. Which transaction type typically uses the most gas?
A) Simple ETH transfer B) ERC-20 transfer C) Uniswap swap D) Contract deployment

Quiz (11–15)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000
Answer: C – Clearing storage (SSTORE to zero) refunds 15,000 gas (after 5,000 cost).

Q13. What is the maximum gas refund cap introduced by EIP-3529?
A) 10% of gas used B) 20% of gas used C) 50% of gas used D) No cap
Answer: B – EIP-3529 caps refunds at 20% of gas used to prevent exploitation.

Q14. Which transaction type typically uses the most gas?
A) Simple ETH transfer B) ERC-20 transfer C) Uniswap swap D) Contract deployment
Answer: D – Deploying contracts costs 200k-500k+ gas, far exceeding other operations.

Q15. What is the advantage of using event logs instead of storage?
A) Events are faster B) Events cost much less gas (375 vs 20,000)
C) Events are on-chain accessible D) No advantage

Quiz (11–15)

Q11. What is the gas cost for a cold SLOAD (first storage read in a transaction)?
A) 100 B) 700 C) 2,100 D) 5,000
Answer: C – Cold SLOAD costs 2,100 gas; warm costs 100 gas (EIP-2929).

Q12. How much gas refund does setting a storage slot to zero provide?
A) 5,000 B) 10,000 C) 15,000 D) 20,000
Answer: C – Clearing storage (SSTORE to zero) refunds 15,000 gas (after 5,000 cost).

Q13. What is the maximum gas refund cap introduced by EIP-3529?
A) 10% of gas used B) 20% of gas used C) 50% of gas used D) No cap
Answer: B – EIP-3529 caps refunds at 20% of gas used to prevent exploitation.

Q14. Which transaction type typically uses the most gas?
A) Simple ETH transfer B) ERC-20 transfer C) Uniswap swap D) Contract deployment
Answer: D – Deploying contracts costs 200k-500k+ gas, far exceeding other operations.

Q15. What is the advantage of using event logs instead of storage?
A) Events are faster B) Events cost much less gas (375 vs 20,000)
C) Events are on-chain accessible D) No advantage
Answer: B – Events cost 375 gas + 8/byte vs 20,000+ for storage.

Quiz (16–20)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return

Quiz (16–20)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs

Quiz (16–20)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs
Answer: B – Target is 3 blobs/block (384 KB), max 6 blobs (768 KB).

Q18. What optimization technique reduces gas by packing multiple values in one storage slot?
A) Memory arrays B) Packed storage C) Short-circuiting D) Event logging

Quiz (16–20)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs
Answer: B – Target is 3 blobs/block (384 KB), max 6 blobs (768 KB).

Q18. What optimization technique reduces gas by packing multiple values in one storage slot?
A) Memory arrays B) Packed storage C) Short-circuiting D) Event logging
Answer: B – Packing multiple small values into one uint256 slot saves SSTORE costs.

Q19. In a require statement with AND logic, which condition should come first?
A) Most expensive B) Cheapest (to short-circuit and save gas)
C) Random order D) Order doesn't matter

Quiz (16–20)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs
Answer: B – Target is 3 blobs/block (384 KB), max 6 blobs (768 KB).

Q18. What optimization technique reduces gas by packing multiple values in one storage slot?
A) Memory arrays B) Packed storage C) Short-circuiting D) Event logging
Answer: B – Packing multiple small values into one uint256 slot saves SSTORE costs.

Q19. In a require statement with AND logic, which condition should come first?
A) Most expensive B) Cheapest (to short-circuit and save gas)
C) Random order D) Order doesn't matter
Answer: B – Place cheap checks first; if they fail, expensive operations are skipped.

Q20. If base fee is 30 Gwei, priority fee is 2 Gwei, and max fee is 50 Gwei, what is the effective gas price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What does EIP-4844 introduce to Ethereum?
A) Higher block gas limit B) Blob gas market for L2 data
C) Free transactions D) Proof-of-Work return
Answer: B – EIP-4844 (Dencun, March 2024) adds blob gas market for L2 data.

Q17. How many blobs does EIP-4844 target per block?
A) 1 blob B) 3 blobs C) 6 blobs D) 12 blobs
Answer: B – Target is 3 blobs/block (384 KB), max 6 blobs (768 KB).

Q18. What optimization technique reduces gas by packing multiple values in one storage slot?
A) Memory arrays B) Packed storage C) Short-circuiting D) Event logging
Answer: B – Packing multiple small values into one uint256 slot saves SSTORE costs.

Q19. In a require statement with AND logic, which condition should come first?
A) Most expensive B) Cheapest (to short-circuit and save gas)
C) Random order D) Order doesn't matter
Answer: B – Place cheap checks first; if they fail, expensive operations are skipped.

Q20. If base fee is 30 Gwei, priority fee is 2 Gwei, and max fee is 50 Gwei, what is the effective gas price?
A) 30 Gwei B) 32 Gwei C) 50 Gwei D) 2 Gwei
Answer: B – Effective gas price = min(base + priority, max) = min(30+2, 50) = 32 Gwei.

(c) Joerg Osterrieder 2025

L15: Solidity Fundamentals

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Describe Solidity's role as a smart contract language
- Declare and use fundamental data types (uint, address, bool, string, bytes)
- Write functions with appropriate visibility and state mutability modifiers
- Implement events for logging and monitoring
- Use mappings and arrays for data storage
- Apply inheritance and interfaces

(c) Joerg Osterrieder 2025

The Problem: How do we write bug-free financial code?

The Challenge
Smart contracts handle billions of dollars in value, yet bugs are irreversible once deployed. Unlike traditional software, there's no "update" button—a single logic error can drain funds permanently.

Why It Matters

- Smart contract bugs are publicly exploitable by anyone monitoring the blockchain
- Historical losses: The DAO ($60M, 2016), Parity multisig freeze ($280M, 2017), Poly Network ($611M, 2021)

Today's lesson: How Solidity Fundamentals addresses this challenge

What We Need

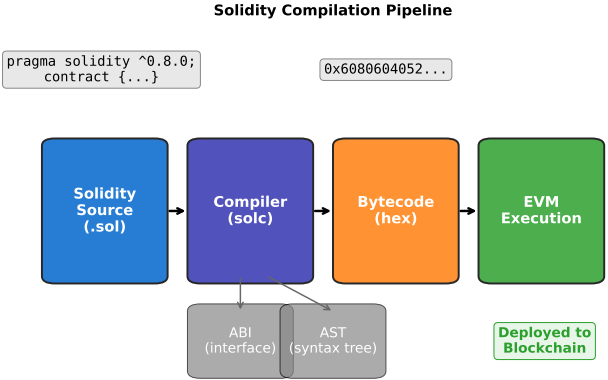
- Risk management and mitigation
- Language features that prevent common vulnerability patterns (reentrancy, integer overflow, access control failures)

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

What is Solidity?

Solidity is a statically-typed, contract-oriented programming language:

- Created specifically for Ethereum smart contracts
- Syntax similar to JavaScript/C++, compiles to EVM bytecode
- Current stable version: 0.8.x (as of 2025)



Basic Contract Structure

Every Solidity file starts with a version pragma:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract HelloWorld {
    string public message;

    constructor(string memory initialMessage) {
        message = initialMessage;
    }

    function setMessage(string memory newMessage) public {
        message = newMessage;
    }

    function getMessage() public view returns (string memory) {
        return message;
    }
}
```

Key Elements: License identifier, pragma, contract declaration, state variables, constructor, functions

SPDX License and Version Pragma

Required at top of every Solidity file:
Common Licenses:

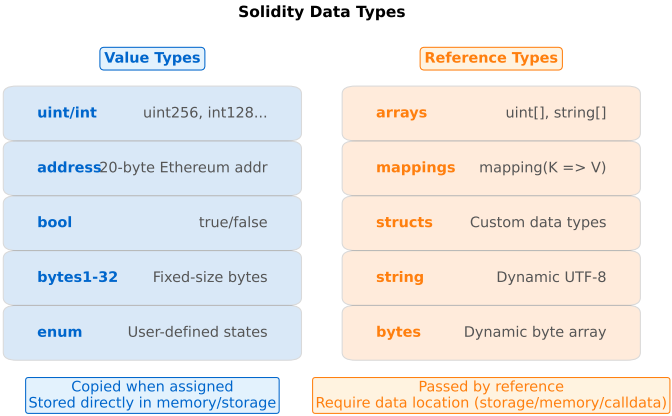
- **MIT:** Permissive open-source license
- **GPL-3.0:** Copyleft license (derivatives must be open-source)
- **UNLICENSED:** Proprietary code

Version Pragma:

- `pragma solidity ^0.8.0;` - Compatible with 0.8.0 to 0.8.x
- `pragma solidity >=0.8.0 <0.9.0;` - Range specification
- `pragma solidity 0.8.20;` - Exact version

Data Types Overview

Solidity has two categories of data types:



Value Types: Integers and Booleans

Integers:

- `uint` (unsigned): 0 to $2^{256} - 1$ (alias for `uint256`)
- `int` (signed): -2^{255} to $2^{255} - 1$ (alias for `int256`)
- Sized variants: `uint8, uint16, ..., uint256`

Booleans:

- `bool`: `true` or `false`
- Operators: `!` (not), `&&` (and), `||` (or)

```
contract Types {
    uint256 public largeNumber = 1000000000000000000;  // 1e18
    uint8 public smallNumber = 255;  // Max value for uint8
    int256 public signedNumber = -42;
    bool public isActive = true;
}
```

Value Types: Address

Address type holds 20-byte Ethereum addresses:

- `address`: Basic address type
- `address payable`: Can receive Ether via `transfer()` or `send()`

Address Members:

- `<address>.balance`: Returns Ether balance (in Wei)
- `<address payable>.transfer(uint amount)`: Send Ether, reverts on failure

```
contract AddressExample {
    address public owner;
    address payable public recipient;

    constructor() {
        owner = msg.sender;  // Address of contract deployer
        recipient = payable(msg.sender);  // Convert to payable
    }

    function checkBalance() public view returns (uint) {
        return owner.balance;  // Balance in Wei
    }
}
```

Reference Types: Arrays

Fixed-Size Arrays:

```
uint[5] public fixedArray;  // Array of 5 uints
```

Dynamic Arrays:

```
uint[] public dynamicArray;
string[] public names;

function addElement(uint value) public {
    dynamicArray.push(value);  // Append to array
}

function getLength() public view returns (uint) {
    return dynamicArray.length;
}

function removeLastElement() public {
    dynamicArray.pop();  // Remove last element
}
```

Reference Types: Mappings

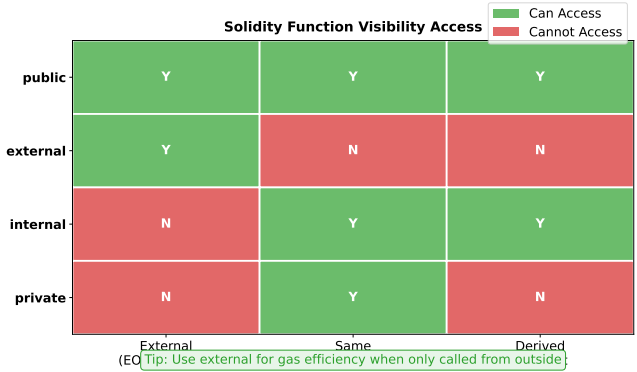
Key-value storage (like hash tables):

```
contract MappingExample {
    // Mapping from address to balance
    mapping(address => uint256) public balances;

    // Nested mapping (address to address to allowance)
    mapping(address => mapping(address => uint256)) public allowances;

    function updateBalance(address account, uint256 amount) public {
        balances[account] = amount;
    }

    function getBalance(address account) public view returns (uint256) {
        return balances[account];  // Returns 0 if key doesn't exist
    }
}
```

Key Properties: All keys exist with default value, cannot iterate, only in storage

Functions: Visibility Modifiers

Four visibility levels determine who can call a function:



Functions: State Mutability

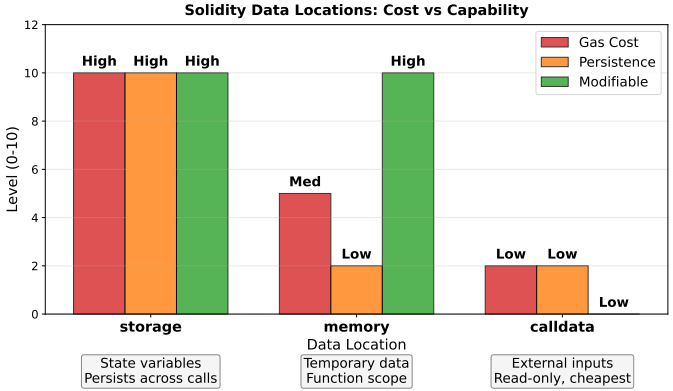
Three state mutability levels:

1. **view:** Reads state but doesn't modify it (no gas when called off-chain)
2. **pure:** Doesn't read or modify state
3. **(none):** Can read and modify state (always costs gas)

```
contract Mutability {
    uint public value = 10;

    function getValue() public view returns (uint) {
        return value;  // Reads state (view)
    }

    function add(uint a, uint b) public pure returns (uint) {
        return a + b;  // No state access (pure)
    }

    function setValue(uint newValue) public {
        value = newValue;  // Modifies state (no modifier)
    }
}
```

Data Locations: storage vs memory vs calldata

Reference types require explicit data location:



Events

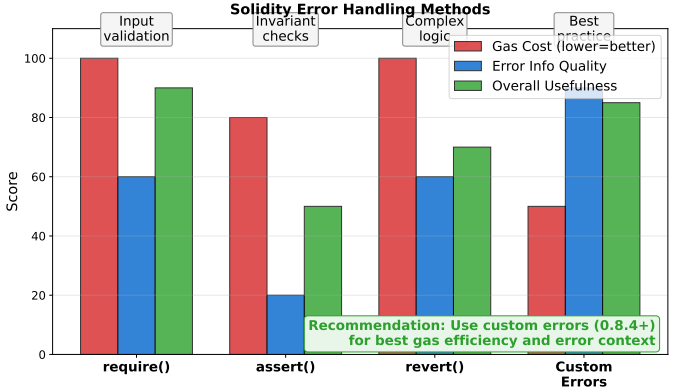
Events enable logging for off-chain monitoring:

```
contract EventExample {
    event Transfer(address indexed from, address indexed to, uint256 amount);
    event Approval(address indexed owner, address indexed spender, uint256 amount);

    mapping(address => uint256) public balances;

    function transfer(address to, uint256 amount) public {
        require(balances[msg.sender] >= amount, "Insufficient balance");
        balances[msg.sender] -= amount;
        balances[to] += amount;
        emit Transfer(msg.sender, to, amount);  // Emit event
    }
}
```

Indexed Parameters: Up to 3 parameters can be `indexed` for efficient filtering

Error Handling Methods

Solidity provides multiple error handling mechanisms:



Error Handling: require, assert, revert

1. **require(condition, message):** Validate inputs/conditions, refunds gas
2. **assert(condition):** Check invariants (should never fail)
3. **revert(message):** Unconditional revert with message

```
function transfer(address to, uint amount) public {
    require(to != address(0), "Cannot transfer to zero address");
    require(balances[msg.sender] >= amount, "Insufficient balance");

    balances[msg.sender] -= amount;
    balances[to] += amount;

    assert(balances[msg.sender] + balances[to] == totalSupply);  // Invariant
}
```

Custom Errors (Solidity 0.8.4+)

More gas-efficient than string error messages:

```
contract CustomErrors {
    error InsufficientBalance(uint requested, uint available);
    error Unauthorized(address caller);

    address public owner;

    function withdraw(uint amount) public {
        if (msg.sender != owner) {
            revert Unauthorized(msg.sender);
        }
        if (balances[msg.sender] < amount) {
            revert InsufficientBalance(amount, balances[msg.sender]);
        }
        // ... transfer logic
    }
}
```

Benefits: Lower gas cost, typed parameters, better error context

Modifiers

Reusable code for function preconditions:

```
contract ModifierExample {
    address public owner;
    bool public paused = false;

    constructor() { owner = msg.sender; }

    modifier onlyOwner() {
        require(msg.sender == owner, "Not the owner");
        _;  // Placeholder for function body
    }

    modifier whenNotPaused() {
        require(!paused, "Contract is paused");
        _;
    }

    function pause() public onlyOwner { paused = true; }
    function unpause() public onlyOwner { paused = false; }

    function criticalFunction() public onlyOwner whenNotPaused {
        // Only owner can call, and only when not paused
    }
}
```

Inheritance

Solidity supports multiple inheritance:

```
contract Ownable {
    address public owner;
    constructor() { owner = msg.sender; }
    modifier onlyOwner() {
        require(msg.sender == owner, "Not owner");
        _;
    }
}

contract Pausable is Ownable {
    bool public paused;
    function pause() public onlyOwner { paused = true; }
}

contract MyContract is Pausable {
    function doSomething() public onlyOwner {
        // Inherits owner, onlyOwner, paused, pause()
    }
}
```

Key: `is` for inheritance, `virtual`/`override` for polymorphism

Interfaces

Define contract structure without implementation:

```
interface IERC20 {
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address to, uint256 amount) external returns (bool);
    event Transfer(address indexed from, address indexed to, uint256 value);
}

contract MyToken is IERC20 {
    mapping(address => uint256) private _balances;
    uint256 private _totalSupply;

    function totalSupply() public view override returns (uint256) {
        return _totalSupply;
    }
    // ... implement other functions
}
```

Problem Solved? Solidity Fundamentals

The Original Problem

How do we write bug-free financial code?

How Solidity Fundamentals Solves It

- Static typing catches type mismatches at compile time (e.g., can't send ETH to non-payable address)
- Visibility modifiers enforce access control patterns (onlyOwner prevents unauthorized actions)
- State mutability (view/pure) prevents accidental state changes in read-only functions

Remaining Limitations

- No formal verification by default—compiler doesn't prove absence of logic bugs
- Tooling maturity lags traditional languages (limited IDE support, debuggers)

Open Questions

- Will formal verification tools (Certora, K Framework) become standard for high-value contracts?
- Risk: Black swan events (0-day compiler bugs), cascading failures (reentrancy across protocols)

Solidity Fundamentals partially solves "we write bug-free financial code" but introduces new trade-offs

Key Takeaways

1. **Solidity Basics:** Statically-typed language compiling to EVM bytecode
2. **Data Types:** Value types (uint, address, bool) vs reference types (arrays, mappings)
3. **Visibility:** public, external, internal, private determine access
4. **State Mutability:** view (read-only), pure (no state), default (modify)
5. **Data Locations:** storage (persistent), memory (temp), calldata (cheapest)
6. **Error Handling:** Use custom errors (0.8.4+) for gas efficiency

Discussion Questions

1. Why is `string` more expensive than `bytes32` for storing short text?
2. When should you use `external` vs `public` for function visibility?
3. Why can't you iterate over a mapping's keys in Solidity?
4. What are the tradeoffs between events vs state variables for historical records?
5. How does the `indexed` keyword in events affect gas costs and queryability?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L16 - Lab: Contract Interaction

Coming up next (hands-on lab):

- Introduction to Remix IDE
- Deploying SimpleStorage contract
- Interacting with deployed contracts
- Using MetaMask with test networks
- Deploying to Sepolia testnet

Preparation:

- Install MetaMask browser extension
- Create Ethereum account and save recovery phrase
- Get Sepolia testnet ETH from faucet

Quiz: Questions 1-5

Q1. What is the maximum value that can be stored in a uint8 variable?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is an 8-bit unsigned integer with range 0 to $2^8 - 1 = 255$.

Q2. Which data type should be used for an Ethereum address that needs to receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive Ether via transfer() or send().

Q3. What does the "view" state mutability modifier indicate?
A) Function can modify state B) Function cannot read or modify state
C) Function reads state but cannot modify it D) Function is only visible internally
Answer: C – view functions read state without modifying it, consuming no gas when called off-chain.

Q4. Which visibility modifier allows a function to be called ONLY from within the same contract?
A) public B) external C) internal D) private
Answer: D – private functions can only be called from within the same contract, not from derived contracts.

Q5. What is the default value for an uninitialized mapping entry?
A) null B) undefined C) Zero/default value of the value type D) Throws an error
Answer: C – All keys in a mapping exist with their type's default value (0 for uint, false for bool, etc.).

Quiz: Questions 6-10

Q6. Which error handling method should be used to check invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors and invariant checking; it should never fail in correct code.

Q7. What is the purpose of the constructor in a Solidity contract?
A) To destroy the contract B) To initialize state variables when contract is deployed
C) To create new instances of the contract D) To define contract visibility
Answer: B – The constructor runs once during deployment to initialize state variables.

Q8. Which data location is the cheapest for function parameters in terms of gas?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest because data is not copied into memory.

Q9. How many parameters in an event can be marked as "indexed" for efficient filtering?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 parameters can be indexed in an event for efficient off-chain filtering.

Q10. What does the underscore (_) represent in a modifier?
A) A comment marker B) A private variable prefix
C) Placeholder for the function body D) An unused parameter
Answer: C – The underscore is replaced by the modified function's body during execution.

Quiz: Questions 11-15

Q11. Which keyword is used to inherit from another contract?
A) extends B) implements C) is D) inherits
Answer: C – Solidity uses "is" for inheritance (e.g., contract MyToken is ERC20).

Q12. What is the difference between "pure" and "view" functions?
A) pure is faster than view B) pure cannot read state, view can read but not modify
C) pure is for external calls only D) No difference, they are aliases
Answer: B – pure functions access no state variables; view functions read but don't modify state.

Q13. Which of the following is TRUE about mappings in Solidity?
A) They can be iterated like arrays B) They are stored in memory
C) All possible keys exist with default values D) They have a length property
Answer: C – Mappings have no concept of undefined keys; all keys map to their type's default value.

Q14. What is the recommended error handling method in Solidity 0.8.4+ for gas efficiency?
A) String-based require() B) Custom errors with revert
C) assert() for all checks D) try-catch blocks
Answer: B – Custom errors are more gas-efficient than string error messages in require().

Q15. Which visibility modifier allows external contracts to call a function but NOT internal calls?
A) public B) external C) internal D) private
Answer: B – external functions can only be called from outside the contract, saving gas for calldata.

Quiz: Questions 16-20

Q16. What is the size of the address type in Solidity?
A) 16 bytes B) 20 bytes C) 32 bytes D) 40 bytes
Answer: B – Ethereum addresses are 20 bytes (160 bits) long.

Q17. Which method is used to add an element to a dynamic array?
A) append() B) add() C) push() D) insert()
Answer: C – push() appends an element to the end of a dynamic array.

Q18. What happens when a function marked "view" attempts to modify state?
A) Compilation warning B) Compilation error
C) Runtime error D) State modification is ignored
Answer: B – Solidity compiler will reject code where view functions attempt state modifications.

Q19. Which of the following can be declared in an interface?
A) State variables B) Function implementations
C) Function signatures only D) Constructors
Answer: C – Interfaces can only declare function signatures, events, and errors, not implementations or state.

Q20. What is the purpose of the "memory" keyword for reference types?
A) Optimize for low memory usage B) Indicate temporary storage during function execution
C) Enable garbage collection D) Allow dynamic resizing
Answer: B – memory indicates data is stored temporarily during function execution, not persisted to blockchain.

L15: Solidity Fundamentals

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Hello World Pride

[COMIC: Developer beaming with pride shows laptop screen with "contract HelloWorld { string public message = 'Hello!'; }" to friends. One friend asks "So it stores one word... for how much?" Developer's pride deflates as they mumble "...twenty thousand gas."]

Frame the Concept:

- Your first smart contract feels magical—code that controls real value on a global network
- But Solidity has unique constraints: immutability, gas costs, and security implications

Every Solidity developer's journey begins with Hello World and ends with reentrancy nightmares

Learning Objectives

By the end of this lesson, you will be able to:

- Describe Solidity's role as a smart contract language
- Declare and use fundamental data types (uint, address, bool, string, bytes)
- Write functions with appropriate visibility and state mutability modifiers
- Implement events for logging and monitoring
- Use mappings and arrays for data storage
- Apply inheritance and interfaces

Building on L14: Gas Mechanics

The Problem: How do we write bug-free financial code?

The Challenge
Smart contracts handle billions of dollars in value, yet bugs are irreversible once deployed. Unlike traditional software, there's no "update" button—a single logic error can drain funds permanently.

Why It Matters

- Smart contract bugs are publicly exploitable by anyone monitoring the blockchain
- Historical losses: The DAO ($60M, 2016), Parity multisig freeze ($280M, 2017), Poly Network ($611M, 2021)

What We Need

- Risk management and mitigation
- Language features that prevent common vulnerability patterns (reentrancy, integer overflow, access control failures)

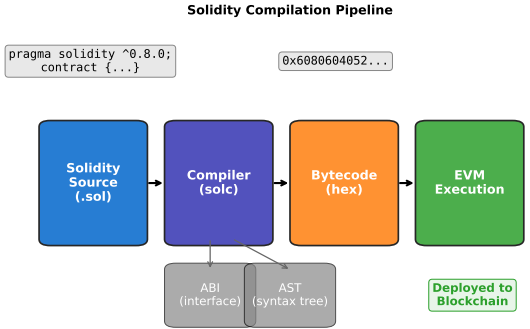
The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Solidity Fundamentals addresses this challenge

How Does Solidity Enable Smart Contracts?

Solidity is a statically-typed (variable types fixed at compile time, catching type errors early), contract-oriented programming language:

- Created specifically for Ethereum smart contracts
- Syntax similar to JavaScript/C++, compiles to EVM bytecode
- Current stable version: 0.8.x (as of 2025)



→ *Solidity's static typing catches errors at compile time, before deployment*

What Is the Basic Contract Structure?

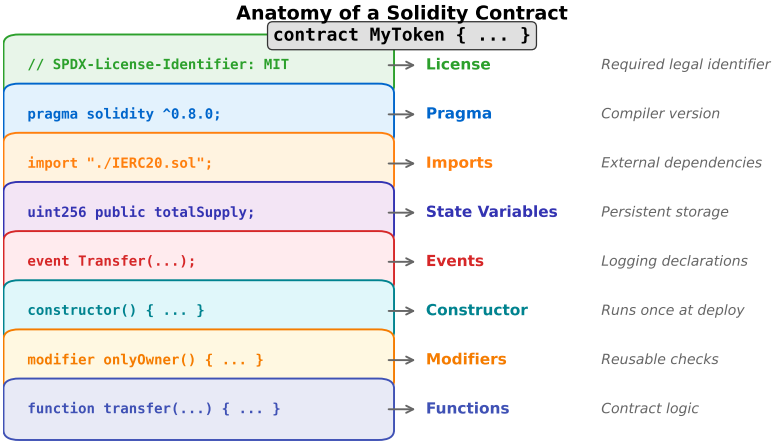
Every Solidity file starts with a version pragma:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract HelloWorld {
    string public message;

    constructor(string memory initialMessage) {
        message = initialMessage;
    }

    function setMessage(string memory newMessage) public {
        message = newMessage;
    }

    function getMessage() public view returns (string memory) {
        return message;
    }
}
```

Key Elements: License identifier, pragma, contract declaration, state variables, constructor, functions

How Is a Solidity Contract Organized?

Structure of a Solidity contract from top to bottom:



Order matters: License > Pragma > Imports > State > Events > Constructor > Modifiers > Functions

What Are SPDX Licenses and Version Pragmas?

Required at top of every Solidity file:
Common Licenses:

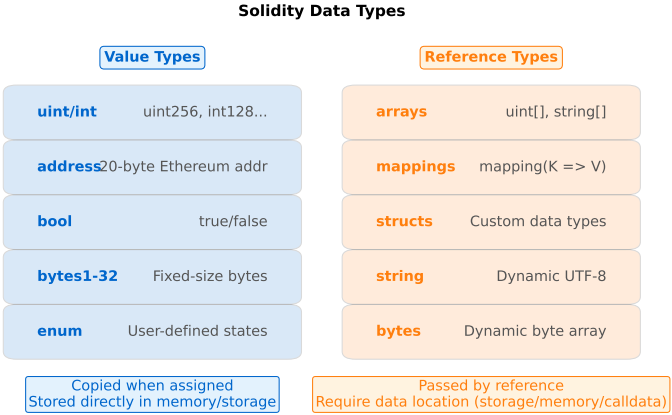
- **MIT:** Permissive open-source license
- **GPL-3.0:** Copyleft license (derivatives must be open-source)
- **UNLICENSED:** Proprietary code

Version Pragma:

- `pragma solidity ^0.8.0;` - Compatible with 0.8.0 to 0.8.x
- `pragma solidity >=0.8.0 <0.9.0;` - Range specification
- `pragma solidity 0.8.20;` - Exact version

What Data Types Does Solidity Support?

Solidity has two categories of data types:



What Are Integer and Boolean Value Types?

Integers:

- `uint` (unsigned): 0 to $2^{256} - 1$ (alias for `uint256`)
- `int` (signed): -2^{255} to $2^{255} - 1$ (alias for `int256`)
- Sized variants: `uint8, uint16, ..., uint256`

Booleans:

- `bool`: `true` or `false`
- Operators: `!` (not), `&&` (and), `||` (or)

```
contract Types {
    uint256 public largeNumber = 1000000000000000000;  // 1e18
    uint8 public smallNumber = 255;  // Max value for uint8
    int256 public signedNumber = -42;
    bool public isActive = true;
}
```

→ *Problem: How do we write bug-free financial code? — Value Types: Integers and Booleans Static typing prevents overflow bugs: Solidity 0.8+ reverts on overflow instead of wrapping*

What Is the Address Type?

Address type holds 20-byte Ethereum addresses:

- `address`: Basic address type
- `address payable`: Can receive Ether via `transfer()` or `send()`

Address Members:

- `<address>.balance`: Returns Ether balance (in Wei)
- `<address payable>.transfer(uint amount)`: Send Ether, reverts on failure

```
contract AddressExample {
    address public owner;
    address payable public recipient;

    constructor() {
        owner = msg.sender;  // Address of contract deployer
        recipient = payable(msg.sender);  // Convert to payable
    }

    function checkBalance() public view returns (uint) {
        return owner.balance;  // Balance in Wei
    }
}
```

How Do Arrays Work in Solidity?

Fixed-Size Arrays:

```
uint[5] public fixedArray;  // Array of 5 uints
```

Dynamic Arrays:

```
uint[] public dynamicArray;
string[] public names;

function addElement(uint value) public {
    dynamicArray.push(value);  // Append to array
}

function getLength() public view returns (uint) {
    return dynamicArray.length;
}

function removeLastElement() public {
    dynamicArray.pop();  // Remove last element
}
```

How Do Mappings Work in Solidity?

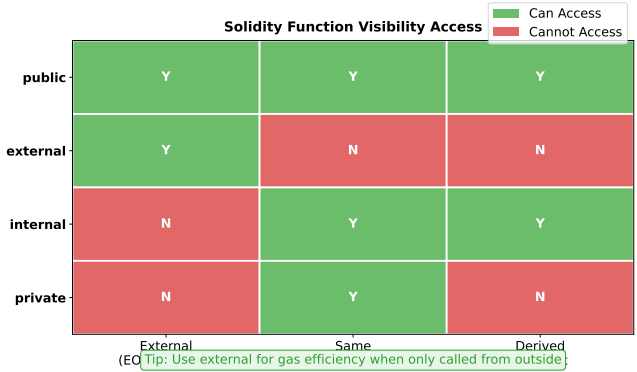
Key-value storage (like hash tables):

```
contract MappingExample {
    // Mapping from address to balance
    mapping(address => uint256) public balances;

    // Nested mapping (address to address to allowance)
    mapping(address => mapping(address => uint256)) public allowances;

    function updateBalance(address account, uint256 amount) public {
        balances[account] = amount;
    }

    function getBalance(address account) public view returns (uint256) {
        return balances[account];  // Returns 0 if key doesn't exist
    }
}
```

Key Properties: All keys exist with default value, cannot iterate, only in storage

How Do Visibility Modifiers Control Access?

Four visibility levels determine who can call a function:



Problem Check-In: Solidity Fundamentals

Recall Our Problem

How do we write bug-free financial code?

What We've Learned So Far

- Static typing catches type mismatches at compile time (before deployment)
- Visibility modifiers (public/private/internal/external) control who can call functions
- Compile-time checks + access control = fewer bugs in immutable financial code

Still to Address

- How do error handling mechanisms (require/assert/revert) prevent runtime bugs?
- How would YOU design a language for bug-free financial code?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we write bug-free financial code?"?

What Are State Mutability Modifiers?

Three state mutability levels:

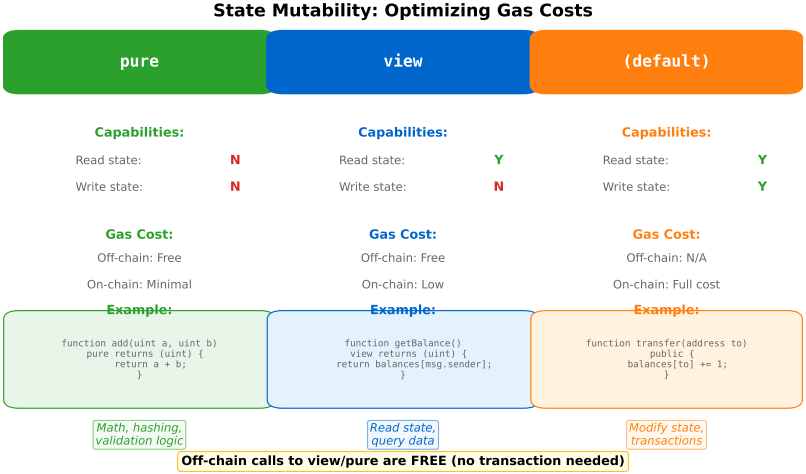
1. **view:** Reads state but doesn't modify it (no gas when called off-chain)
2. **pure:** Doesn't read or modify state
3. **(none):** Can read and modify state (always costs gas)

```
contract Mutability {
    uint public value = 10;

    function getValue() public view returns (uint) {
        return value;  // Reads state (view)
    }

    function add(uint a, uint b) public pure returns (uint) {
        return a + b;  // No state access (pure)
    }

    function setValue(uint newValue) public {
        value = newValue;  // Modifies state (no modifier)
    }
}
```

→ *Problem: How do we write bug-free financial code? — Functions: State Mutability State mutability (view/pure) prevents accidental state changes in read-only functions*

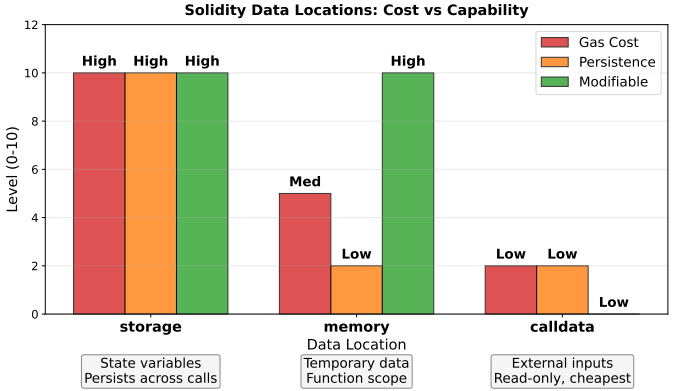
How Do State Mutability Levels Compare?

Choosing the right mutability saves gas:



Where Is Data Stored During Execution?

Reference types require explicit data location:



How Do Events Enable Logging?

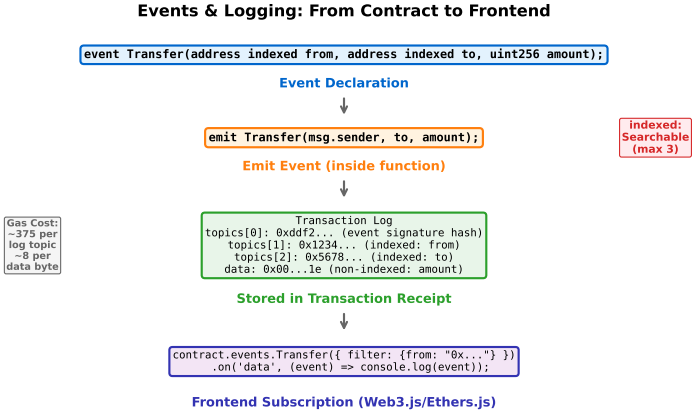
Events enable logging for off-chain monitoring:

```
contract EventExample {
    event Transfer(address indexed from, address indexed to, uint256 amount);
    event Approval(address indexed owner, address indexed spender, uint256 amount);

    mapping(address => uint256) public balances;

    function transfer(address to, uint256 amount) public {
        require(balances[msg.sender] >= amount, "Insufficient balance");
        balances[msg.sender] -= amount;
        balances[to] += amount;
        emit Transfer(msg.sender, to, amount);  // Emit event
    }
}
```

Indexed Parameters: Up to 3 parameters can be `indexed` (searchable in event logs, max 3 per event) for efficient filtering

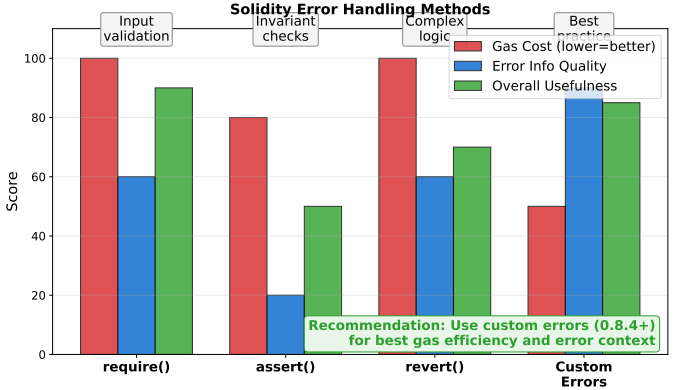
How Do Events Flow from Contract to Frontend?

How events connect on-chain activity to off-chain applications:



How Does Solidity Handle Errors?

Solidity provides multiple error handling mechanisms:



How Do require, assert, and revert Work?

1. **require(condition, message):** Validate inputs/conditions, refunds gas
2. **assert(condition):** Check invariants (should never fail)
3. **revert(message):** Unconditional revert with message

```
function transfer(address to, uint amount) public {
    require(to != address(0), "Cannot transfer to zero address");
    require(balances[msg.sender] >= amount, "Insufficient balance");

    balances[msg.sender] -= amount;
    balances[to] += amount;

    assert(balances[msg.sender] + balances[to] == totalSupply);  // Invariant
}
```

→ Problem: How do we write bug-free financial code? — Error Handling: require, assert, revert require() validates inputs, assert() checks invariants, revert() with custom errors saves gas

How Do Custom Errors Save Gas?

More gas-efficient than string error messages:

```
contract CustomErrors {
    error InsufficientBalance(uint requested, uint available);
    error Unauthorized(address caller);

    address public owner;

    function withdraw(uint amount) public {
        if (msg.sender != owner) {
            revert Unauthorized(msg.sender);
        }
        if (balances[msg.sender] < amount) {
            revert InsufficientBalance(amount, balances[msg.sender]);
        }
        // ... transfer logic
    }
}
```

Benefits: Lower gas cost, typed parameters, better error context

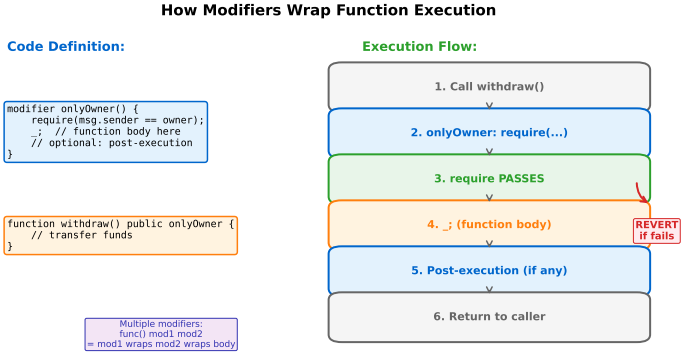
What Are Modifiers and How Do They Work?

Reusable code for function preconditions:

```
contract ModifierExample {
    address public owner;
    bool public paused = false;

    constructor() { owner = msg.sender; }

    modifier onlyOwner() {
        require(msg.sender == owner, "Not the owner");
        _;  // Placeholder for function body
    }

    modifier whenNotPaused() {
        require(!paused, "Contract is paused");
        _;
    }

    function pause() public onlyOwner { paused = true; }
    function unpause() public onlyOwner { paused = false; }

    function criticalFunction() public onlyOwner whenNotPaused {
        // Only owner can call, and only when not paused
    }
}
```

How Does Modifier Execution Flow Work?

How modifiers wrap and control function execution:



How Does Inheritance Work in Solidity?

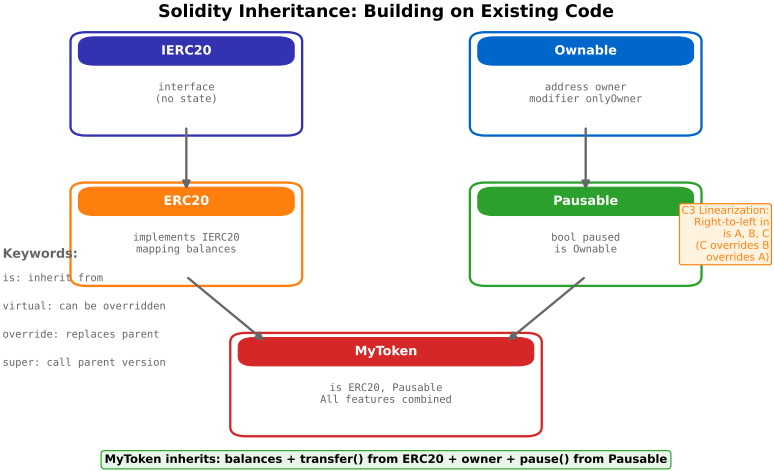
Solidity supports multiple inheritance:

```
contract Ownable {
    address public owner;
    constructor() { owner = msg.sender; }
    modifier onlyOwner() {
        require(msg.sender == owner, "Not owner");
        _;
    }
}

contract Pausable is Ownable {
    bool public paused;
    function pause() public onlyOwner { paused = true; }
}

contract MyContract is Pausable {
    function doSomething() public onlyOwner {
        // Inherits owner, onlyOwner, paused, pause()
    }
}
```

Key: `is` for inheritance, `virtual`/`override` for polymorphism

How Do Inheritance Hierarchies Build Contracts?

Building contracts by combining existing code:



What Are Interfaces and Why Use Them?

Define contract structure without implementation:

```
interface IERC20 {
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address to, uint256 amount) external returns (bool);
    event Transfer(address indexed from, address indexed to, uint256 value);
}

contract MyToken is IERC20 {
    mapping(address => uint256) private _balances;
    uint256 private _totalSupply;

    function totalSupply() public view override returns (uint256) {
        return _totalSupply;
    }
    // ... implement other functions
}
```

Problem Solved? Solidity Fundamentals

The Original Problem

How do we write bug-free financial code?

How Solidity Fundamentals Solves It

- Static typing catches type mismatches at compile time (e.g., can't send ETH to non-payable address)
- Visibility modifiers enforce access control patterns (onlyOwner prevents unauthorized actions)
- State mutability (view/pure) prevents accidental state changes in read-only functions

Remaining Limitations

- No formal verification by default—compiler doesn't prove absence of logic bugs
- Tooling maturity lags traditional languages (limited IDE support, debuggers)

Open Questions

- Will formal verification tools (Certora, K Framework) become standard for high-value contracts?
- Risk: Black swan events (0-day compiler bugs), cascading failures (reentrancy across protocols)

Solidity Fundamentals partially solves "we write bug-free financial code" but introduces new trade-offs

The Economics of Solidity Fundamentals

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Solidity Fundamentals

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Solidity Fundamentals

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Compiler Error Frustration

[COMIC: Developer has written 200 lines of Solidity. Hits compile. Screen fills with red: "TypeError: Member 'balances' not found or not visible." "DeclarationError: Identifier already declared." "ParserError: Expected ';' but got '}'." Developer's coffee cup is empty. Clock shows 3 AM.]

Key Insight:

- Solidity's strict compiler is your friend—it catches bugs before deployment, not after
- Every compiler error you fix is a potential $1M exploit you avoided

Red errors at compile time beat red transactions on mainnet

Key Takeaways

1. **Solidity Basics:** Statically-typed language compiling to EVM bytecode
2. **Data Types:** Value types (uint, address, bool) vs reference types (arrays, mappings)
3. **Visibility:** public, external, internal, private determine access
4. **State Mutability:** view (read-only), pure (no state), default (modify)
5. **Data Locations:** storage (persistent), memory (temp), calldata (cheapest)
6. **Error Handling:** Use custom errors (0.8.4+) for gas efficiency

Next Lesson: L16 – Lab: Contract Interaction

Discussion Questions

1. Why is `string` more expensive than `bytes32` for storing short text?
2. When should you use `external` vs `public` for function visibility?
3. Why can't you iterate over a mapping's keys in Solidity?
4. What are the tradeoffs between events vs state variables for historical records?
5. How does the `indexed` keyword in events affect gas costs and queryability?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L16 - Lab: Contract Interaction

Coming up next (hands-on lab):

- Introduction to Remix IDE
- Deploying SimpleStorage contract
- Interacting with deployed contracts
- Using MetaMask with test networks
- Deploying to Sepolia testnet

Preparation:

- Install MetaMask browser extension
- Create Ethereum account and save recovery phrase
- Get Sepolia testnet ETH from faucet

Quiz: Questions 1-5

Q1. What is the maximum value that can be stored in a uint8 variable?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is an 8-bit unsigned integer with range 0 to $2^8 - 1 = 255$.

Q2. Which data type should be used for an Ethereum address that needs to receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive Ether via transfer() or send().

Q3. What does the "view" state mutability modifier indicate?
A) Function can modify state B) Function cannot read or modify state
C) Function reads state but cannot modify it D) Function is only visible internally
Answer: C – view functions read state without modifying it, consuming no gas when called off-chain.

Q4. Which visibility modifier allows a function to be called ONLY from within the same contract?
A) public B) external C) internal D) private
Answer: D – private functions can only be called from within the same contract, not from derived contracts.

Q5. What is the default value for an uninitialized mapping entry?
A) null B) undefined C) Zero/default value of the value type D) Throws an error
Answer: C – All keys in a mapping exist with their type's default value (0 for uint, false for bool, etc.).

Quiz: Questions 6-10

Q6. Which error handling method should be used to check invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors and invariant checking; it should never fail in correct code.

Q7. What is the purpose of the constructor in a Solidity contract?
A) To destroy the contract B) To initialize state variables when contract is deployed
C) To create new instances of the contract D) To define contract visibility
Answer: B – The constructor runs once during deployment to initialize state variables.

Q8. Which data location is the cheapest for function parameters in terms of gas?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest because data is not copied into memory.

Q9. How many parameters in an event can be marked as "indexed" for efficient filtering?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 parameters can be indexed in an event for efficient off-chain filtering.

Q10. What does the underscore (_) represent in a modifier?
A) A comment marker B) A private variable prefix
C) Placeholder for the function body D) An unused parameter
Answer: C – The underscore is replaced by the modified function's body during execution.

Quiz: Questions 11-15

Q11. Which keyword is used to inherit from another contract?
A) extends B) implements C) is D) inherits
Answer: C – Solidity uses "is" for inheritance (e.g., contract MyToken is ERC20).

Q12. What is the difference between "pure" and "view" functions?
A) pure is faster than view B) pure cannot read state, view can read but not modify
C) pure is for external calls only D) No difference, they are aliases
Answer: B – pure functions access no state variables; view functions read but don't modify state.

Q13. Which of the following is TRUE about mappings in Solidity?
A) They can be iterated like arrays B) They are stored in memory
C) All possible keys exist with default values D) They have a length property
Answer: C – Mappings have no concept of undefined keys; all keys map to their type's default value.

Q14. What is the recommended error handling method in Solidity 0.8.4+ for gas efficiency?
A) String-based require() B) Custom errors with revert
C) assert() for all checks D) try-catch blocks
Answer: B – Custom errors are more gas-efficient than string error messages in require().

Q15. Which visibility modifier allows external contracts to call a function but NOT internal calls?
A) public B) external C) internal D) private
Answer: B – external functions can only be called from outside the contract, saving gas for calldata.

Quiz: Questions 16-20

Q16. What is the size of the address type in Solidity?
A) 16 bytes B) 20 bytes C) 32 bytes D) 40 bytes
Answer: B – Ethereum addresses are 20 bytes (160 bits) long.

Q17. Which method is used to add an element to a dynamic array?
A) append() B) add() C) push() D) insert()
Answer: C – push() appends an element to the end of a dynamic array.

Q18. What happens when a function marked "view" attempts to modify state?
A) Compilation warning B) Compilation error
C) Runtime error D) State modification is ignored
Answer: B – Solidity compiler will reject code where view functions attempt state modifications.

Q19. Which of the following can be declared in an interface?
A) State variables B) Function implementations
C) Function signatures only D) Constructors
Answer: C – Interfaces can only declare function signatures, events, and errors, not implementations or state.

Q20. What is the purpose of the "memory" keyword for reference types?
A) Optimize for low memory usage B) Indicate temporary storage during function execution
C) Enable garbage collection D) Allow dynamic resizing
Answer: B – memory indicates data is stored temporarily during function execution, not persisted to blockchain.

L15: Solidity Fundamentals

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

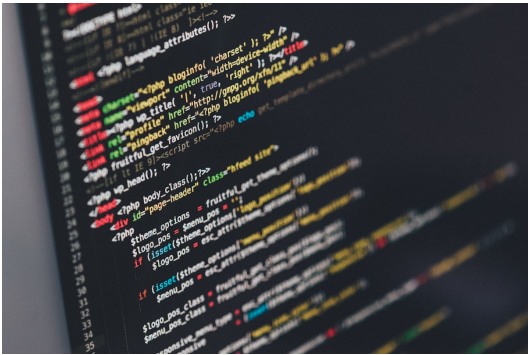
By the end of this mini-lecture, you will be able to:

- Understand Solidity's role as Ethereum's smart contract language
- Declare and use fundamental data types (uint, address, bool, mappings)
- Write functions with appropriate visibility and state mutability modifiers
- Apply error handling with require, assert, and custom errors

What is Solidity?

Solidity is a statically-typed, contract-oriented programming language:

- Created specifically for Ethereum smart contracts
- Syntax similar to JavaScript/C++, compiles to EVM bytecode
- Current stable version: 0.8.x (as of December 2025)



Basic Contract Structure

Every Solidity file starts with a version pragma:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract HelloWorld {
    string public message;

    constructor(string memory initialMessage) {
        message = initialMessage;
    }

    function setMessage(string memory newMessage) public {
        message = newMessage;
    }

    function getMessage() public view returns (string memory) {
        return message;
    }
}
```

Key Elements: License identifier, pragma, contract declaration, state variables, constructor, functions

Core Data Types

Solidity has two categories of data types:

Value Types:

- `uint256`: Unsigned integers (0 to $2^{256} - 1$)
- `int256`: Signed integers
- `bool`: true or false
- `address`: 20-byte Ethereum address
- `address payable`: Can receive Ether

Reference Types:

- `string`: UTF-8 text (dynamic)
- `bytes`: Raw byte data
- `arrays`: Fixed or dynamic size
- `mapping`: Key-value storage
- `struct`: Custom composite types

Note: Reference types require explicit data location (storage, memory, calldata)

Mappings: Key-Value Storage

Mappings are hash tables for efficient key-value storage:

```
contract MappingExample {
    // Mapping from address to balance
    mapping(address => uint256) public balances;

    // Nested mapping (address -> address -> allowance)
    mapping(address => mapping(address => uint256)) public allowances;

    function updateBalance(address account, uint256 amount) public {
        balances[account] = amount;
    }

    function getBalance(address account) public view returns (uint256) {
        return balances[account];  // Returns 0 if key doesn't exist
    }
}
```

Key Properties: All keys exist with default value, cannot iterate, only in storage

Function Visibility Modifiers

Four visibility levels determine who can call a function:

Visibility	Contract	Derived	External	Use Case
`public`	Yes	Yes	Yes	General access
`external`	No	No	Yes	Gas-efficient API
`internal`	Yes	Yes	No	Inheritance-based
`private`	Yes	No	No	Contract-only

State Mutability:

- `view`: Reads state but doesn't modify (no gas when called off-chain)
- `pure`: Doesn't read or modify state (for calculations)
- `(none)`: Can read and modify state (always costs gas)

Events for Logging

Events enable off-chain monitoring and indexing:

```
contract EventExample {
    event Transfer(address indexed from, address indexed to, uint256 amount);
    event Approval(address indexed owner, address indexed spender, uint256 amount);

    mapping(address => uint256) public balances;

    function transfer(address to, uint256 amount) public {
        require(balances[msg.sender] >= amount, "Insufficient balance");
        balances[msg.sender] -= amount;
        balances[to] += amount;
        emit Transfer(msg.sender, to, amount);  // Emit event
    }
}
```

Indexed Parameters: Up to 3 parameters can be `indexed` for efficient filtering by dApps

Error Handling

Three primary error handling mechanisms:

1. **require(condition, message):** Validate inputs/conditions, refunds remaining gas
2. **assert(condition):** Check invariants that should never fail
3. **Custom Errors (0.8.4+):** Gas-efficient alternative to string messages

```
error InsufficientBalance(uint requested, uint available);

function withdraw(uint amount) public {
    require(amount > 0, "Amount must be positive");

    if (balances[msg.sender] < amount) {
        revert InsufficientBalance(amount, balances[msg.sender]);
    }

    balances[msg.sender] -= amount;
    assert(totalSupply >= balances[msg.sender]);  // Invariant check
}
```

Modifiers and Inheritance

Modifiers are reusable code for function preconditions:

```
contract Ownable {
    address public owner;
    constructor() { owner = msg.sender; }

    modifier onlyOwner() {
        require(msg.sender == owner, "Not the owner");
        _;  // Placeholder for function body
    }
}

contract MyContract is Ownable {  // Inheritance with 'is'
    bool public paused;

    function pause() public onlyOwner {
        paused = true;  // Only owner can call
    }
}
```

Key: Use `virtual`/`override` for polymorphism, `is` for inheritance

Key Takeaways

1. **Solidity Basics:** Statically-typed language compiling to EVM bytecode
2. **Data Types:** Value types (uint, address, bool) vs reference types (arrays, mappings)
3. **Visibility:** public, external, internal, private determine function access
4. **State Mutability:** view (read-only), pure (no state), default (can modify)
5. **Error Handling:** Use custom errors (0.8.4+) for gas efficiency
6. **Best Practice:** Use modifiers for access control, events for logging

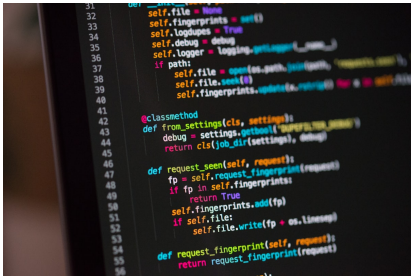


Image Credits

All images are used under the Unsplash License (free for commercial and non-commercial use):

- **Code Screen Image:** Ilya Pavlov via Unsplash
  `https://unsplash.com/photos/OqtafYT5kTw`
- **Programming Image:** Florian Olivo via Unsplash
  `https://unsplash.com/photos/4hbJ-eymZ1o`
- **Blockchain/Ethereum Image:** Shubham Dhage via Unsplash
  `https://unsplash.com/photos/T9rKvI3NONM`

Unsplash License: Free to use, no attribution required, modification allowed.

Quiz: Questions 1-5

Q1. What is the maximum value that can be stored in a uint8 variable?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is an 8-bit unsigned integer with range 0 to $2^8 - 1 = 255$.

Q2. Which data type should be used for an Ethereum address that needs to receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive Ether via transfer() or send().

Q3. What does the "view" state mutability modifier indicate?
A) Function can modify state B) Function cannot read or modify state
C) Function reads state but cannot modify it D) Function is only visible internally
Answer: C – view functions read state without modifying it.

Q4. Which visibility modifier allows a function to be called ONLY from within the same contract?
A) public B) external C) internal D) private
Answer: D – private functions can only be called from within the same contract.

Q5. What is the default value for an uninitialized mapping entry?
A) null B) undefined C) Zero/default value of the value type D) Throws an error
Answer: C – All keys in a mapping exist with their type's default value.

Quiz: Questions 6-10

Q6. Which error handling method should be used to check invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors and invariant checking.

Q7. What is the purpose of the constructor in a Solidity contract?
A) To destroy the contract B) To initialize state variables when contract is deployed
C) To create new instances of the contract D) To define contract visibility
Answer: B – The constructor runs once during deployment to initialize state.

Q8. Which data location is the cheapest for function parameters in terms of gas?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest because data is not copied.

Q9. How many parameters in an event can be marked as "indexed"?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 parameters can be indexed for efficient filtering.

Q10. What does the underscore (_) represent in a modifier?
A) A comment marker B) A private variable prefix
C) Placeholder for the function body D) An unused parameter
Answer: C – The underscore is replaced by the modified function's body.

L15: Solidity Fundamentals

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

January 2026

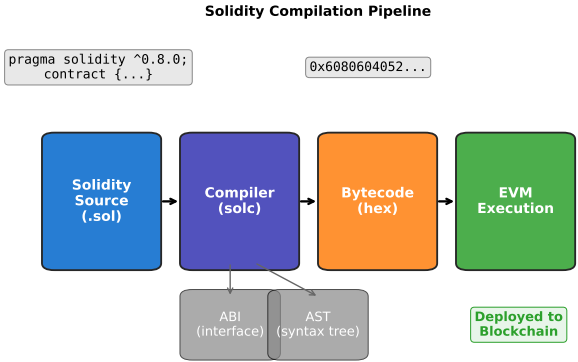
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

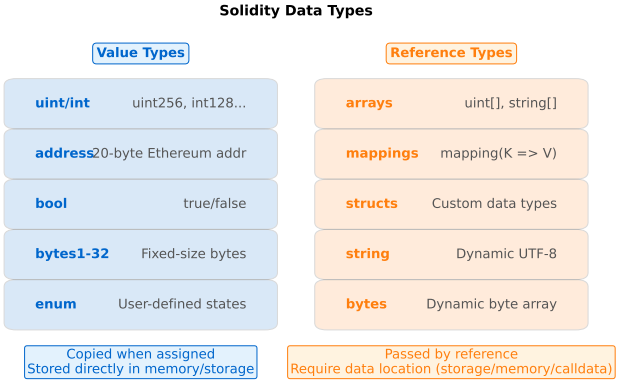
- Describe Solidity's role as a smart contract language
- Use fundamental data types (uint, address, bool, mappings)
- Apply visibility and state mutability modifiers
- Implement events, error handling, and modifiers

What is Solidity?



Statically-typed, contract-oriented language compiling to EVM bytecode.

Data Types Overview



Value types: uint, int, bool, address — **Reference types:** arrays, mappings, structs

Key Data Types

Integers:

- `uint256`: 0 to $2^{256} - 1$ (default `uint`)
- `int256`: -2^{255} to $2^{255} - 1$
- Sized variants: `uint8, uint16, ..., uint256`

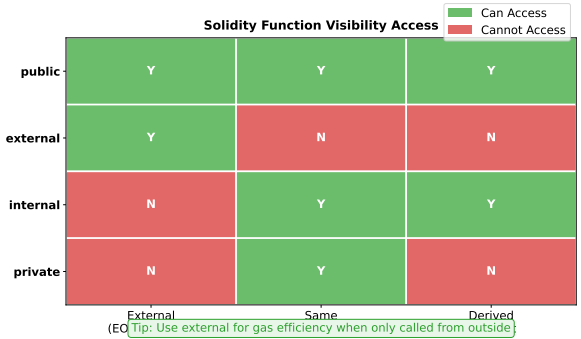
Address:

- `address`: 20-byte Ethereum address
- `address payable`: Can receive ETH via `transfer()`

Mappings:

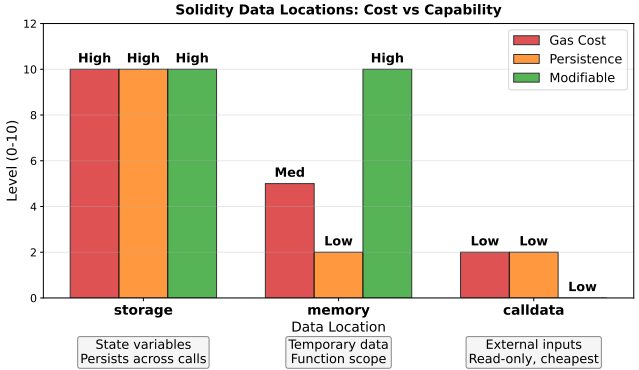
- Key-value storage: `mapping(address => uint256)`
- All keys exist with default values, cannot iterate

Function Visibility Modifiers



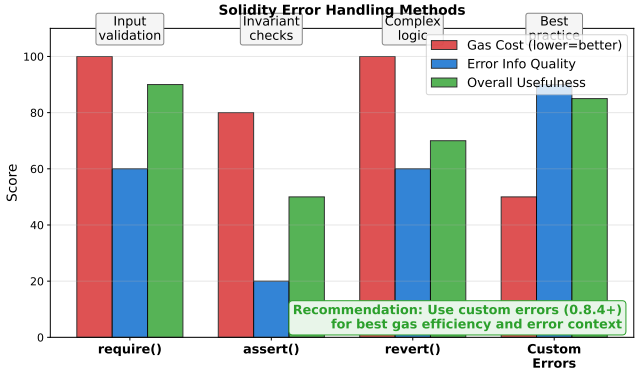
public: Anyone — **external:** Only external — **internal:** Contract + derived — **private:** Only this contract

Data Locations: storage vs memory vs calldata



storage: Persistent (expensive) — **memory:** Temporary — **calldata:** Cheapest (read-only)

Error Handling



require(): Input validation — **assert():** Invariants — **Custom errors (0.8.4+):** Gas-efficient

State Mutability & Modifiers

State Mutability:

- **view:** Reads state, doesn't modify (free off-chain)
- **pure:** No state access at all
- **(none):** Can read and modify state (costs gas)

Custom Modifiers:

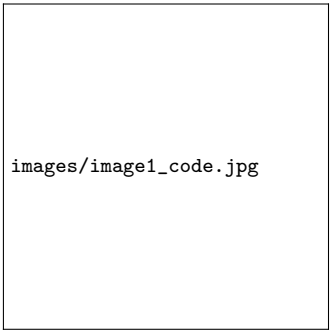
- Reusable preconditions: `onlyOwner`, `whenNotPaused`
- _ placeholder for function body
- Can chain multiple modifiers

Key Takeaways

1. **Solidity:** Statically-typed language compiling to EVM bytecode
2. **Data Types:** Value types (uint, address) vs reference types (arrays, mappings)
3. **Visibility:** public, external, internal, private determine access
4. **Data Locations:** storage (persistent), memory (temp), calldata (cheapest)
5. **Error Handling:** Use custom errors (0.8.4+) for gas efficiency

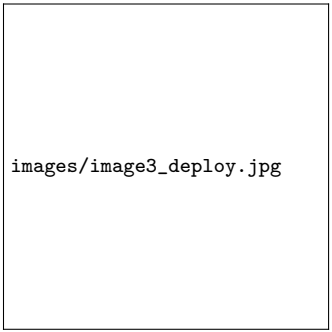
Best Practice: Current stable version is 0.8.x (2025).

Solidity Development in Practice



Smart Contract Code

Contract Logic



Deployment

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the max value for uint8?
A) 128 B) 255 C) 256 D) 65535

Quiz (1/2)

Q1. What is the max value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 ranges from 0 to $2^8 - 1 = 255$.

Q2. Which data type can receive ETH?
A) address B) address payable C) bytes20 D) uint160

Quiz (1/2)

Q1. What is the max value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 ranges from 0 to $2^8 - 1 = 255$.

Q2. Which data type can receive ETH?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive ETH via transfer().

Q3. What does "view" modifier indicate?
A) Modifies state B) No state access C) Reads but doesn't modify state D) Private function

Quiz (1/2)

Q1. What is the max value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 ranges from 0 to $2^8 - 1 = 255$.

Q2. Which data type can receive ETH?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive ETH via transfer().

Q3. What does "view" modifier indicate?
A) Modifies state B) No state access C) Reads but doesn't modify state D) Private function
Answer: C – view reads state without modifying it.

Q4. Which visibility allows only internal calls?
A) public B) external C) internal D) private

Quiz (1/2)

Q1. What is the max value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 ranges from 0 to $2^8 - 1 = 255$.

Q2. Which data type can receive ETH?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive ETH via transfer().

Q3. What does "view" modifier indicate?
A) Modifies state B) No state access C) Reads but doesn't modify state D) Private function
Answer: C – view reads state without modifying it.

Q4. Which visibility allows only internal calls?
A) public B) external C) internal D) private
Answer: D – private functions only callable within same contract.

Q5. Default value for uninitialized mapping entry?
A) null B) undefined C) Zero/default of value type D) Error

Quiz (1/2)

Q1. What is the max value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 ranges from 0 to $2^8 - 1 = 255$.

Q2. Which data type can receive ETH?
A) address B) address payable C) bytes20 D) uint160
Answer: B – address payable can receive ETH via transfer().

Q3. What does "view" modifier indicate?
A) Modifies state B) No state access C) Reads but doesn't modify state D) Private function
Answer: C – view reads state without modifying it.

Q4. Which visibility allows only internal calls?
A) public B) external C) internal D) private
Answer: D – private functions only callable within same contract.

Q5. Default value for uninitialized mapping entry?
A) null B) undefined C) Zero/default of value type D) Error
Answer: C – All keys exist with type's default value.

Quiz (2/2)

Q6. Which error handling for invariant checks?
A) require() B) assert() C) revert() D) throw

Quiz (2/2)

Q6. Which error handling for invariant checks?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() for internal invariants that should never fail.

Q7. Cheapest data location for function parameters?
A) storage B) memory C) calldata D) stack

Quiz (2/2)

Q6. Which error handling for invariant checks?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() for internal invariants that should never fail.

Q7. Cheapest data location for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest.

Q8. Max indexed parameters in an event?
A) 1 B) 2 C) 3 D) Unlimited

Quiz (2/2)

Q6. Which error handling for invariant checks?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() for internal invariants that should never fail.

Q7. Cheapest data location for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest.

Q8. Max indexed parameters in an event?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 parameters can be indexed.

Q9. Keyword for inheritance in Solidity?
A) extends B) implements C) is D) inherits

Quiz (2/2)

Q6. Which error handling for invariant checks?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() for internal invariants that should never fail.

Q7. Cheapest data location for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest.

Q8. Max indexed parameters in an event?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 parameters can be indexed.

Q9. Keyword for inheritance in Solidity?
A) extends B) implements C) is D) inherits
Answer: C – Use "is" for inheritance.

Q10. What does _ represent in a modifier?
A) Comment B) Private variable C) Function body placeholder D) Unused parameter

Quiz (2/2)

Q6. Which error handling for invariant checks?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() for internal invariants that should never fail.

Q7. Cheapest data location for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and cheapest.

Q8. Max indexed parameters in an event?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 parameters can be indexed.

Q9. Keyword for inheritance in Solidity?
A) extends B) implements C) is D) inherits
Answer: C – Use "is" for inheritance.

Q10. What does _ represent in a modifier?
A) Comment B) Private variable C) Function body placeholder D) Unused parameter
Answer: C – _ is replaced by modified function's body.

Thank you

Questions?

Next: L16 Lab – Contract Interaction

Quiz: Solidity Fundamentals

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the maximum value for uint8?
A) 128 B) 255 C) 256 D) 65535

Quiz (1–5)

Q1. What is the maximum value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is 8 bits, range 0 to $2^8 - 1 = 255$.

Q2. Which address type can receive Ether?
A) address B) address payable C) bytes20 D) uint160

Quiz (1–5)

Q1. What is the maximum value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is 8 bits, range 0 to $2^8 - 1 = 255$.

Q2. Which address type can receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – Only address payable has transfer() and send() methods.

Q3. What does "view" indicate about a function?
A) Modifies state B) No state access C) Reads but cannot modify D) Internal only

Quiz (1–5)

Q1. What is the maximum value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is 8 bits, range 0 to $2^8 - 1 = 255$.

Q2. Which address type can receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – Only address payable has transfer() and send() methods.

Q3. What does "view" indicate about a function?
A) Modifies state B) No state access C) Reads but cannot modify D) Internal only
Answer: C – view reads state without modification, no gas when called off-chain.

Q4. Which visibility allows ONLY internal contract calls?
A) public B) external C) internal D) private

Quiz (1–5)

Q1. What is the maximum value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is 8 bits, range 0 to $2^8 - 1 = 255$.

Q2. Which address type can receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – Only address payable has transfer() and send() methods.

Q3. What does "view" indicate about a function?
A) Modifies state B) No state access C) Reads but cannot modify D) Internal only
Answer: C – view reads state without modification, no gas when called off-chain.

Q4. Which visibility allows ONLY internal contract calls?
A) public B) external C) internal D) private
Answer: D – private restricts to same contract only, not even derived contracts.

Q5. What is the default value for uninitialized mapping entries?
A) null B) undefined C) Zero/default D) Error

Quiz (1–5)

Q1. What is the maximum value for uint8?
A) 128 B) 255 C) 256 D) 65535
Answer: B – uint8 is 8 bits, range 0 to $2^8 - 1 = 255$.

Q2. Which address type can receive Ether?
A) address B) address payable C) bytes20 D) uint160
Answer: B – Only address payable has transfer() and send() methods.

Q3. What does "view" indicate about a function?
A) Modifies state B) No state access C) Reads but cannot modify D) Internal only
Answer: C – view reads state without modification, no gas when called off-chain.

Q4. Which visibility allows ONLY internal contract calls?
A) public B) external C) internal D) private
Answer: D – private restricts to same contract only, not even derived contracts.

Q5. What is the default value for uninitialized mapping entries?
A) null B) undefined C) Zero/default D) Error
Answer: C – All keys exist with type's default (0 for uint, false for bool).

Quiz (6–10)

Q6. Which error method checks invariants that should never fail?
A) require() B) assert() C) revert() D) throw

Quiz (6–10)

Q6. Which error method checks invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors; failure indicates a bug.

Q7. Which data location is cheapest for function parameters?
A) storage B) memory C) calldata D) stack

Quiz (6–10)

Q6. Which error method checks invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors; failure indicates a bug.

Q7. Which data location is cheapest for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and does not copy data.

Q8. How many event parameters can be indexed?
A) 1 B) 2 C) 3 D) Unlimited

Quiz (6–10)

Q6. Which error method checks invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors; failure indicates a bug.

Q7. Which data location is cheapest for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and does not copy data.

Q8. How many event parameters can be indexed?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 indexed parameters for efficient off-chain filtering.

Q9. What does _ (underscore) represent in a modifier?
A) Comment B) Private prefix C) Function body placeholder D) Unused param

Quiz (6–10)

Q6. Which error method checks invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors; failure indicates a bug.

Q7. Which data location is cheapest for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and does not copy data.

Q8. How many event parameters can be indexed?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 indexed parameters for efficient off-chain filtering.

Q9. What does _ (underscore) represent in a modifier?
A) Comment B) Private prefix C) Function body placeholder D) Unused param
Answer: C – The underscore is replaced by the modified function's body.

Q10. Which keyword is used for contract inheritance?
A) extends B) implements C) is D) inherits

Quiz (6–10)

Q6. Which error method checks invariants that should never fail?
A) require() B) assert() C) revert() D) throw
Answer: B – assert() is for internal errors; failure indicates a bug.

Q7. Which data location is cheapest for function parameters?
A) storage B) memory C) calldata D) stack
Answer: C – calldata is read-only and does not copy data.

Q8. How many event parameters can be indexed?
A) 1 B) 2 C) 3 D) Unlimited
Answer: C – Up to 3 indexed parameters for efficient off-chain filtering.

Q9. What does _ (underscore) represent in a modifier?
A) Comment B) Private prefix C) Function body placeholder D) Unused param
Answer: C – The underscore is replaced by the modified function's body.

Q10. Which keyword is used for contract inheritance?
A) extends B) implements C) is D) inherits
Answer: C – Solidity uses "is" (e.g., contract MyToken is ERC20).

Lab Session: Smart Contract Interaction

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module B: Ethereum & Smart Contracts

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Deploy smart contracts using Remix IDE
- Interact with contract read functions (view/pure)
- Execute contract write functions (state-changing)
- Monitor events and transaction logs
- Debug failed transactions

The Problem: Hands-on Smart Contract Deployment

The Challenge
How do we interact with autonomous code on a decentralized network? Smart contracts execute automatically, but developers need tools to deploy, test, and monitor them without centralized infrastructure.

Why It Matters

- Failed transactions still consume gas—costly mistakes
- Events and logs reveal hidden state changes

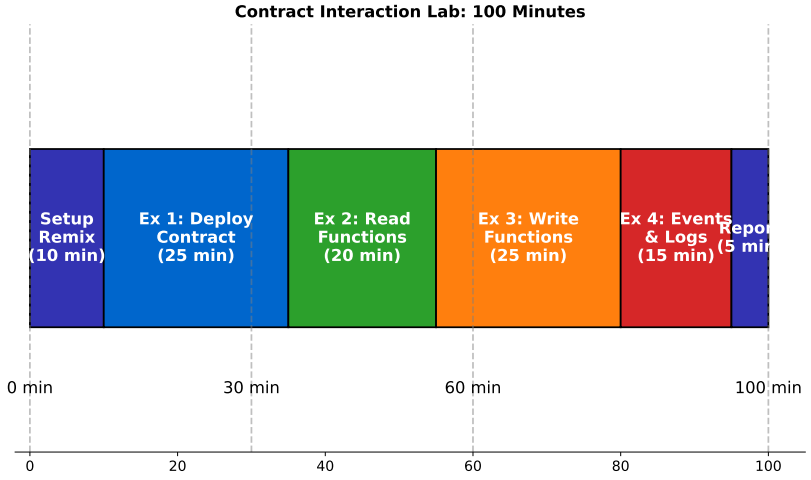
What You'll Explore

- Remix IDE for contract deployment
- Read vs. write functions (gas costs)
- Event logs and transaction debugging

The Cryptoeconomics Question
Gas costs reveal the true computational complexity of contract execution

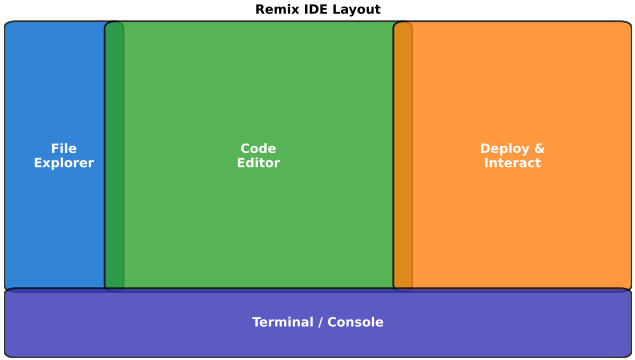
Today's lesson: How to deploy and interact with smart contracts using Remix IDE

Lab Session Structure



Focus on hands-on interaction with deployed contracts

Remix IDE Interface



Deploy & Interact panel is where you'll spend most of your time

Exercise 1: Deploy a Simple Contract

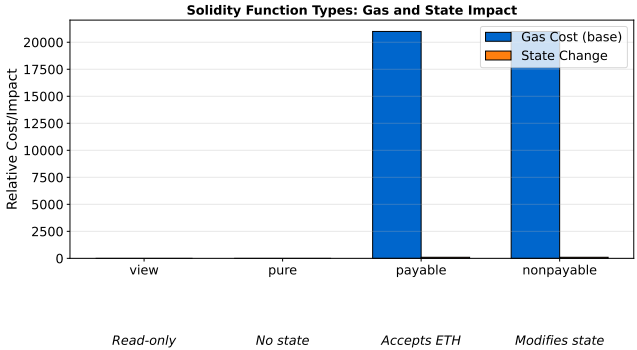
Steps:

1. Open Remix IDE: `https://remix.ethereum.org`
2. Create new file: `SimpleStorage.sol`
3. Write a storage contract with get/set functions
4. Compile using Solidity compiler
5. Deploy to JavaScript VM (local testing)

Key Concepts:

- Contract deployment creates new address
- Constructor runs once at deployment
- State variables persist on blockchain

Function Types in Solidity



View/pure functions are free; write functions cost gas

Exercise 2: Read Functions

Characteristics:

- `view`: Reads state, no modification
- `pure`: No state access, computation only
- No gas cost when called externally
- Instant response (no transaction needed)

Tasks:

1. Call `get()` function to read stored value
2. Observe: no MetaMask popup, instant result
3. Note the return value in Remix console

Exercise 3: Write Functions

Characteristics:

- Modify blockchain state
- Require gas payment
- Create transaction (needs confirmation)
- May emit events

Tasks:

1. Call `set(42)` to store new value
2. Observe: transaction created, gas consumed
3. Verify change by calling `get()`
4. Check transaction in Remix terminal

Exercise 4: Events and Logs

Why Events?

- Notify external applications of state changes
- Cheaper than storage for historical data
- Indexed parameters enable efficient filtering

Tasks:

1. Add event to contract: `event ValueChanged(uint newValue)`
2. Emit event in set function
3. Redeploy and test
4. View logs in Remix console

Lab Deliverables

Submit:

1. **Solidity Contract:**
   - SimpleStorage.sol with get, set, and event
2. **Screenshots:**
   - Deployed contract interface
   - Read function result
   - Write function transaction
   - Event log output

Submission Deadline: One week from lab session

Problem Solved? Contract Interaction

The Original Problem

How to interact with autonomous code on a decentralized network?

How Contract Interaction Solves It

- **Remix IDE**: Browser-based development environment eliminates setup friction
- **Gas transparency**: View functions cost nothing; write functions reveal true execution cost
- **Event logs**: Cheap notification mechanism for off-chain applications

Remaining Limitations

- Failed transactions still consume gas—no refunds for reverted operations
- Reentrancy vulnerabilities remain if contracts call untrusted code

Open Questions

- How can developers predict gas costs before deployment?
- Risk: Complex contract interactions may trigger unexpected failures

Contract interaction tools democratize blockchain development but introduce new cost and security risks

Key Takeaways

- Remix IDE is the standard tool for contract development
- View/pure functions are free (no gas)
- Write functions cost gas and create transactions
- Events provide efficient notification mechanism
- Always test on local VM before deploying to testnet

Quiz Questions (1/4)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters
Answer: B – The constructor executes only at deployment to initialize the contract.

Q3. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without modification, requiring no gas when called externally.

Q4. Which Remix panel is used to deploy and interact with contracts?
A) File Explorer B) Solidity Compiler C) Deploy & Run D) Plugin Manager
Answer: C – Deploy & Run Transactions panel handles deployment and function calls.

Q5. What does a contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator
Answer: B – Deployment creates a unique contract address where the code resides.

Quiz Questions (2/4)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted
Answer: C – Write functions create transactions that modify state and consume gas.

Q8. Why do write functions require gas payment?
A) To pay developers B) Computational work & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates network validators for computation and state storage.

Q9. What is the primary purpose of Solidity events?
A) Store large data cheaply B) Replace functions C) Notify external apps D) Increase gas costs
Answer: C – Events emit logs that external applications can monitor for state changes.

Q10. Where can you view event logs in Remix after a transaction?
A) Solidity Compiler B) Terminal/console C) File Explorer D) Settings panel
Answer: B – Transaction logs appear in the Remix terminal showing emitted events.

Quiz Questions (3/4)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix
Answer: B – View functions read current state to verify write operations succeeded.

Q13. What does the Solidity compiler in Remix produce?
A) JavaScript code B) Bytecode & ABI C) Python scripts D) Database files
Answer: B – Compiler generates bytecode (for EVM) and ABI (interface specification).

Q14. When should you test contracts on JavaScript VM before testnet?
A) Never B) Only for mainnet C) Always D) Only if complex
Answer: C – Always test locally first to catch errors without spending testnet ETH.

Q15. What information does a transaction receipt contain?
A) Source code B) Gas used & logs C) Compiler version D) Developer name
Answer: B – Receipts include gas consumed, status, emitted events, and other execution details.

Quiz Questions (4/4)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output
Answer: B – State variables are stored permanently on the blockchain at the contract address.

Q18. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types for external interaction.

Q19. When deploying to a testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet
Answer: C – Testnet deployment requires a wallet (MetaMask) and testnet ETH for gas.

Q20. What advantage do events have over storing data in state variables?
A) Faster execution B) Lower gas cost for logs C) Easier to code D) No difference
Answer: B – Events are significantly cheaper than storage for historical data recording.

Lab Session: Smart Contract Interaction

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module B: Ethereum & Smart Contracts

(c) Joerg Osterrieder 2025

MetaMask Popup Fatigue

[COMIC: Developer testing a DApp. MetaMask popup appears: "Confirm Transaction?" Click. Another popup. Click. Another popup. Fifth popup in a row. Developer's eye twitches. Caption: "Just testing one function..."]

Frame the Concept:

- Every state-changing interaction requires explicit user confirmation—a security feature
- Understanding the difference between read (free) and write (costs gas) functions is essential

Web3 UX: Where every click is a commitment and every popup is a reminder

Learning Objectives

By the end of this lab session, you will be able to:

- Deploy smart contracts using Remix IDE
- Interact with contract read functions (view/pure)
- Execute contract write functions (state-changing)
- Monitor events and transaction logs
- Debug failed transactions

Building on L15: Solidity Fundamentals

The Problem: Hands-on Smart Contract Deployment

The Challenge
How do we interact with autonomous code on a decentralized network? Smart contracts execute automatically, but developers need tools to deploy, test, and monitor them without centralized infrastructure.

Why It Matters

- Failed transactions still consume gas—costly mistakes
- Events and logs reveal hidden state changes

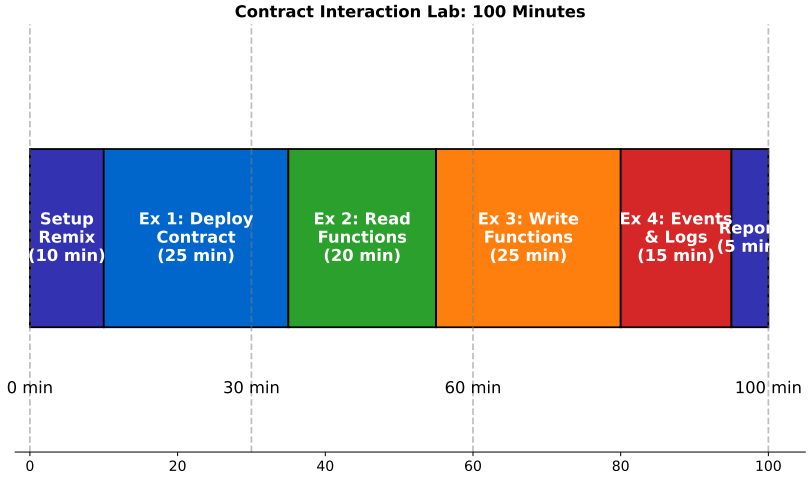
What You'll Explore

- Remix IDE for contract deployment
- Read vs. write functions (gas costs)
- Event logs and transaction debugging

The Cryptoeconomics Question
Gas costs reveal the true computational complexity of contract execution

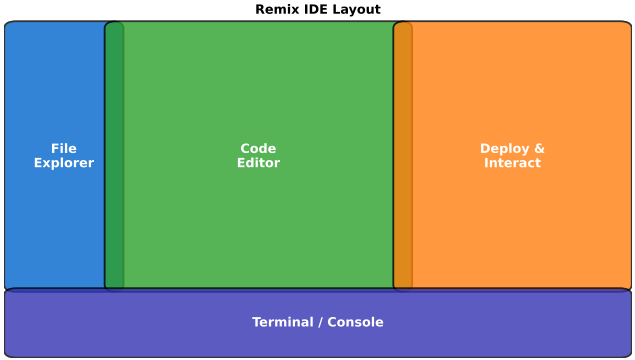
Today's lesson: How to deploy and interact with smart contracts using Remix IDE

What Is Our Workflow Today?



Focus on hands-on interaction with deployed contracts

How Do You Navigate the Remix IDE?



Deploy & Interact panel is where you'll spend most of your time

Exercise 1: Deploy a Simple Contract

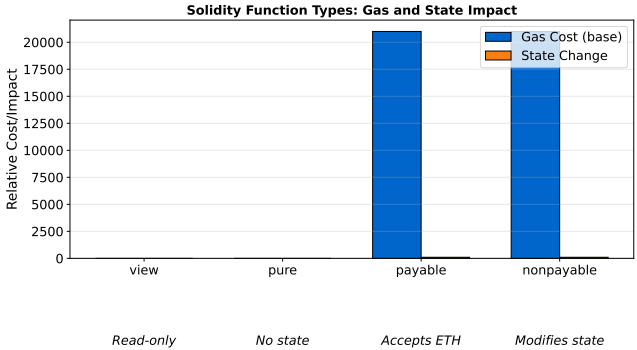
Steps:

1. Open Remix IDE: `https://remix.ethereum.org`
2. Create new file: `SimpleStorage.sol`
3. Write a storage contract with get/set functions
4. Compile using Solidity compiler
5. Deploy to JavaScript VM (local testing)

Key Concepts:

- Contract deployment creates new address
- Constructor runs once at deployment
- State variables persist on blockchain

What Are the Different Function Types?



View/pure functions are free; write functions cost gas

Exercise 2: Read Functions

Characteristics:

- `view`: Reads state, no modification
- `pure`: No state access, computation only
- No gas cost when called externally
- Instant response (no transaction needed)

Tasks:

1. Call `get()` function to read stored value
2. Observe: no MetaMask popup, instant result
3. Note the return value in Remix console

Exercise 3: Write Functions

Characteristics:

- Modify blockchain state
- Require gas payment
- Create transaction (needs confirmation)
- May emit events

Tasks:

1. Call `set(42)` to store new value
2. Observe: transaction created, gas consumed
3. Verify change by calling `get()`
4. Check transaction in Remix terminal

Exercise 4: Events and Logs

Why Events?

- Notify external applications of state changes
- Cheaper than storage for historical data
- Indexed parameters enable efficient filtering

Tasks:

1. Add event to contract: `event ValueChanged(uint newValue)`
2. Emit event in set function
3. Redeploy and test
4. View logs in Remix console

Lab Deliverables

Submit:

1. **Solidity Contract:**
   - SimpleStorage.sol with get, set, and event
2. **Screenshots:**
   - Deployed contract interface
   - Read function result
   - Write function transaction
   - Event log output

Submission Deadline: One week from lab session

Problem Solved? Contract Interaction

The Original Problem

How to interact with autonomous code on a decentralized network?

How Contract Interaction Solves It

- **Remix IDE**: Browser-based development environment eliminates setup friction
- **Gas transparency**: View functions cost nothing; write functions reveal true execution cost
- **Event logs**: Cheap notification mechanism for off-chain applications

Remaining Limitations

- Failed transactions still consume gas—no refunds for reverted operations
- Reentrancy vulnerabilities remain if contracts call untrusted code

Open Questions

- How can developers predict gas costs before deployment?
- Risk: Complex contract interactions may trigger unexpected failures

Contract interaction tools democratize blockchain development but introduce new cost and security risks

The Economics of Contract Interaction

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Contract Interaction

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Contract Interaction

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Approve Unlimited Regret

[COMIC: User clicks "Approve" on a DApp. MetaMask shows "Approve UNLIMITED tokens." User thinks "Seems fine, it's a trusted site." Six months later: "Your wallet has been drained by ApprovedContract." User checks Etherscan: the approval is still active. Caption: "Unlimited means unlimited."]

Key Insight:

- Token approvals persist until explicitly revoked—unlimited approvals are permanent attack vectors
- Always review approval amounts and use tools like Revoke.cash to audit outstanding permissions

Trust, but verify. And then revoke.

Key Takeaways

- Remix IDE is the standard tool for contract development
- View/pure functions are free (no gas)
- Write functions cost gas and create transactions
- Events provide efficient notification mechanism
- Always test on local VM before deploying to testnet

Next Lesson: L17 – ERC-20 Token Standard

Quiz Questions (1/4)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters
Answer: B – The constructor executes only at deployment to initialize the contract.

Q3. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without modification, requiring no gas when called externally.

Q4. Which Remix panel is used to deploy and interact with contracts?
A) File Explorer B) Solidity Compiler C) Deploy & Run D) Plugin Manager
Answer: C – Deploy & Run Transactions panel handles deployment and function calls.

Q5. What does a contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator
Answer: B – Deployment creates a unique contract address where the code resides.

Quiz Questions (2/4)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted
Answer: C – Write functions create transactions that modify state and consume gas.

Q8. Why do write functions require gas payment?
A) To pay developers B) Computational work & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates network validators for computation and state storage.

Q9. What is the primary purpose of Solidity events?
A) Store large data cheaply B) Replace functions C) Notify external apps D) Increase gas costs
Answer: C – Events emit logs that external applications can monitor for state changes.

Q10. Where can you view event logs in Remix after a transaction?
A) Solidity Compiler B) Terminal/console C) File Explorer D) Settings panel
Answer: B – Transaction logs appear in the Remix terminal showing emitted events.

Quiz Questions (3/4)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix
Answer: B – View functions read current state to verify write operations succeeded.

Q13. What does the Solidity compiler in Remix produce?
A) JavaScript code B) Bytecode & ABI C) Python scripts D) Database files
Answer: B – Compiler generates bytecode (for EVM) and ABI (interface specification).

Q14. When should you test contracts on JavaScript VM before testnet?
A) Never B) Only for mainnet C) Always D) Only if complex
Answer: C – Always test locally first to catch errors without spending testnet ETH.

Q15. What information does a transaction receipt contain?
A) Source code B) Gas used & logs C) Compiler version D) Developer name
Answer: B – Receipts include gas consumed, status, emitted events, and other execution details.

Quiz Questions (4/4)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output
Answer: B – State variables are stored permanently on the blockchain at the contract address.

Q18. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types for external interaction.

Q19. When deploying to a testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet
Answer: C – Testnet deployment requires a wallet (MetaMask) and testnet ETH for gas.

Q20. What advantage do events have over storing data in state variables?
A) Faster execution B) Lower gas cost for logs C) Easier to code D) No difference
Answer: B – Events are significantly cheaper than storage for historical data recording.

Lab 16: Smart Contract Interaction

Mini-Lecture – BSc Blockchain, Crypto Economy & NFTs

Joerg Osterrieder

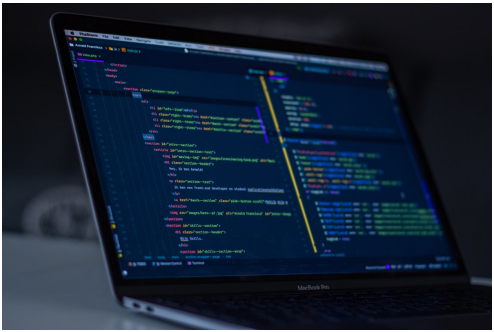
Module B: Ethereum & Smart Contracts

(c) Joerg Osterrieder 2025

Learning Objectives

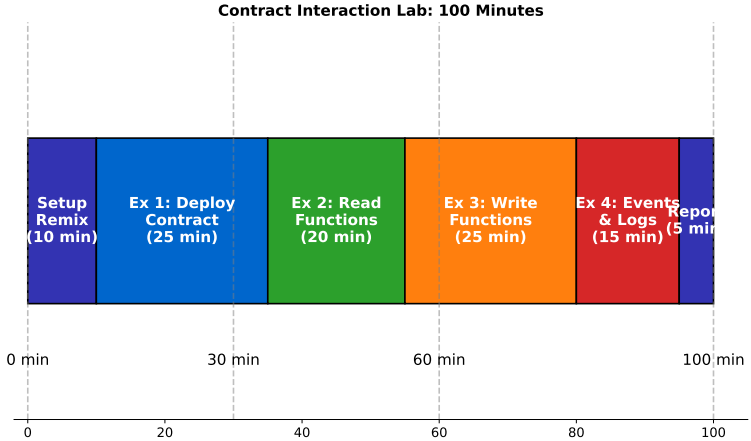
By the end of this lab, you will:

- Deploy contracts using Remix IDE
- Call read functions (view/pure)
- Execute write functions (state changes)
- Monitor events and logs



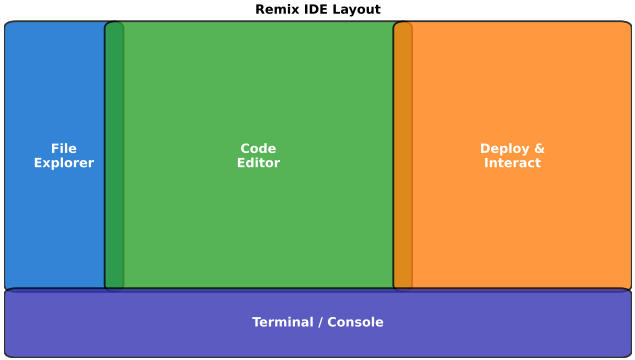
Focus: Hands-on interaction with deployed smart contracts

Lab Workflow Overview



Four exercises: Deploy, Read, Write, Events

Remix IDE – Your Development Environment



Deploy & Run panel is where you interact with contracts

Exercise 1: Deploy a Contract

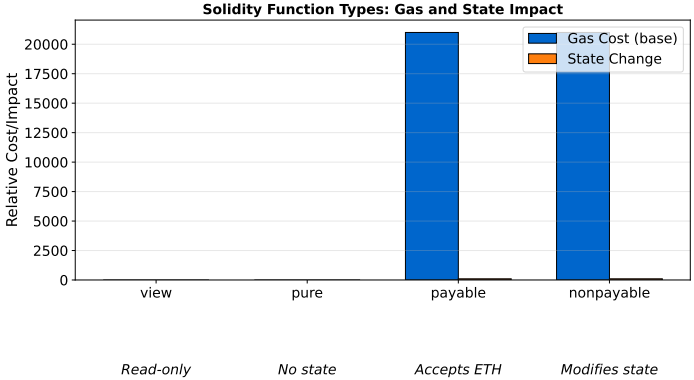
Steps:

1. Open `remix.ethereum.org`
2. Create `SimpleStorage.sol`
3. Write get/set functions
4. Compile and deploy to JavaScript VM

Key Points:

- Deployment creates contract address
- Constructor runs once

Solidity Function Types



View/pure = free reads; Write = gas costs

Exercise 2: Read Functions

Characteristics of View/Pure Functions:

- `view`: Reads state without modification
- `pure`: No state access, computation only
- No gas cost when called externally
- Instant response (no transaction)

Your Task:

1. Call `get()` to read stored value
2. Observe: No MetaMask popup, instant result
3. Note return value in Remix console

Exercise 3: Write Functions

Write Function Characteristics:

- Modify blockchain state
- Require gas payment
- Create transaction
- May emit events

Your Task:

1. Call `set(42)` to store value
2. Verify with `get()`

Exercise 4: Events and Logs

Why Events?

- Notify external applications of state changes
- Cheaper than storage for historical data
- `indexed` parameters enable efficient filtering

Your Task:

1. Add event: `event ValueChanged(uint newValue)`
2. Emit in `set()` function
3. Redeploy and test
4. View logs in Remix console

Understanding Transaction Flow

When You Call a Write Function:

1. Transaction created with function call data
2. Gas estimated and reserved
3. EVM executes contract code
4. State changes applied (or reverted on failure)
5. Receipt returned with status and logs

Key Insight:

- Failed transactions still consume gas
- State changes revert on failure
- Events only emitted on success

Debugging Failed Transactions

Common Failure Reasons:

- Out of gas – increase gas limit
- Require/assert failed – check conditions
- Invalid function parameters
- Insufficient permissions

Debugging Steps:

1. Check Remix terminal for error message
2. Look for “revert” reason string
3. Verify function inputs
4. Test with simpler inputs first

Lab Deliverables

Submit the following:

1. **Solidity Contract:** SimpleStorage.sol with:
   - get() and set() functions
   - ValueChanged event
2. **Screenshots:**
   - Deployed contract interface
   - Read function result
   - Write function transaction
   - Event log output

Deadline: One week from lab session

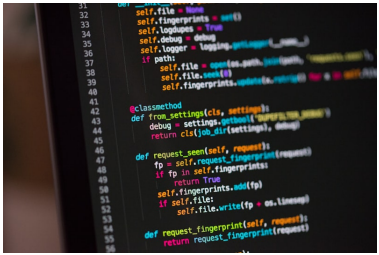
Key Takeaways

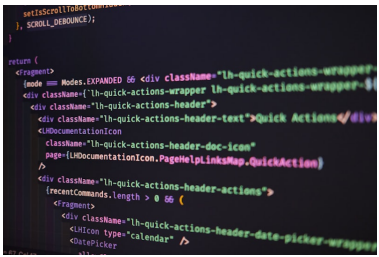
- **Remix IDE:** Standard tool for Solidity development and testing
- **View/Pure:** Free to call, read-only, instant response
- **Write Functions:** Cost gas, create transactions, modify state
- **Events:** Efficient notification mechanism for off-chain apps
- **Best Practice:** Always test on JavaScript VM before testnet

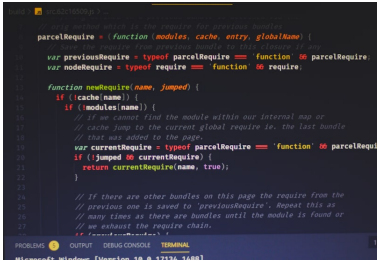
Next Steps: Deploy to Sepolia testnet with MetaMask

Lab: Smart Contract Interaction

Learning Objectives: Deploy contracts in Remix IDE — Interact with read/write functions — Monitor events and logs — Debug failed transactions



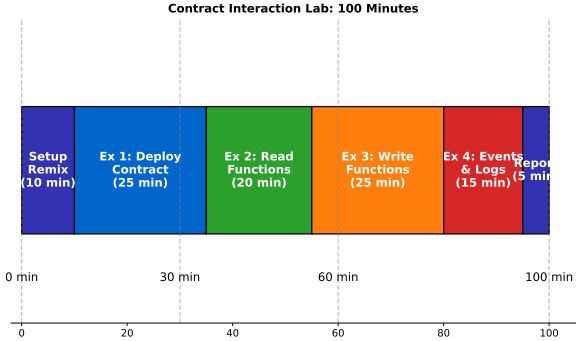




Lab Session Structure

Session Flow:

- **Step 1:** Deploy SimpleStorage contract
- **Step 2:** Test read functions (free)
- **Step 3:** Execute write functions (gas)
- **Step 4:** Add and monitor events



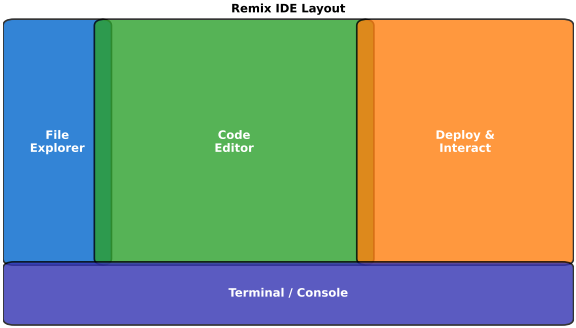
Complete workflow: compile, deploy, interact, verify state changes

Remix IDE Interface

Key Panels:

- **File Explorer:** Manage .sol files
- **Compiler:** Solidity to bytecode + ABI
- **Deploy & Run:** Execute contracts
- **Terminal:** View logs and results

Access at: remix.ethereum.org



Deploy & Run panel is where you spend most of your lab time

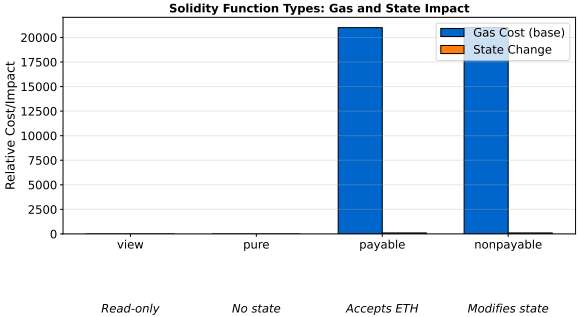
Solidity Function Types

Read Functions (Free):

- `view`: Reads state only
- `pure`: No state access
- No gas cost, instant response

Write Functions (Gas Required):

- Modify blockchain state
- Create transaction, emit events
- Require confirmation



View/pure functions are free; write functions cost gas and modify state

Exercise 1: Deploy a Simple Contract

Deployment Steps:

1. Open Remix IDE
2. Create `SimpleStorage.sol`
3. Write get/set functions
4. Compile with Solidity compiler
5. Deploy to JavaScript VM

Key Concepts:

- Deployment creates new address (0x5B38...)
- Constructor runs once
- State variables persist on-chain

JavaScript VM simulates blockchain locally – no real ETH needed

Always test on JavaScript VM before deploying to testnet

Exercise 2 & 3: Read and Write Functions

Read Function Test:

1. Call `get()` function
2. Observe: no MetaMask popup
3. Result appears instantly
4. No gas consumed

View functions return data without transaction

Write Function Test:

1. Call `set(42)`
2. Observe: transaction created
3. Gas consumed (45,000 gas)
4. Verify with `get()`

Write functions modify state and cost gas

Compare: read = instant + free; write = transaction + gas cost

(c) Joerg Osterrieder 2025

Exercise 4: Events and Logs

Why Events?

- Notify external applications
- Cheaper than storage (8 gas/byte vs 20,000 gas/slot)
- `indexed` enables filtering

Implementation Steps:

1. Add: `event ValueChanged(uint newValue)`
2. Emit in set(): `emit ValueChanged(_value)`
3. Redeploy contract
4. View logs in Remix terminal

Events appear in transaction receipts – accessible to frontends via web3.js/ethers.js

(c) Joerg Osterrieder 2025

Key Takeaways

1. **Remix IDE** is the standard tool for contract development – always test on JavaScript VM first
2. **View/pure functions** are free (no gas) and return data instantly without transactions
3. **Write functions** cost gas, create transactions, and permanently modify blockchain state
4. **Events** provide efficient notification mechanism at lower cost than storage

Bottom Line: Master the deploy-interact-verify workflow in Remix before moving to testnet deployment.

(c) Joerg Osterrieder 2025

Lab Deliverables

Submit Solidity Contract:

- `SimpleStorage.sol`
- Must include get(), set(), event
- Compile without errors

Submit Screenshots:

- Deployed contract interface
- Read function result
- Write function transaction
- Event log output

Deadline: One week from lab session

All submissions via course LMS – include contract address from Remix

(c) Joerg Osterrieder 2025

Concrete Examples: Making It Real

Contract Addresses (Sepolia Testnet)

- Format: `0x5B38Da6a...` (20 bytes)
- Each deployment = unique address
- Viewable on Etherscan

Gas Costs (Dec 2025)

- Deploy: 300,000 gas
- Write (set): 45,000 gas
- Read (get): 0 gas

Transaction Data

- Status: Success / Reverted
- Gas Used: Actual consumption
- Logs: Emitted events

ABI Components

- Function names and types
- Input/output parameters
- Event definitions

All data verified Dec 2025 — Sepolia faucet: sepoliafaucet.com

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What does the Remix JavaScript VM environment do?
A) Deploys to mainnet B) Simulates blockchain locally C) Compiles Python D) Mines real ETH

Quiz Questions (1–5)

Q1. What does the Remix JavaScript VM environment do?
A) Deploys to mainnet B) Simulates blockchain locally C) Compiles Python D) Mines real ETH
Answer: B – JavaScript VM provides local blockchain simulation for testing.

Q2. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified

Quiz Questions (1–5)

Q1. What does the Remix JavaScript VM environment do?
A) Deploys to mainnet B) Simulates blockchain locally C) Compiles Python D) Mines real ETH
Answer: B – JavaScript VM provides local blockchain simulation for testing.

Q2. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without gas cost when called externally.

Q3. What does contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator

Quiz Questions (1–5)

Q1. What does the Remix JavaScript VM environment do?
A) Deploys to mainnet B) Simulates blockchain locally C) Compiles Python D) Mines real ETH
Answer: B – JavaScript VM provides local blockchain simulation for testing.

Q2. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without gas cost when called externally.

Q3. What does contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator
Answer: B – Deployment creates a unique contract address.

Q4. What distinguishes `pure` from `view` functions?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask

Quiz Questions (1–5)

Q1. What does the Remix JavaScript VM environment do?
A) Deploys to mainnet B) Simulates blockchain locally C) Compiles Python D) Mines real ETH
Answer: B – JavaScript VM provides local blockchain simulation for testing.

Q2. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without gas cost when called externally.

Q3. What does contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator
Answer: B – Deployment creates a unique contract address.

Q4. What distinguishes `pure` from `view` functions?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading state.

Q5. What is the primary purpose of Solidity events?
A) Store data cheaply B) Replace functions C) Notify external apps D) Increase gas

Quiz Questions (1–5)

Q1. What does the Remix JavaScript VM environment do?
A) Deploys to mainnet B) Simulates blockchain locally C) Compiles Python D) Mines real ETH
Answer: B – JavaScript VM provides local blockchain simulation for testing.

Q2. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without gas cost when called externally.

Q3. What does contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator
Answer: B – Deployment creates a unique contract address.

Q4. What distinguishes `pure` from `view` functions?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading state.

Q5. What is the primary purpose of Solidity events?
A) Store data cheaply B) Replace functions C) Notify external apps D) Increase gas
Answer: C – Events emit logs that external applications can monitor.

Quiz Questions (6–10)

Q6. Why do write functions require gas payment?
A) Pay developers B) Computation & storage C) Remix licensing D) Internet fees

Quiz Questions (6–10)

Q6. Why do write functions require gas payment?
A) Pay developers B) Computation & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates validators for computation and state storage.

Q7. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules

Quiz Questions (6–10)

Q6. Why do write functions require gas payment?
A) Pay developers B) Computation & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates validators for computation and state storage.

Q7. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types.

Q8. What happens if a write function call fails (reverts)?
A) State persists B) Gas refunded C) State reverted, gas consumed D) Contract deleted

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. Why do write functions require gas payment?
A) Pay developers B) Computation & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates validators for computation and state storage.

Q7. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types.

Q8. What happens if a write function call fails (reverts)?
A) State persists B) Gas refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state but still consume gas.

Q9. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. Why do write functions require gas payment?
A) Pay developers B) Computation & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates validators for computation and state storage.

Q7. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types.

Q8. What happens if a write function call fails (reverts)?
A) State persists B) Gas refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state but still consume gas.

Q9. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering.

Q10. When deploying to testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. Why do write functions require gas payment?
A) Pay developers B) Computation & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates validators for computation and state storage.

Q7. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types.

Q8. What happens if a write function call fails (reverts)?
A) State persists B) Gas refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state but still consume gas.

Q9. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering.

Q10. When deploying to testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet
Answer: C – Testnet deployment requires MetaMask wallet and testnet ETH.

Quiz: Lab: Contract Interaction

Instructions: Multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether

Quiz (1–5)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters

Quiz (1–5)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters
Answer: B – The constructor executes only at deployment to initialize the contract.

Q3. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified

Quiz (1–5)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters
Answer: B – The constructor executes only at deployment to initialize the contract.

Q3. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without modification, requiring no gas when called externally.

Q4. Which Remix panel is used to deploy and interact with contracts?
A) File Explorer B) Solidity Compiler C) Deploy & Run D) Plugin Manager

Quiz (1–5)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters
Answer: B – The constructor executes only at deployment to initialize the contract.

Q3. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without modification, requiring no gas when called externally.

Q4. Which Remix panel is used to deploy and interact with contracts?
A) File Explorer B) Solidity Compiler C) Deploy & Run D) Plugin Manager
Answer: C – Deploy & Run Transactions panel handles deployment and function calls.

Q5. What does a contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator

Quiz (1–5)

Q1. What does the Remix IDE JavaScript VM environment do?
A) Deploys to Ethereum mainnet B) Simulates blockchain locally C) Compiles Python code D) Mines real Ether
Answer: B – JavaScript VM provides a local blockchain simulation for testing without real funds.

Q2. When deploying a contract in Remix, what runs exactly once?
A) View functions B) The constructor C) All state variables D) Event emitters
Answer: B – The constructor executes only at deployment to initialize the contract.

Q3. What happens when you call a `view` function externally?
A) Transaction created B) Gas charged C) Instant free read D) State modified
Answer: C – View functions read state without modification, requiring no gas when called externally.

Q4. Which Remix panel is used to deploy and interact with contracts?
A) File Explorer B) Solidity Compiler C) Deploy & Run D) Plugin Manager
Answer: C – Deploy & Run Transactions panel handles deployment and function calls.

Q5. What does a contract deployment create on the blockchain?
A) New token B) New address C) New block D) New validator
Answer: B – Deployment creates a unique contract address where the code resides.

Quiz (6–10)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask

Quiz (6–10)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted

Quiz (6–10)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted
Answer: C – Write functions create transactions that modify state and consume gas.

Q8. Why do write functions require gas payment?
A) To pay developers B) Computational work & storage C) Remix licensing D) Internet fees

Quiz (6–10)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted
Answer: C – Write functions create transactions that modify state and consume gas.

Q8. Why do write functions require gas payment?
A) To pay developers B) Computational work & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates network validators for computation and state storage.

Q9. What is the primary purpose of Solidity events?
A) Store large data cheaply B) Replace functions C) Notify external apps D) Increase gas costs

Quiz (6–10)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted
Answer: C – Write functions create transactions that modify state and consume gas.

Q8. Why do write functions require gas payment?
A) To pay developers B) Computational work & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates network validators for computation and state storage.

Q9. What is the primary purpose of Solidity events?
A) Store large data cheaply B) Replace functions C) Notify external apps D) Increase gas costs
Answer: C – Events emit logs that external applications can monitor for state changes.

Q10. Where can you view event logs in Remix after a transaction?
A) Solidity Compiler B) Terminal/console C) File Explorer D) Settings panel

Quiz (6–10)

Q6. What distinguishes a `pure` function from a `view` function?
A) Pure costs gas B) Pure doesn't read state C) Pure modifies state D) Pure requires MetaMask
Answer: B – Pure functions perform computations without reading or writing state.

Q7. When calling a write function, what do you observe in Remix?
A) Instant result B) Compiler error C) Transaction created D) Contract deleted
Answer: C – Write functions create transactions that modify state and consume gas.

Q8. Why do write functions require gas payment?
A) To pay developers B) Computational work & storage C) Remix licensing D) Internet fees
Answer: B – Gas compensates network validators for computation and state storage.

Q9. What is the primary purpose of Solidity events?
A) Store large data cheaply B) Replace functions C) Notify external apps D) Increase gas costs
Answer: C – Events emit logs that external applications can monitor for state changes.

Q10. Where can you view event logs in Remix after a transaction?
A) Solidity Compiler B) Terminal/console C) File Explorer D) Settings panel
Answer: B – Transaction logs appear in the Remix terminal showing emitted events.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`

Quiz (11–15)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix

Quiz (11–15)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix
Answer: B – View functions read current state to verify write operations succeeded.

Q13. What does the Solidity compiler in Remix produce?
A) JavaScript code B) Bytecode & ABI C) Python scripts D) Database files

Quiz (11–15)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix
Answer: B – View functions read current state to verify write operations succeeded.

Q13. What does the Solidity compiler in Remix produce?
A) JavaScript code B) Bytecode & ABI C) Python scripts D) Database files
Answer: B – Compiler generates bytecode (for EVM) and ABI (interface specification).

Q14. When should you test contracts on JavaScript VM before testnet?
A) Never B) Only for mainnet C) Always D) Only if complex

Quiz (11–15)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix
Answer: B – View functions read current state to verify write operations succeeded.

Q13. What does the Solidity compiler in Remix produce?
A) JavaScript code B) Bytecode & ABI C) Python scripts D) Database files
Answer: B – Compiler generates bytecode (for EVM) and ABI (interface specification).

Q14. When should you test contracts on JavaScript VM before testnet?
A) Never B) Only for mainnet C) Always D) Only if complex
Answer: C – Always test locally first to catch errors without spending testnet ETH.

Q15. What information does a transaction receipt contain?
A) Source code B) Gas used & logs C) Compiler version D) Developer name

Quiz (11–15)

Q11. What parameter in events enables efficient filtering?
A) `public` B) `indexed` C) `memory` D) `payable`
Answer: B – Indexed parameters create topics for efficient log filtering and searching.

Q12. After deploying a contract, how do you verify state changes?
A) Recompile the contract B) Call view functions C) Delete the contract D) Restart Remix
Answer: B – View functions read current state to verify write operations succeeded.

Q13. What does the Solidity compiler in Remix produce?
A) JavaScript code B) Bytecode & ABI C) Python scripts D) Database files
Answer: B – Compiler generates bytecode (for EVM) and ABI (interface specification).

Q14. When should you test contracts on JavaScript VM before testnet?
A) Never B) Only for mainnet C) Always D) Only if complex
Answer: C – Always test locally first to catch errors without spending testnet ETH.

Q15. What information does a transaction receipt contain?
A) Source code B) Gas used & logs C) Compiler version D) Developer name
Answer: B – Receipts include gas consumed, status, emitted events, and other execution details.

Quiz (16–20)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted

Quiz (16–20)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output

Quiz (16–20)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output
Answer: B – State variables are stored permanently on the blockchain at the contract address.

Q18. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output
Answer: B – State variables are stored permanently on the blockchain at the contract address.

Q18. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types for external interaction.

Q19. When deploying to a testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet

Quiz (16–20)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output
Answer: B – State variables are stored permanently on the blockchain at the contract address.

Q18. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types for external interaction.

Q19. When deploying to a testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet
Answer: C – Testnet deployment requires a wallet (MetaMask) and testnet ETH for gas.

Q20. What advantage do events have over storing data in state variables?
A) Faster execution B) Lower gas cost for logs C) Easier to code D) No difference

Quiz (16–20)

Q16. What happens if a write function call fails (reverts)?
A) State changes persist B) Gas fully refunded C) State reverted, gas consumed D) Contract deleted
Answer: C – Failed transactions revert state changes but still consume gas for computation.

Q17. How do state variables persist in smart contracts?
A) In Remix cache B) On the blockchain C) In browser memory D) In compiler output
Answer: B – State variables are stored permanently on the blockchain at the contract address.

Q18. What does the ABI (Application Binary Interface) define?
A) Gas prices B) Function signatures & types C) Block times D) Validator rules
Answer: B – ABI specifies function names, parameters, and return types for external interaction.

Q19. When deploying to a testnet, what do you need beyond Remix?
A) Physical hardware B) Mining software C) MetaMask & test ETH D) Bitcoin wallet
Answer: C – Testnet deployment requires a wallet (MetaMask) and testnet ETH for gas.

Q20. What advantage do events have over storing data in state variables?
A) Faster execution B) Lower gas cost for logs C) Easier to code D) No difference
Answer: B – Events are significantly cheaper than storage for historical data recording.

(c) Joerg Osterrieder 2025

L17: ERC-20 Token Standard

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the purpose and importance of the ERC-20 standard
- Describe the six required ERC-20 interface functions
- Explain the allowance mechanism for delegated transfers
- Implement a basic ERC-20 token from scratch
- Use OpenZeppelin's audited ERC-20 implementation
- Analyze real-world ERC-20 tokens (USDC, DAI, LINK)

(c) Joerg Osterrieder 2025

The Problem: How do we create interoperable digital assets?

The Challenge
How do we create interoperable digital assets that any wallet or exchange can support without custom integration? Before ERC-20, each token required bespoke code to integrate.

Why It Matters

- Without standards, every token needs custom wallet integration, limiting adoption
- Early tokens (pre-2015) were incompatible - exchanges rejected listing due to integration costs

What We Need

- System design principles
- Common interface for fungible token operations (transfer, balance, approval)

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How ERC-20 Token Standard addresses this challenge

What is ERC-20?

ERC-20 is the dominant fungible token standard on Ethereum:

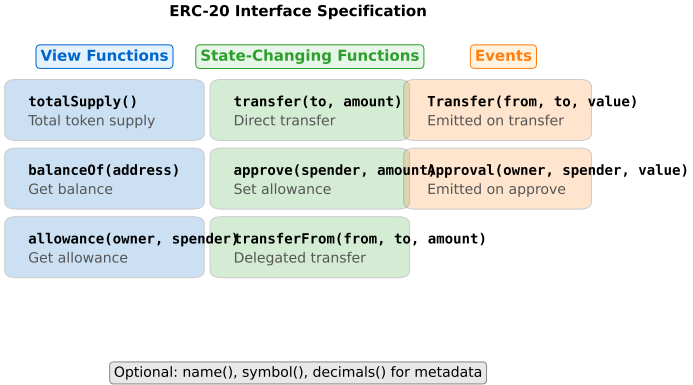
- **ERC:** Ethereum Request for Comments (proposal process)
- **Fungible:** Each token is identical and interchangeable
- **Standard:** Common interface enables interoperability

Why Standardization Matters:

- Wallets support all ERC-20 tokens without custom code
- Exchanges can list new tokens easily
- Smart contracts can interact with any ERC-20 token

ERC-20 Interface Overview

Six required functions + two required events:



ERC-20 Interface: Required Functions

```
interface IERC20 {
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address recipient, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address sender, address recipient, uint256 amount)
        external returns (bool);

    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);
}
```

Optional Metadata Functions

Not required but widely used:

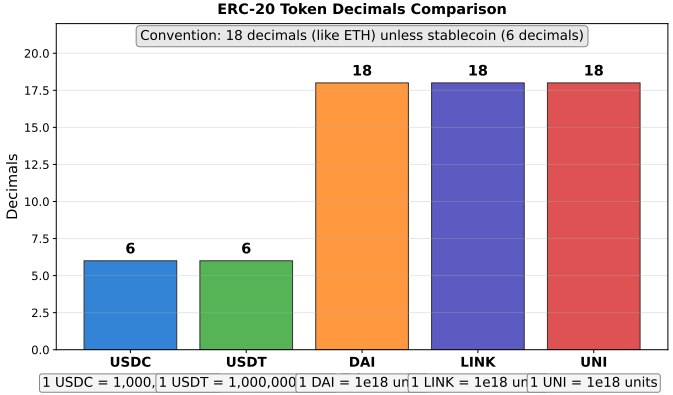
```
function name() public view returns (string memory);    // e.g., "US Dollar Coin"
function symbol() public view returns (string memory);  // e.g., "USDC"
function decimals() public view returns (uint8);        // e.g., 18 or 6
```

Decimals Explained:

- Tokens are stored as integers (no floating point on EVM)
- `decimals` defines how to display token amounts
- Example: 1 USDC = 1,000,000 units (6 decimals)
- Example: 1 DAI = 1e18 units (18 decimals)

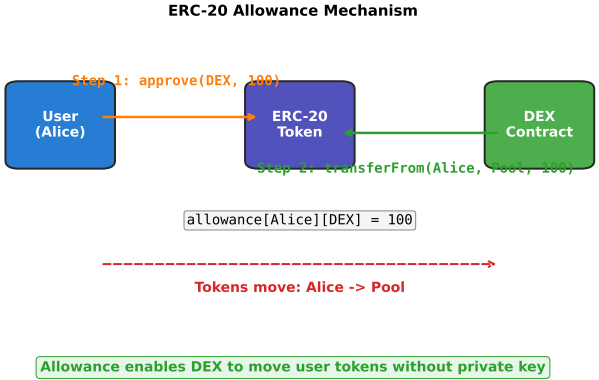
Token Decimals Comparison

Different tokens use different decimal places:



Understanding Allowance Mechanism

Problem: How can a smart contract spend your tokens?
Solution: Two-step approve + transferFrom pattern



Allowance Example: DEX Trading

Scenario: Alice wants to trade 100 DAI for ETH on Uniswap
Step-by-Step:

1. Alice calls `DAI.approve(UniswapRouter, 100e18)`
   - Sets allowance: Uniswap can spend 100 DAI
2. Alice calls `UniswapRouter.swapTokensForETH(100e18, ...)`
   - Uniswap calls `DAI.transferFrom(Alice, Pool, 100e18)`
   - Alice receives ETH in return

Infinite Approval:

- Users often approve `type(uint256).max` to avoid repeated approvals
- Risk: If DEX contract is hacked, all approved tokens can be stolen

Basic ERC-20 Implementation (Part 1)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BasicERC20 {
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;

    mapping(address => uint256) public balanceOf;
    mapping(address => mapping(address => uint256)) public allowance;

    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);

    constructor(string memory _name, string memory _symbol, uint8 _decimals,
                uint256 _initialSupply) {
        name = _name;
        symbol = _symbol;
        decimals = _decimals;
        totalSupply = _initialSupply * 10**_decimals;
        balanceOf[msg.sender] = totalSupply;
        emit Transfer(address(0), msg.sender, totalSupply);
    }
```

Basic ERC-20 Implementation (Part 2)

```
    function transfer(address recipient, uint256 amount) public returns (bool) {
        require(recipient != address(0), "Transfer to zero address");
        require(balanceOf[msg.sender] >= amount, "Insufficient balance");
        balanceOf[msg.sender] -= amount;
        balanceOf[recipient] += amount;
        emit Transfer(msg.sender, recipient, amount);
        return true;
    }

    function approve(address spender, uint256 amount) public returns (bool) {
        require(spender != address(0), "Approve to zero address");
        allowance[msg.sender][spender] = amount;
        emit Approval(msg.sender, spender, amount);
        return true;
    }

    function transferFrom(address sender, address recipient, uint256 amount) public returns (bool) {
        require(balanceOf[sender] >= amount, "Insufficient balance");
        require(allowance[sender][msg.sender] >= amount, "Insufficient allowance");
        balanceOf[sender] -= amount;
        balanceOf[recipient] += amount;
        allowance[sender][msg.sender] -= amount;
        emit Transfer(sender, recipient, amount);
        return true;
    }
}
```

Security Considerations

Common ERC-20 Vulnerabilities:

1. **Approve Race Condition:**
   - Problem: Changing allowance from A to B allows spender to spend A+B
   - Solution: Use `increaseAllowance()` and `decreaseAllowance()`
2. **Integer Overflow (pre-0.8.0):**
   - Solution: Use Solidity 0.8+ (built-in overflow checks) or SafeMath
3. **Fee-on-Transfer Tokens:**
   - Some tokens deduct fees on transfer (e.g., SAFEMOON)
   - Breaks assumption that `transfer(amount)` sends exactly `amount`

OpenZeppelin ERC-20 Implementation

Industry-standard audited implementation:

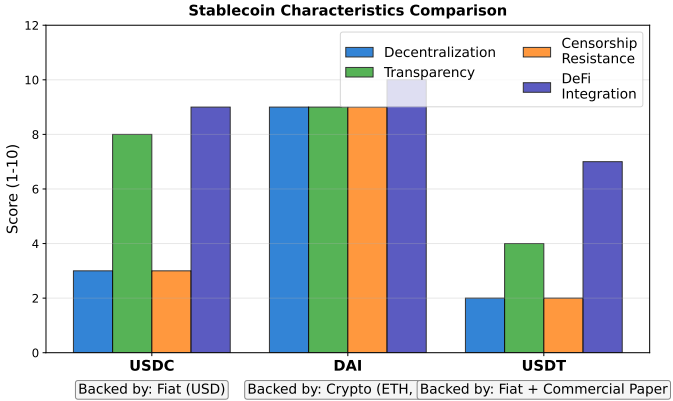
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract MyToken is ERC20 {
    constructor(uint256 initialSupply) ERC20("My Token", "MTK") {
        _mint(msg.sender, initialSupply * 10**decimals());
    }
}
```

Advantages:

- Battle-tested code (used by USDC, LINK, thousands of projects)
- Security audits by leading firms
- Extensions: ERC20Burnable, ERC20Pausable, ERC20Permit

Real-World Stablecoin Comparison

USDC vs DAI vs USDT characteristics:



Real-World Example: USDC

USD Coin (USDC) - Circle's stablecoin:
Key Features:

- Pegged 1:1 to US Dollar, backed by cash and Treasuries
- 6 decimals (not 18, to match fiat cents)
- Upgradable proxy pattern
- Blacklist function (regulatory compliance)
- Pausable (emergency circuit breaker)

Contract Address: 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48

Real-World Example: DAI

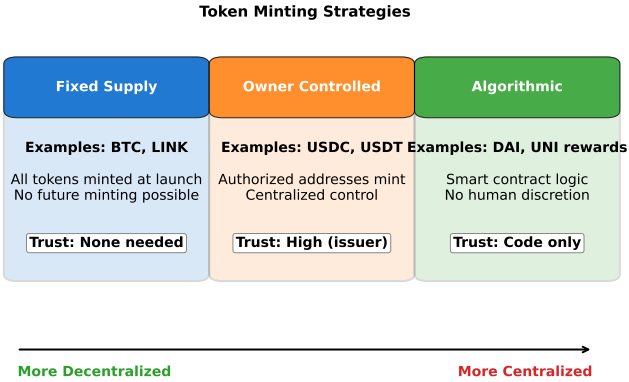
DAI - MakerDAO's decentralized stablecoin:
Key Features:

- Pegged to 1 USD via collateralized debt positions (CDPs)
- Over-collateralized by crypto assets (ETH, wBTC, USDC)
- 18 decimals (standard)
- No admin blacklist or pause (more decentralized than USDC)
- `permit()` - EIP-2612 gasless approvals

Contract Address: 0x6B175474E89094C44Da98b954EedeAC495271d0F

Token Minting Strategies

Different approaches to token supply management:



ERC-20 Variants and Improvements

Extensions to standard ERC-20:

1. **EIP-2612 (Permit):** Approve via off-chain signature
2. **ERC-20 Snapshot:** Capture balances at specific block for governance
3. **ERC-20 Votes:** Delegation of voting power (UNI, COMP)
4. **Rebase Tokens:** Balance changes automatically (Ampleforth)
5. **Wrapped Tokens:** ERC-20 wrapper around native assets (WETH)

Problem Solved? ERC-20 Token Standard

The Original Problem

How do we create interoperable digital assets?

How ERC-20 Token Standard Solves It

- Standard functions (transfer, approve, transferFrom) enable universal wallet/DEX support
- Transfer and Approval events enable off-chain indexing and tracking
- Metadata (name, symbol, decimals) makes tokens human-readable across platforms

Remaining Limitations

- Approve/transferFrom race condition - changing allowance can let spender use old+new values
- No native batch transfers or gasless approvals in base standard (require extensions)

Open Questions

- Will ERC-20 extensions (permit, hooks) become standard or fragment ecosystem?
- Risk: Fee-on-transfer tokens break DEX assumptions, infinite approvals risk total loss if contract hacked

ERC-20 Token Standard solved interoperability but introduced new trade-offs around security and composability

Key Takeaways

1. **ERC-20 Standard:** Common interface for fungible tokens enabling interoperability
2. **Core Functions:** totalSupply, balanceOf, transfer, approve, allowance, transferFrom
3. **Allowance Mechanism:** Two-step approve + transferFrom for smart contract spending
4. **Security:** Use OpenZeppelin, beware of approve race condition
5. **Decimals:** Convention is 18, stablecoins often use 6
6. **Minting:** Fixed supply, owner-controlled, or algorithmic approaches

(c) Joerg Osterrieder 2025

Discussion Questions

1. Why do stablecoins like USDC use 6 decimals instead of 18?
2. What are the security tradeoffs between limited vs infinite approval?
3. How does EIP-2612 permit() improve user experience?
4. What are the regulatory implications of USDC's blacklist function?
5. How might fee-on-transfer tokens break DEX contracts?

Next Lesson Preview: L18 - ERC-721 and ERC-1155 Standards

Coming up next:

- Non-fungible tokens (NFTs) and the ERC-721 standard
- ownerOf, tokenURI, safeTransferFrom functions
- Metadata standards and IPFS integration
- ERC-1155 multi-token standard (fungible + non-fungible)
- Real-world examples: CryptoPunks, Bored Apes, ENS domains

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens
Answer: B – Allows smart contracts to spend tokens on behalf of the owner.

Q3. What decimal value does USDC use?
A) 18 B) 12 C) 8 D) 6

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens
Answer: B – Allows smart contracts to spend tokens on behalf of the owner.

Q3. What decimal value does USDC use?
A) 18 B) 12 C) 8 D) 6
Answer: D – USDC uses 6 decimals to match fiat currency cents.

Q4. Which function must be called BEFORE transferFrom can work?
A) transfer B) approve C) mint D) burn

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens
Answer: B – Allows smart contracts to spend tokens on behalf of the owner.

Q3. What decimal value does USDC use?
A) 18 B) 12 C) 8 D) 6
Answer: D – USDC uses 6 decimals to match fiat currency cents.

Q4. Which function must be called BEFORE transferFrom can work?
A) transfer B) approve C) mint D) burn
Answer: B – The owner must approve a spender before transferFrom succeeds.

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?

A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy
Answer: B – Transfer and Approval events are required by the standard.

Q7. Why might a user set infinite approval (type(uint256).max)?
A) Higher security B) Lower gas for repeated trades C) Required by law D) Creates more tokens

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy
Answer: B – Transfer and Approval events are required by the standard.

Q7. Why might a user set infinite approval (type(uint256).max)?
A) Higher security B) Lower gas for repeated trades C) Required by law D) Creates more tokens
Answer: B – Avoids repeated approval transactions, saving gas.

Q8. Which EIP introduces gasless approvals via off-chain signatures?
A) EIP-20 B) EIP-721 C) EIP-2612 D) EIP-1559

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy
Answer: B – Transfer and Approval events are required by the standard.

Q7. Why might a user set infinite approval (type(uint256).max)?
A) Higher security B) Lower gas for repeated trades C) Required by law D) Creates more tokens
Answer: B – Avoids repeated approval transactions, saving gas.

Q8. Which EIP introduces gasless approvals via off-chain signatures?
A) EIP-20 B) EIP-721 C) EIP-2612 D) EIP-1559
Answer: C – EIP-2612 permit() allows approval via signed messages.

(c) Joerg Osterrieder 2025

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18
Answer: D – 18 decimals is the convention, matching ETH's wei.

Q11. How is DAI different from USDC in terms of admin controls?
A) DAI has more controls B) DAI has no blacklist/pause functions
C) DAI is centralized D) No difference

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18
Answer: D – 18 decimals is the convention, matching ETH's wei.

Q11. How is DAI different from USDC in terms of admin controls?
A) DAI has more controls B) DAI has no blacklist/pause functions
C) DAI is centralized D) No difference
Answer: B – DAI is more decentralized with no admin blacklist or pause.

Q12. What advantage does OpenZeppelin's ERC-20 provide?
A) Lower gas costs B) More features C) Battle-tested and audited D) Faster execution

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18
Answer: D – 18 decimals is the convention, matching ETH's wei.

Q11. How is DAI different from USDC in terms of admin controls?
A) DAI has more controls B) DAI has no blacklist/pause functions
C) DAI is centralized D) No difference
Answer: B – DAI is more decentralized with no admin blacklist or pause.

Q12. What advantage does OpenZeppelin's ERC-20 provide?
A) Lower gas costs B) More features C) Battle-tested and audited D) Faster execution
Answer: C – OpenZeppelin code is audited and used by major projects.

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard
Answer: B – Wrapped Ether is an ERC-20 representation of native ETH.

Q15. What pattern does USDC use for upgradability?
A) Diamond pattern B) Transparent proxy C) No upgrades possible D) Beacon proxy

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard
Answer: B – Wrapped Ether is an ERC-20 representation of native ETH.

Q15. What pattern does USDC use for upgradability?
A) Diamond pattern B) Transparent proxy C) No upgrades possible D) Beacon proxy
Answer: B – USDC uses an upgradable proxy pattern.

Q16. What is a rebase token?
A) Token with fixed supply B) Token whose balance changes automatically
C) Token that can be refunded D) Token with metadata

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard
Answer: B – Wrapped Ether is an ERC-20 representation of native ETH.

Q15. What pattern does USDC use for upgradability?
A) Diamond pattern B) Transparent proxy C) No upgrades possible D) Beacon proxy
Answer: B – USDC uses an upgradable proxy pattern.

Q16. What is a rebase token?
A) Token with fixed supply B) Token whose balance changes automatically
C) Token that can be refunded D) Token with metadata
Answer: B – Rebase tokens like Ampleforth adjust balances algorithmically.

L17: ERC-20 Token Standard

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Token Creation Enthusiasm

[COMIC: Developer excitedly deploying token contract]

"I made a token!"

The Excitement

- Anyone can create an ERC-20 token
- Deployment costs only $10-50 in gas
- Instant compatibility with all wallets

But Also...

- Great power, great responsibility
- Design choices have consequences
- Today: understanding the standard

Creating tokens is easy. Creating good tokens requires understanding the ERC-20 standard deeply.

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the purpose and importance of the ERC-20 standard
- Describe the six required ERC-20 interface functions
- Explain the allowance mechanism for delegated transfers
- Implement a basic ERC-20 token from scratch
- Use OpenZeppelin's audited ERC-20 implementation
- Analyze real-world ERC-20 tokens (USDC, DAI, LINK)

Building on L16: Lab: Contract Interaction

The Problem: How do we create interoperable digital assets?

The Challenge
How do we create interoperable digital assets that any wallet or exchange can support without custom integration? Before ERC-20, each token required bespoke code to integrate.

Why It Matters

- Without standards, every token needs custom wallet integration, limiting adoption
- Early tokens (pre-2015) were incompatible - exchanges rejected listing due to integration costs

What We Need

- System design principles
- Common interface for fungible token operations (transfer, balance, approval)

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How ERC-20 Token Standard addresses this challenge

What Makes ERC-20 the Standard for Tokens?

ERC-20 is the dominant fungible token standard on Ethereum:

- **ERC:** Ethereum Request for Comments (proposal process)
- **Fungible (interchangeable, like dollar bills):** Each token is identical and interchangeable
- **Standard:** Common interface enables interoperability

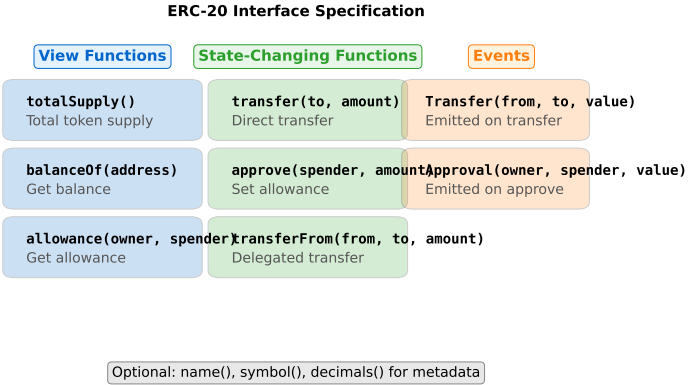
Why Standardization Matters:

- Wallets support all ERC-20 tokens without custom code
- Exchanges can list new tokens easily
- Smart contracts can interact with any ERC-20 token

→ **Problem: How do we create interoperable digital... — What is ERC-20? ERC-20's standard interface means any wallet supports any token automatically**

What Functions Does the ERC-20 Interface Require?

Six required functions + two required events:



What Are the ERC-20 Function Details?

Complete interface specification with types:

ERC-20 Interface Specification

`interface IERC20`

Functions (6 Required)

view	`totalSupply() -> uint256`	Returns total tokens in existence
view	`balanceOf(address) -> uint256`	Returns balance of account
view	`allowance(owner, spender) -> uint256`	Returns remaining allowance
state	`transfer(to, amount) -> bool`	Moves tokens to recipient
state	`approve(spender, amount) -> bool`	Sets spending allowance
state	`transferFrom(from, to, amount) -> bool`	Moves tokens using allowance

Events (2 Required) = view (no gas) = state-changing (gas) = event (logged)

event	`Transfer(from, to, value)`	Emitted on any transfer
event	`Approval(owner, spender, value)`	Emitted on approve()

View functions cost no gas; state-changing functions require transaction

What Functions Must the ERC-20 Interface Implement?

```
interface IERC20 {
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function transfer(address recipient, uint256 amount) external returns (bool);
    function allowance(address owner, address spender) external view returns (uint256);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address sender, address recipient, uint256 amount)
        external returns (bool);

    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);
}
```

What Optional Metadata Functions Do Tokens Typically Include?

Not required but widely used:

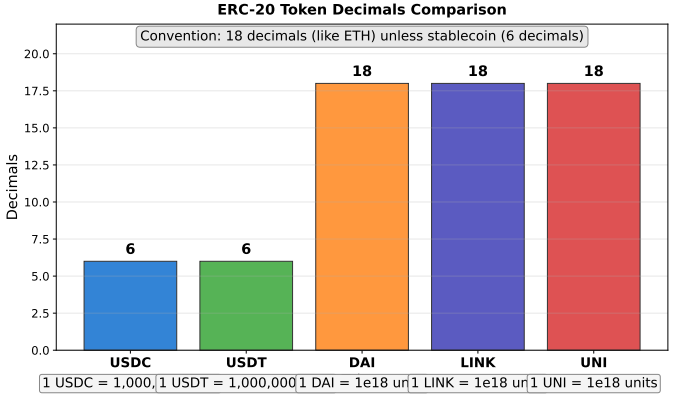
```
function name() public view returns (string memory);     // e.g., "US Dollar Coin"
function symbol() public view returns (string memory);   // e.g., "USDC"
function decimals() public view returns (uint8);         // e.g., 18 or 6
```

Decimals Explained:

- Tokens are stored as integers (no floating point on EVM)
- `decimals` defines how to display token amounts
- Example: 1 USDC = 1,000,000 units (6 decimals)
- Example: 1 DAI = 1e18 units (18 decimals)

How Do Token Decimals Differ Across Tokens?

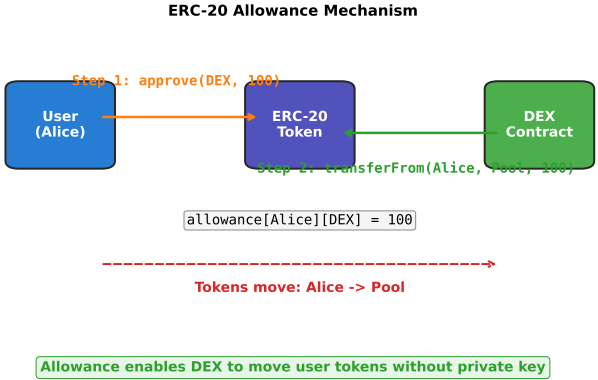
Different tokens use different decimal places:



→ **Problem: How do we create interoperable digital... — Token Decimals Comparison Decimals convention enables human-readable amounts: 1 USDC = 1,000,000 units (6 decimals)**

How Do Smart Contracts Spend Your Tokens?

Problem: How can a smart contract spend your tokens?
Solution: Two-step approve + transferFrom pattern



How Does the Allowance Mechanism Work in DEX Trading?

Scenario: Alice wants to trade 100 DAI for ETH on Uniswap
Step-by-Step:

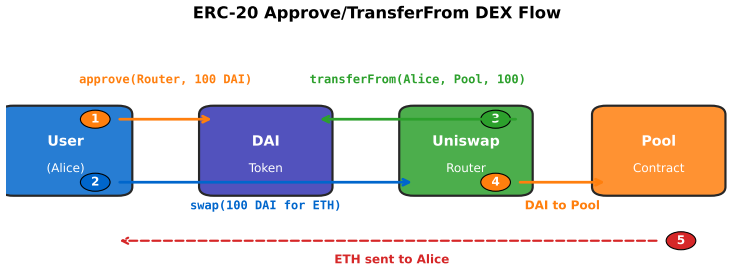
1. Alice calls `DAI.approve(UniswapRouter, 100e18)`
   - Sets allowance: Uniswap can spend 100 DAI
2. Alice calls `UniswapRouter.swapTokensForETH(100e18, ...)`
   - Uniswap calls `DAI.transferFrom(Alice, Pool, 100e18)`
   - Alice receives ETH in return

Infinite Approval:

- Users often approve `type(uint256).max` to avoid repeated approvals
- Risk: If DEX contract is hacked, all approved tokens can be stolen

How Does the Approval and TransferFrom Flow Work?

Complete DEX trading flow with allowance tracking:



How Do You Implement a Basic ERC-20 Token? (Part 1)

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract BasicERC20 {
    string public name;
    string public symbol;
    uint8 public decimals;
    uint256 public totalSupply;

    mapping(address => uint256) public balanceOf;
    mapping(address => mapping(address => uint256)) public allowance;

    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);

    constructor(string memory _name, string memory _symbol, uint8 _decimals,
                uint256 _initialSupply) {
        name = _name;
        symbol = _symbol;
        decimals = _decimals;
        totalSupply = _initialSupply * 10**_decimals;
        balanceOf[msg.sender] = totalSupply;
        emit Transfer(address(0), msg.sender, totalSupply);
    }
```

Problem Check-In: ERC-20 Token Standard

Recall Our Problem

How do we create interoperable digital assets?

What We've Learned So Far

- 6 standard functions: totalSupply, balanceOf, transfer, approve, allowance, transferFrom
- Allowance mechanism enables smart contracts to spend tokens on your behalf
- Standard interface = any wallet works with any token = interoperability achieved

Still to Address

- What security vulnerabilities exist? (approve race condition) How do real tokens differ?
- How would YOU design a token standard for interoperable digital assets?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we create interoperable digital..."?

How Do You Implement a Basic ERC-20 Token? (Part 2)

```
    function transfer(address recipient, uint256 amount) public returns (bool) {
        require(recipient != address(0), "Transfer to zero address");
        require(balanceOf[msg.sender] >= amount, "Insufficient balance");
        balanceOf[msg.sender] -= amount;
        balanceOf[recipient] += amount;
        emit Transfer(msg.sender, recipient, amount);
        return true;
    }

    function approve(address spender, uint256 amount) public returns (bool) {
        require(spender != address(0), "Approve to zero address");
        allowance[msg.sender][spender] = amount;
        emit Approval(msg.sender, spender, amount);
        return true;
    }

    function transferFrom(address sender, address recipient, uint256 amount) public returns (bool) {
        require(balanceOf[sender] >= amount, "Insufficient balance");
        require(allowance[sender][msg.sender] >= amount, "Insufficient allowance");
        balanceOf[sender] -= amount;
        balanceOf[recipient] += amount;
        allowance[sender][msg.sender] -= amount;
        emit Transfer(sender, recipient, amount);
        return true;
    }
}
```

→ **Problem: How do we create interoperable digital... — Basic ERC-20 Implementation (Part 2) transfer() and transferFrom() implement the core token movement logic**

What Are the Common ERC-20 Vulnerabilities?

Common ERC-20 Vulnerabilities:

1. **Approve Race Condition:**
   - Problem: Changing allowance from A to B allows spender to spend A+B
   - Solution: Use `increaseAllowance()` and `decreaseAllowance()`
2. **Integer Overflow (pre-0.8.0):**
   - Solution: Use Solidity 0.8+ (built-in overflow checks) or SafeMath (overflow protection library, obsolete in Solidity 0.8+)
3. **Fee-on-Transfer Tokens:**
   - Some tokens deduct fees on transfer (e.g., SAFEMOON)
   - Breaks assumption that `transfer(amount)` sends exactly `amount`

How Does OpenZeppelin Simplify ERC-20 Implementation?

Industry-standard audited implementation:

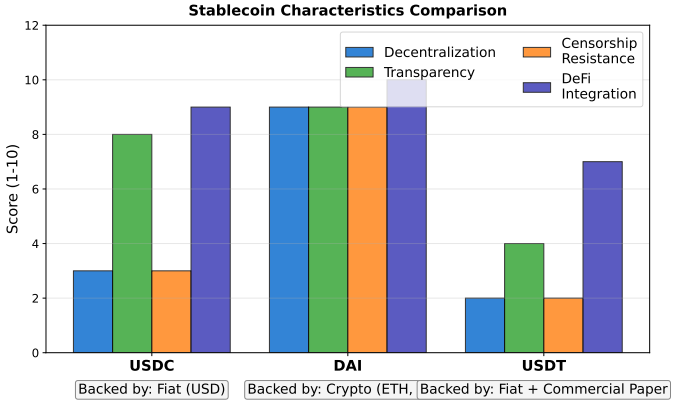
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract MyToken is ERC20 {
    constructor(uint256 initialSupply) ERC20("My Token", "MTK") {
        _mint(msg.sender, initialSupply * 10**decimals());
    }
}
```

Advantages:

- Battle-tested code (used by USDC, LINK, thousands of projects)
- Security audits by leading firms
- Extensions: ERC20Burnable, ERC20Pausable, ERC20Permit

How Do Major Stablecoins Compare?

USDC vs DAI vs USDT characteristics:



What Makes USDC Different from Basic ERC-20?

USD Coin (USDC) - Circle's stablecoin:
Key Features:

- Pegged 1:1 to US Dollar, backed by cash and Treasuries
- 6 decimals (not 18, to match fiat cents)
- Upgradable proxy pattern (allows contract code to be upgraded after deployment)
- Blacklist function (regulatory compliance)
- Pausable (emergency circuit breaker)

Contract Address: 0xA0b86991c6218b36c1d19D4a2e9Eb0cE3606eB48

→ Problem: How do we create interoperable digital... — Real-World Example: USDC USDC adds blacklist and pause functions for regulatory compliance – less decentralized

What Makes DAI Different from USDC?

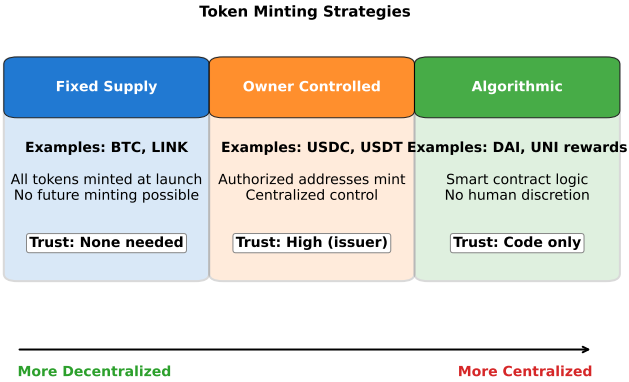
DAI - MakerDAO's decentralized stablecoin:
Key Features:

- Pegged to 1 USD via collateralized debt positions (CDPs)
- Over-collateralized by crypto assets (ETH, wBTC, USDC)
- 18 decimals (standard)
- No admin blacklist or pause (more decentralized than USDC)
- `permit()` - EIP-2612 gasless approvals

Contract Address: 0x6B175474E89094C44Da98b954EedeAC495271d0F

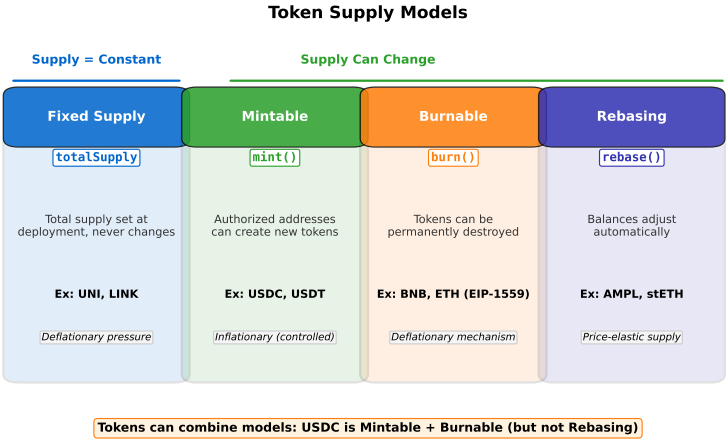
What Token Minting Strategies Exist?

Different approaches to token supply management:



How Do Different Tokens Manage Supply?

Four fundamental approaches to token supply:



Most tokens combine models: USDC is mintable + burnable

What ERC-20 Variants and Improvements Exist?

Extensions to standard ERC-20:

1. **EIP-2612 (Permit):** Approve via off-chain signature
2. **ERC-20 Snapshot:** Capture balances at specific block for governance
3. **ERC-20 Votes:** Delegation of voting power (UNI, COMP)
4. **Rebase Tokens:** Balance changes automatically (Ampleforth)
5. **Wrapped Tokens:** ERC-20 wrapper around native assets (WETH)

Problem Solved? ERC-20 Token Standard

The Original Problem

How do we create interoperable digital assets?

How ERC-20 Token Standard Solves It

- Standard functions (transfer, approve, transferFrom) enable universal wallet/DEX support
- Transfer and Approval events enable off-chain indexing and tracking
- Metadata (name, symbol, decimals) makes tokens human-readable across platforms

Remaining Limitations

- Approve/transferFrom race condition - changing allowance can let spender use old+new values
- No native batch transfers or gasless approvals in base standard (require extensions)

Open Questions

- Will ERC-20 extensions (permit, hooks) become standard or fragment ecosystem?
- Risk: Fee-on-transfer tokens break DEX assumptions, infinite approvals risk total loss if contract hacked

ERC-20 Token Standard solved interoperability but introduced new trade-offs around security and composability

The Economics of ERC-20 Token Standard

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: ERC-20 Token Standard

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: ERC-20 Token Standard

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

The Approve/TransferFrom Trap

[COMIC: User realizing infinite approval mistake]

"Wait, I approved how much?!"

The Hidden Risk

- Infinite approvals seem convenient
- One compromised contract = total loss
- Race condition on allowance changes

What We Learned

- Approve + transferFrom enables DeFi
- But also creates attack surface
- EIP-2612 permit improves UX safely

The allowance mechanism is powerful but dangerous. Always review approvals and consider using permit().

Key Takeaways

1. **ERC-20 Standard:** Common interface for fungible tokens enabling interoperability
2. **Core Functions:** totalSupply, balanceOf, transfer, approve, allowance, transferFrom
3. **Allowance Mechanism:** Two-step approve + transferFrom for smart contract spending
4. **Security:** Use OpenZeppelin, beware of approve race condition
5. **Decimals:** Convention is 18, stablecoins often use 6
6. **Minting:** Fixed supply, owner-controlled, or algorithmic approaches

Next Lesson: L18 – ERC-721 and ERC-1155

(c) Joerg Osterrieder 2025

Discussion Questions

1. Why do stablecoins like USDC use 6 decimals instead of 18?
2. What are the security tradeoffs between limited vs infinite approval?
3. How does EIP-2612 permit() improve user experience?
4. What are the regulatory implications of USDC's blacklist function?
5. How might fee-on-transfer tokens break DEX contracts?

Next Lesson Preview: L18 - ERC-721 and ERC-1155 Standards

Coming up next:

- Non-fungible tokens (NFTs) and the ERC-721 standard
- ownerOf, tokenURI, safeTransferFrom functions
- Metadata standards and IPFS integration
- ERC-1155 multi-token standard (fungible + non-fungible)
- Real-world examples: CryptoPunks, Bored Apes, ENS domains

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens
Answer: B – Allows smart contracts to spend tokens on behalf of the owner.

Q3. What decimal value does USDC use?
A) 18 B) 12 C) 8 D) 6

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens
Answer: B – Allows smart contracts to spend tokens on behalf of the owner.

Q3. What decimal value does USDC use?
A) 18 B) 12 C) 8 D) 6
Answer: D – USDC uses 6 decimals to match fiat currency cents.

Q4. Which function must be called BEFORE transferFrom can work?
A) transfer B) approve C) mint D) burn

Quiz Questions (1/4)

Q1. How many required functions does the ERC-20 standard specify?
A) 4 B) 6 C) 8 D) 10
Answer: B – Six required: totalSupply, balanceOf, transfer, allowance, approve, transferFrom.

Q2. What is the purpose of the allowance mechanism?
A) Track token price B) Enable delegated spending C) Burn tokens D) Create new tokens
Answer: B – Allows smart contracts to spend tokens on behalf of the owner.

Q3. What decimal value does USDC use?
A) 18 B) 12 C) 8 D) 6
Answer: D – USDC uses 6 decimals to match fiat currency cents.

Q4. Which function must be called BEFORE transferFrom can work?
A) transfer B) approve C) mint D) burn
Answer: B – The owner must approve a spender before transferFrom succeeds.

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?

A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy
Answer: B – Transfer and Approval events are required by the standard.

Q7. Why might a user set infinite approval (type(uint256).max)?
A) Higher security B) Lower gas for repeated trades C) Required by law D) Creates more tokens

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy
Answer: B – Transfer and Approval events are required by the standard.

Q7. Why might a user set infinite approval (type(uint256).max)?
A) Higher security B) Lower gas for repeated trades C) Required by law D) Creates more tokens
Answer: B – Avoids repeated approval transactions, saving gas.

Q8. Which EIP introduces gasless approvals via off-chain signatures?
A) EIP-20 B) EIP-721 C) EIP-2612 D) EIP-1559

Quiz Questions (2/4)

Q5. What is the approve race condition vulnerability?
A) Two users approve same address B) Changing allowance lets spender use old+new
C) Approval expires too fast D) Transfer fails after approval
Answer: B – Spender can spend both old and new allowance during change.

Q6. What are the two required events in ERC-20?
A) Mint, Burn B) Transfer, Approval C) Send, Receive D) Create, Destroy
Answer: B – Transfer and Approval events are required by the standard.

Q7. Why might a user set infinite approval (type(uint256).max)?
A) Higher security B) Lower gas for repeated trades C) Required by law D) Creates more tokens
Answer: B – Avoids repeated approval transactions, saving gas.

Q8. Which EIP introduces gasless approvals via off-chain signatures?
A) EIP-20 B) EIP-721 C) EIP-2612 D) EIP-1559
Answer: C – EIP-2612 permit() allows approval via signed messages.

(c) Joerg Osterrieder 2025

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18
Answer: D – 18 decimals is the convention, matching ETH's wei.

Q11. How is DAI different from USDC in terms of admin controls?
A) DAI has more controls B) DAI has no blacklist/pause functions
C) DAI is centralized D) No difference

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18
Answer: D – 18 decimals is the convention, matching ETH's wei.

Q11. How is DAI different from USDC in terms of admin controls?
A) DAI has more controls B) DAI has no blacklist/pause functions
C) DAI is centralized D) No difference
Answer: B – DAI is more decentralized with no admin blacklist or pause.

Q12. What advantage does OpenZeppelin's ERC-20 provide?
A) Lower gas costs B) More features C) Battle-tested and audited D) Faster execution

Quiz Questions (3/4)

Q9. What is a fee-on-transfer token?
A) Token with gas fees B) Token that deducts on each transfer
C) Token with subscription model D) Token with approval fees
Answer: B – Some tokens deduct a percentage on every transfer.

Q10. What is the standard number of decimals for most ERC-20 tokens?
A) 6 B) 8 C) 12 D) 18
Answer: D – 18 decimals is the convention, matching ETH's wei.

Q11. How is DAI different from USDC in terms of admin controls?
A) DAI has more controls B) DAI has no blacklist/pause functions
C) DAI is centralized D) No difference
Answer: B – DAI is more decentralized with no admin blacklist or pause.

Q12. What advantage does OpenZeppelin's ERC-20 provide?
A) Lower gas costs B) More features C) Battle-tested and audited D) Faster execution
Answer: C – OpenZeppelin code is audited and used by major projects.

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard
Answer: B – Wrapped Ether is an ERC-20 representation of native ETH.

Q15. What pattern does USDC use for upgradability?
A) Diamond pattern B) Transparent proxy C) No upgrades possible D) Beacon proxy

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard
Answer: B – Wrapped Ether is an ERC-20 representation of native ETH.

Q15. What pattern does USDC use for upgradability?
A) Diamond pattern B) Transparent proxy C) No upgrades possible D) Beacon proxy
Answer: B – USDC uses an upgradable proxy pattern.

Q16. What is a rebase token?
A) Token with fixed supply B) Token whose balance changes automatically
C) Token that can be refunded D) Token with metadata

Quiz Questions (4/4)

Q13. What does the totalSupply() function return?
A) User's balance B) Maximum possible supply C) Current total tokens in existence D) Burned tokens
Answer: C – Returns the current total number of tokens that exist.

Q14. What is WETH?
A) A stablecoin B) ERC-20 wrapper for native ETH C) Governance token D) NFT standard
Answer: B – Wrapped Ether is an ERC-20 representation of native ETH.

Q15. What pattern does USDC use for upgradability?
A) Diamond pattern B) Transparent proxy C) No upgrades possible D) Beacon proxy
Answer: B – USDC uses an upgradable proxy pattern.

Q16. What is a rebase token?
A) Token with fixed supply B) Token whose balance changes automatically
C) Token that can be refunded D) Token with metadata
Answer: B – Rebase tokens like Ampleforth adjust balances algorithmically.

L17: ERC-20 Token Standard

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Explain the purpose and importance of the ERC-20 standard
- Describe the six required ERC-20 interface functions
- Understand the allowance mechanism for delegated transfers
- Recognize security considerations for token implementations

(c) Joerg Osterrieder 2025

What is ERC-20?

ERC-20 is the dominant fungible token standard on Ethereum:

- **ERC:** Ethereum Request for Comments (proposal process)
- **Fungible:** Each token is identical and interchangeable
- **Standard:** Common interface enables interoperability

Why Standardization Matters:

- Wallets support all ERC-20 tokens without custom code
- Exchanges can list new tokens easily
- Smart contracts can interact with any ERC-20 token

ERC-20 Interface: Six Required Functions

```
interface IERC20 {
    // Read functions
    function totalSupply() external view returns (uint256);
    function balanceOf(address account) external view returns (uint256);
    function allowance(address owner, address spender) external view returns (uint256);

    // Write functions
    function transfer(address recipient, uint256 amount) external returns (bool);
    function approve(address spender, uint256 amount) external returns (bool);
    function transferFrom(address sender, address recipient, uint256 amount)
        external returns (bool);

    // Required events
    event Transfer(address indexed from, address indexed to, uint256 value);
    event Approval(address indexed owner, address indexed spender, uint256 value);
}
```

Understanding Token Decimals

Tokens are stored as integers (no floating point on EVM):

Token	Decimals	1 Token Stored As
DAI, LINK, UNI	18	1,000,000,000,000,000,000
USDC, USDT	6	1,000,000
WBTC	8	100,000,000

Why Different Decimals?

- 18 decimals: Standard for most tokens (matches ETH wei)
- 6 decimals: Stablecoins match fiat cent precision (0.01)
- 8 decimals: WBTC matches Bitcoin's satoshi

Allowance Mechanism: Two-Step Spending

Problem: How can a smart contract spend your tokens?
Solution: Two-step approve + transferFrom pattern

Example: Alice trades 100 DAI on Uniswap

1. **Step 1 – Approve:** Alice calls `DAI.approve(UniswapRouter, 100e18)`
2. **Step 2 – Swap:** Uniswap calls `DAI.transferFrom(Alice, Pool, 100e18)`

Infinite Approval Risk:

- Users often approve `type(uint256).max` to avoid repeated approvals
- Risk: If contract is hacked, all approved tokens can be stolen

Security Considerations

Common ERC-20 Vulnerabilities:

1. **Approve Race Condition:**
   - Changing allowance from A to B allows spender to spend A+B
   - Solution: Use `increaseAllowance()` and `decreaseAllowance()`
2. **Integer Overflow (pre-Solidity 0.8.0):**
   - Solution: Use Solidity 0.8+ with built-in overflow checks
3. **Fee-on-Transfer Tokens:**
   - Some tokens deduct fees on transfer (e.g., SAFEMOON)
   - Breaks assumption that `transfer(amount)` sends exactly `amount`

OpenZeppelin: Industry Standard

Audited implementation used by thousands of projects:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract MyToken is ERC20 {
    constructor(uint256 initialSupply) ERC20("My Token", "MTK") {
        _mint(msg.sender, initialSupply * 10**decimals());
    }
}
```

Popular Extensions:

- **ERC20Burnable:** Allows token holders to burn tokens
- **ERC20Pausable:** Emergency circuit breaker for all transfers
- **ERC20Permit:** Gasless approvals via off-chain signatures (EIP-2612)

Real-World Examples: USDC vs DAI

Two approaches to stablecoin design:

Feature	USDC	DAI
Issuer	Circle (centralized)	MakerDAO (decentralized)
Backing	Cash + Treasuries	Crypto collateral
Decimals	6	18
Blacklist	Yes (regulatory)	No
Pausable	Yes	No
Permit (EIP-2612)	No	Yes

Key Tradeoff: Centralized tokens offer regulatory compliance; decentralized tokens offer censorship resistance.

Key Takeaways

1. **ERC-20 Standard:** Common interface for fungible tokens enabling universal wallet/exchange/DeFi support
2. **Core Functions:** totalSupply, balanceOf, transfer, approve, allowance, transferFrom
3. **Allowance Mechanism:** Two-step approve + transferFrom enables smart contract spending
4. **Decimals:** Convention is 18 for most tokens; stablecoins often use 6
5. **Security:** Use OpenZeppelin; beware approve race condition and fee-on-transfer tokens
6. **Extensions:** Permit (gasless approvals), Snapshot (governance), Pausable (emergency)

(c) Joerg Osterrieder 2025

The Token Ecosystem

Fungible Tokens

Digital Assets

Currency Standards

Images: Unsplash (CC0) – Erling Andersen, Ferhat Deniz Fors, Shubham Dhage

Quiz: ERC20 Token Standard

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does ERC-20's `totalSupply()` function return?
A) Number of token holders B) Total tokens ever minted C) Current circulating supply D) Maximum possible supply

Quiz (1–5)

Q1. What does ERC-20's `totalSupply()` function return?
A) Number of token holders B) Total tokens ever minted C) Current circulating supply D) Maximum possible supply
Answer: B – Returns total tokens minted minus burned tokens.

Q2. Which function allows a smart contract to spend tokens on your behalf?
A) transfer() B) approve() C) transferFrom() D) allowance()

Quiz (1–5)

Q1. What does ERC-20's `totalSupply()` function return?
A) Number of token holders B) Total tokens ever minted C) Current circulating supply D) Maximum possible supply
Answer: B – Returns total tokens minted minus burned tokens.

Q2. Which function allows a smart contract to spend tokens on your behalf?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: B – approve() grants permission; transferFrom() executes the transfer.

Q3. A token has 6 decimals. How is 1.5 tokens stored on-chain?
A) 1.5 B) 150 C) 1500 D) 1500000

Quiz (1–5)

Q1. What does ERC-20's `totalSupply()` function return?
A) Number of token holders B) Total tokens ever minted C) Current circulating supply D) Maximum possible supply
Answer: B – Returns total tokens minted minus burned tokens.

Q2. Which function allows a smart contract to spend tokens on your behalf?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: B – approve() grants permission; transferFrom() executes the transfer.

Q3. A token has 6 decimals. How is 1.5 tokens stored on-chain?
A) 1.5 B) 150 C) 1500 D) 1500000
Answer: D – $1.5 \times 10^6 = 1{,}500{,}000$ base units.

Q4. Which ERC-20 function is NOT required by the standard?
A) balanceOf() B) transfer() C) decimals() D) totalSupply()

Quiz (1–5)

Q1. What does ERC-20's `totalSupply()` function return?
A) Number of token holders B) Total tokens ever minted C) Current circulating supply D) Maximum possible supply
Answer: B – Returns total tokens minted minus burned tokens.

Q2. Which function allows a smart contract to spend tokens on your behalf?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: B – approve() grants permission; transferFrom() executes the transfer.

Q3. A token has 6 decimals. How is 1.5 tokens stored on-chain?
A) 1.5 B) 150 C) 1500 D) 1500000
Answer: D – $1.5 \times 10^6 = 1{,}500{,}000$ base units.

Q4. Which ERC-20 function is NOT required by the standard?
A) balanceOf() B) transfer() C) decimals() D) totalSupply()
Answer: C – decimals() is optional metadata; others are mandatory.

Q5. What does `allowance(owner, spender)` return?
A) Owner's balance B) Spender's balance C) Tokens spender can transfer D) Total approved tokens

Quiz (1–5)

Q1. What does ERC-20's `totalSupply()` function return?
A) Number of token holders B) Total tokens ever minted C) Current circulating supply D) Maximum possible supply
Answer: B – Returns total tokens minted minus burned tokens.

Q2. Which function allows a smart contract to spend tokens on your behalf?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: B – approve() grants permission; transferFrom() executes the transfer.

Q3. A token has 6 decimals. How is 1.5 tokens stored on-chain?
A) 1.5 B) 150 C) 1500 D) 1500000
Answer: D – $1.5 \times 10^6 = 1{,}500{,}000$ base units.

Q4. Which ERC-20 function is NOT required by the standard?
A) balanceOf() B) transfer() C) decimals() D) totalSupply()
Answer: C – decimals() is optional metadata; others are mandatory.

Q5. What does `allowance(owner, spender)` return?
A) Owner's balance B) Spender's balance C) Tokens spender can transfer D) Total approved tokens
Answer: C – Returns remaining tokens spender is allowed to transfer from owner.

Quiz (6–10)

Q6. What happens when you call `transfer(recipient, amount)` with insufficient balance?
A) Transfer 0 tokens B) Transaction reverts C) Transfer partial amount D) Return false

Quiz (6–10)

Q6. What happens when you call `transfer(recipient, amount)` with insufficient balance?
A) Transfer 0 tokens B) Transaction reverts C) Transfer partial amount D) Return false
Answer: B – require() statement causes revert if balance insufficient.

Q7. In a DEX swap, which function does the router contract call to get your tokens?
A) transfer() B) approve() C) transferFrom() D) allowance()

Quiz (6–10)

Q6. What happens when you call `transfer(recipient, amount)` with insufficient balance?
A) Transfer 0 tokens B) Transaction reverts C) Transfer partial amount D) Return false
Answer: B – require() statement causes revert if balance insufficient.

Q7. In a DEX swap, which function does the router contract call to get your tokens?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: C – After approval, DEX uses transferFrom() to move tokens.

Q8. Why do users approve `type(uint256).max` to DEX contracts?
A) Required by standard B) Saves gas on future trades C) More secure D) Prevents front-running

Quiz (6–10)

Q6. What happens when you call `transfer(recipient, amount)` with insufficient balance?
A) Transfer 0 tokens B) Transaction reverts C) Transfer partial amount D) Return false
Answer: B – require() statement causes revert if balance insufficient.

Q7. In a DEX swap, which function does the router contract call to get your tokens?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: C – After approval, DEX uses transferFrom() to move tokens.

Q8. Why do users approve `type(uint256).max` to DEX contracts?
A) Required by standard B) Saves gas on future trades C) More secure D) Prevents front-running
Answer: B – Infinite approval avoids repeated approval transactions.

Q9. What event must be emitted when tokens are transferred?
A) Approval B) Transfer C) Mint D) No event required

Quiz (6–10)

Q6. What happens when you call `transfer(recipient, amount)` with insufficient balance?
A) Transfer 0 tokens B) Transaction reverts C) Transfer partial amount D) Return false
Answer: B – require() statement causes revert if balance insufficient.

Q7. In a DEX swap, which function does the router contract call to get your tokens?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: C – After approval, DEX uses transferFrom() to move tokens.

Q8. Why do users approve `type(uint256).max` to DEX contracts?
A) Required by standard B) Saves gas on future trades C) More secure D) Prevents front-running
Answer: B – Infinite approval avoids repeated approval transactions.

Q9. What event must be emitted when tokens are transferred?
A) Approval B) Transfer C) Mint D) No event required
Answer: B – Transfer event logs from, to, and amount.

Q10. If Alice approves Bob for 100 tokens then transfers 40 to Carol, how many can Bob transfer?
A) 0 B) 40 C) 60 D) 100

Quiz (6–10)

Q6. What happens when you call `transfer(recipient, amount)` with insufficient balance?
A) Transfer 0 tokens B) Transaction reverts C) Transfer partial amount D) Return false
Answer: B – require() statement causes revert if balance insufficient.

Q7. In a DEX swap, which function does the router contract call to get your tokens?
A) transfer() B) approve() C) transferFrom() D) allowance()
Answer: C – After approval, DEX uses transferFrom() to move tokens.

Q8. Why do users approve `type(uint256).max` to DEX contracts?
A) Required by standard B) Saves gas on future trades C) More secure D) Prevents front-running
Answer: B – Infinite approval avoids repeated approval transactions.

Q9. What event must be emitted when tokens are transferred?
A) Approval B) Transfer C) Mint D) No event required
Answer: B – Transfer event logs from, to, and amount.

Q10. If Alice approves Bob for 100 tokens then transfers 40 to Carol, how many can Bob transfer?
A) 0 B) 40 C) 60 D) 100
Answer: D – Allowance is separate from balance; Bob can still transfer 100 if Alice has enough.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. Why does USDC use 6 decimals instead of 18?
A) Gas savings B) Matches fiat cents C) Required by Circle D) Security reasons

Quiz (11–15)

Q11. Why does USDC use 6 decimals instead of 18?
A) Gas savings B) Matches fiat cents C) Required by Circle D) Security reasons
Answer: B – 6 decimals aligns with USD cent precision (0.01).

Q12. What is the approve race condition vulnerability?
A) Front-running approvals B) Spending A+B when changing from A to B C) Approving 0 address D) Integer overflow

Quiz (11–15)

Q11. Why does USDC use 6 decimals instead of 18?
A) Gas savings B) Matches fiat cents C) Required by Circle D) Security reasons
Answer: B – 6 decimals aligns with USD cent precision (0.01).

Q12. What is the approve race condition vulnerability?
A) Front-running approvals B) Spending A+B when changing from A to B C) Approving 0 address D) Integer overflow
Answer: B – Malicious spender can spend old + new allowance if timed correctly.

Q13. Which minting strategy does Bitcoin (via WBTC) use?
A) Fixed supply B) Owner-controlled C) Algorithmic D) Proof-of-burn

Quiz (11–15)

Q11. Why does USDC use 6 decimals instead of 18?
A) Gas savings B) Matches fiat cents C) Required by Circle D) Security reasons
Answer: B – 6 decimals aligns with USD cent precision (0.01).

Q12. What is the approve race condition vulnerability?
A) Front-running approvals B) Spending A+B when changing from A to B C) Approving 0 address D) Integer overflow
Answer: B – Malicious spender can spend old + new allowance if timed correctly.

Q13. Which minting strategy does Bitcoin (via WBTC) use?
A) Fixed supply B) Owner-controlled C) Algorithmic D) Proof-of-burn
Answer: A – WBTC has fixed supply matching locked BTC; Bitcoin itself is algorithmic.

Q14. What does OpenZeppelin's ERC20Pausable extension enable?
A) Pause individual accounts B) Halt all transfers C) Pause approvals only D) Pause minting

Quiz (11–15)

Q11. Why does USDC use 6 decimals instead of 18?
A) Gas savings B) Matches fiat cents C) Required by Circle D) Security reasons
Answer: B – 6 decimals aligns with USD cent precision (0.01).

Q12. What is the approve race condition vulnerability?
A) Front-running approvals B) Spending A+B when changing from A to B C) Approving 0 address D) Integer overflow
Answer: B – Malicious spender can spend old + new allowance if timed correctly.

Q13. Which minting strategy does Bitcoin (via WBTC) use?
A) Fixed supply B) Owner-controlled C) Algorithmic D) Proof-of-burn
Answer: A – WBTC has fixed supply matching locked BTC; Bitcoin itself is algorithmic.

Q14. What does OpenZeppelin's ERC20Pausable extension enable?
A) Pause individual accounts B) Halt all transfers C) Pause approvals only D) Pause minting
Answer: B – Emergency circuit breaker stops all token transfers.

Q15. How does EIP-2612 permit() improve user experience?
A) Cheaper transfers B) Gasless approvals via signatures C) No allowance needed D) Batch transfers

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. Why does USDC use 6 decimals instead of 18?
A) Gas savings B) Matches fiat cents C) Required by Circle D) Security reasons
Answer: B – 6 decimals aligns with USD cent precision (0.01).

Q12. What is the approve race condition vulnerability?
A) Front-running approvals B) Spending A+B when changing from A to B C) Approving 0 address D) Integer overflow
Answer: B – Malicious spender can spend old + new allowance if timed correctly.

Q13. Which minting strategy does Bitcoin (via WBTC) use?
A) Fixed supply B) Owner-controlled C) Algorithmic D) Proof-of-burn
Answer: A – WBTC has fixed supply matching locked BTC; Bitcoin itself is algorithmic.

Q14. What does OpenZeppelin's ERC20Pausable extension enable?
A) Pause individual accounts B) Halt all transfers C) Pause approvals only D) Pause minting
Answer: B – Emergency circuit breaker stops all token transfers.

Q15. How does EIP-2612 permit() improve user experience?
A) Cheaper transfers B) Gasless approvals via signatures C) No allowance needed D) Batch transfers
Answer: B – Off-chain signature approval avoids separate approval transaction.

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What distinguishes DAI from USDC in terms of decentralization?
A) DAI has no blacklist B) DAI uses 18 decimals C) DAI is algorithmic D) All of the above

Quiz (16–20)

Q16. What distinguishes DAI from USDC in terms of decentralization?
A) DAI has no blacklist B) DAI uses 18 decimals C) DAI is algorithmic D) All of the above
Answer: D – DAI is more decentralized: no admin pause/blacklist, crypto-backed, 18 decimals.

Q17. What is a fee-on-transfer token?
A) Charges gas in tokens B) Deducts fee from transferred amount C) Requires ETH payment D) Burns on transfer

Quiz (16–20)

Q16. What distinguishes DAI from USDC in terms of decentralization?
A) DAI has no blacklist B) DAI uses 18 decimals C) DAI is algorithmic D) All of the above
Answer: D – DAI is more decentralized: no admin pause/blacklist, crypto-backed, 18 decimals.

Q17. What is a fee-on-transfer token?
A) Charges gas in tokens B) Deducts fee from transferred amount C) Requires ETH payment D) Burns on transfer
Answer: B – Some tokens (e.g., SAFEMOON) deduct percentage on each transfer.

Q18. What is WETH (Wrapped Ether)?
A) ERC-20 version of ETH B) Staked ETH C) Layer 2 ETH D) Synthetic ETH

Quiz (16–20)

Q16. What distinguishes DAI from USDC in terms of decentralization?
A) DAI has no blacklist B) DAI uses 18 decimals C) DAI is algorithmic D) All of the above
Answer: D – DAI is more decentralized: no admin pause/blacklist, crypto-backed, 18 decimals.

Q17. What is a fee-on-transfer token?
A) Charges gas in tokens B) Deducts fee from transferred amount C) Requires ETH payment D) Burns on transfer
Answer: B – Some tokens (e.g., SAFEMOON) deduct percentage on each transfer.

Q18. What is WETH (Wrapped Ether)?
A) ERC-20 version of ETH B) Staked ETH C) Layer 2 ETH D) Synthetic ETH
Answer: A – ERC-20 wrapper making ETH compatible with token standards.

Q19. If a token has 18 decimals, what is 1 wei in token terms?
A) 0.000000000000000001 tokens B) 1 token C) 0.01 tokens D) Depends on price

Quiz (16–20)

Q16. What distinguishes DAI from USDC in terms of decentralization?
A) DAI has no blacklist B) DAI uses 18 decimals C) DAI is algorithmic D) All of the above
Answer: D – DAI is more decentralized: no admin pause/blacklist, crypto-backed, 18 decimals.

Q17. What is a fee-on-transfer token?
A) Charges gas in tokens B) Deducts fee from transferred amount C) Requires ETH payment D) Burns on transfer
Answer: B – Some tokens (e.g., SAFEMOON) deduct percentage on each transfer.

Q18. What is WETH (Wrapped Ether)?
A) ERC-20 version of ETH B) Staked ETH C) Layer 2 ETH D) Synthetic ETH
Answer: A – ERC-20 wrapper making ETH compatible with token standards.

Q19. If a token has 18 decimals, what is 1 wei in token terms?
A) 0.000000000000000001 tokens B) 1 token C) 0.01 tokens D) Depends on price
Answer: A – 1 wei = 10^{-18} tokens (smallest unit).

Q20. What is the purpose of ERC-20 Snapshot extension?
A) Backup balances B) Capture balances at specific block for voting C) Prevent front-running D) Gas optimization

Quiz (16–20)

Q16. What distinguishes DAI from USDC in terms of decentralization?
A) DAI has no blacklist B) DAI uses 18 decimals C) DAI is algorithmic D) All of the above
Answer: D – DAI is more decentralized: no admin pause/blacklist, crypto-backed, 18 decimals.

Q17. What is a fee-on-transfer token?
A) Charges gas in tokens B) Deducts fee from transferred amount C) Requires ETH payment D) Burns on transfer
Answer: B – Some tokens (e.g., SAFEMOON) deduct percentage on each transfer.

Q18. What is WETH (Wrapped Ether)?
A) ERC-20 version of ETH B) Staked ETH C) Layer 2 ETH D) Synthetic ETH
Answer: A – ERC-20 wrapper making ETH compatible with token standards.

Q19. If a token has 18 decimals, what is 1 wei in token terms?
A) 0.000000000000000001 tokens B) 1 token C) 0.01 tokens D) Depends on price
Answer: A – 1 wei = 10^{-18} tokens (smallest unit).

Q20. What is the purpose of ERC-20 Snapshot extension?
A) Backup balances B) Capture balances at specific block for voting C) Prevent front-running D) Gas optimization
Answer: B – Records historical balances for governance votes or airdrops.

L18: ERC-721 and ERC-1155 Standards

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the difference between fungible and non-fungible tokens
- Describe the ERC-721 interface for NFTs
- Describe token metadata and IPFS storage
- Implement safe transfer mechanisms to prevent token loss
- Explain the ERC-1155 multi-token standard
- Compare batch operations and gas efficiency across standards
- Analyze real-world NFT projects (CryptoPunks, BAYC, ENS)

The Problem: How do we represent unique digital ownership?

The Challenge
Fungible tokens (ERC-20) represent interchangeable units like currency. But how do we represent unique digital items like art, collectibles, or real estate on-chain? Each item needs provable uniqueness and individual ownership tracking.

Why It Matters

- Without unique identifiers, we cannot represent scarce digital assets
- CryptoKitties (2017) congested Ethereum with custom NFT implementation, highlighting need for standard

What We Need

- System design principles
- Standard interface for non-fungible tokens with unique IDs
- Safe transfer mechanisms to prevent permanent loss
- Efficient batch operations for gaming/multi-asset use cases

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How ERC-721 and ERC-1155 standards address this challenge

Fungible vs Non-Fungible Tokens

Fungible (ERC-20):

- Interchangeable (1 USDC = 1 USDC)
- Divisible (can send 0.5 tokens)
- Uniform value
- Examples: Currencies, commodities

Analogy:

- Dollar bills
- Bitcoin
- Gold bars (fungible)

Non-Fungible (ERC-721):

- Unique (token ID 1 $\neq$ token ID 2)
- Indivisible (cannot send 0.5 NFT)
- Individual value
- Examples: Art, collectibles

Analogy:

- Real estate deeds
- Baseball cards
- Concert tickets (numbered seats)

Key Insight: ERC-721 tracks ownership of individual items, not aggregate balances

(c) Joerg Osterrieder 2025

Visual Comparison: Fungible vs Non-Fungible

Fungible vs Non-Fungible Tokens

Fungible (ERC-20)

1 USDC = 1 USDC

Interchangeable
Divisible
Uniform value

Examples: USDC, DAI, UNI

Non-Fungible (ERC-721)

Token #1 ≠ Token #2

Unique ownership
Indivisible
Individual value

Examples: BAYC, CryptoPunks, ENS

Fungible tokens are interchangeable; NFTs have unique identities and individual value

ERC-721 Interface: Core Functions

```
interface IERC721 {
    // Returns number of NFTs owned by owner
    function balanceOf(address owner) external view returns (uint256);

    // Returns owner of token ID
    function ownerOf(uint256 tokenId) external view returns (address);

    // Transfers token from 'from' to 'to' (unsafe, checks if recipient is contract)
    function transferFrom(address from, address to, uint256 tokenId) external;

    // Safe transfer with data (checks if recipient can receive NFTs)
    function safeTransferFrom(address from, address to, uint256 tokenId, bytes data)
        external;

    // Approve address to transfer specific token
    function approve(address to, uint256 tokenId) external;

    // Approve operator to transfer all tokens owned by caller
    function setApprovalForAll(address operator, bool approved) external;

    // Get approved address for specific token
    function getApproved(uint256 tokenId) external view returns (address);
}
```

ERC-721 Interface: Events

```
interface IERC721 {
    // Emitted when token is transferred (including minting and burning)
    event Transfer(address indexed from, address indexed to, uint256 indexed tokenId);

    // Emitted when approval is set for specific token
    event Approval(address indexed owner, address indexed approved,
                   uint256 indexed tokenId);

    // Emitted when operator approval is set for all tokens
    event ApprovalForAll(address indexed owner, address indexed operator, bool approved);
}
```

Key Differences from ERC-20:

- `tokenId` is indexed (can filter by specific NFT)
- Minting: `from = address(0)`, Burning: `to = address(0)`
- `ApprovalForAll` enables operators (e.g., OpenSea) to manage all NFTs

Safe Transfer Mechanism

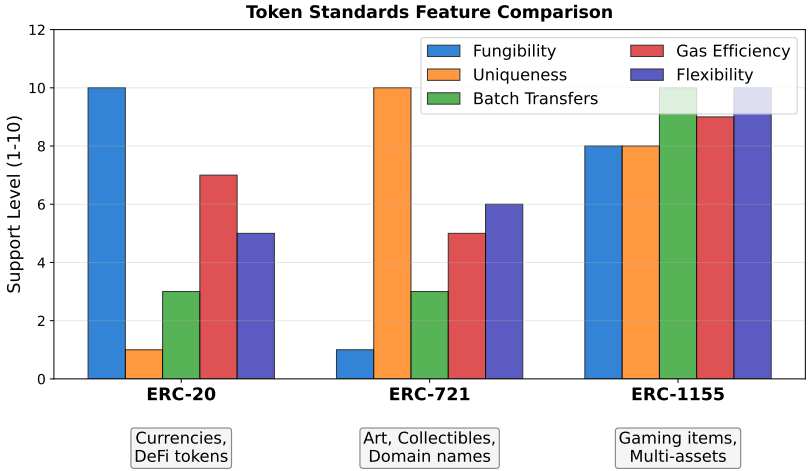
Problem: Transferring NFT to contract that cannot handle it = permanent loss

Solution: `safeTransferFrom()` checks if recipient is contract

```
interface IERC721Receiver {
    function onERC721Received(address operator, address from, uint256 tokenId,
                              bytes calldata data) external returns (bytes4);
}

// Safe transfer checks if recipient is contract
function safeTransferFrom(address from, address to, uint256 tokenId) public {
    transferFrom(from, to, tokenId);

    if (to.code.length > 0) {  // Recipient is contract
        require(
            IERC721Receiver(to).onERC721Received(msg.sender, from, tokenId, "")
                == IERC721Receiver.onERC721Received.selector,
            "Recipient cannot receive NFT"
        );
    }
}
```

Recipient must implement `onERC721Received()` to accept NFTs

Token Standards Comparison



ERC-1155 combines best features of both ERC-20 and ERC-721

ERC-721 Metadata Extension

Optional but widely used:

```
interface IERC721Metadata {
    function name() external view returns (string memory);    // Collection name
    function symbol() external view returns (string memory);  // Collection symbol
    function tokenURI(uint256 tokenId) external view returns (string memory);
}
```

Metadata JSON Structure:

```
{
  "name": "Bored Ape #1234",
  "description": "A unique Bored Ape Yacht Club NFT",
  "image": "ipfs://QmX7H9K2pZ3.../1234.png",
  "attributes": [
    {"trait_type": "Background", "value": "Blue"},
    {"trait_type": "Eyes", "value": "Laser"}
  ]
}
```

Metadata Storage: On-Chain vs IPFS

On-Chain Storage:

- Store metadata in contract storage
- Expensive (20,000 gas per 32 bytes)
- Permanent and immutable
- Example: Loot (full text on-chain)

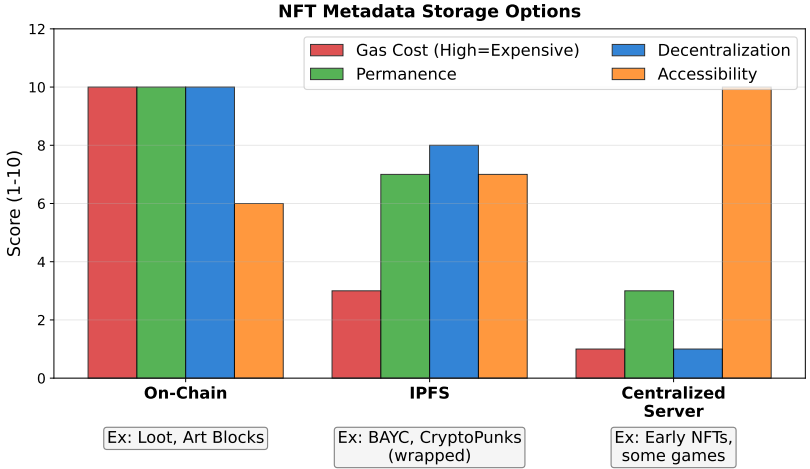
Cost: Storing 1 KB = approximately 640,000 gas (approximately $20-100)

IPFS Storage:

- Store only IPFS hash on-chain
- Cheap (approximately 20,000 gas per token)
- Content-addressable (hash = content)
- Example: Bored Ape Yacht Club

Cost: Storing hash = approximately 20,000 gas (approximately $1-5)

Metadata Storage Options Comparison



IPFS offers best balance of cost, decentralization, and permanence

IPFS: InterPlanetary File System

Key Concepts:

- **Content-Addressed:** hash = CID
- **Immutable:** change = new hash
- **Distributed:** peer network
- **Pinning:** keeps files alive

URIs:

`ipfs://QmX7H9K2pZ3.../meta.json`

Pros:

- Cheap storage
- Decentralized
- Immutable content

Cons:

- Needs IPFS node
- Not guaranteed available

Basic ERC-721 Implementation

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract MyNFT is ERC721, Ownable {
    uint256 private _tokenIdCounter;
    string private _baseTokenURI;

    constructor(string memory baseURI) ERC721("My NFT Collection", "MNFT") {
        _baseTokenURI = baseURI;
    }

    function mint(address to) public onlyOwner {
        _tokenIdCounter++;
        _safeMint(to, _tokenIdCounter);
    }

    function _baseURI() internal view override returns (string memory) {
        return _baseTokenURI;
    }
}
```

Real-World Example: CryptoPunks

Characteristics (2017):

- Pre-dates ERC-721
- 10,000 unique 24x24 punks
- On-chain images
- No royalties
- Wrapped for ERC-721

Key Functions:

- `getPunk`: claim
- `transferPunk`: transfer
- `offerPunkForSale`: list

Address:

0xb47e3cd837dDF8e4c...BBB

Real-World Example: Bored Ape Yacht Club (BAYC)

Technical (2021):

- Standard ERC-721 (OZ)
- 10,000 unique apes
- IPFS metadata
- Provenance hash

Contract Features:

- Fixed 10,000 supply
- Mint: 0.08 ETH
- Commercial rights

Address:

0xBC4CA0EdA7647A8aB...13D

Real-World Example: Ethereum Name Service (ENS)

Implementation:

- ERC-721 domains
- Token ID = name hash
- Own = control resolution
- Annual renewal fees

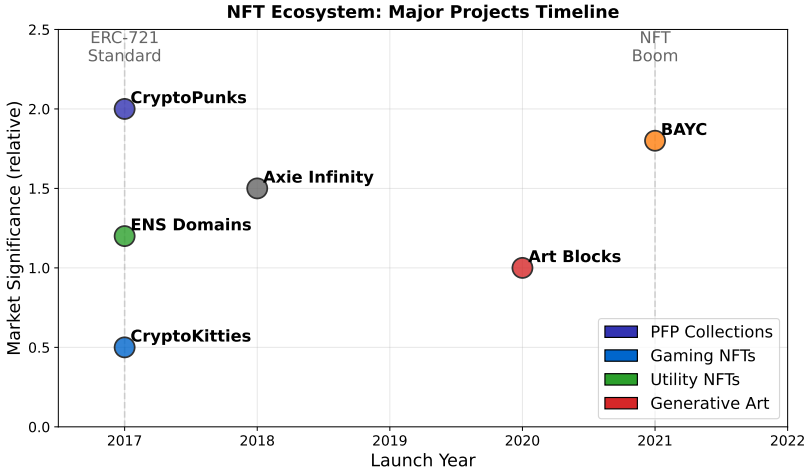
Key Contracts:

- Registry: name -¿ owner
- BaseRegistrar: ERC-721
- Resolver: name -¿ address

Unique Features:

- Subdomains (pay.alice.eth)
- Reverse resolution
- Text records
- Avatar support

NFT Ecosystem Overview



Major NFT projects span PFP collections, gaming, utility, and generative art categories

ERC-1155: Multi-Token Standard

Key Innovation:

- Multi-token contract
- Unique ID per type
- Fungible or NFT per ID
- Batch operations

Use Cases:

- Gaming: items + weapons
- Collectibles: common + rare
- Tickets: GA + VIP seats

vs ERC-20 + ERC-721:

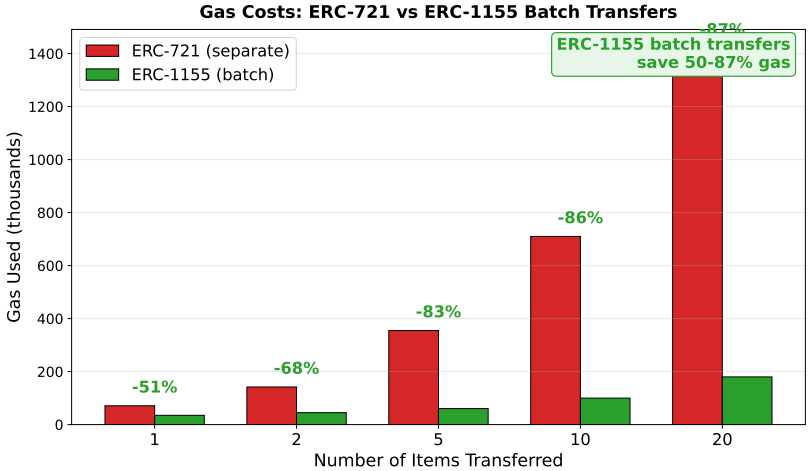
- One contract vs many
- Gas-efficient batches
- Atomic multi-swaps
- Reduced deployment

ERC-1155 Interface

```
interface IERC1155 {
    // Returns balance of token type id for account
    function balanceOf(address account, uint256 id) external view returns (uint256);

    // Returns balances of multiple account/id pairs
    function balanceOfBatch(address[] accounts, uint256[] ids)
        external view returns (uint256[]);

    // Transfer amount of token type id from 'from' to 'to'
    function safeTransferFrom(address from, address to, uint256 id, uint256 amount,
                              bytes data) external;

    // Batch transfer multiple token types
    function safeBatchTransferFrom(address from, address to, uint256[] ids,
                                   uint256[] amounts, bytes data) external;

    // Approve operator to manage all tokens for caller
    function setApprovalForAll(address operator, bool approved) external;
}
```

Note: No per-token approval (only operator approval)

Batch Operations: Gas Efficiency



ERC-1155 batch transfers reduce gas costs by 50-87% compared to separate ERC-721 transfers

Batch Operations: Cost Breakdown

Example: Transfer 5 different items

ERC-721 (5 separate transactions):

- Transaction 1: 71,000 gas
- Transaction 2: 71,000 gas
- Transaction 3: 71,000 gas
- Transaction 4: 71,000 gas
- Transaction 5: 71,000 gas

Total: 355,000 gas
At 30 Gwei: 0.01065 ETH

ERC-1155 (1 batch transaction):

- Transaction: 21,000 (base)
- + 5,000 per token (cold SLOAD)
- + 2,900 per token (storage update)
- = 60,500 gas total

Total: 60,500 gas
At 30 Gwei: 0.001815 ETH

Savings: 83% gas reduction

Royalties: EIP-2981

Standard for NFT royalties on secondary sales:

```
interface IERC2981 {
    // Returns royalty receiver and amount for given sale price
    function royaltyInfo(uint256 tokenId, uint256 salePrice)
        external view returns (address receiver, uint256 royaltyAmount);
}

contract MyNFTWithRoyalties is ERC721, ERC2981 {
    constructor() ERC721("My NFT", "MNFT") {
        _setDefaultRoyalty(msg.sender, 500);  // 5% royalty to deployer
    }

    function supportsInterface(bytes4 interfaceId)
        public view override(ERC721, ERC2981) returns (bool) {
        return super.supportsInterface(interfaceId);
    }
}
```

Note: Marketplaces (OpenSea, Blur) voluntarily honor royalties
Challenge: No on-chain enforcement, purely marketplace-enforced

Problem Solved? NFT Standards

The Original Problem

How do we represent unique digital ownership?

How NFT Standards Solve It

- ERC-721 assigns unique tokenId to each item, tracking individual ownership on-chain
- Safe transfer mechanisms prevent permanent loss via onERC721Received() callback
- ERC-1155 supports both fungible and non-fungible tokens in one contract, enabling efficient gaming/multi-asset use cases

Remaining Limitations

- Metadata typically stored off-chain (IPFS), creating availability dependency
- Royalty enforcement (EIP-2981) not guaranteed on-chain, relies on marketplace cooperation

Open Questions

- How to ensure creator royalties in a permissionless system where direct peer-to-peer transfers bypass marketplaces?
- Risk: IPFS content may become unavailable if unpinned, leaving NFT as pointer to missing data

NFT standards solve unique digital ownership representation but introduce trade-offs around off-chain metadata and royalty enforcement

(c) Joerg Osterrieder 2025

Key Takeaways

ERC-721:

- Unique, indivisible assets
- Safe transfers check recipients
- Metadata via tokenURI + IPFS
- Real: CryptoPunks, BAYC, ENS

ERC-1155:

- Multi-token standard
- Fungible + NFT in one contract
- Batch saves 83% gas
- Gaming, collectibles, tickets

Discussion Questions

1. Why is the `onERC721Received()` callback necessary for safe NFT transfers?
2. What are the tradeoffs between storing NFT metadata on-chain vs IPFS vs centralized servers?
3. How does ERC-1155 achieve gas savings compared to ERC-721 for batch operations?
4. Should NFT royalties (EIP-2981) be enforceable on-chain, or remain voluntary for marketplaces?
5. What are the implications of ENS domains being NFTs for domain squatting?

Next Lesson Preview: L19 - Token Lifecycle Management

Coming Up:

- Minting strategies
- Burning mechanisms
- Emergency pausing
- Access control patterns
- Upgradeability (proxy)

Preparation:

- OZ Ownable, Pausable
- Proxy patterns
- Gnosis Safe multi-sig

Quiz Questions - Part 1

Q1. What is the fundamental difference between fungible and non-fungible tokens?
A) Fungible tokens are divisible, NFTs are not B) Fungible tokens have uniform value, NFTs have individual value
C) Both A and B D) NFTs can only be images
Answer: C – Fungible tokens are interchangeable and divisible with uniform value, while NFTs are unique, indivisible, and have individual value.

Q2. Which ERC-721 function returns the owner of a specific token ID?
A) balanceOf() B) ownerOf() C) getApproved() D) tokenURI()
Answer: B – ownerOf(uint256 tokenId) returns the address that owns the specified token ID.

Q3. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if the recipient is a contract and whether it implements onERC721Received() to prevent token loss.

Q4. What must a contract implement to safely receive ERC-721 tokens?
A) IERC721 interface B) onERC721Received() function C) approve() function D) balanceOf() function
Answer: B – Contracts must implement onERC721Received() to signal they can handle incoming NFTs.

Q5. What is the purpose of setApprovalForAll() in ERC-721?
A) Approve a single token transfer B) Approve an operator to manage all tokens C) Set metadata D) Burn tokens
Answer: B – setApprovalForAll() allows an operator (e.g., OpenSea) to manage all of the owner's NFTs.

Quiz Questions - Part 2

Q6. What does tokenURI() return in the ERC-721 metadata extension?
A) Owner address B) Token ID C) URL to metadata JSON D) Token balance
Answer: C – tokenURI() returns a URI (typically IPFS) pointing to the token's metadata JSON file.

Q7. What does IPFS stand for and what is its key characteristic?
A) International Protocol File System - centralized B) InterPlanetary File System - content-addressable
C) Internal Permanent File Storage - blockchain-based D) Integrated Persistent File Server - cloud-based
Answer: B – IPFS is InterPlanetary File System, a decentralized content-addressable storage where file hash equals file identifier.

Q8. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – Storing 1 KB on-chain costs approximately 640,000 gas (20,000 gas per 32 bytes $\times$ 32).

Q9. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized, using a custom implementation.

Q10. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency while maintaining decentralization.

Quiz Questions - Part 3

Q11. What makes Ethereum Name Service (ENS) domains unique as NFTs?
A) They are renewable, not permanent B) They use ERC-20 instead of ERC-721 C) They are free D) They are burned after use
Answer: A – ENS domains are ERC-721 NFTs that require annual renewal fees, unlike most NFTs which are permanent.

Q12. What is the key innovation of ERC-1155?
A) Higher gas costs B) Single contract managing multiple token types C) Only fungible tokens D) No metadata support
Answer: B – ERC-1155 allows a single contract to manage both fungible and non-fungible token types.

Q13. How much gas can ERC-1155 batch transfers save compared to ERC-721?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – ERC-1155 batch operations reduce gas costs by 50-87% compared to separate ERC-721 transfers.

Q14. In ERC-1155, what does balanceOf() require compared to ERC-721?
A) Only account address B) Only token ID C) Both account address and token ID D) Operator approval
Answer: C – ERC-1155's balanceOf(address account, uint256 id) requires both parameters since tokens can be fungible.

Q15. What is a primary use case for ERC-1155?
A) Simple art collectibles B) Gaming items (fungible + non-fungible) C) Currency only D) Domain names
Answer: B – ERC-1155 is ideal for gaming where contracts manage both fungible items (potions) and unique items (legendary weapons).

Quiz Questions - Part 4

Q16. What does EIP-2981 standardize?
A) Token transfers B) NFT royalties C) Metadata format D) Batch operations
Answer: B – EIP-2981 defines a standard interface for NFT royalties on secondary sales.

Q17. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155
Answer: B – Royalties are not on-chain enforceable; marketplaces like OpenSea and Blur choose to honor them.

Q18. What happens when Transfer event has from = address(0)?
A) Token is transferred B) Token is burned C) Token is minted D) Token is approved
Answer: C – from = address(0) indicates token minting; to = address(0) indicates burning.

Q19. What is a provenance hash in NFT collections?
A) Owner's address hash B) Single hash proving pre-reveal image order C) IPFS content hash D) Token ID hash
Answer: B – Provenance hash is a cryptographic proof of the original order of NFTs before reveal, preventing manipulation.

Q20. Which statement about IPFS is FALSE?
A) Content is addressable by hash B) Files are guaranteed permanently available C) Changing content changes the hash D) It is decentralized
Answer: B – IPFS files are NOT guaranteed available unless actively pinned to IPFS nodes; unpinned files may become unavailable.

L18: ERC-721 and ERC-1155 Standards

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

NFT Ownership Proof

[COMIC: Person showing phone with NFT ownership on-chain]

"See? The blockchain proves I own this!"

The Promise

- Unique digital ownership
- Verifiable on-chain proof
- No intermediary needed

Today's Questions

- How does ERC-721 track uniqueness?
- What makes NFTs non-fungible?
- When is ERC-1155 better?

NFTs transform digital scarcity from promise to cryptographic proof. Let's see how.

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the difference between fungible and non-fungible tokens
- Describe the ERC-721 interface for NFTs
- Describe token metadata and IPFS storage
- Implement safe transfer mechanisms to prevent token loss
- Explain the ERC-1155 multi-token standard
- Compare batch operations and gas efficiency across standards
- Analyze real-world NFT projects (CryptoPunks, BAYC, ENS)

Building on L17: ERC-20 Token Standard

The Problem: How do we represent unique digital ownership?

The Challenge
Fungible tokens (ERC-20) represent interchangeable units like currency. But how do we represent unique digital items like art, collectibles, or real estate on-chain? Each item needs provable uniqueness and individual ownership tracking.

Why It Matters

- Without unique identifiers, we cannot represent scarce digital assets
- CryptoKitties (2017) congested Ethereum with custom NFT implementation, highlighting need for standard

What We Need

- System design principles
- Standard interface for non-fungible tokens with unique IDs
- Safe transfer mechanisms to prevent permanent loss
- Efficient batch operations for gaming/multi-asset use cases

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How ERC-721 and ERC-1155 standards address this challenge

What Makes NFTs Different from Regular Tokens?

Fungible (ERC-20):

- Interchangeable (1 USDC = 1 USDC)
- Divisible (can send 0.5 tokens)
- Uniform value
- Examples: Currencies, commodities

Analogy:

- Dollar bills
- Bitcoin
- Gold bars (fungible)

Non-Fungible (ERC-721):

- Unique (token ID 1 $\neq$ token ID 2)
- Indivisible (cannot send 0.5 NFT)
- Individual value
- Examples: Art, collectibles

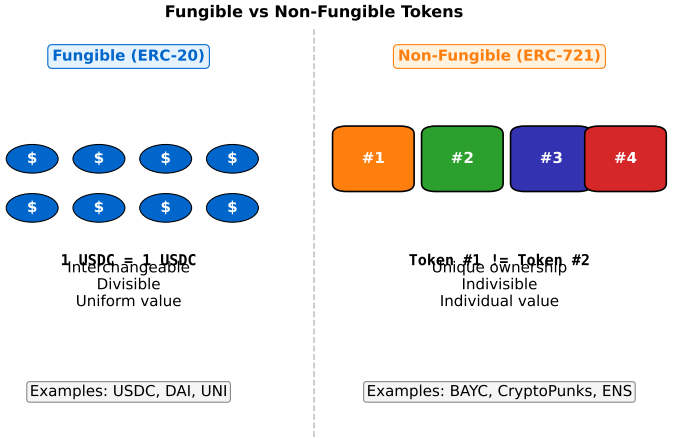
Analogy:

- Real estate deeds
- Baseball cards
- Concert tickets (numbered seats)

Key Insight: ERC-721 tracks ownership of individual items, not aggregate balances

Problem: How do we represent unique digital ownership? — Fungible tokens (like currency) are interchangeable, but NFTs use unique tokenIds to represent one-of-a-kind items like art or collectibles

How Do Fungible and Non-Fungible Tokens Differ Visually?



Fungible tokens are interchangeable; NFTs have unique identities and individual value

What Are the Core Functions of ERC-721?

```
interface IERC721 {
    // Returns number of NFTs owned by owner
    function balanceOf(address owner) external view returns (uint256);

    // Returns owner of token ID
    function ownerOf(uint256 tokenId) external view returns (address);

    // Transfers token from 'from' to 'to' (unsafe, checks if recipient is contract)
    function transferFrom(address from, address to, uint256 tokenId) external;

    // Safe transfer with data (checks if recipient can receive NFTs)
    function safeTransferFrom(address from, address to, uint256 tokenId, bytes data)
        external;

    // Approve address to transfer specific token
    function approve(address to, uint256 tokenId) external;

    // Approve operator to transfer all tokens owned by caller
    function setApprovalForAll(address operator, bool approved) external;

    // Get approved address for specific token
    function getApproved(uint256 tokenId) external view returns (address);
}
```

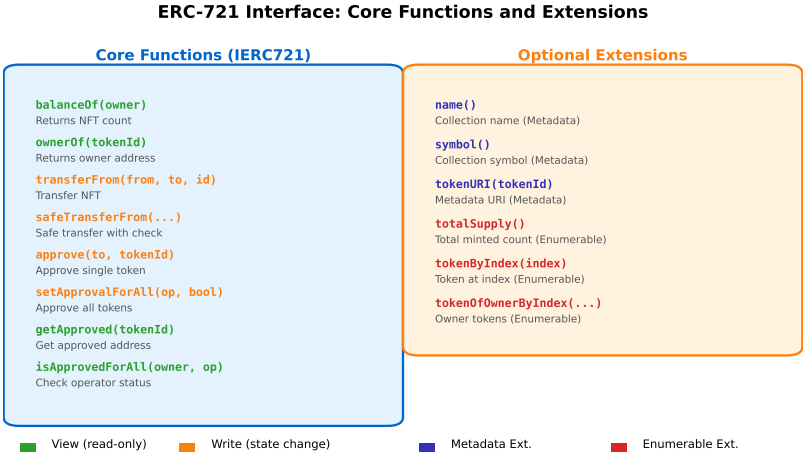
What Events Does ERC-721 Emit?

```
interface IERC721 {
    // Emitted when token is transferred (including minting and burning)
    event Transfer(address indexed from, address indexed to, uint256 indexed tokenId);

    // Emitted when approval is set for specific token
    event Approval(address indexed owner, address indexed approved,
                   uint256 indexed tokenId);

    // Emitted when operator approval is set for all tokens
    event ApprovalForAll(address indexed owner, address indexed operator, bool approved);
}
```

Key Differences from ERC-20:

- `tokenId` is indexed (can filter by specific NFT)
- Minting: `from = address(0)`, Burning: `to = address(0)`
- `ApprovalForAll` enables operators (e.g., OpenSea) to manage all NFTs

How Is the ERC-721 Interface Structured?



Core functions handle ownership and transfers; optional extensions add metadata and enumeration

How Does safeTransferFrom Prevent Token Loss?

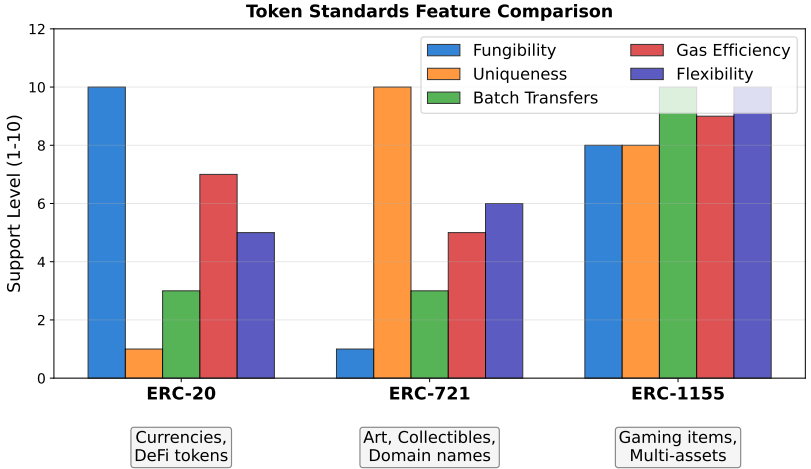
Problem: Transferring NFT to contract that cannot handle it = permanent loss

Solution: `safeTransferFrom()` checks if recipient is contract

```
interface IERC721Receiver {
    function onERC721Received(address operator, address from, uint256 tokenId,
                              bytes calldata data) external returns (bytes4);
}

// Safe transfer checks if recipient is contract
function safeTransferFrom(address from, address to, uint256 tokenId) public {
    transferFrom(from, to, tokenId);

    if (to.code.length > 0) {  // Recipient is contract
        require(
            IERC721Receiver(to).onERC721Received(msg.sender, from, tokenId, "")
                == IERC721Receiver.onERC721Received.selector,
            "Recipient cannot receive NFT"
        );
    }
}
```

Recipient must implement `onERC721Received()` to accept NFTs

How Do Token Standards Compare?



Problem: How do we represent unique digital ownership? — ERC-721 provides uniqueness via tokenId; ERC-1155 extends this to handle both unique items AND bulk quantities in one contract

What Does the ERC-721 Metadata Extension Provide?

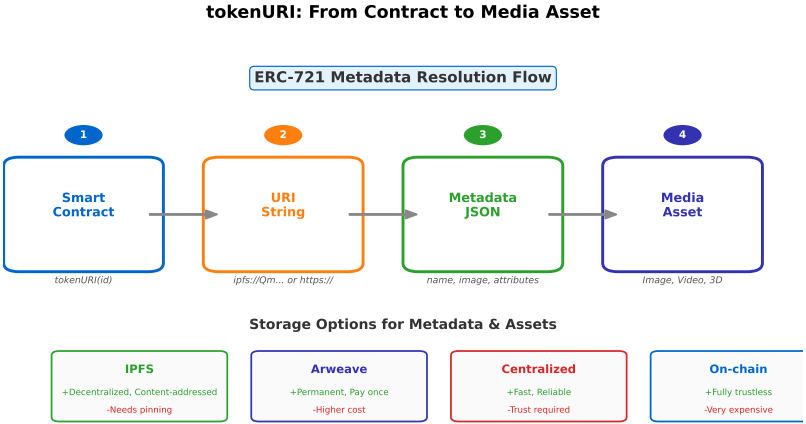
Optional but widely used:

```
interface IERC721Metadata {
    function name() external view returns (string memory);    // Collection name
    function symbol() external view returns (string memory);  // Collection symbol
    function tokenURI(uint256 tokenId) external view returns (string memory);
}
```

Metadata JSON Structure:

```
{
  "name": "Bored Ape #1234",
  "description": "A unique Bored Ape Yacht Club NFT",
  "image": "ipfs://QmX7H9K2pZ3.../1234.png",
  "attributes": [
    {"trait_type": "Background", "value": "Blue"},
    {"trait_type": "Eyes", "value": "Laser"}
  ]
}
```

How Does tokenURI Link Contracts to Media?



tokenURI returns a URI pointing to JSON metadata, which in turn points to the actual media asset

Where Should NFT Metadata Be Stored?

On-Chain Storage:

- Store metadata in contract storage
- Expensive (20,000 gas per 32 bytes)
- Permanent and immutable
- Example: Loot (full text on-chain)

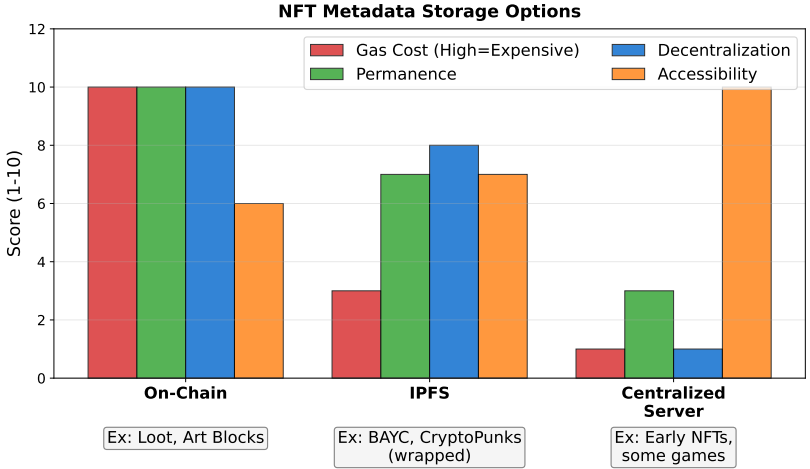
Cost: Storing 1 KB = approximately 640,000 gas (approximately $20-100)

IPFS Storage:

- Store only IPFS hash on-chain
- Cheap (approximately 20,000 gas per token)
- Content-addressable (hash = content)
- Example: Bored Ape Yacht Club

Cost: Storing hash = approximately 20,000 gas (approximately $1-5)

How Do Metadata Storage Options Compare?



IPFS offers best balance of cost, decentralization, and permanence

How Does IPFS Work for NFT Storage?

Key Concepts:

- **Content-Addressed:** hash = CID
- **Immutable:** change = new hash
- **Distributed:** peer network
- **Pinning:** keeps files alive

URIs:

`ipfs://QmX7H9K2pZ3.../meta.json`

Pros:

- Cheap storage
- Decentralized
- Immutable content

Cons:

- Needs IPFS node
- Not guaranteed available

How Do You Implement a Basic ERC-721 Contract?

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract MyNFT is ERC721, Ownable {
    uint256 private _tokenIdCounter;
    string private _baseTokenURI;

    constructor(string memory baseURI) ERC721("My NFT Collection", "MNFT") {
        _baseTokenURI = baseURI;
    }

    function mint(address to) public onlyOwner {
        _tokenIdCounter++;
        _safeMint(to, _tokenIdCounter);
    }

    function _baseURI() internal view override returns (string memory) {
        return _baseTokenURI;
    }
}
```

Problem: How do we represent unique digital ownership? — This implementation shows how _safeMint assigns each NFT a unique tokenId that maps to exactly one owner address

Problem Check-In: NFT Standards

Recall Our Problem

How do we represent unique digital ownership?

What We've Learned So Far

- ERC-721 uses a unique tokenId (a number) to identify each NFT – only one wallet can own tokenId 1 at any time
- safeTransferFrom() checks if the recipient can handle NFTs, preventing permanent loss to incompatible contracts
- Together, unique IDs + safe transfers create provable digital ownership that cannot be duplicated or lost

Still to Address

- ERC-1155 for efficient multi-token handling (gaming items, batch operations)
- How do we store the actual artwork if blockchain storage is too expensive?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we represent unique digital..."?

How Did CryptoPunks Implement NFTs?

Characteristics (2017):

- Pre-dates ERC-721
- 10,000 unique 24x24 punks
- On-chain images
- No royalties
- Wrapped for ERC-721

Key Functions:

- `getPunk`: claim
- `transferPunk`: transfer
- `offerPunkForSale`: list

Address:

0xb47e3cd837dDF8e4c...BBB

What Makes Bored Ape Yacht Club's Implementation Unique?

Technical (2021):

- Standard ERC-721 (OZ)
- 10,000 unique apes
- IPFS metadata
- Provenance hash

Contract Features:

- Fixed 10,000 supply
- Mint: 0.08 ETH
- Commercial rights

Address:

0xBC4CA0EdA7647A8aB...13D

How Does ENS Use ERC-721 for Domain Names?

Implementation:

- ERC-721 domains
- Token ID = name hash
- Own = control resolution
- Annual renewal fees

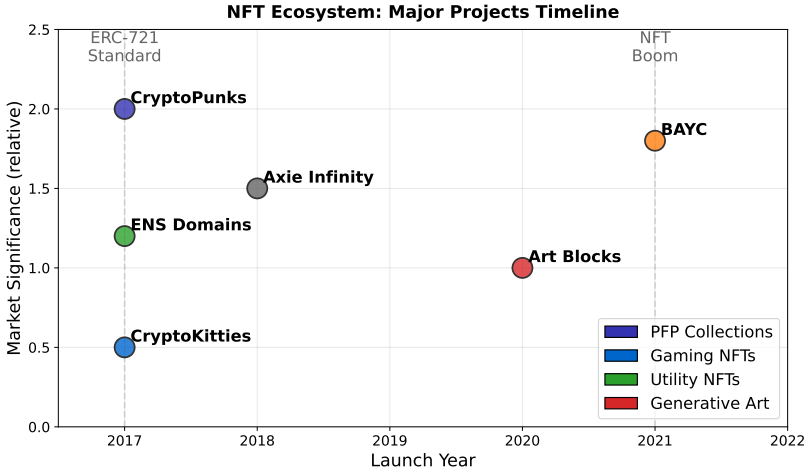
Key Contracts:

- Registry: name -¿ owner
- BaseRegistrar: ERC-721
- Resolver: name -¿ address

Unique Features:

- Subdomains (pay.alice.eth)
- Reverse resolution
- Text records
- Avatar support

What Does the NFT Ecosystem Look Like?



Major NFT projects span PFP collections, gaming, utility, and generative art categories

Why Use ERC-1155 Instead of ERC-721?

Key Innovation:

- Multi-token contract
- Unique ID per type
- Fungible or NFT per ID
- Batch operations

Use Cases:

- Gaming: items + weapons
- Collectibles: common + rare
- Tickets: GA + VIP seats

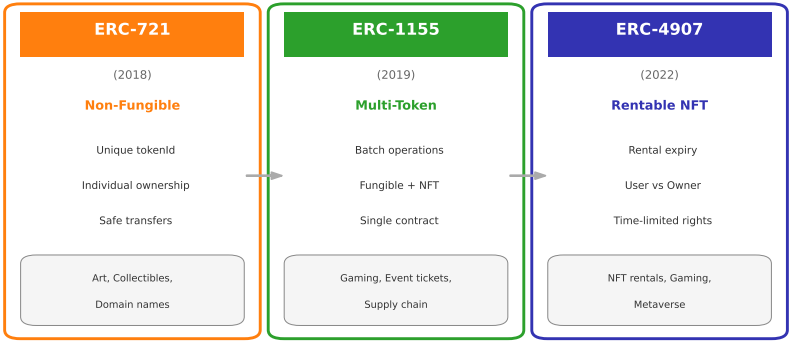
vs ERC-20 + ERC-721:

- One contract vs many
- Gas-efficient batches
- Atomic multi-swaps
- Reduced deployment

Problem: How do we represent unique digital ownership? — ERC-1155 solves the multi-asset problem: games need both unique weapons (NFTs) AND stackable potions (fungible) in one efficient contract

How Have NFT Standards Evolved?

NFT Standards: Features and Use Cases



Standard Evolution: More flexible + more efficient over time

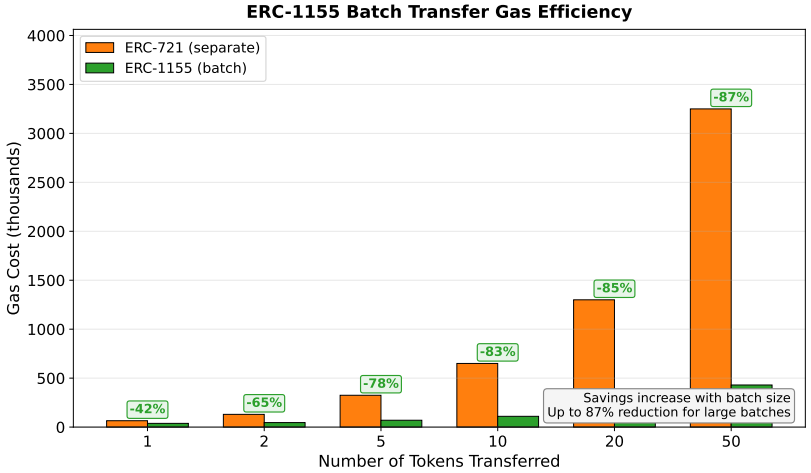
NFT standards have evolved to support more flexible and efficient use cases

What Functions Does ERC-1155 Provide?

```
interface IERC1155 {
    // Returns balance of token type id for account
    function balanceOf(address account, uint256 id) external view returns (uint256);

    // Returns balances of multiple account/id pairs
    function balanceOfBatch(address[] accounts, uint256[] ids)
        external view returns (uint256[]);

    // Transfer amount of token type id from 'from' to 'to'
    function safeTransferFrom(address from, address to, uint256 id, uint256 amount,
                              bytes data) external;

    // Batch transfer multiple token types
    function safeBatchTransferFrom(address from, address to, uint256[] ids,
                                   uint256[] amounts, bytes data) external;

    // Approve operator to manage all tokens for caller
    function setApprovalForAll(address operator, bool approved) external;
}
```

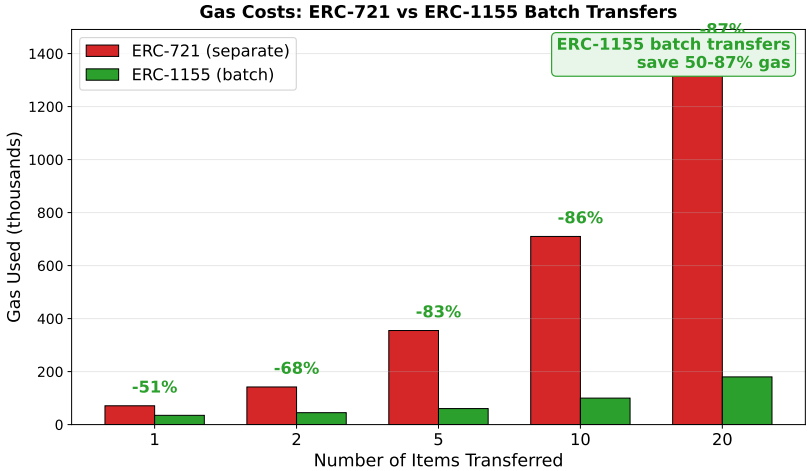
Note: No per-token approval (only operator approval)

How Efficient Are ERC-1155 Batch Transfers?



Batch operations become increasingly efficient as the number of tokens increases

How Much Gas Do Batch Transfers Save?



ERC-1155 batch transfers reduce gas costs by 50-87% compared to separate ERC-721 transfers

What Are the Real Costs of Batch Operations?

Example: Transfer 5 different items

ERC-721 (5 separate transactions):

- Transaction 1: 71,000 gas
- Transaction 2: 71,000 gas
- Transaction 3: 71,000 gas
- Transaction 4: 71,000 gas
- Transaction 5: 71,000 gas

Total: 355,000 gas
At 30 Gwei: 0.01065 ETH

ERC-1155 (1 batch transaction):

- Transaction: 21,000 (base)
- + 5,000 per token (cold SLOAD)
- + 2,900 per token (storage update)
- = 60,500 gas total

Total: 60,500 gas
At 30 Gwei: 0.001815 ETH

Savings: 83% gas reduction

How Do NFT Royalties Work with EIP-2981?

Standard for NFT royalties on secondary sales:

```
interface IERC2981 {
    // Returns royalty receiver and amount for given sale price
    function royaltyInfo(uint256 tokenId, uint256 salePrice)
        external view returns (address receiver, uint256 royaltyAmount);
}

contract MyNFTWithRoyalties is ERC721, ERC2981 {
    constructor() ERC721("My NFT", "MNFT") {
        _setDefaultRoyalty(msg.sender, 500);  // 5% royalty to deployer
    }

    function supportsInterface(bytes4 interfaceId)
        public view override(ERC721, ERC2981) returns (bool) {
        return super.supportsInterface(interfaceId);
    }
}
```

Note: Marketplaces (OpenSea, Blur) voluntarily honor royalties
Challenge: No on-chain enforcement, purely marketplace-enforced

Problem Solved? NFT Standards

The Original Problem

How do we represent unique digital ownership?

How NFT Standards Solve It

- ERC-721 assigns unique tokenId to each item, tracking individual ownership on-chain
- Safe transfer mechanisms prevent permanent loss via onERC721Received() callback
- ERC-1155 supports both fungible and non-fungible tokens in one contract, enabling efficient gaming/multi-asset use cases

Remaining Limitations

- Metadata typically stored off-chain (IPFS), creating availability dependency
- Royalty enforcement (EIP-2981) not guaranteed on-chain, relies on marketplace cooperation

Open Questions

- How to ensure creator royalties in a permissionless system where direct peer-to-peer transfers bypass marketplaces?
- Risk: IPFS content may become unavailable if unpinned, leaving NFT as pointer to missing data

NFT standards solve unique digital ownership representation but introduce trade-offs around off-chain metadata and royalty enforcement

(c) Joerg Osterrieder 2025

The Economics of NFT Standards

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: NFT Standards

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: NFT Standards

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

The Right-Click Save Debate

[COMIC: Person right-clicking NFT image vs owner with on-chain proof]

"I just saved your million-dollar JPEG!"

The Misconception

- Anyone can copy the image file
- But ownership is on-chain
- tokenId maps to exactly one address

What We Learned

- NFTs prove ownership, not exclusivity of viewing
- Value comes from verifiable provenance
- IPFS stores media, blockchain stores proof

Right-click saving copies pixels. Blockchain ownership is the social consensus that matters.

Key Takeaways

ERC-721:

- Unique, indivisible assets
- Safe transfers check recipients
- Metadata via tokenURI + IPFS
- Real: CryptoPunks, BAYC, ENS

Next Lesson: L19 – Token Lifecycle

ERC-1155:

- Multi-token standard
- Fungible + NFT in one contract
- Batch saves 83% gas
- Gaming, collectibles, tickets

Discussion Questions

1. Why is the `onERC721Received()` callback necessary for safe NFT transfers?
2. What are the tradeoffs between storing NFT metadata on-chain vs IPFS vs centralized servers?
3. How does ERC-1155 achieve gas savings compared to ERC-721 for batch operations?
4. Should NFT royalties (EIP-2981) be enforceable on-chain, or remain voluntary for marketplaces?
5. What are the implications of ENS domains being NFTs for domain squatting?

Next Lesson Preview: L19 - Token Lifecycle Management

Coming Up:

- Minting strategies
- Burning mechanisms
- Emergency pausing
- Access control patterns
- Upgradeability (proxy)

Preparation:

- OZ Ownable, Pausable
- Proxy patterns
- Gnosis Safe multi-sig

Quiz Questions - Part 1

Q1. What is the fundamental difference between fungible and non-fungible tokens?
A) Fungible tokens are divisible, NFTs are not B) Fungible tokens have uniform value, NFTs have individual value
C) Both A and B D) NFTs can only be images
Answer: C – Fungible tokens are interchangeable and divisible with uniform value, while NFTs are unique, indivisible, and have individual value.

Q2. Which ERC-721 function returns the owner of a specific token ID?
A) balanceOf() B) ownerOf() C) getApproved() D) tokenURI()
Answer: B – ownerOf(uint256 tokenId) returns the address that owns the specified token ID.

Q3. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if the recipient is a contract and whether it implements onERC721Received() to prevent token loss.

Q4. What must a contract implement to safely receive ERC-721 tokens?
A) IERC721 interface B) onERC721Received() function C) approve() function D) balanceOf() function
Answer: B – Contracts must implement onERC721Received() to signal they can handle incoming NFTs.

Q5. What is the purpose of setApprovalForAll() in ERC-721?
A) Approve a single token transfer B) Approve an operator to manage all tokens C) Set metadata D) Burn tokens
Answer: B – setApprovalForAll() allows an operator (e.g., OpenSea) to manage all of the owner's NFTs.

Quiz Questions - Part 2

Q6. What does tokenURI() return in the ERC-721 metadata extension?
A) Owner address B) Token ID C) URL to metadata JSON D) Token balance
Answer: C – tokenURI() returns a URI (typically IPFS) pointing to the token's metadata JSON file.

Q7. What does IPFS stand for and what is its key characteristic?
A) International Protocol File System - centralized B) InterPlanetary File System - content-addressable
C) Internal Permanent File Storage - blockchain-based D) Integrated Persistent File Server - cloud-based
Answer: B – IPFS is InterPlanetary File System, a decentralized content-addressable storage where file hash equals file identifier.

Q8. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – Storing 1 KB on-chain costs approximately 640,000 gas (20,000 gas per 32 bytes $\times$ 32).

Q9. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized, using a custom implementation.

Q10. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency while maintaining decentralization.

Quiz Questions - Part 3

Q11. What makes Ethereum Name Service (ENS) domains unique as NFTs?
A) They are renewable, not permanent B) They use ERC-20 instead of ERC-721 C) They are free D) They are burned after use
Answer: A – ENS domains are ERC-721 NFTs that require annual renewal fees, unlike most NFTs which are permanent.

Q12. What is the key innovation of ERC-1155?
A) Higher gas costs B) Single contract managing multiple token types C) Only fungible tokens D) No metadata support
Answer: B – ERC-1155 allows a single contract to manage both fungible and non-fungible token types.

Q13. How much gas can ERC-1155 batch transfers save compared to ERC-721?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – ERC-1155 batch operations reduce gas costs by 50-87% compared to separate ERC-721 transfers.

Q14. In ERC-1155, what does balanceOf() require compared to ERC-721?
A) Only account address B) Only token ID C) Both account address and token ID D) Operator approval
Answer: C – ERC-1155's balanceOf(address account, uint256 id) requires both parameters since tokens can be fungible.

Q15. What is a primary use case for ERC-1155?
A) Simple art collectibles B) Gaming items (fungible + non-fungible) C) Currency only D) Domain names
Answer: B – ERC-1155 is ideal for gaming where contracts manage both fungible items (potions) and unique items (legendary weapons).

Quiz Questions - Part 4

Q16. What does EIP-2981 standardize?
A) Token transfers B) NFT royalties C) Metadata format D) Batch operations
Answer: B – EIP-2981 defines a standard interface for NFT royalties on secondary sales.

Q17. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155
Answer: B – Royalties are not on-chain enforceable; marketplaces like OpenSea and Blur choose to honor them.

Q18. What happens when Transfer event has from = address(0)?
A) Token is transferred B) Token is burned C) Token is minted D) Token is approved
Answer: C – from = address(0) indicates token minting; to = address(0) indicates burning.

Q19. What is a provenance hash in NFT collections?
A) Owner's address hash B) Single hash proving pre-reveal image order C) IPFS content hash D) Token ID hash
Answer: B – Provenance hash is a cryptographic proof of the original order of NFTs before reveal, preventing manipulation.

Q20. Which statement about IPFS is FALSE?
A) Content is addressable by hash B) Files are guaranteed permanently available C) Changing content changes the hash D) It is decentralized
Answer: B – IPFS files are NOT guaranteed available unless actively pinned to IPFS nodes; unpinned files may become unavailable.

L18: ERC-721 and ERC-1155 Standards

Condensed Mini-Lecture (13 Slides)

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Distinguish between fungible (ERC-20) and non-fungible tokens (ERC-721)
- Describe the core ERC-721 interface functions and safe transfer mechanism
- Explain metadata storage options (on-chain vs IPFS)
- Understand ERC-1155 multi-token standard and batch operations
- Compare gas efficiency across token standards

Fungible vs Non-Fungible Tokens

Fungible (ERC-20):

- Interchangeable (1 USDC = 1 USDC)
- Divisible (can send 0.5 tokens)
- Uniform value
- Examples: Currencies, commodities

Analogy: Dollar bills, Bitcoin, gold bars

Non-Fungible (ERC-721):

- Unique (token ID 1 $\neq$ token ID 2)
- Indivisible (cannot send 0.5 NFT)
- Individual value
- Examples: Art, collectibles

Analogy: Real estate deeds, baseball cards

Key Insight: ERC-721 tracks ownership of individual items, not aggregate balances

(c) Joerg Osterrieder 2025

ERC-721 Interface: Core Functions

```
interface IERC721 {
    function balanceOf(address owner) external view returns (uint256);
    function ownerOf(uint256 tokenId) external view returns (address);
    function transferFrom(address from, address to, uint256 tokenId) external;
    function safeTransferFrom(address from, address to, uint256 tokenId) external;
    function approve(address to, uint256 tokenId) external;
    function setApprovalForAll(address operator, bool approved) external;
    function getApproved(uint256 tokenId) external view returns (address);

    event Transfer(address indexed from, address indexed to, uint256 indexed tokenId);
    event Approval(address indexed owner, address indexed approved, uint256 indexed tokenId);
    event ApprovalForAll(address indexed owner, address indexed operator, bool approved);
}
```

Key Differences from ERC-20:

- `tokenId` replaces amount – each NFT is uniquely identified
- `setApprovalForAll` enables operators (e.g., OpenSea) to manage all NFTs

Safe Transfer Mechanism

Problem: Transferring NFT to contract that cannot handle it = permanent loss

Solution: `safeTransferFrom()` checks if recipient can receive NFTs

```
interface IERC721Receiver {
    function onERC721Received(address operator, address from,
                              uint256 tokenId, bytes calldata data)
        external returns (bytes4);
}

// Safe transfer checks if recipient is contract
if (to.code.length > 0) {  // Recipient is contract
    require(
        IERC721Receiver(to).onERC721Received(msg.sender, from, tokenId, "")
            == IERC721Receiver.onERC721Received.selector,
        "Recipient cannot receive NFT"
    );
}
```

Contracts must implement `onERC721Received()` to accept NFTs

Metadata Storage: On-Chain vs IPFS

On-Chain Storage:

- Store metadata in contract storage
- Expensive (640,000 gas per 1 KB)
- Permanent and immutable
- Example: Loot (full text on-chain)

Cost: $20–100 per KB

IPFS Storage:

- Store only hash on-chain
- Cheap (20,000 gas per token)
- Content-addressable (hash = content)
- Example: Bored Ape Yacht Club

Cost: $1–5 per token

IPFS URI Format: `ipfs://QmX7H9K2pZ3.../metadata.json`
Tradeoff: IPFS requires pinning for guaranteed availability

ERC-1155: Multi-Token Standard

Unified standard for fungible and non-fungible tokens:

Key Innovation:

- Single contract manages multiple token types
- Each token ID can be fungible (multiple units) or non-fungible (single unit)
- Batch operations: transfer multiple types in one transaction

Use Cases:

- **Gaming:** Swords (fungible) + unique armor (non-fungible) in same contract
- **Collectibles:** Common cards (fungible) + legendary cards (non-fungible)
- **Event tickets:** General admission (fungible) + VIP seats (non-fungible)

Advantages: Reduced deployment costs, gas-efficient batch transfers, atomic swaps

(c) Joerg Osterrieder 2025

ERC-1155 Interface

```
interface IERC1155 {
    // Balance includes both account and token type ID
    function balanceOf(address account, uint256 id) external view returns (uint256);

    // Batch balance query
    function balanceOfBatch(address[] accounts, uint256[] ids) external view returns (uint256[]);

    // Transfer with amount (can be > 1 for fungible types)
    function safeTransferFrom(address from, address to, uint256 id,
                              uint256 amount, bytes data) external;

    // Batch transfer multiple token types in single transaction
    function safeBatchTransferFrom(address from, address to, uint256[] ids,
                                   uint256[] amounts, bytes data) external;

    // Only operator approval (no per-token approval)
    function setApprovalForAll(address operator, bool approved) external;
}
```

Note: No per-token approval like ERC-721 – only operator-level approval

Batch Operations: Gas Efficiency

Example: Transfer 5 different items

ERC-721 (5 separate transactions):

- 5 $\times$ 71,000 gas each
- **Total: 355,000 gas**
- At 30 Gwei: 0.01065 ETH

ERC-1155 (1 batch transaction):

- 21,000 base + 7,900 per token
- **Total: 60,500 gas**
- At 30 Gwei: 0.001815 ETH

Savings: 83% gas reduction with ERC-1155 batch transfers

ERC-1155 batch transfers reduce gas costs by 50–87% compared to separate ERC-721 transfers

Real-World NFT Projects

CryptoPunks (2017):

- Pre-dates ERC-721 standard (custom implementation)
- 10,000 unique 24x24 pixel art characters, images stored on-chain

Bored Ape Yacht Club (2021):

- Standard ERC-721 implementation (OpenZeppelin)
- Metadata stored on IPFS, provenance hash for pre-reveal order

Ethereum Name Service (ENS):

- ENS domains are ERC-721 NFTs (e.g., `vitalik.eth`)
- Renewable (annual fees), supports subdomains and reverse resolution

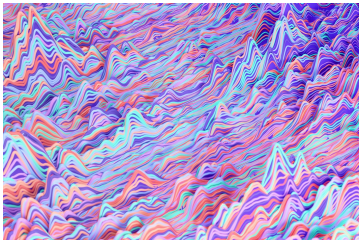
EIP-2981 Royalties: Standard for secondary sale royalties (voluntarily enforced)

Key Takeaways

1. **ERC-721:** Standard for unique, indivisible NFTs with individual ownership
2. **Safe Transfers:** `safeTransferFrom()` prevents token loss by checking recipient compatibility
3. **Metadata:** Token URIs point to JSON metadata, typically stored on IPFS for cost efficiency
4. **ERC-1155:** Multi-token standard supporting both fungible and non-fungible tokens in single contract
5. **Batch Operations:** ERC-1155 batch transfers reduce gas costs by up to 83%
6. **Real-World:** CryptoPunks (pre-ERC-721), BAYC (standard ERC-721), ENS (renewable NFT domains)

NFT Ecosystem: Visual Gallery

Digital Art NFTs



Generative Collectibles

Unique Digital Assets

Images: Unsplash (CC0) – Viktor Forgacs, Maxim Berg, rc.xyz NFT gallery

Quiz Questions – Part 1

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference
Answer: B – ERC-721 tokens have unique token IDs and cannot be divided.

Q2. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if recipient implements onERC721Received().

Q3. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – Storing 1 KB costs approximately 640,000 gas (20,000 gas per 32 bytes).

Q4. What is the key innovation of ERC-1155?
A) Higher gas costs B) Single contract managing multiple token types C) Only fungible tokens D) No metadata
Answer: B – ERC-1155 allows one contract to manage both fungible and non-fungible tokens.

Quiz Questions – Part 2

Q5. How much gas can ERC-1155 batch transfers save compared to ERC-721?
A) 10–20% B) 30–40% C) 50–87% D) No savings
Answer: C – ERC-1155 batch operations reduce gas costs by 50–87%.

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized.

Q7. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency.

Q8. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155
Answer: B – Royalties are not on-chain enforceable; marketplaces choose to honor them.

L18: ERC-721 and ERC-1155 Standards

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

January 2026

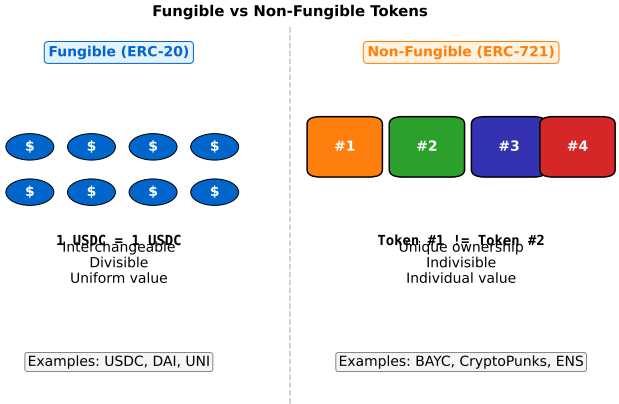
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

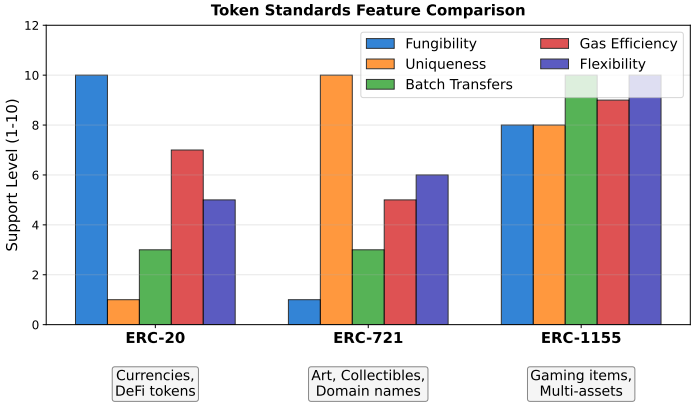
- Distinguish fungible from non-fungible tokens
- Describe ERC-721 interface for NFTs
- Explain metadata storage (on-chain vs IPFS)
- Compare ERC-1155 batch operations and gas efficiency

Fungible vs Non-Fungible Tokens



Fungible: Interchangeable, divisible — **Non-Fungible:** Unique, indivisible

Token Standards Comparison



ERC-20: Fungible — **ERC-721:** NFT — **ERC-1155:** Multi-token (both)

ERC-721 Core Functions

Ownership:

- `balanceOf(owner)`: Number of NFTs owned
- `ownerOf(tokenId)`: Owner of specific token

Transfer:

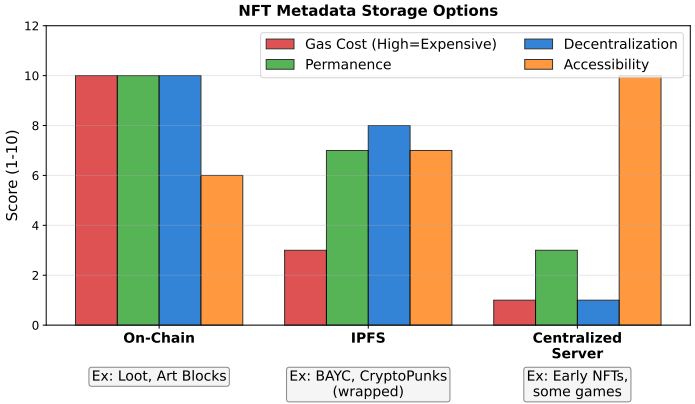
- `transferFrom()`: Basic transfer (unsafe)
- `safeTransferFrom()`: Checks if recipient can receive NFTs

Approval:

- `approve()`: Approve single token transfer
- `setApprovalForAll()`: Approve operator for all tokens

Safe Transfer: Prevents token loss by checking recipient implements `onERC721Received()`.

Metadata Storage Options



IPFS: Best balance of cost, decentralization, and permanence.

ERC-1155: Multi-Token Standard

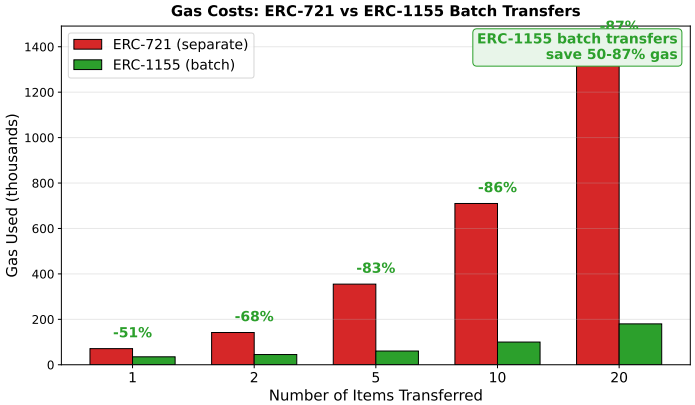
Key Innovation:

- Single contract manages multiple token types
- Each token ID can be fungible OR non-fungible
- Batch operations: Transfer multiple types in one transaction

Use Cases:

- Gaming: Swords (fungible) + unique armor (NFT) in same contract
- Collectibles: Common cards + legendary cards
- Event tickets: General admission + VIP seats

Batch Operations: Gas Savings



ERC-1155 batch transfers reduce gas by 50-87% vs separate ERC-721 transfers.

NFT Case Studies

CryptoPunks (2017):

- Pre-dates ERC-721, 10,000 pixel art characters
- Images stored on-chain

Bored Ape Yacht Club (2021):

- Standard ERC-721, metadata on IPFS
- Commercial rights to holders

ENS Domains:

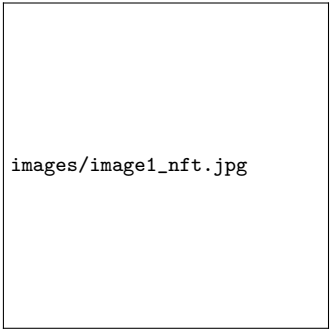
- ERC-721 NFTs representing .eth domains
- Renewable (annual fees), not permanent

Key Takeaways

1. **ERC-721:** NFT standard for unique, indivisible assets
2. **Safe Transfers:** Prevent token loss via `onERC721Received()` check
3. **Metadata:** IPFS offers cost-efficient decentralized storage
4. **ERC-1155:** Multi-token standard for fungible + non-fungible
5. **Batch Operations:** 50-87% gas savings with ERC-1155

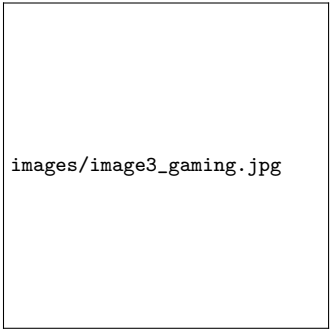
Royalties (EIP-2981): Standard interface, but marketplace-enforced (not on-chain).

NFT Standards in Practice



NFT Art

Digital Collectibles



Gaming Items

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Fundamental difference: fungible vs non-fungible?
A) Divisibility only B) Both divisibility and uniqueness C) Price only D) Storage only

Quiz (1/2)

Q1. Fundamental difference: fungible vs non-fungible?
A) Divisibility only B) Both divisibility and uniqueness C) Price only D) Storage only
Answer: B – Fungible: interchangeable, divisible. NFT: unique, indivisible.

Q2. What does safeTransferFrom() check?
A) Balance B) Approval C) Whether recipient can receive NFTs D) Gas limit

Quiz (1/2)

Q1. Fundamental difference: fungible vs non-fungible?
A) Divisibility only B) Both divisibility and uniqueness C) Price only D) Storage only
Answer: B – Fungible: interchangeable, divisible. NFT: unique, indivisible.

Q2. What does safeTransferFrom() check?
A) Balance B) Approval C) Whether recipient can receive NFTs D) Gas limit
Answer: C – Checks if recipient implements onERC721Received().

Q3. Approximate gas to store 1 KB on-chain?
A) 20,000 B) 160,000 C) 640,000 D) 1,000,000

Quiz (1/2)

Q1. Fundamental difference: fungible vs non-fungible?
A) Divisibility only B) Both divisibility and uniqueness C) Price only D) Storage only
Answer: B – Fungible: interchangeable, divisible. NFT: unique, indivisible.

Q2. What does safeTransferFrom() check?
A) Balance B) Approval C) Whether recipient can receive NFTs D) Gas limit
Answer: C – Checks if recipient implements onERC721Received().

Q3. Approximate gas to store 1 KB on-chain?
A) 20,000 B) 160,000 C) 640,000 D) 1,000,000
Answer: C – 640,000 gas (20,000 per 32 bytes).

Q4. Which NFT project pre-dates ERC-721?
A) BAYC B) CryptoPunks C) ENS D) Decentraland

Quiz (1/2)

Q1. Fundamental difference: fungible vs non-fungible?
A) Divisibility only B) Both divisibility and uniqueness C) Price only D) Storage only
Answer: B – Fungible: interchangeable, divisible. NFT: unique, indivisible.

Q2. What does safeTransferFrom() check?
A) Balance B) Approval C) Whether recipient can receive NFTs D) Gas limit
Answer: C – Checks if recipient implements onERC721Received().

Q3. Approximate gas to store 1 KB on-chain?
A) 20,000 B) 160,000 C) 640,000 D) 1,000,000
Answer: C – 640,000 gas (20,000 per 32 bytes).

Q4. Which NFT project pre-dates ERC-721?
A) BAYC B) CryptoPunks C) ENS D) Decentraland
Answer: B – CryptoPunks launched 2017, before ERC-721 was finalized.

Q5. Key innovation of ERC-1155?
A) Higher gas B) Single contract for multiple token types C) Only fungible D) No metadata

Quiz (1/2)

Q1. Fundamental difference: fungible vs non-fungible?
A) Divisibility only B) Both divisibility and uniqueness C) Price only D) Storage only
Answer: B – Fungible: interchangeable, divisible. NFT: unique, indivisible.

Q2. What does safeTransferFrom() check?
A) Balance B) Approval C) Whether recipient can receive NFTs D) Gas limit
Answer: C – Checks if recipient implements onERC721Received().

Q3. Approximate gas to store 1 KB on-chain?
A) 20,000 B) 160,000 C) 640,000 D) 1,000,000
Answer: C – 640,000 gas (20,000 per 32 bytes).

Q4. Which NFT project pre-dates ERC-721?
A) BAYC B) CryptoPunks C) ENS D) Decentraland
Answer: B – CryptoPunks launched 2017, before ERC-721 was finalized.

Q5. Key innovation of ERC-1155?
A) Higher gas B) Single contract for multiple token types C) Only fungible D) No metadata
Answer: B – One contract manages both fungible and non-fungible.

Quiz (2/2)

Q6. How much can ERC-1155 batch transfers save?
A) 10-20% B) 30-40% C) 50-87% D) No savings

Quiz (2/2)

Q6. How much can ERC-1155 batch transfers save?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – 50-87% gas reduction vs separate ERC-721 transfers.

Q7. What makes ENS domains unique as NFTs?
A) Renewable, not permanent B) Use ERC-20 C) Free D) Burned after use

Quiz (2/2)

Q6. How much can ERC-1155 batch transfers save?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – 50-87% gas reduction vs separate ERC-721 transfers.

Q7. What makes ENS domains unique as NFTs?
A) Renewable, not permanent B) Use ERC-20 C) Free D) Burned after use
Answer: A – ENS requires annual renewal fees.

Q8. What does IPFS stand for?
A) International Protocol B) InterPlanetary File System C) Internal Permanent D) Integrated Persistent

Quiz (2/2)

Q6. How much can ERC-1155 batch transfers save?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – 50-87% gas reduction vs separate ERC-721 transfers.

Q7. What makes ENS domains unique as NFTs?
A) Renewable, not permanent B) Use ERC-20 C) Free D) Burned after use
Answer: A – ENS requires annual renewal fees.

Q8. What does IPFS stand for?
A) International Protocol B) InterPlanetary File System C) Internal Permanent D) Integrated Persistent
Answer: B – InterPlanetary File System, content-addressable storage.

Q9. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically B) No, marketplace-enforced C) Only OpenSea D) Only ERC-1155

Quiz (2/2)

Q6. How much can ERC-1155 batch transfers save?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – 50-87% gas reduction vs separate ERC-721 transfers.

Q7. What makes ENS domains unique as NFTs?
A) Renewable, not permanent B) Use ERC-20 C) Free D) Burned after use
Answer: A – ENS requires annual renewal fees.

Q8. What does IPFS stand for?
A) International Protocol B) InterPlanetary File System C) Internal Permanent D) Integrated Persistent
Answer: B – InterPlanetary File System, content-addressable storage.

Q9. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically B) No, marketplace-enforced C) Only OpenSea D) Only ERC-1155
Answer: B – Royalties are voluntarily honored by marketplaces.

Q10. What indicates minting in Transfer event?
A) to = 0x0 B) from = 0x0 C) amount = 0 D) tokenId = 0

Quiz (2/2)

Q6. How much can ERC-1155 batch transfers save?
A) 10-20% B) 30-40% C) 50-87% D) No savings
Answer: C – 50-87% gas reduction vs separate ERC-721 transfers.

Q7. What makes ENS domains unique as NFTs?
A) Renewable, not permanent B) Use ERC-20 C) Free D) Burned after use
Answer: A – ENS requires annual renewal fees.

Q8. What does IPFS stand for?
A) International Protocol B) InterPlanetary File System C) Internal Permanent D) Integrated Persistent
Answer: B – InterPlanetary File System, content-addressable storage.

Q9. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically B) No, marketplace-enforced C) Only OpenSea D) Only ERC-1155
Answer: B – Royalties are voluntarily honored by marketplaces.

Q10. What indicates minting in Transfer event?
A) to = 0x0 B) from = 0x0 C) amount = 0 D) tokenId = 0
Answer: B – from = address(0) indicates minting.

Thank you

Questions?

Next: L19 – Token Lifecycle Management

Quiz: ERC721 ERC1155 Standards

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference

Quiz (1–5)

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference
Answer: B – ERC-721 tokens have unique token IDs and cannot be divided.

Q2. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits

Quiz (1–5)

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference
Answer: B – ERC-721 tokens have unique token IDs and cannot be divided.

Q2. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if recipient implements onERC721Received().

Q3. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference
Answer: B – ERC-721 tokens have unique token IDs and cannot be divided.

Q2. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if recipient implements onERC721Received().

Q3. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – Storing 1 KB costs approximately 640,000 gas (20,000 gas per 32 bytes).

Q4. What is the key innovation of ERC-1155?
A) Higher gas costs B) Single contract managing multiple token types C) Only fungible tokens D) No metadata

Quiz (1–5)

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference
Answer: B – ERC-721 tokens have unique token IDs and cannot be divided.

Q2. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if recipient implements onERC721Received().

Q3. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – Storing 1 KB costs approximately 640,000 gas (20,000 gas per 32 bytes).

Q4. What is the key innovation of ERC-1155?
A) Higher gas costs B) Single contract managing multiple token types C) Only fungible tokens D) No metadata
Answer: B – ERC-1155 allows one contract to manage both fungible and non-fungible tokens.

Q5. How much gas can ERC-1155 batch transfers save compared to ERC-721?
A) 10–20% B) 30–40% C) 50–87% D) No savings

Quiz (1–5)

Q1. What is the fundamental difference between ERC-20 and ERC-721 tokens?
A) ERC-20 is newer B) ERC-721 tokens are unique and indivisible C) ERC-20 cannot be transferred D) No difference
Answer: B – ERC-721 tokens have unique token IDs and cannot be divided.

Q2. What does safeTransferFrom() check that transferFrom() does not?
A) Sufficient balance B) Token approval C) Whether recipient can receive NFTs D) Gas limits
Answer: C – safeTransferFrom() checks if recipient implements onERC721Received().

Q3. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – Storing 1 KB costs approximately 640,000 gas (20,000 gas per 32 bytes).

Q4. What is the key innovation of ERC-1155?
A) Higher gas costs B) Single contract managing multiple token types C) Only fungible tokens D) No metadata
Answer: B – ERC-1155 allows one contract to manage both fungible and non-fungible tokens.

Q5. How much gas can ERC-1155 batch transfers save compared to ERC-721?
A) 10–20% B) 30–40% C) 50–87% D) No savings
Answer: C – ERC-1155 batch operations reduce gas costs by 50–87%.

Quiz (6–10)

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland

Quiz (6–10)

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized.

Q7. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave

Quiz (6–10)

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized.

Q7. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency.

Q8. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155

Quiz (6–10)

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized.

Q7. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency.

Q8. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155
Answer: B – Royalties are not on-chain enforceable; marketplaces choose to honor them.

Q9. What must a contract implement to safely receive ERC-721 tokens?
A) IERC721 interface B) onERC721Received() function C) approve() function D) balanceOf() function

Quiz (6–10)

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized.

Q7. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency.

Q8. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155
Answer: B – Royalties are not on-chain enforceable; marketplaces choose to honor them.

Q9. What must a contract implement to safely receive ERC-721 tokens?
A) IERC721 interface B) onERC721Received() function C) approve() function D) balanceOf() function
Answer: B – Contracts must implement onERC721Received() returning the correct selector.

Q10. What makes ENS domains unique compared to typical NFTs?
A) They are renewable, not permanent B) They use ERC-20 C) They are free D) They cannot be transferred

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which NFT project pre-dates the ERC-721 standard?
A) Bored Ape Yacht Club B) CryptoPunks C) Ethereum Name Service D) Decentraland
Answer: B – CryptoPunks launched in 2017 before ERC-721 was finalized.

Q7. What storage method does Bored Ape Yacht Club use for metadata?
A) On-chain storage B) Centralized AWS server C) IPFS D) Arweave
Answer: C – BAYC stores metadata on IPFS for cost efficiency.

Q8. Are EIP-2981 royalties enforceable on-chain?
A) Yes, automatically enforced B) No, marketplaces voluntarily honor them C) Only on OpenSea D) Only for ERC-1155
Answer: B – Royalties are not on-chain enforceable; marketplaces choose to honor them.

Q9. What must a contract implement to safely receive ERC-721 tokens?
A) IERC721 interface B) onERC721Received() function C) approve() function D) balanceOf() function
Answer: B – Contracts must implement onERC721Received() returning the correct selector.

Q10. What makes ENS domains unique compared to typical NFTs?
A) They are renewable, not permanent B) They use ERC-20 C) They are free D) They cannot be transferred
Answer: A – ENS domains require annual renewal fees, unlike most permanent NFTs.

(c) Joerg Osterrieder 2025

L19: Token Lifecycle Management

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Implement various minting strategies (owner, public, allowlist, merkle tree)
- Design burning mechanisms for deflationary tokenomics
- Use Pausable pattern for emergency circuit breakers
- Apply access control patterns (Ownable, AccessControl, multi-sig)
- Apply upgradeability patterns (Transparent Proxy, UUPS)
- Implement time-locked operations and governance mechanisms

(c) Joerg Osterrieder 2025

The Problem: How do we align stakeholder incentives?

The Challenge
How do we design token distribution and lifecycle mechanisms that align team, investor, and user incentives over time? Without proper alignment, early stakeholders can dump tokens immediately, destroying long-term value.

Why It Matters

- Poor tokenomics leads to pump-and-dump schemes and rug pulls
- ICO boom/bust (2017-2018) showed consequences of misaligned vesting

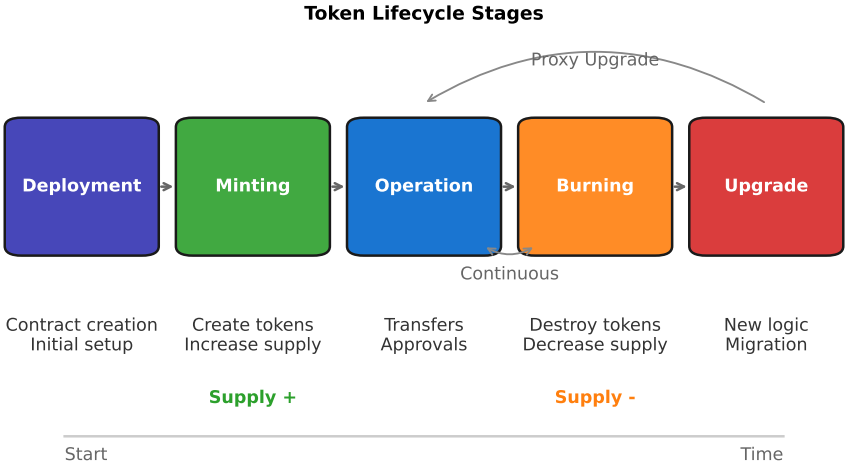
What We Need

- Economic alignment of actors
- Mechanisms preventing immediate token dumps by insiders

The Cryptoeconomics Question
Aligning individual and collective interests

Today's lesson: How Token Lifecycle addresses this challenge

Token Lifecycle Overview



Tokens progress through deployment, minting, operation, burning, and potential upgrades

Token Lifecycle Stages

Complete lifecycle of a token contract:

1. **Deployment:** Contract creation, owner/admin setup, initial distribution
2. **Minting:** Creating new tokens (increasing supply), controlled by governance or owner
3. **Operation:** Normal transfers, approvals, staking, may include pause capability
4. **Burning:** Destroying tokens (decreasing supply), voluntary or forced mechanisms
5. **Upgrade/Migration:** Proxy upgrades or token swaps, governance-controlled

Minting Strategy 1: Owner-Controlled

Simple admin-based minting:

```
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract OwnerMintToken is ERC20, Ownable {
    constructor() ERC20("Owner Mint Token", "OMT") {}

    function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
    }
}
```

Advantages: Simple, flexible timing, useful for airdrops and team allocation
Disadvantages: Centralized control, risk of unlimited inflation, regulatory concerns

Minting Strategy 2: Public Mint with Cap

Anyone can mint up to a maximum supply:

```
contract PublicMintToken is ERC20 {
    uint256 public constant MAX_SUPPLY = 1_000_000 * 10**18;
    uint256 public constant MINT_PRICE = 0.01 ether;
    uint256 public constant MAX_PER_TX = 10 * 10**18;

    function mint(uint256 amount) public payable {
        require(totalSupply() + amount <= MAX_SUPPLY, "Max supply exceeded");
        require(amount <= MAX_PER_TX, "Exceeds max per transaction");
        require(msg.value >= amount * MINT_PRICE / 10**18, "Insufficient payment");
        _mint(msg.sender, amount);
    }
}
```

Use Cases: NFT mints, fair launch tokens, crowdfunding

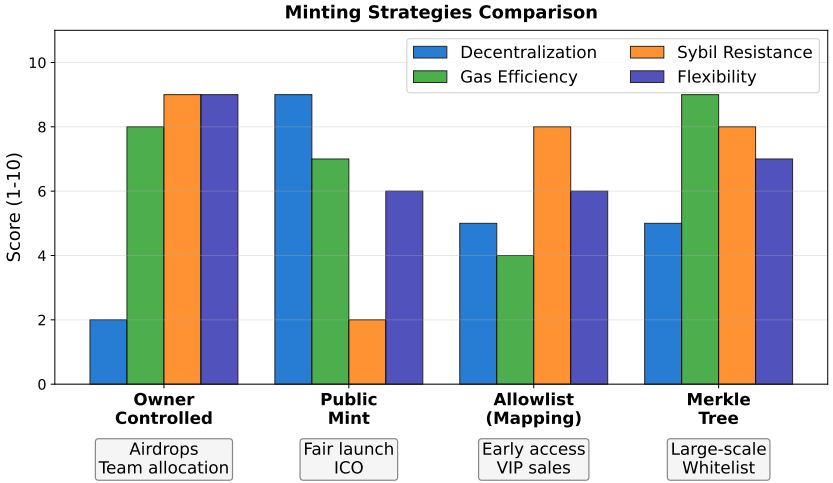
Minting Strategy 3: Merkle Tree Allowlist

Gas-efficient allowlist using Merkle proofs:

```
import "@openzeppelin/contracts/utils/cryptography/MerkleProof.sol";

contract MerkleMintToken is ERC20 {
    bytes32 public merkleRoot;
    mapping(address => bool) public hasClaimed;

    constructor(bytes32 _merkleRoot) ERC20("Merkle Token", "MTK") {
        merkleRoot = _merkleRoot;
    }

    function claim(uint256 amount, bytes32[] calldata merkleProof) public {
        require(!hasClaimed[msg.sender], "Already claimed");
        bytes32 leaf = keccak256(abi.encodePacked(msg.sender, amount));
        require(MerkleProof.verify(merkleProof, merkleRoot, leaf), "Invalid proof");
        hasClaimed[msg.sender] = true;
        _mint(msg.sender, amount);
    }
}
```

Advantage: Store single root hash (32 bytes) instead of entire allowlist

Minting Strategies Comparison



Merkle tree offers best gas efficiency for large allowlists

Burning Mechanisms

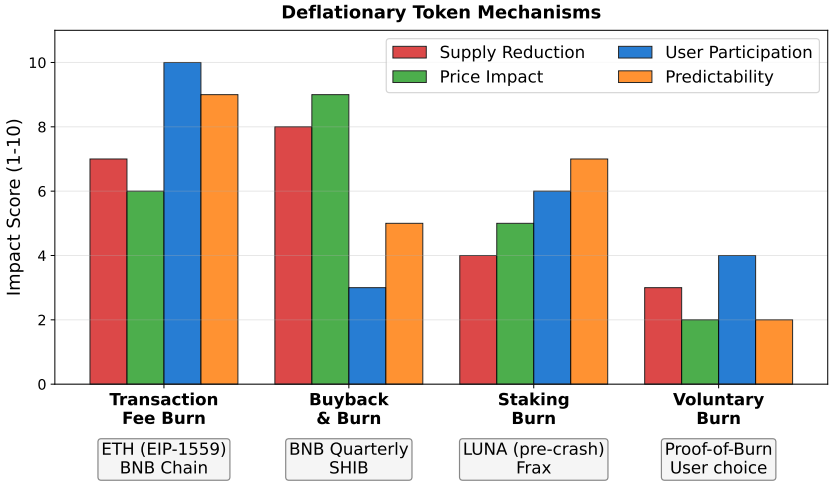
Destroying tokens to reduce supply:

```
import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";

contract BurnableToken is ERC20Burnable {
    constructor() ERC20("Burnable Token", "BURN") {
        _mint(msg.sender, 1_000_000 * 10**18);
    }
    // Inherited: burn(uint256 amount) - burns caller's tokens
    // Inherited: burnFrom(address account, uint256 amount) - burns with allowance
}
```

Burn Strategies:

- **Voluntary:** Users burn their own tokens (e.g., for utility)
- **Fee Burn:** Transaction fees burned automatically (EIP-1559 model)
- **Buyback & Burn:** Protocol buys tokens from market and burns them

Deflationary Token Mechanisms



Transaction fee burns are most predictable; buyback has highest price impact

Access Control: Ownable Pattern

Single owner with full control:

```
import "@openzeppelin/contracts/access/Ownable.sol";

contract OwnedToken is ERC20, Ownable {
    constructor() ERC20("Owned Token", "OWN") {}

    function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
    }

    function renounceOwnership() public override onlyOwner {
        // Irreversibly give up ownership (contract becomes unmanaged)
        super.renounceOwnership();
    }
}
```

Risk: Single point of failure (owner key compromise = full control loss)
Mitigation: Use multi-sig wallet as owner (Gnosis Safe)

Access Control: Multi-Signature Wallets

Require multiple approvals for critical operations:

Gnosis Safe Example:

- 3-of-5 multi-sig: Requires 3 out of 5 owners to approve transaction
- Prevents single key compromise
- Common setup: Deploy token with Gnosis Safe as owner

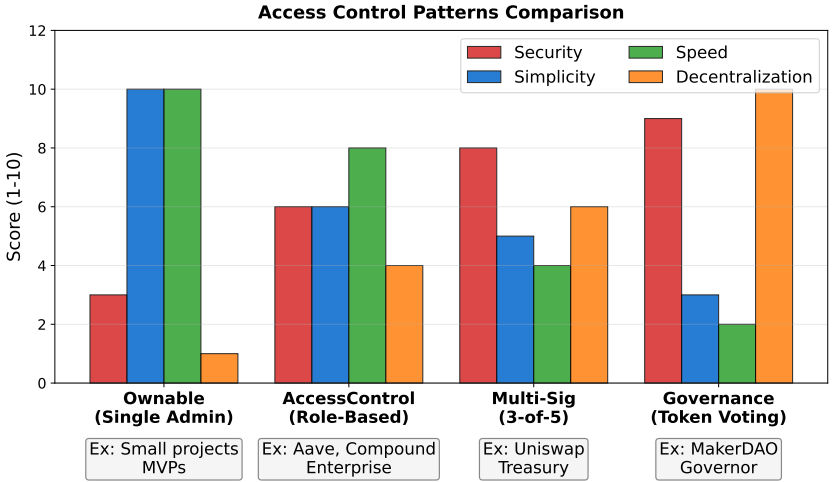
Workflow:

1. Owner 1 proposes transaction (e.g., `mint(alice, 1000)`)
2. Owners 2 and 3 approve transaction
3. Transaction executes automatically when threshold reached

Real-World Usage:

- Uniswap: 4-of-7 multi-sig controls protocol fees
- Compound: Timelock + multi-sig for governance execution

Access Control Patterns Comparison



Multi-sig balances security and speed; governance offers maximum decentralization

Upgradeability: Why and Risks

Motivation for upgradeable contracts:

- Fix critical bugs without redeploying
- Add new features (e.g., staking, governance)
- Comply with changing regulations

Fundamental Challenge:

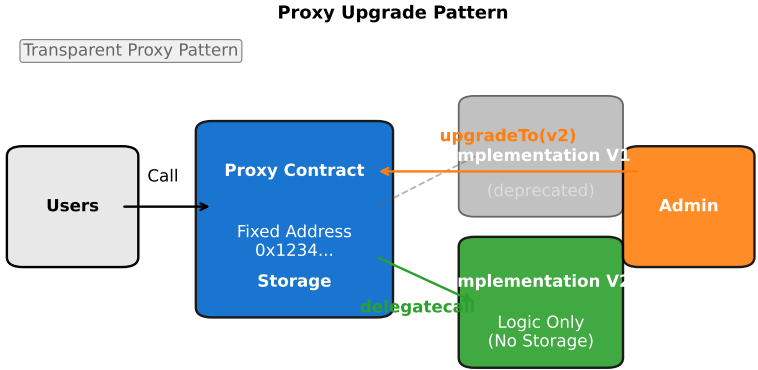
- Smart contracts are immutable after deployment
- Bytecode cannot be changed

Solution: Proxy Pattern

- **Proxy Contract:** Fixed address, users interact with this
- **Implementation Contract:** Contains logic, can be swapped
- Proxy uses `delegatecall` to execute implementation logic

Risks: Admin can rug pull, storage layout collisions, requires trust

Proxy Upgrade Pattern



Storage stays in proxy; only logic is upgraded via delegatecall

Upgradeability: Transparent Proxy

Separate admin and user interfaces:

```
// Proxy Contract (deployed once, never changes)
contract TransparentProxy {
    address public implementation;
    address public admin;

    function upgradeTo(address newImplementation) external {
        require(msg.sender == admin, "Not admin");
        implementation = newImplementation;
    }

    fallback() external payable {
        address impl = implementation;
        assembly {
            calldatacopy(0, 0, calldatasize())
            let result := delegatecall(gas(), impl, 0, calldatasize(), 0, 0)
            returndatacopy(0, 0, returndatasize())
            switch result
            case 0 { revert(0, returndatasize()) }
            default { return(0, returndatasize()) }
        }
    }
}
```

Problem Solved? Token Lifecycle

The Original Problem

How do we align stakeholder incentives?

How Token Lifecycle Solves It

- Vesting schedules prevent immediate token dumps by team/investors
- Time-locked operations create commitment mechanisms and allow community oversight
- Multi-sig and governance distribute control, reducing centralization risk

Remaining Limitations

- Smart contract vesting can be gamed (secondary market sales, wrapped tokens)
- Governance attacks possible with sufficient token accumulation

Open Questions

- What vesting periods optimize long-term alignment without restricting legitimate liquidity?
- Risk: Incentive misalignment, free-rider problems in governance

Token Lifecycle partially solves stakeholder alignment but introduces new trade-offs in governance and flexibility

(c) Joerg Osterrieder 2025

Key Takeaways

1. **Minting Strategies:** Owner-controlled (centralized), public mint (open), Merkle tree (gas-efficient allowlist)
2. **Burning:** Voluntary burn, fee burn, buyback and burn for deflationary tokenomics
3. **Pausable:** Emergency circuit breaker halts transfers during critical bugs
4. **Access Control:** Ownable (single admin), AccessControl (role-based), multi-sig (distributed trust)
5. **Upgradeability:** Transparent Proxy separates storage from logic, enabling upgrades
6. **Timelock:** Delay critical operations to allow community reaction and exit
7. **Governance:** Token-weighted voting enables decentralized control

Discussion Questions

1. What are the security tradeoffs between Merkle tree allowlists and simple mapping-based allowlists?
2. Should all tokens be pausable, or does this introduce too much centralization risk?
3. How can upgradeable contracts maintain credible neutrality when admins can change the code?
4. What is the optimal timelock delay for different types of governance actions?
5. How do deflationary tokenomics affect long-term protocol sustainability?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L20 - Lab: Token Analysis

Coming up next (hands-on lab):

- Analyzing USDC and DAI contracts on Etherscan
- Examining token holder distribution and centralization
- Tracking transaction patterns and whale movements
- Identifying upgrade events and governance actions
- Deploying your own ERC-20 token with custom features

Preparation:

- Review Etherscan contract reading interface
- Familiarize with USDC and DAI token pages
- Prepare Sepolia testnet ETH for deployment

Quiz Questions 1/4

Q1. Which minting strategy is most gas-efficient for a large allowlist of 10,000 addresses?
A) Mapping-based allowlist B) Array-based allowlist C) Merkle tree allowlist D) Owner-controlled manual approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses on-chain.

Q2. What is the main security risk of the Ownable pattern?
A) Too many admins B) Single point of failure C) High gas costs D) Slow execution
Answer: B – Owner key compromise gives attacker full control; use multi-sig to mitigate.

Q3. In ERC20Burnable, what happens when you call burn(amount)?
A) Tokens sent to 0x0 B) Tokens deleted, supply unchanged C) Tokens destroyed, supply reduced D) Tokens locked permanently
Answer: C – burn() reduces totalSupply and caller balance by amount.

Q4. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage context C) Creates new contract D) Sends ETH
Answer: B – delegatecall runs implementation code using proxy's storage.

Q5. Which burn mechanism is used by Ethereum after EIP-1559?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn
Answer: B – Base fees are burned automatically, reducing ETH supply.

Quiz Questions 2/4

Q6. What is the purpose of the Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up transactions D) Reduce fees
Answer: B – Pausable halts transfers during critical bugs or exploits.

Q7. In a 3-of-5 multi-sig wallet, how many approvals are needed to execute a transaction?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3-of-5 means 3 signatures required out of 5 total owners.

Q8. What is the main disadvantage of upgradeable contracts?
A) High deployment cost B) Admin can rug pull C) Slow performance D) Limited functionality
Answer: B – Admin can upgrade to malicious implementation; requires trust.

Q9. Which access control pattern offers role-based permissions?
A) Ownable B) Pausable C) AccessControl D) ReentrancyGuard
Answer: C – AccessControl allows multiple roles (MINTER, PAUSER, etc.).

Q10. What happens when a token contract renounces ownership?
A) Ownership transfers to 0x0 B) Contract becomes unmanaged C) All tokens burn D) Contract pauses
Answer: B – renounceOwnership() irreversibly removes admin control.

Quiz Questions 3/4

Q11. In a public mint with MAX_SUPPLY, what happens when the cap is reached?
A) Minting continues B) Transaction reverts C) Tokens burn automatically D) Price increases
Answer: B – require(totalSupply() + amount ¡= MAX_SUPPLY) will revert.

Q12. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas costs D) Increase voting power
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q13. Which deflationary mechanism has the highest price impact?
A) Transaction fee burn B) Voluntary burn C) Buyback and burn D) Governance burn
Answer: C – Buyback creates buy pressure before burning, directly affecting price.

Q14. In Transparent Proxy, where is state stored?
A) Implementation contract B) Proxy contract C) Both contracts D) External storage
Answer: B – Storage lives in proxy; implementation is stateless logic.

Q15. What does burnFrom(address account, uint256 amount) require?
A) Owner role B) Allowance from account C) Paused contract D) Multi-sig approval
Answer: B – burnFrom() burns tokens from account using ERC20 allowance mechanism.

Quiz Questions 4/4

Q16. Why is Merkle tree minting more efficient than storing all addresses on-chain?
A) Faster execution B) Only stores 32-byte root C) No verification needed D) Lower deployment cost
Answer: B – Single merkleRoot replaces potentially thousands of address mappings.

Q17. What is the main risk of making all tokens pausable?
A) High gas costs B) Slow transfers C) Centralization risk D) Incompatibility with DEXs
Answer: C – Pausable gives admin power to halt all transfers, centralizing control.

Q18. In token-weighted governance, voting power is determined by:
A) Number of transactions B) Token balance C) Account age D) Staking duration
Answer: B – Standard governance uses token balance as voting weight.

Q19. What is a storage layout collision in upgradeable contracts?
A) Two functions with same name B) Variables in different positions across versions C) Gas limit exceeded D) Proxy and implementation conflict
Answer: B – New implementation must maintain exact variable order to avoid data corruption.

Q20. Which real-world protocol uses a 4-of-7 multi-sig for fee control?
A) Compound B) Aave C) Uniswap D) MakerDAO
Answer: C – Uniswap uses 4-of-7 multi-sig to control protocol fee distribution.

L19: Token Lifecycle Management

Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Token Birth to Death

[COMIC: Token lifecycle from mint to burn as journey]

"From genesis block to final burn..."

The Full Journey

- Minting: token creation
- Operation: transfers, staking
- Burning: permanent destruction

Today's Questions

- Who can mint new tokens?
- When should tokens be burned?
- How do we prevent abuse?

Every token has a lifecycle. Understanding it reveals the economic design behind tokenomics.

Learning Objectives

By the end of this lesson, you will be able to:

- Implement various minting strategies (owner, public, allowlist, merkle tree)
- Design burning mechanisms for deflationary tokenomics
- Use Pausable pattern for emergency circuit breakers
- Apply access control patterns (Ownable, AccessControl, multi-sig)
- Apply upgradeability patterns (Transparent Proxy, UUPS)
- Implement time-locked operations and governance mechanisms

Building on L18: ERC-721 and ERC-1155

The Problem: How do we align stakeholder incentives?

The Challenge
How do we design token distribution and lifecycle mechanisms that align team, investor, and user incentives over time? Without proper alignment, early stakeholders can dump tokens immediately, destroying long-term value.

Why It Matters

- Poor tokenomics leads to pump-and-dump schemes and rug pulls
- ICO boom/bust (2017-2018) showed consequences of misaligned vesting

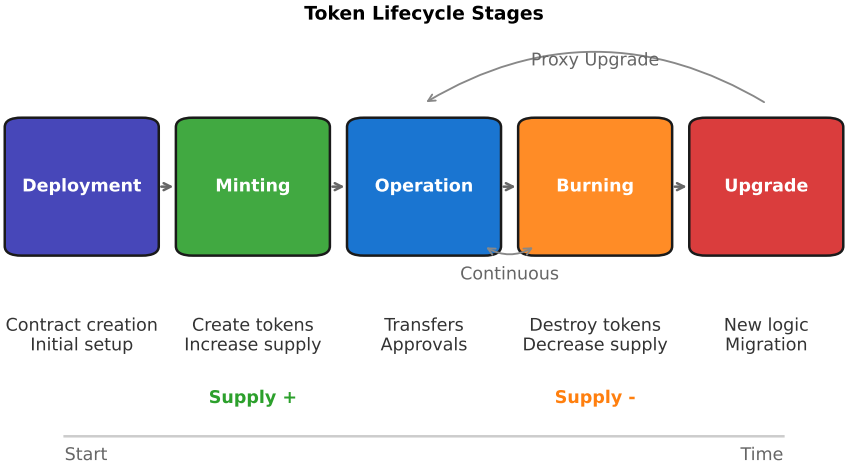
What We Need

- Economic alignment of actors
- Mechanisms preventing immediate token dumps by insiders

The Cryptoeconomics Question
Aligning individual and collective interests

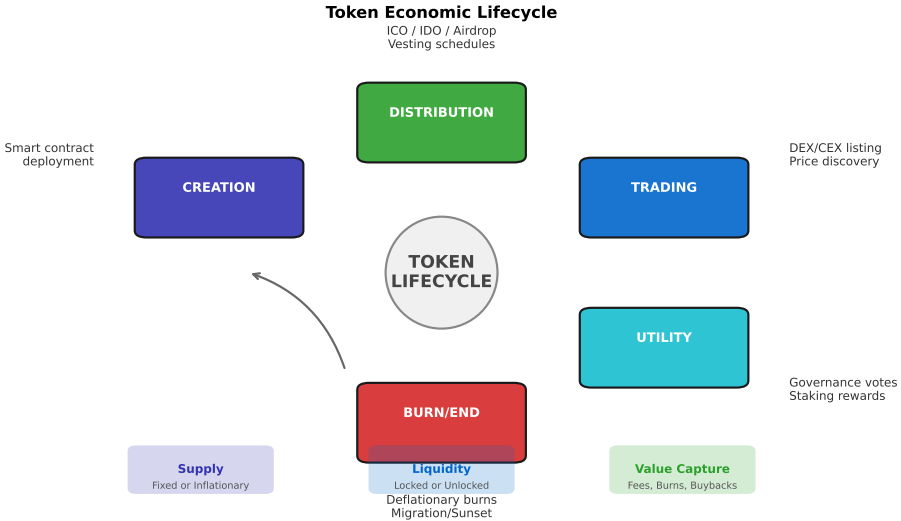
Today's lesson: How Token Lifecycle addresses this challenge

What Are the Key Stages of Token Lifecycle?



Problem: How do we align stakeholder incentives? — Each lifecycle stage creates opportunities for alignment: vesting at minting, governance during operation, buybacks via burning

How Do Economic Forces Shape Token Lifecycle?



Economic perspective: Creation sets supply policy, distribution determines initial ownership, trading establishes price, utility drives demand, burns create scarcity

What Are the Stages of a Token's Lifecycle?

Complete lifecycle of a token contract:

1. **Deployment:** Contract creation, owner/admin setup, initial distribution
2. **Minting:** Creating new tokens (increasing supply), controlled by governance or owner
3. **Operation:** Normal transfers, approvals, staking, may include pause capability
4. **Burning:** Destroying tokens (decreasing supply), voluntary or forced mechanisms
5. **Upgrade/Migration:** Proxy upgrades or token swaps, governance-controlled

How Does Owner-Controlled Minting Work?

Simple admin-based minting:

```
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
import "@openzeppelin/contracts/access/Ownable.sol";

contract OwnerMintToken is ERC20, Ownable {
    constructor() ERC20("Owner Mint Token", "OMT") {}

    function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
    }
}
```

Advantages: Simple, flexible timing, useful for airdrops and team allocation
Disadvantages: Centralized control, risk of unlimited inflation, regulatory concerns

How Does Public Minting with Cap Work?

Anyone can mint up to a maximum supply:

```
contract PublicMintToken is ERC20 {
    uint256 public constant MAX_SUPPLY = 1_000_000 * 10**18;
    uint256 public constant MINT_PRICE = 0.01 ether;
    uint256 public constant MAX_PER_TX = 10 * 10**18;

    function mint(uint256 amount) public payable {
        require(totalSupply() + amount <= MAX_SUPPLY, "Max supply exceeded");
        require(amount <= MAX_PER_TX, "Exceeds max per transaction");
        require(msg.value >= amount * MINT_PRICE / 10**18, "Insufficient payment");
        _mint(msg.sender, amount);
    }
}
```

Use Cases: NFT mints, fair launch tokens, crowdfunding

Problem: How do we align stakeholder incentives? — Public mints with caps create fair access (anyone can participate) and scarcity (MAX_SUPPLY prevents inflation), aligning early and late adopters

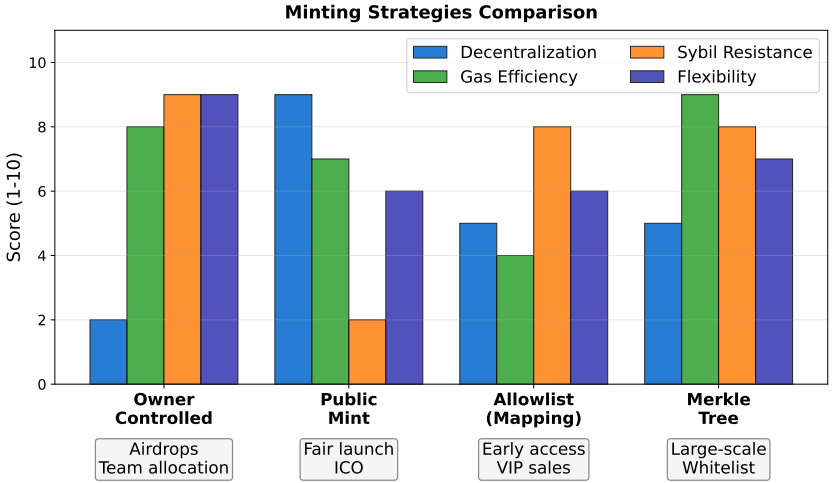
How Do Merkle Tree Allowlists Work?

Gas-efficient allowlist using Merkle proofs:

```
import "@openzeppelin/contracts/utils/cryptography/MerkleProof.sol";

contract MerkleMintToken is ERC20 {
    bytes32 public merkleRoot;
    mapping(address => bool) public hasClaimed;

    constructor(bytes32 _merkleRoot) ERC20("Merkle Token", "MTK") {
        merkleRoot = _merkleRoot;
    }

    function claim(uint256 amount, bytes32[] calldata merkleProof) public {
        require(!hasClaimed[msg.sender], "Already claimed");
        bytes32 leaf = keccak256(abi.encodePacked(msg.sender, amount));
        require(MerkleProof.verify(merkleProof, merkleRoot, leaf), "Invalid proof");
        hasClaimed[msg.sender] = true;
        _mint(msg.sender, amount);
    }
}
```

Advantage: Store single root hash (32 bytes) instead of entire allowlist

Minting Strategies Comparison



Merkle tree offers best gas efficiency for large allowlists

How Do Tokens Get Burned?

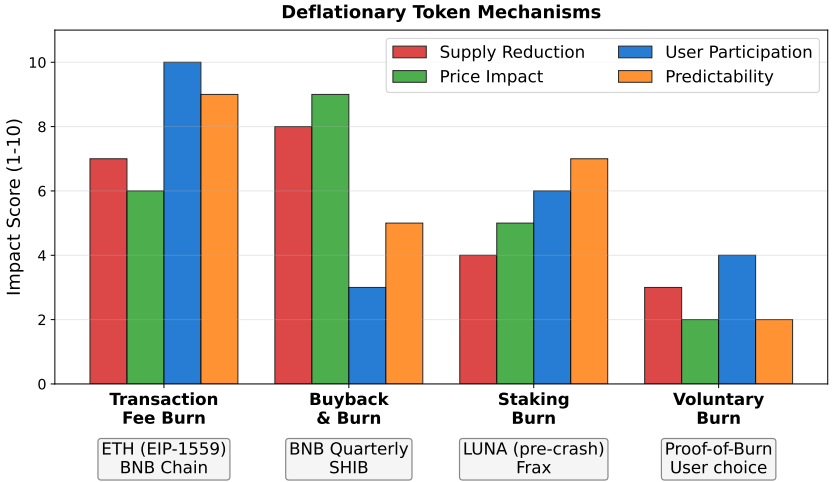
Destroying tokens to reduce supply:

```
import "@openzeppelin/contracts/token/ERC20/extensions/ERC20Burnable.sol";

contract BurnableToken is ERC20Burnable {
    constructor() ERC20("Burnable Token", "BURN") {
        _mint(msg.sender, 1_000_000 * 10**18);
    }
    // Inherited: burn(uint256 amount) - burns caller's tokens
    // Inherited: burnFrom(address account, uint256 amount) - burns with allowance
}
```

Burn Strategies:

- **Voluntary:** Users burn their own tokens (e.g., for utility)
- **Fee Burn:** Transaction fees burned automatically (EIP-1559 model)
- **Buyback & Burn:** Protocol buys tokens from market and burns them

Deflationary Token Mechanisms



Problem: How do we align stakeholder incentives? — Deflationary mechanisms (burning tokens) align incentives by making remaining tokens more scarce, benefiting long-term holders over short-term speculators

Problem Check-In: Token Lifecycle

Recall Our Problem

How do we align stakeholder incentives?

What We've Learned So Far

- Minting strategies (owner-controlled, public, Merkle allowlist) determine who can create new tokens and when
- Burning mechanisms (voluntary, fee burn, buyback) reduce supply, creating scarcity for remaining holders
- Controlled minting prevents insider dumps; burning aligns incentives by rewarding long-term commitment

Still to Address

- Access control patterns (Ownable, multi-sig, governance) and upgradeability mechanisms
- How do we prevent admin abuse while still allowing necessary contract updates?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we align stakeholder incentives?"?

How Does the Ownable Pattern Work?

Single owner with full control:

```
import "@openzeppelin/contracts/access/Ownable.sol";

contract OwnedToken is ERC20, Ownable {
    constructor() ERC20("Owned Token", "OWN") {}

    function mint(address to, uint256 amount) public onlyOwner {
        _mint(to, amount);
    }

    function renounceOwnership() public override onlyOwner {
        // Irreversibly give up ownership (contract becomes unmanaged)
        super.renounceOwnership();
    }
}
```

Risk: Single point of failure (owner key compromise = full control loss)
Mitigation: Use multi-sig wallet as owner (Gnosis Safe)

How Do Multi-Signature Wallets Improve Security?

Require multiple approvals for critical operations:

Gnosis Safe Example:

- 3-of-5 multi-sig: Requires 3 out of 5 owners to approve transaction
- Prevents single key compromise
- Common setup: Deploy token with Gnosis Safe as owner

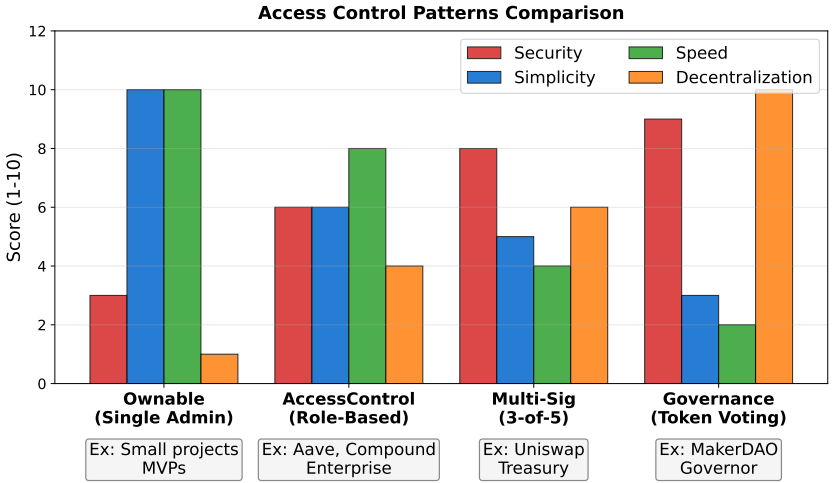
Workflow:

1. Owner 1 proposes transaction (e.g., `mint(alice, 1000)`)
2. Owners 2 and 3 approve transaction
3. Transaction executes automatically when threshold reached

Real-World Usage:

- Uniswap: 4-of-7 multi-sig controls protocol fees
- Compound: Timelock + multi-sig for governance execution

Access Control Patterns Comparison



Problem: How do we align stakeholder incentives? — Multi-sig prevents single-person abuse (no rug pulls); governance gives token holders control, aligning decision-makers with those affected by decisions

Why Make Contracts Upgradeable?

Motivation for upgradeable contracts:

- Fix critical bugs without redeploying
- Add new features (e.g., staking, governance)
- Comply with changing regulations

Fundamental Challenge:

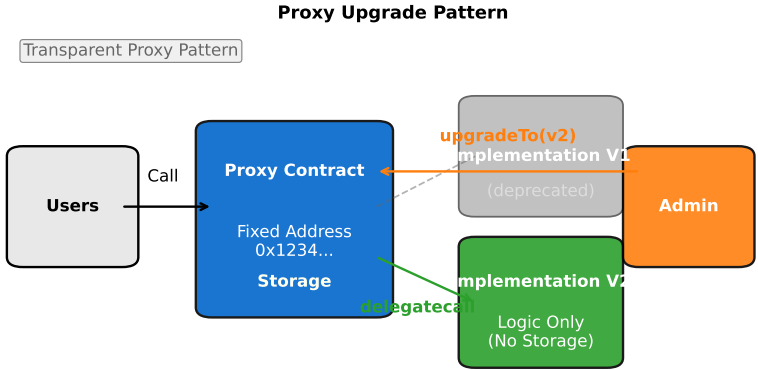
- Smart contracts are immutable after deployment
- Bytecode cannot be changed

Solution: Proxy Pattern

- **Proxy Contract:** Fixed address, users interact with this
- **Implementation Contract:** Contains logic, can be swapped
- Proxy uses `delegatecall` to execute implementation logic

Risks: Admin can rug pull, storage layout collisions, requires trust

Proxy Upgrade Pattern



Storage stays in proxy; only logic is upgraded via delegatecall

How Does Transparent Proxy Upgradeability Work?

Separate admin and user interfaces:

```
// Proxy Contract (deployed once, never changes)
contract TransparentProxy {
    address public implementation;
    address public admin;

    function upgradeTo(address newImplementation) external {
        require(msg.sender == admin, "Not admin");
        implementation = newImplementation;
    }

    fallback() external payable {
        address impl = implementation;
        assembly {
            calldatacopy(0, 0, calldatasize())
            let result := delegatecall(gas(), impl, 0, calldatasize(), 0, 0)
            returndatacopy(0, 0, returndatasize())
            switch result
            case 0 { revert(0, returndatasize()) }
            default { return(0, returndatasize()) }
        }
    }
}
```

Problem Solved? Token Lifecycle

The Original Problem

How do we align stakeholder incentives?

How Token Lifecycle Solves It

- Vesting schedules prevent immediate token dumps by team/investors
- Time-locked operations create commitment mechanisms and allow community oversight
- Multi-sig and governance distribute control, reducing centralization risk

Remaining Limitations

- Smart contract vesting can be gamed (secondary market sales, wrapped tokens)
- Governance attacks possible with sufficient token accumulation

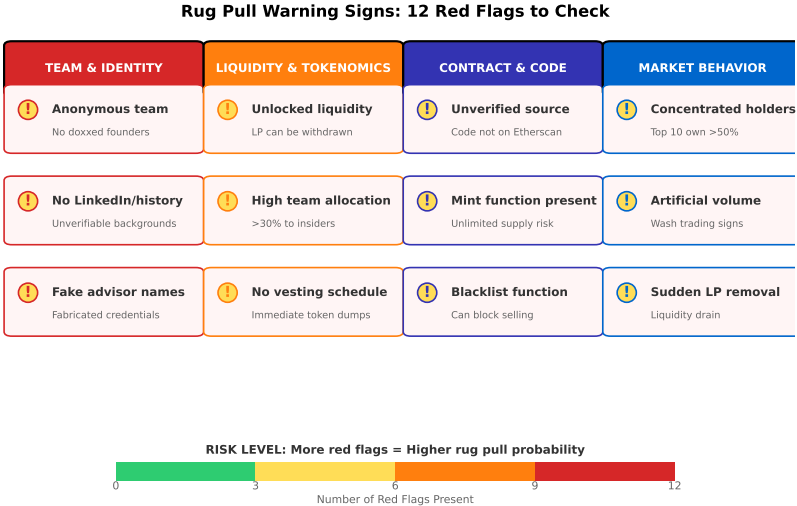
Open Questions

- What vesting periods optimize long-term alignment without restricting legitimate liquidity?
- Risk: Incentive misalignment, free-rider problems in governance

Token Lifecycle partially solves stakeholder alignment but introduces new trade-offs in governance and flexibility

(c) Joerg Osterrieder 2025

How Do You Spot Rug Pull Warning Signs?



Due diligence: Always check for these red flags before investing in new tokens

The Economics of Token Lifecycle

Incentive Structure

- **Core Problem:** Aligning individual and collective interests
- **Why act honestly?** Rewards for honest behavior, penalties for cheating
- **Value Flow:** Protocol gains security, participants earn rewards

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Protocol gains security, participants earn rewards

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Token Lifecycle

Alternatives Considered

1. **Chosen Design:** Reward curves, slashing conditions
2. **Alternative:** Alternative reward mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Token Lifecycle

Critical Failure Mode

- **What breaks:** Incentive misalignment, free-rider problems
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Rug Pull Warning Signs

[COMIC: Investor spotting red flags in token contract]

"Unlimited mint? No timelock? Anonymous team?"

The Red Flags

- Owner can mint unlimited tokens
- No vesting for team allocation
- Upgradeable without timelock

What We Learned

- Lifecycle controls reveal intent
- Multi-sig and timelocks add safety
- Due diligence before investment

Token lifecycle design reveals whether a project prioritizes long-term value or quick extraction.

Key Takeaways

1. **Minting Strategies:** Owner-controlled (centralized), public mint (open), Merkle tree (gas-efficient allowlist)
2. **Burning:** Voluntary burn, fee burn, buyback and burn for deflationary tokenomics
3. **Pausable:** Emergency circuit breaker halts transfers during critical bugs
4. **Access Control:** Ownable (single admin), AccessControl (role-based), multi-sig (distributed trust)
5. **Upgradeability:** Transparent Proxy separates storage from logic, enabling upgrades
6. **Timelock:** Delay critical operations to allow community reaction and exit
7. **Governance:** Token-weighted voting enables decentralized control

Next Lesson: L20 – Lab: Token Analysis

(c) Joerg Osterrieder 2025

Discussion Questions

1. What are the security tradeoffs between Merkle tree allowlists and simple mapping-based allowlists?
2. Should all tokens be pausable, or does this introduce too much centralization risk?
3. How can upgradeable contracts maintain credible neutrality when admins can change the code?
4. What is the optimal timelock delay for different types of governance actions?
5. How do deflationary tokenomics affect long-term protocol sustainability?

(c) Joerg Osterrieder 2025

Next Lesson Preview: L20 - Lab: Token Analysis

Coming up next (hands-on lab):

- Analyzing USDC and DAI contracts on Etherscan
- Examining token holder distribution and centralization
- Tracking transaction patterns and whale movements
- Identifying upgrade events and governance actions
- Deploying your own ERC-20 token with custom features

Preparation:

- Review Etherscan contract reading interface
- Familiarize with USDC and DAI token pages
- Prepare Sepolia testnet ETH for deployment

Quiz Questions 1/4

Q1. Which minting strategy is most gas-efficient for a large allowlist of 10,000 addresses?
A) Mapping-based allowlist B) Array-based allowlist C) Merkle tree allowlist D) Owner-controlled manual approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses on-chain.

Q2. What is the main security risk of the Ownable pattern?
A) Too many admins B) Single point of failure C) High gas costs D) Slow execution
Answer: B – Owner key compromise gives attacker full control; use multi-sig to mitigate.

Q3. In ERC20Burnable, what happens when you call burn(amount)?
A) Tokens sent to 0x0 B) Tokens deleted, supply unchanged C) Tokens destroyed, supply reduced D) Tokens locked permanently
Answer: C – burn() reduces totalSupply and caller balance by amount.

Q4. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage context C) Creates new contract D) Sends ETH
Answer: B – delegatecall runs implementation code using proxy's storage.

Q5. Which burn mechanism is used by Ethereum after EIP-1559?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn
Answer: B – Base fees are burned automatically, reducing ETH supply.

Quiz Questions 2/4

Q6. What is the purpose of the Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up transactions D) Reduce fees
Answer: B – Pausable halts transfers during critical bugs or exploits.

Q7. In a 3-of-5 multi-sig wallet, how many approvals are needed to execute a transaction?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3-of-5 means 3 signatures required out of 5 total owners.

Q8. What is the main disadvantage of upgradeable contracts?
A) High deployment cost B) Admin can rug pull C) Slow performance D) Limited functionality
Answer: B – Admin can upgrade to malicious implementation; requires trust.

Q9. Which access control pattern offers role-based permissions?
A) Ownable B) Pausable C) AccessControl D) ReentrancyGuard
Answer: C – AccessControl allows multiple roles (MINTER, PAUSER, etc.).

Q10. What happens when a token contract renounces ownership?
A) Ownership transfers to 0x0 B) Contract becomes unmanaged C) All tokens burn D) Contract pauses
Answer: B – renounceOwnership() irreversibly removes admin control.

Quiz Questions 3/4

Q11. In a public mint with MAX_SUPPLY, what happens when the cap is reached?
A) Minting continues B) Transaction reverts C) Tokens burn automatically D) Price increases
Answer: B – require(totalSupply() + amount ¡= MAX_SUPPLY) will revert.

Q12. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas costs D) Increase voting power
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q13. Which deflationary mechanism has the highest price impact?
A) Transaction fee burn B) Voluntary burn C) Buyback and burn D) Governance burn
Answer: C – Buyback creates buy pressure before burning, directly affecting price.

Q14. In Transparent Proxy, where is state stored?
A) Implementation contract B) Proxy contract C) Both contracts D) External storage
Answer: B – Storage lives in proxy; implementation is stateless logic.

Q15. What does burnFrom(address account, uint256 amount) require?
A) Owner role B) Allowance from account C) Paused contract D) Multi-sig approval
Answer: B – burnFrom() burns tokens from account using ERC20 allowance mechanism.

Quiz Questions 4/4

Q16. Why is Merkle tree minting more efficient than storing all addresses on-chain?
A) Faster execution B) Only stores 32-byte root C) No verification needed D) Lower deployment cost
Answer: B – Single merkleRoot replaces potentially thousands of address mappings.

Q17. What is the main risk of making all tokens pausable?
A) High gas costs B) Slow transfers C) Centralization risk D) Incompatibility with DEXs
Answer: C – Pausable gives admin power to halt all transfers, centralizing control.

Q18. In token-weighted governance, voting power is determined by:
A) Number of transactions B) Token balance C) Account age D) Staking duration
Answer: B – Standard governance uses token balance as voting weight.

Q19. What is a storage layout collision in upgradeable contracts?
A) Two functions with same name B) Variables in different positions across versions C) Gas limit exceeded D) Proxy and implementation conflict
Answer: B – New implementation must maintain exact variable order to avoid data corruption.

Q20. Which real-world protocol uses a 4-of-7 multi-sig for fee control?
A) Compound B) Aave C) Uniswap D) MakerDAO
Answer: C – Uniswap uses 4-of-7 multi-sig to control protocol fee distribution.

L19: Token Lifecycle Management

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

January 2026

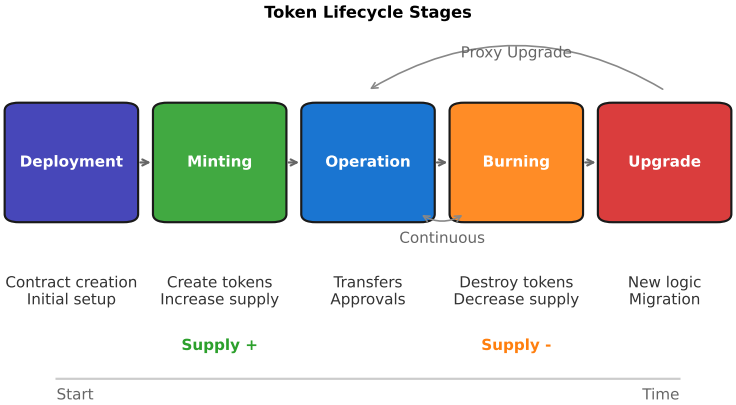
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

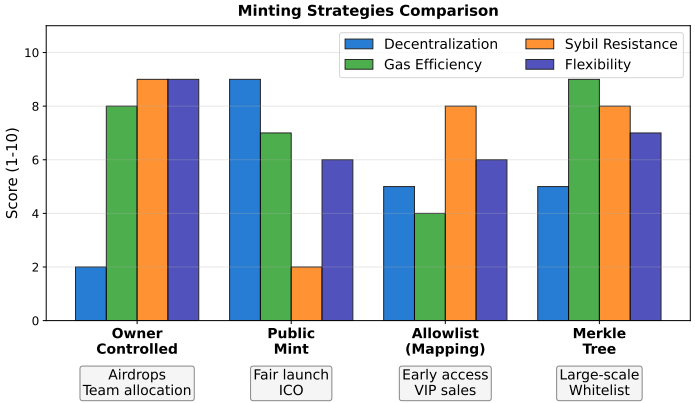
- Implement various minting strategies (owner, public, Merkle)
- Design burning mechanisms for deflationary tokenomics
- Apply access control patterns (Ownable, multi-sig)
- Understand upgradeability patterns (Proxy)

Token Lifecycle Overview



Stages: Deployment → Minting → Operation → Burning → Upgrade

Minting Strategies Comparison

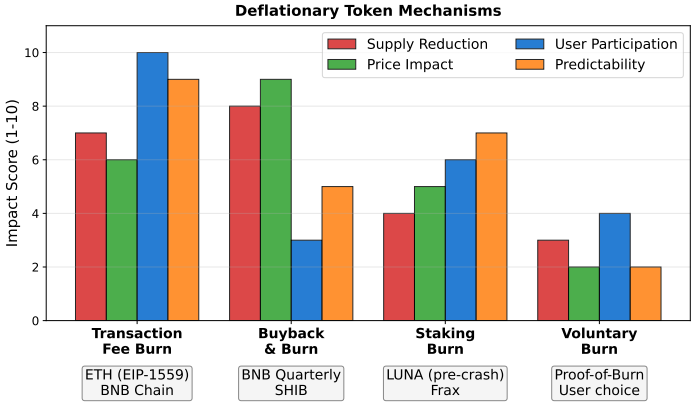


Merkle Tree: Most gas-efficient for large allowlists (stores single 32-byte root).

Minting Strategy Types

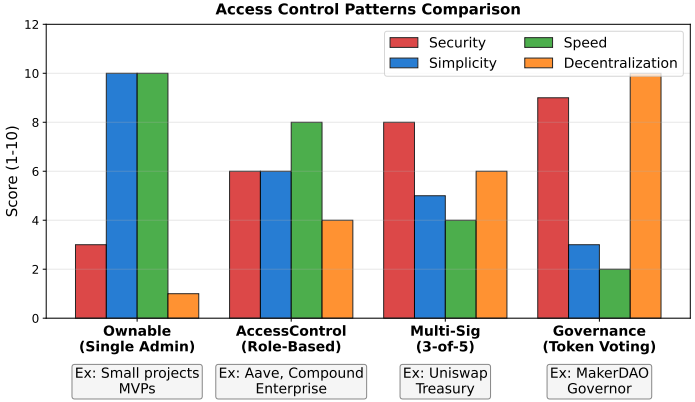
1. **Owner-Controlled:**
   - Simple admin minting via `onlyOwner` modifier
   - Centralized but flexible for airdrops/team allocation
2. **Public Mint with Cap:**
   - Anyone can mint up to MAX_SUPPLY
   - Often with MINT_PRICE and MAX_PER_TX limits
3. **Merkle Tree Allowlist:**
   - Store single root hash instead of thousands of addresses
   - Users provide proof to claim allocation

Deflationary Token Mechanisms



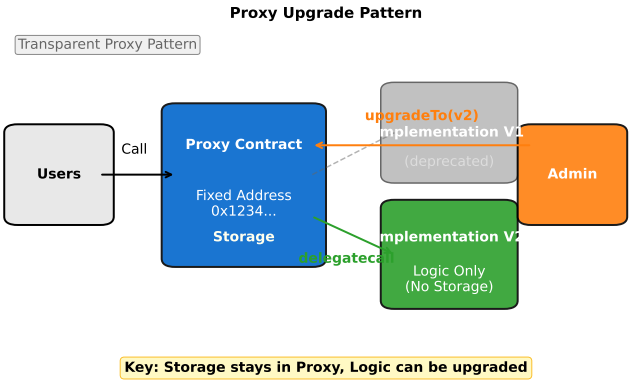
Buyback & Burn: Highest price impact — **Fee Burn:** Most predictable (EIP-1559)

Access Control Patterns



Ownable: Single admin — **Multi-sig:** Distributed trust — **Governance:** Decentralized

Upgradeability: Proxy Pattern



Key: Storage in proxy, logic in implementation. `delegatecall` executes new code.

Security Considerations

Pausable Pattern:

- Emergency circuit breaker halts transfers during exploits
- Risk: Centralized control

Multi-Sig (Gnosis Safe):

- 3-of-5: Requires 3 out of 5 owners to approve
- Uniswap uses 4-of-7 for protocol fee control

Timelock:

- Delays critical operations (24-48 hours typical)
- Allows community to react and exit if disagreeing

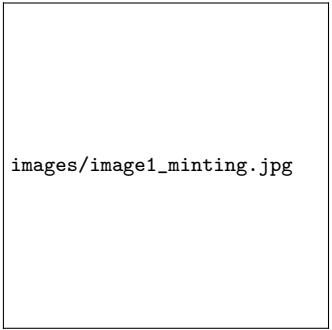
Key Takeaways

1. **Minting:** Owner-controlled, public, or Merkle tree for gas efficiency
2. **Burning:** Voluntary, fee burn (EIP-1559), or buyback for deflation
3. **Access Control:** Ownable (simple), multi-sig (distributed), governance (decentralized)
4. **Upgradeability:** Proxy pattern enables bug fixes but adds trust assumptions
5. **Pausable:** Emergency stop capability with centralization trade-off

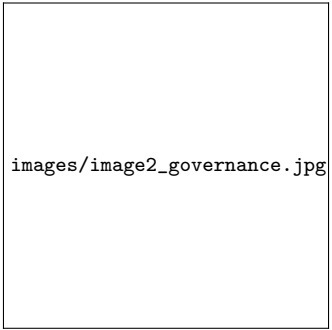
Risk: Upgradeable contracts allow admin to rug pull – requires trust.

(c) Joerg Osterrieder 2025

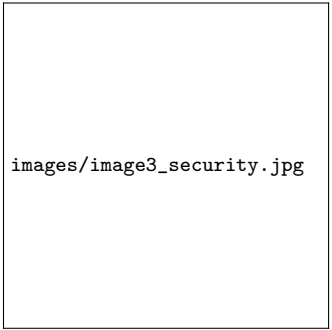
Token Lifecycle in Practice



Token Minting



Governance



Security

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Most gas-efficient minting for 10,000 address allowlist?
A) Mapping B) Array C) Merkle tree D) Owner approval

Quiz (1/2)

Q1. Most gas-efficient minting for 10,000 address allowlist?
A) Mapping B) Array C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root.

Q2. Main risk of Ownable pattern?
A) Too many admins B) Single point of failure C) High gas D) Slow execution

Quiz (1/2)

Q1. Most gas-efficient minting for 10,000 address allowlist?
A) Mapping B) Array C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root.

Q2. Main risk of Ownable pattern?
A) Too many admins B) Single point of failure C) High gas D) Slow execution
Answer: B – Key compromise = full control loss.

Q3. What does burn() do?
A) Send to 0x0 B) Lock permanently C) Destroy tokens, reduce supply D) Lock temporarily

Quiz (1/2)

Q1. Most gas-efficient minting for 10,000 address allowlist?
A) Mapping B) Array C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root.

Q2. Main risk of Ownable pattern?
A) Too many admins B) Single point of failure C) High gas D) Slow execution
Answer: B – Key compromise = full control loss.

Q3. What does burn() do?
A) Send to 0x0 B) Lock permanently C) Destroy tokens, reduce supply D) Lock temporarily
Answer: C – burn() reduces totalSupply and caller balance.

Q4. What does delegatecall do in proxy pattern?
A) Transfer ownership B) Execute logic in proxy's storage context C) Create new contract D) Send ETH

Quiz (1/2)

Q1. Most gas-efficient minting for 10,000 address allowlist?
A) Mapping B) Array C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root.

Q2. Main risk of Ownable pattern?
A) Too many admins B) Single point of failure C) High gas D) Slow execution
Answer: B – Key compromise = full control loss.

Q3. What does burn() do?
A) Send to 0x0 B) Lock permanently C) Destroy tokens, reduce supply D) Lock temporarily
Answer: C – burn() reduces totalSupply and caller balance.

Q4. What does delegatecall do in proxy pattern?
A) Transfer ownership B) Execute logic in proxy's storage context C) Create new contract D) Send ETH
Answer: B – Runs implementation code using proxy's storage.

Q5. Ethereum's burn mechanism after EIP-1559?
A) Voluntary B) Transaction fee burn C) Buyback D) Governance

Quiz (1/2)

Q1. Most gas-efficient minting for 10,000 address allowlist?
A) Mapping B) Array C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root.

Q2. Main risk of Ownable pattern?
A) Too many admins B) Single point of failure C) High gas D) Slow execution
Answer: B – Key compromise = full control loss.

Q3. What does burn() do?
A) Send to 0x0 B) Lock permanently C) Destroy tokens, reduce supply D) Lock temporarily
Answer: C – burn() reduces totalSupply and caller balance.

Q4. What does delegatecall do in proxy pattern?
A) Transfer ownership B) Execute logic in proxy's storage context C) Create new contract D) Send ETH
Answer: B – Runs implementation code using proxy's storage.

Q5. Ethereum's burn mechanism after EIP-1559?
A) Voluntary B) Transaction fee burn C) Buyback D) Governance
Answer: B – Base fees are burned automatically.

Quiz (2/2)

Q6. Purpose of Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up tx D) Reduce fees

Quiz (2/2)

Q6. Purpose of Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up tx D) Reduce fees
Answer: B – Halts transfers during critical bugs.

Q7. In 3-of-5 multi-sig, approvals needed?
A) 2 B) 3 C) 4 D) 5

Quiz (2/2)

Q6. Purpose of Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up tx D) Reduce fees
Answer: B – Halts transfers during critical bugs.

Q7. In 3-of-5 multi-sig, approvals needed?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3 signatures required out of 5 owners.

Q8. Main disadvantage of upgradeable contracts?
A) High deployment cost B) Admin can rug pull C) Slow performance D) Limited functionality

Quiz (2/2)

Q6. Purpose of Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up tx D) Reduce fees
Answer: B – Halts transfers during critical bugs.

Q7. In 3-of-5 multi-sig, approvals needed?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3 signatures required out of 5 owners.

Q8. Main disadvantage of upgradeable contracts?
A) High deployment cost B) Admin can rug pull C) Slow performance D) Limited functionality
Answer: B – Admin can upgrade to malicious implementation.

Q9. What happens when renounceOwnership() is called?
A) Transfer to 0x0 B) Contract becomes unmanaged C) Tokens burn D) Contract pauses

Quiz (2/2)

Q6. Purpose of Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up tx D) Reduce fees
Answer: B – Halts transfers during critical bugs.

Q7. In 3-of-5 multi-sig, approvals needed?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3 signatures required out of 5 owners.

Q8. Main disadvantage of upgradeable contracts?
A) High deployment cost B) Admin can rug pull C) Slow performance D) Limited functionality
Answer: B – Admin can upgrade to malicious implementation.

Q9. What happens when renounceOwnership() is called?
A) Transfer to 0x0 B) Contract becomes unmanaged C) Tokens burn D) Contract pauses
Answer: B – Irreversibly removes admin control.

Q10. Which protocol uses 4-of-7 multi-sig for fees?
A) Compound B) Aave C) Uniswap D) MakerDAO

Quiz (2/2)

Q6. Purpose of Pausable pattern?
A) Save gas B) Emergency circuit breaker C) Speed up tx D) Reduce fees
Answer: B – Halts transfers during critical bugs.

Q7. In 3-of-5 multi-sig, approvals needed?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3 signatures required out of 5 owners.

Q8. Main disadvantage of upgradeable contracts?
A) High deployment cost B) Admin can rug pull C) Slow performance D) Limited functionality
Answer: B – Admin can upgrade to malicious implementation.

Q9. What happens when renounceOwnership() is called?
A) Transfer to 0x0 B) Contract becomes unmanaged C) Tokens burn D) Contract pauses
Answer: B – Irreversibly removes admin control.

Q10. Which protocol uses 4-of-7 multi-sig for fees?
A) Compound B) Aave C) Uniswap D) MakerDAO
Answer: C – Uniswap uses 4-of-7 for protocol fee control.

Thank you

Questions?

Next: L20 Lab – Token Analysis

Quiz: Token Lifecycle

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. Which minting strategy is most gas-efficient for 10,000 addresses?
A) Mapping allowlist B) Array allowlist C) Merkle tree D) Owner approval

Quiz (1–5)

Q1. Which minting strategy is most gas-efficient for 10,000 addresses?
A) Mapping allowlist B) Array allowlist C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses.

Q2. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage C) Creates new contract D) Sends ETH

Quiz (1–5)

Q1. Which minting strategy is most gas-efficient for 10,000 addresses?
A) Mapping allowlist B) Array allowlist C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses.

Q2. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage C) Creates new contract D) Sends ETH
Answer: B – delegatecall runs implementation code using proxy's storage context.

Q3. Which burn mechanism has the highest price impact?
A) Fee burn B) Voluntary burn C) Buyback and burn D) Governance burn

Quiz (1–5)

Q1. Which minting strategy is most gas-efficient for 10,000 addresses?
A) Mapping allowlist B) Array allowlist C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses.

Q2. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage C) Creates new contract D) Sends ETH
Answer: B – delegatecall runs implementation code using proxy's storage context.

Q3. Which burn mechanism has the highest price impact?
A) Fee burn B) Voluntary burn C) Buyback and burn D) Governance burn
Answer: C – Buyback creates buy pressure before burning.

Q4. What is the main risk of the Ownable pattern?
A) Too many admins B) Single point of failure C) High gas costs D) Slow execution

Quiz (1–5)

Q1. Which minting strategy is most gas-efficient for 10,000 addresses?
A) Mapping allowlist B) Array allowlist C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses.

Q2. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage C) Creates new contract D) Sends ETH
Answer: B – delegatecall runs implementation code using proxy's storage context.

Q3. Which burn mechanism has the highest price impact?
A) Fee burn B) Voluntary burn C) Buyback and burn D) Governance burn
Answer: C – Buyback creates buy pressure before burning.

Q4. What is the main risk of the Ownable pattern?
A) Too many admins B) Single point of failure C) High gas costs D) Slow execution
Answer: B – Owner key compromise gives attacker full control.

Q5. In a 3-of-5 multi-sig, how many approvals are needed?
A) 2 B) 3 C) 4 D) 5

Quiz (1–5)

Q1. Which minting strategy is most gas-efficient for 10,000 addresses?
A) Mapping allowlist B) Array allowlist C) Merkle tree D) Owner approval
Answer: C – Merkle tree stores single 32-byte root instead of 10,000 addresses.

Q2. What does delegatecall do in a proxy pattern?
A) Transfers ownership B) Executes logic in proxy's storage C) Creates new contract D) Sends ETH
Answer: B – delegatecall runs implementation code using proxy's storage context.

Q3. Which burn mechanism has the highest price impact?
A) Fee burn B) Voluntary burn C) Buyback and burn D) Governance burn
Answer: C – Buyback creates buy pressure before burning.

Q4. What is the main risk of the Ownable pattern?
A) Too many admins B) Single point of failure C) High gas costs D) Slow execution
Answer: B – Owner key compromise gives attacker full control.

Q5. In a 3-of-5 multi-sig, how many approvals are needed?
A) 2 B) 3 C) 4 D) 5
Answer: B – 3-of-5 means 3 signatures required out of 5 total owners.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas D) Increase voting

Quiz (6–10)

Q6. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas D) Increase voting
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q7. Which deflationary mechanism is used by Ethereum (EIP-1559)?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas D) Increase voting
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q7. Which deflationary mechanism is used by Ethereum (EIP-1559)?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn
Answer: B – Base fees are burned automatically, reducing ETH supply.

Q8. What happens when a contract calls renounceOwnership()?
A) Transfers to 0x0 B) Contract becomes unmanaged C) All tokens burn D) Contract pauses

Quiz (6–10)

Q6. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas D) Increase voting
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q7. Which deflationary mechanism is used by Ethereum (EIP-1559)?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn
Answer: B – Base fees are burned automatically, reducing ETH supply.

Q8. What happens when a contract calls renounceOwnership()?
A) Transfers to 0x0 B) Contract becomes unmanaged C) All tokens burn D) Contract pauses
Answer: B – renounceOwnership() irreversibly removes admin control.

Q9. Which stablecoin is NOT pausable?
A) USDC B) USDT C) DAI D) BUSD

Quiz (6–10)

Q6. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas D) Increase voting
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q7. Which deflationary mechanism is used by Ethereum (EIP-1559)?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn
Answer: B – Base fees are burned automatically, reducing ETH supply.

Q8. What happens when a contract calls renounceOwnership()?
A) Transfers to 0x0 B) Contract becomes unmanaged C) All tokens burn D) Contract pauses
Answer: B – renounceOwnership() irreversibly removes admin control.

Q9. Which stablecoin is NOT pausable?
A) USDC B) USDT C) DAI D) BUSD
Answer: C – DAI is fully decentralized and cannot be paused or frozen.

Q10. Where is state stored in a Transparent Proxy pattern?
A) Implementation contract B) Proxy contract C) Both contracts D) External storage

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the purpose of a timelock in governance?
A) Speed up execution B) Allow community reaction and exit C) Reduce gas D) Increase voting
Answer: B – Timelock delays critical actions so users can exit if disagreeing.

Q7. Which deflationary mechanism is used by Ethereum (EIP-1559)?
A) Voluntary burn B) Transaction fee burn C) Buyback burn D) Governance burn
Answer: B – Base fees are burned automatically, reducing ETH supply.

Q8. What happens when a contract calls renounceOwnership()?
A) Transfers to 0x0 B) Contract becomes unmanaged C) All tokens burn D) Contract pauses
Answer: B – renounceOwnership() irreversibly removes admin control.

Q9. Which stablecoin is NOT pausable?
A) USDC B) USDT C) DAI D) BUSD
Answer: C – DAI is fully decentralized and cannot be paused or frozen.

Q10. Where is state stored in a Transparent Proxy pattern?
A) Implementation contract B) Proxy contract C) Both contracts D) External storage
Answer: B – Storage lives in proxy; implementation is stateless logic.

(c) Joerg Osterrieder 2025

Lab Session: Token Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module B: Ethereum & Smart Contracts

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Discover and research ERC-20 tokens on Etherscan
- Analyze token contract source code
- Evaluate holder distribution and concentration
- Identify potential red flags in token design
- Use DeFi analytics tools for research

The Problem: Hands-on Token Evaluation

The Challenge
Thousands of ERC-20 tokens exist on Ethereum, but many are scams, have hidden risks, or concentrated ownership. Investors need practical skills to evaluate tokens before interacting with them, but most lack the technical knowledge to read smart contract code or interpret on-chain data.

Why It Matters

- Rug pulls and token scams cost investors billions annually
- Hidden admin functions can freeze funds or mint infinite supply

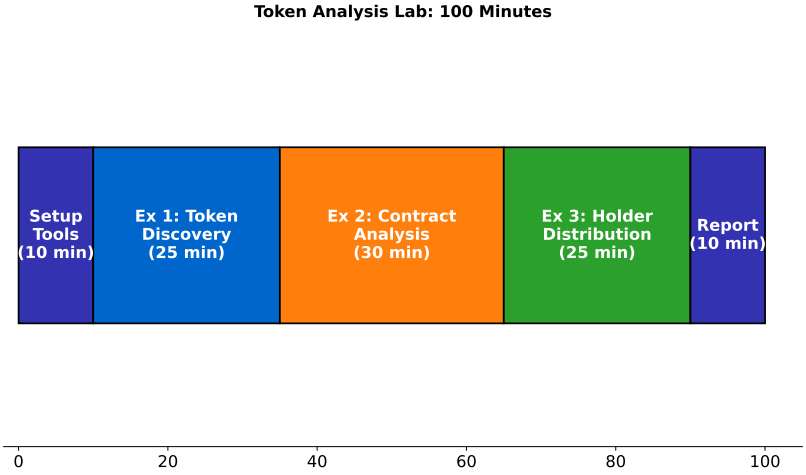
What You'll Explore

- Reading and analyzing token contracts on Etherscan
- Evaluating holder distribution and concentration risk
- Identifying red flags: unlimited minting, blacklists, hidden fees
- Using analytics tools (DeFiLlama, CoinGecko) for due diligence

The Cryptoeconomics Question
How does transparent on-chain analysis protect investors and reveal power dynamics in token economies?

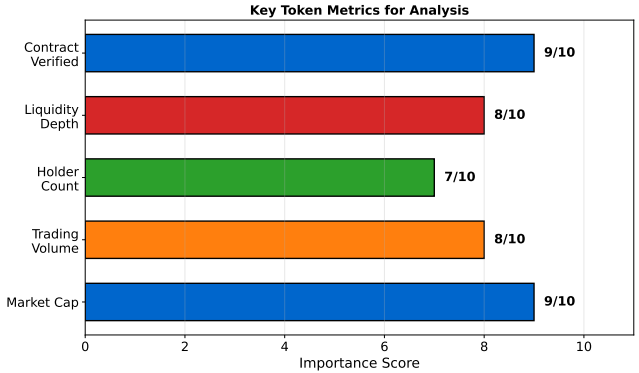
Today's lab: Hands-on skills for evaluating token safety and distribution

Lab Session Structure



Focus on due diligence skills for token evaluation

Key Token Metrics



Contract verification is essential - never interact with unverified contracts

Exercise 1: Token Discovery

Tools:

- Etherscan Token Tracker: `https://etherscan.io/tokens`
- CoinGecko: `https://coingecko.com`
- DeFiLlama: `https://defillama.com`

Tasks:

1. Browse top ERC-20 tokens by market cap
2. Select a token for analysis (e.g., LINK, UNI, AAVE)
3. Note: contract address, total supply, decimals
4. Check if contract is verified

Exercise 2: Contract Analysis

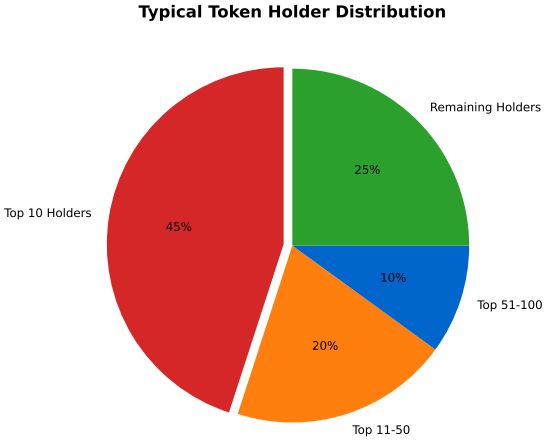
Key Elements to Check:

- **Standard Compliance**: Does it implement ERC-20 correctly?
- **Owner Functions**: Can owner mint, pause, blacklist?
- **Transfer Restrictions**: Any hidden fees or taxes?
- **Proxy Pattern**: Is it upgradeable?

Red Flags:

- Unverified source code
- Owner can mint unlimited tokens
- Hidden transfer fees
- Blacklist functionality without governance

Holder Distribution Analysis



Warning: High concentration (>50% in top 10) = centralization risk

High concentration in top holders indicates centralization risk

Exercise 3: Holder Distribution

Etherscan Holder Analysis:

1. Go to token page -¿ Holders tab
2. Note top 10 holders and their percentages
3. Identify: exchanges, team wallets, contracts
4. Calculate concentration ratio

Healthy Distribution Indicators:

- No single holder ¿ 10% (except exchanges)
- Team tokens locked or vesting
- Wide distribution (1000+ unique holders)
- Active trading volume

Lab Deliverables

Submit:

1. **Token Analysis Report (2-3 pages):**
   - Token name, contract address, basic metrics
   - Contract analysis findings
   - Holder distribution summary
   - Risk assessment (Low/Medium/High)
2. **Screenshots:**
   - Token overview page
   - Contract code snippet
   - Holder distribution

Problem Solved? Token Analysis

The Original Problem
Investors lack skills to evaluate token safety before interaction

What You Learned

- **Contract verification**: Reading source code on Etherscan reveals hidden functions (mint, pause, blacklist)
- **Holder analysis**: Concentration metrics identify centralization risk and potential manipulation
- **Red flag detection**: Spotting unverified contracts, unlimited owner privileges, and hidden transfer fees

Cryptoeconomics Insight
Cost vs Reward:

- **Cost**: Time investment in due diligence (15-30 min per token)
- **Reward**: Avoiding scams, understanding value distribution, informed investment decisions

What Could Still Go Wrong?

- Hidden proxy upgrades can change contract logic post-analysis
- Complex governance can hide extractive tokenomics
- Upgradeable contracts introduce trust assumptions

Token analysis reduces risk but cannot eliminate all threats - ongoing vigilance required

Key Takeaways

- Always verify contract source code before interacting
- Check holder distribution for concentration risk
- Look for red flags: hidden fees, owner privileges
- Use multiple tools for comprehensive analysis
- High market cap does not guarantee safety

(c) Joerg Osterrieder 2025

Quiz Questions (1/4)

Q1. What does a verified contract on Etherscan indicate?
A) The token is safe to invest in B) Source code matches deployed bytecode
C) The token cannot be hacked D) The owner is trustworthy
Answer: B – Verification proves source code matches deployed contract.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% of tokens
C) Contract has 18 decimals D) Token is listed on exchanges
Answer: B – High concentration in few wallets indicates centralization risk.

Q3. What is a major red flag in token contract code?
A) Using SafeMath library B) Owner can mint unlimited tokens
C) Emitting Transfer events D) Implementing ERC-20 standard
Answer: B – Unlimited minting power allows owner to inflate supply.

Q4. On Etherscan, where do you find holder distribution data?
A) Read Contract tab B) Transactions tab
C) Holders tab D) Analytics tab
Answer: C – Holders tab shows top token holders and their percentage.

Q5. What does the "decimals" parameter specify in ERC-20?
A) Token price precision B) Number of divisible units
C) Maximum supply D) Transfer fee percentage
Answer: B – Decimals defines smallest unit divisibility.

Quiz Questions (2/4)

Q6. Which tool is best for comparing token metrics across DeFi protocols?
A) Etherscan only B) CoinGecko only
C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL and metrics across DeFi protocols.

Q7. What indicates healthy token distribution?
A) Single whale owns 50% B) Wide distribution with 1000+ unique holders
C) All tokens locked in contracts D) Only listed on one exchange
Answer: B – Wide distribution reduces manipulation risk.

Q8. What is a proxy pattern in smart contracts?
A) Token with hidden fees B) Upgradeable contract architecture
C) Contract that cannot be changed D) Token standard for NFTs
Answer: B – Proxy pattern allows upgrading contract logic.

Q9. Why should you check if team tokens are vesting?
A) To ensure they cannot dump all tokens immediately
B) To calculate market cap C) To verify contract deployment
D) To check gas costs
Answer: A – Vesting prevents team from selling all tokens at once.

Q10. What does high trading volume relative to market cap indicate?
A) Token is worthless B) High liquidity and active market
C) Contract is broken D) Token will increase in value
Answer: B – High volume/cap ratio indicates liquid market.

Quiz Questions (3/4)

Q11. What is a potential issue with blacklist functionality?
A) Improves security B) Owner can freeze specific addresses without governance
C) Required by ERC-20 D) Reduces gas costs
Answer: B – Centralized blacklist power allows owner to freeze funds.

Q12. On Etherscan, what does the "Max Total Supply" field show?
A) Current circulating supply B) Maximum possible tokens that can exist
C) Number of holders D) Contract deployment date
Answer: B – Max total supply shows the hard cap on token issuance.

Q13. What is a hidden transfer fee?
A) Etherscan listing fee B) Percentage taken on each token transfer not disclosed in UI
C) Gas cost for transactions D) Exchange trading fee
Answer: B – Hidden fees reduce received amount without clear disclosure.

Q14. Which CoinGecko metric helps assess liquidity?
A) All-time high price B) 24h trading volume
C) Total number of holders D) Contract creation date
Answer: B – 24h volume shows trading activity and liquidity.

Q15. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in decentralized exchange
C) Owner controls everything D) Token cannot be traded
Answer: B – DEX contracts holding tokens indicates liquidity pools.

Quiz Questions (4/4)

Q16. Why check if a contract implements pausable functionality?
A) To verify gas efficiency B) Owner can halt all transfers centrally
C) To see transaction history D) To check token decimals
Answer: B – Pausable contracts let owner freeze all activity.

Q17. What is concentration ratio in holder analysis?
A) Number of exchanges listing token B) Percentage owned by top N holders
C) Total supply divided by decimals D) Average transaction size
Answer: B – Concentration ratio measures how much supply top holders control.

Q18. On Etherscan, what does the "Contract Creator" field reveal?
A) Token price history B) Address that deployed the contract
C) Number of token holders D) Current gas price
Answer: B – Shows deployer address, useful for identifying official tokens.

Q19. What is a key benefit of using multiple analysis tools?
A) Reduces gas costs B) Cross-validation of data and comprehensive view
C) Guarantees profit D) Eliminates all risks
Answer: B – Multiple tools provide different perspectives and verify accuracy.

Q20. What should you verify before adding a token to your wallet?
A) Only check if it has a logo B) Verify contract address matches official source
C) Just search by name D) Trust any Etherscan listing
Answer: B – Many scam tokens use similar names; verify exact address.

Lab Session: Token Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module B: Ethereum & Smart Contracts

(c) Joerg Osterrieder 2025

How Do You Conduct Etherscan Detective Work?

[COMIC: Investigator analyzing contract on Etherscan]

"The blockchain never forgets..."

The Investigation

- Every transaction is public
- Contract code reveals intent
- Holder data shows concentration

Today's Lab

- Navigate Etherscan like a pro
- Spot red flags in contracts
- Analyze real token distributions

On-chain analysis is your superpower. Today you learn to use it.

Learning Objectives

By the end of this lab session, you will be able to:

- Discover and research ERC-20 tokens on Etherscan
- Analyze token contract source code
- Evaluate holder distribution and concentration
- Identify potential red flags in token design
- Use DeFi analytics tools for research

Building on L19: Token Lifecycle

The Problem: Hands-on Token Evaluation

The Challenge
Thousands of ERC-20 tokens exist on Ethereum, but many are scams, have hidden risks, or concentrated ownership. Investors need practical skills to evaluate tokens before interacting with them, but most lack the technical knowledge to read smart contract code or interpret on-chain data.

Why It Matters

- Rug pulls and token scams cost investors billions annually
- Hidden admin functions can freeze funds or mint infinite supply

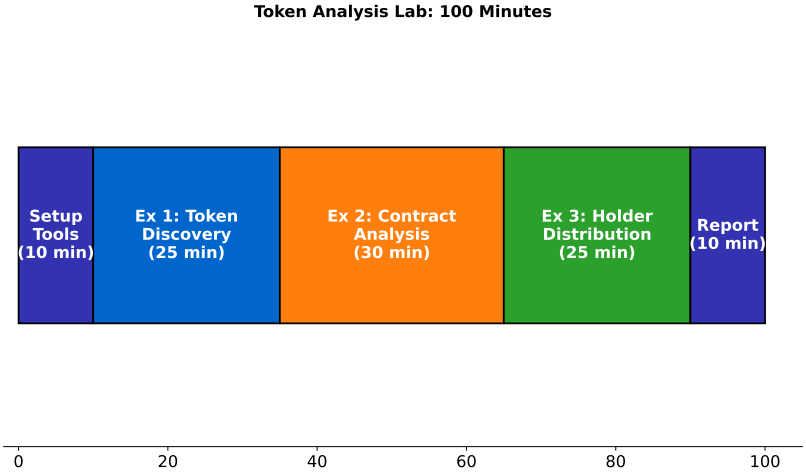
What You'll Explore

- Reading and analyzing token contracts on Etherscan
- Evaluating holder distribution and concentration risk
- Identifying red flags: unlimited minting, blacklists, hidden fees
- Using analytics tools (DeFiLlama, CoinGecko) for due diligence

The Cryptoeconomics Question
How does transparent on-chain analysis protect investors and reveal power dynamics in token economies?

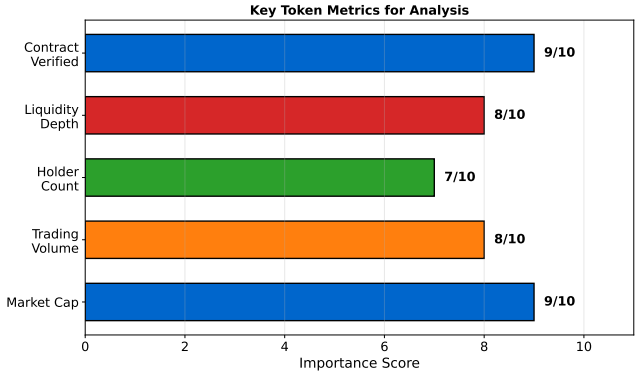
Today's lab: Hands-on skills for evaluating token safety and distribution

How Is This Lab Session Structured?



Focus on due diligence skills for token evaluation

What Are the Key Token Metrics?



Contract verification is essential - never interact with unverified contracts

Exercise 1: Token Discovery

Tools:

- Etherscan Token Tracker: `https://etherscan.io/tokens`
- CoinGecko: `https://coingecko.com`
- DeFiLlama: `https://defillama.com`

Tasks:

1. Browse top ERC-20 tokens by market cap
2. Select a token for analysis (e.g., LINK, UNI, AAVE)
3. Note: contract address, total supply, decimals
4. Check if contract is verified

Exercise 2: Contract Analysis

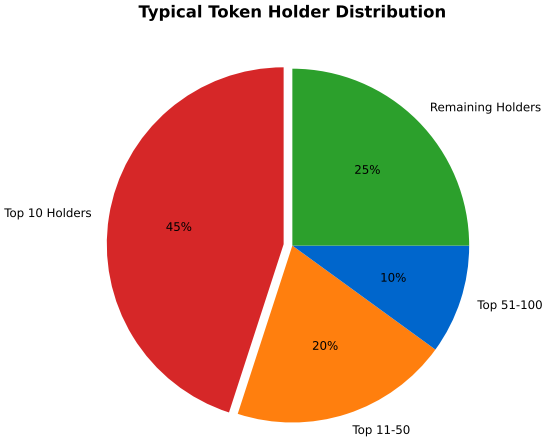
Key Elements to Check:

- **Standard Compliance**: Does it implement ERC-20 correctly?
- **Owner Functions**: Can owner mint, pause, blacklist?
- **Transfer Restrictions**: Any hidden fees or taxes?
- **Proxy Pattern**: Is it upgradeable?

Red Flags:

- Unverified source code
- Owner can mint unlimited tokens
- Hidden transfer fees
- Blacklist functionality without governance

How Do You Analyze Holder Distribution?



Warning: High concentration (>50% in top 10) = centralization risk

High concentration in top holders indicates centralization risk

Exercise 3: Holder Distribution

Etherscan Holder Analysis:

1. Go to token page -¿ Holders tab
2. Note top 10 holders and their percentages
3. Identify: exchanges, team wallets, contracts
4. Calculate concentration ratio

Healthy Distribution Indicators:

- No single holder ¿ 10% (except exchanges)
- Team tokens locked or vesting
- Wide distribution (1000+ unique holders)
- Active trading volume

What Should You Deliver for This Lab?

Submit:

1. **Token Analysis Report (2-3 pages):**
   - Token name, contract address, basic metrics
   - Contract analysis findings
   - Holder distribution summary
   - Risk assessment (Low/Medium/High)
2. **Screenshots:**
   - Token overview page
   - Contract code snippet
   - Holder distribution

Problem Solved? Token Analysis

The Original Problem
Investors lack skills to evaluate token safety before interaction

What You Learned

- **Contract verification**: Reading source code on Etherscan reveals hidden functions (mint, pause, blacklist)
- **Holder analysis**: Concentration metrics identify centralization risk and potential manipulation
- **Red flag detection**: Spotting unverified contracts, unlimited owner privileges, and hidden transfer fees

Cryptoeconomics Insight
Cost vs Reward:

- **Cost**: Time investment in due diligence (15-30 min per token)
- **Reward**: Avoiding scams, understanding value distribution, informed investment decisions

What Could Still Go Wrong?

- Hidden proxy upgrades can change contract logic post-analysis
- Complex governance can hide extractive tokenomics
- Upgradeable contracts introduce trust assumptions

Token analysis reduces risk but cannot eliminate all threats - ongoing vigilance required

The Economics of Token Analysis

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Token Analysis

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Token Analysis

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Why Is Contract Verification Important?

[COMIC: Two contracts - one verified, one not]

"Would you trust a black box with your money?"

The Lesson

- Verified = source matches bytecode
- Unverified = cannot review code
- High market cap $\neq$ safe

What We Practiced

- Reading contract functions
- Analyzing holder concentration
- Cross-referencing multiple tools

Never interact with unverified contracts. Verification is the minimum bar for trust.

Key Takeaways

- Always verify contract source code before interacting
- Check holder distribution for concentration risk
- Look for red flags: hidden fees, owner privileges
- Use multiple tools for comprehensive analysis
- High market cap does not guarantee safety

Next Lesson: L21 – NFT Technology Deep Dive

(c) Joerg Osterrieder 2025

Quiz Questions (1/4)

Q1. What does a verified contract on Etherscan indicate?
A) The token is safe to invest in B) Source code matches deployed bytecode
C) The token cannot be hacked D) The owner is trustworthy
Answer: B – Verification proves source code matches deployed contract.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% of tokens
C) Contract has 18 decimals D) Token is listed on exchanges
Answer: B – High concentration in few wallets indicates centralization risk.

Q3. What is a major red flag in token contract code?
A) Using SafeMath library B) Owner can mint unlimited tokens
C) Emitting Transfer events D) Implementing ERC-20 standard
Answer: B – Unlimited minting power allows owner to inflate supply.

Q4. On Etherscan, where do you find holder distribution data?
A) Read Contract tab B) Transactions tab
C) Holders tab D) Analytics tab
Answer: C – Holders tab shows top token holders and their percentage.

Q5. What does the "decimals" parameter specify in ERC-20?
A) Token price precision B) Number of divisible units
C) Maximum supply D) Transfer fee percentage
Answer: B – Decimals defines smallest unit divisibility.

Quiz Questions (2/4)

Q6. Which tool is best for comparing token metrics across DeFi protocols?
A) Etherscan only B) CoinGecko only
C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL and metrics across DeFi protocols.

Q7. What indicates healthy token distribution?
A) Single whale owns 50% B) Wide distribution with 1000+ unique holders
C) All tokens locked in contracts D) Only listed on one exchange
Answer: B – Wide distribution reduces manipulation risk.

Q8. What is a proxy pattern in smart contracts?
A) Token with hidden fees B) Upgradeable contract architecture
C) Contract that cannot be changed D) Token standard for NFTs
Answer: B – Proxy pattern allows upgrading contract logic.

Q9. Why should you check if team tokens are vesting?
A) To ensure they cannot dump all tokens immediately
B) To calculate market cap C) To verify contract deployment
D) To check gas costs
Answer: A – Vesting prevents team from selling all tokens at once.

Q10. What does high trading volume relative to market cap indicate?
A) Token is worthless B) High liquidity and active market
C) Contract is broken D) Token will increase in value
Answer: B – High volume/cap ratio indicates liquid market.

Quiz Questions (3/4)

Q11. What is a potential issue with blacklist functionality?
A) Improves security B) Owner can freeze specific addresses without governance
C) Required by ERC-20 D) Reduces gas costs
Answer: B – Centralized blacklist power allows owner to freeze funds.

Q12. On Etherscan, what does the "Max Total Supply" field show?
A) Current circulating supply B) Maximum possible tokens that can exist
C) Number of holders D) Contract deployment date
Answer: B – Max total supply shows the hard cap on token issuance.

Q13. What is a hidden transfer fee?
A) Etherscan listing fee B) Percentage taken on each token transfer not disclosed in UI
C) Gas cost for transactions D) Exchange trading fee
Answer: B – Hidden fees reduce received amount without clear disclosure.

Q14. Which CoinGecko metric helps assess liquidity?
A) All-time high price B) 24h trading volume
C) Total number of holders D) Contract creation date
Answer: B – 24h volume shows trading activity and liquidity.

Q15. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in decentralized exchange
C) Owner controls everything D) Token cannot be traded
Answer: B – DEX contracts holding tokens indicates liquidity pools.

Quiz Questions (4/4)

Q16. Why check if a contract implements pausable functionality?
A) To verify gas efficiency B) Owner can halt all transfers centrally
C) To see transaction history D) To check token decimals
Answer: B – Pausable contracts let owner freeze all activity.

Q17. What is concentration ratio in holder analysis?
A) Number of exchanges listing token B) Percentage owned by top N holders
C) Total supply divided by decimals D) Average transaction size
Answer: B – Concentration ratio measures how much supply top holders control.

Q18. On Etherscan, what does the "Contract Creator" field reveal?
A) Token price history B) Address that deployed the contract
C) Number of token holders D) Current gas price
Answer: B – Shows deployer address, useful for identifying official tokens.

Q19. What is a key benefit of using multiple analysis tools?
A) Reduces gas costs B) Cross-validation of data and comprehensive view
C) Guarantees profit D) Eliminates all risks
Answer: B – Multiple tools provide different perspectives and verify accuracy.

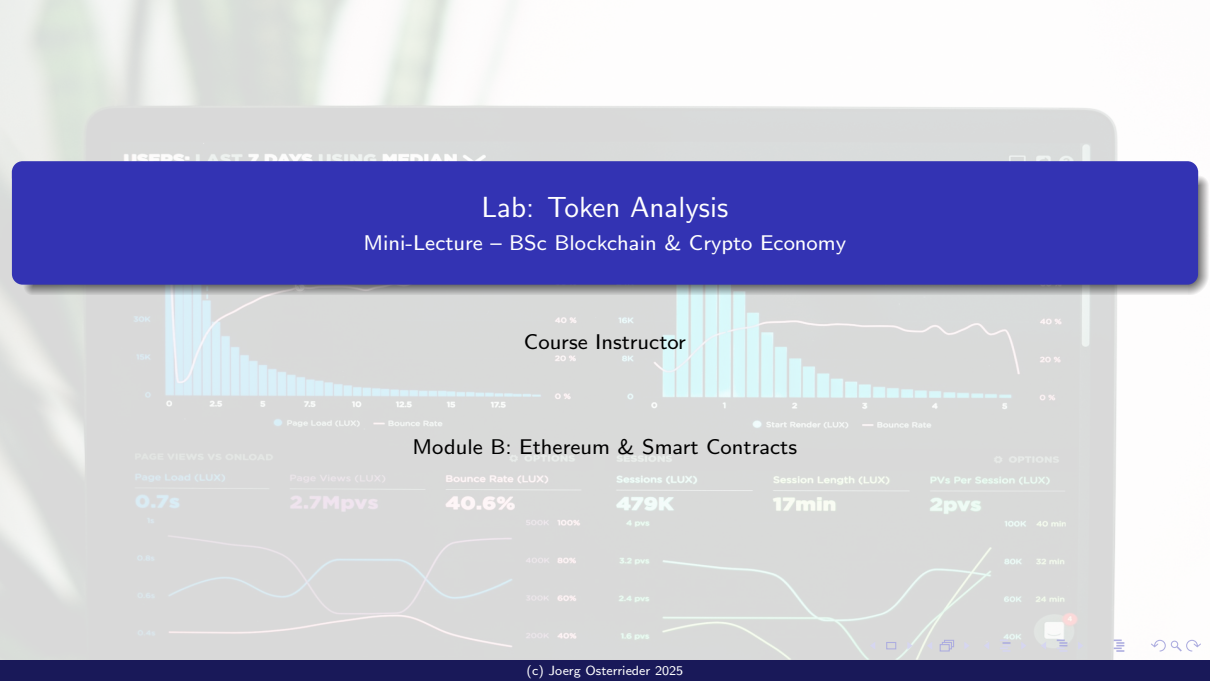
Q20. What should you verify before adding a token to your wallet?
A) Only check if it has a logo B) Verify contract address matches official source
C) Just search by name D) Trust any Etherscan listing
Answer: B – Many scam tokens use similar names; verify exact address.

Lab: Token Analysis

Mini-Lecture – BSc Blockchain & Crypto Economy

Course Instructor

Module B: Ethereum & Smart Contracts



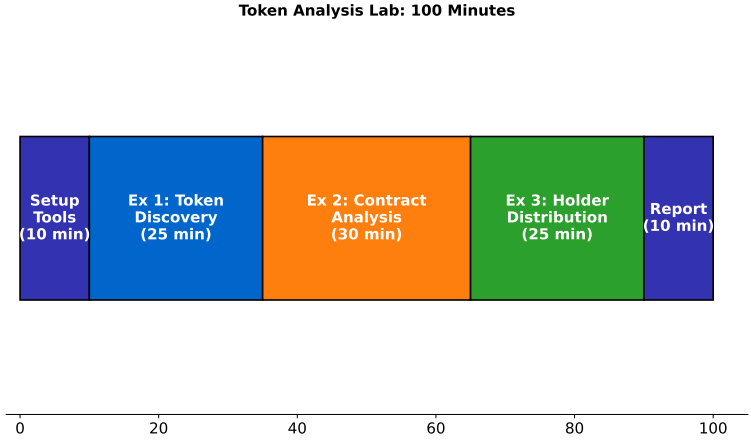
Learning Objectives

By the end of this lab, you will be able to:

- Research ERC-20 tokens using Etherscan
- Analyze token contract source code for red flags
- Evaluate holder distribution and concentration risk
- Use DeFi analytics tools for due diligence

Hands-on skills for token evaluation and risk assessment

Lab Session Structure



Three exercises: Discovery, Contract Analysis, Holder Distribution

Essential Analysis Tools

Primary Tools:

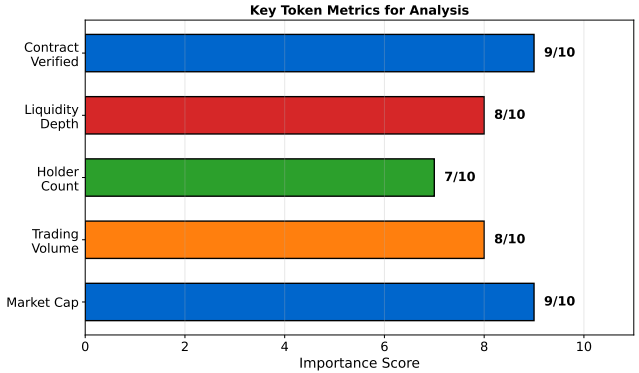
- **Etherscan Token Tracker**: Contract verification, holder data
- **CoinGecko**: Market cap, volume, price history
- **DeFiLlama**: TVL, protocol comparisons

Why Multiple Tools?

- Cross-validation of data accuracy
- Different perspectives on same token
- Comprehensive risk assessment

Never rely on a single data source for investment decisions

Key Token Metrics



Contract verification is essential – never interact with unverified contracts

Exercise 1: Token Discovery

Tasks:

1. Browse top ERC-20 tokens by market cap on Etherscan
2. Select a token for analysis (e.g., LINK, UNI, AAVE)
3. Record: contract address, total supply, decimals
4. Verify the contract is verified (source code available)

Key Data Points:

- Contract address (0x...)
- Total supply and circulating supply
- Decimals (typically 18)

Always copy contract address from official sources, not search results

Exercise 2: Contract Analysis

Key Elements to Check:

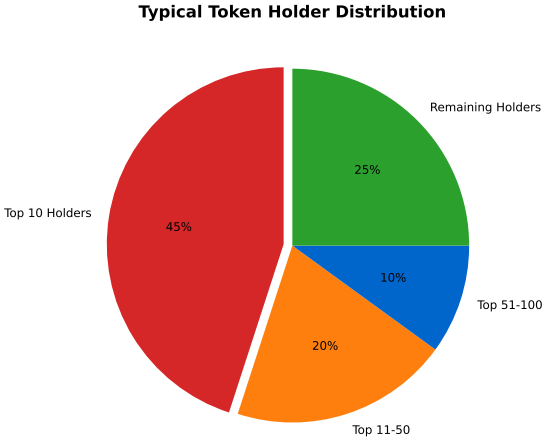
- **Standard Compliance**: Correct ERC-20 implementation?
- **Owner Functions**: Mint, pause, or blacklist capabilities?
- **Transfer Restrictions**: Hidden fees or taxes?
- **Proxy Pattern**: Upgradeable contract?

Major Red Flags:

- Unverified source code
- Owner can mint unlimited tokens
- Hidden transfer fees

Upgradeable contracts can change behavior – check governance process

Holder Distribution Analysis



Warning: High concentration (>50% in top 10) = centralization risk

High concentration in top holders indicates centralization risk

Exercise 3: Holder Distribution

Etherscan Holder Analysis:

1. Navigate to token page, select Holders tab
2. Record top 10 holders and their percentages
3. Identify wallet types: exchanges, team, contracts
4. Calculate concentration ratio (top 10 share)

Healthy Distribution Signs:

- No single holder ¿ 10% (except exchanges)
- Team tokens locked or vesting
- Wide distribution (1000+ holders)

DEX contracts as top holders indicate liquidity pools, not concentration

Lab Deliverables

Submit:

1. **Token Analysis Report (2-3 pages):**
   - Token name, contract address, basic metrics
   - Contract analysis findings (red flags identified)
   - Holder distribution summary with concentration ratio
   - Risk assessment: Low / Medium / High
2. **Screenshots:**
   - Token overview page
   - Contract code snippet showing key function
   - Holder distribution chart

Due: End of next week – submit via course platform

Quiz Sample

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe **B) Source matches bytecode** C) Cannot be hacked

Q2. Which metric indicates high centralization risk?
A) 1B total supply **B) Top 10 own 80%** C) 18 decimals

Q3. What is a major red flag in token code?
A) SafeMath library **B) Owner can mint unlimited** C) Transfer events

Q4. What does the decimals parameter specify?
A) Price precision **B) Divisible units** C) Max supply

Q5. Why check if team tokens are vesting?
A) Prevent immediate dump B) Calculate market cap C) Check gas

Answers: B, B, B, B, A – Full quiz in lab materials

Key Takeaways

- **Always verify** contract source code before interacting
- **Check holder distribution** for concentration risk
- **Look for red flags**: hidden fees, unlimited minting, owner privileges
- **Use multiple tools** for comprehensive analysis
- **High market cap** does not guarantee safety

Remember: Due diligence before any token interaction!

These skills apply to all ERC-20 tokens, DeFi protocols, and NFT projects

Resources

Primary Tools:

- Etherscan: `https://etherscan.io/tokens`
- CoinGecko: `https://coingecko.com`
- DeFiLlama: `https://defillama.com`

Additional Reading:

- ERC-20 Standard: EIP-20 specification
- Token Sniffer: Automated scam detection
- RugDoc: DeFi safety reviews

Questions? Office hours: Monday 2-4pm or by appointment

L20: Lab – Token Analysis

Mini-Lecture – Module B: Ethereum & Smart Contracts

Blockchain & Cryptocurrency Course

January 2026

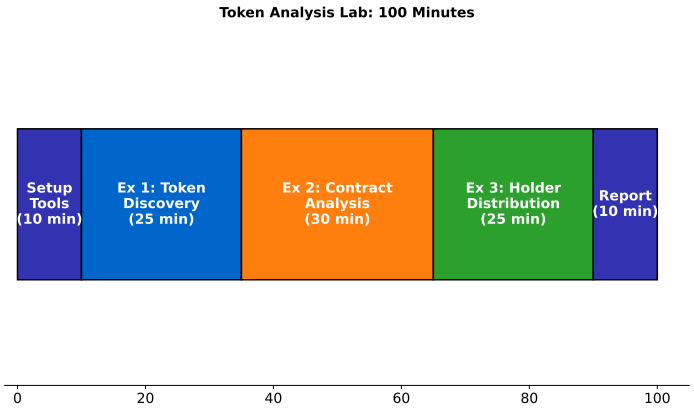
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

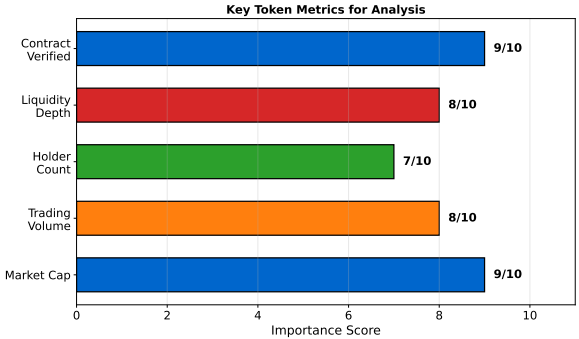
- Research ERC-20 tokens on Etherscan
- Analyze token contract source code for red flags
- Evaluate holder distribution and concentration risk
- Use DeFi analytics tools for due diligence

Token Analysis Workflow



Focus: Due diligence skills for evaluating any token.

Key Token Metrics



Critical: Contract verification is essential – never interact with unverified contracts.

Contract Analysis: Red Flags

Elements to Check:

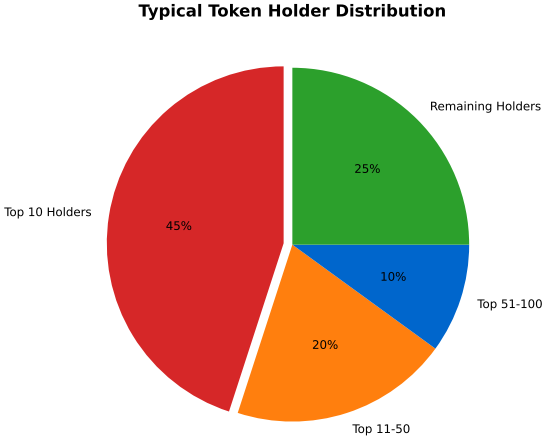
- **Standard Compliance:** Does it implement ERC-20 correctly?
- **Owner Functions:** Can owner mint, pause, blacklist?
- **Transfer Restrictions:** Hidden fees or taxes?
- **Proxy Pattern:** Is it upgradeable?

Red Flags:

- Unverified source code
- Owner can mint unlimited tokens
- Hidden transfer fees (not disclosed in UI)
- Blacklist functionality without governance

(c) Joerg Osterrieder 2025

Holder Distribution Analysis



Warning: High concentration (>50% in top 10) = centralization risk

High concentration in top holders = centralization risk.

Healthy Distribution Indicators

Positive Signs:

- No single holder $> 10\%$ (except exchanges)
- Team tokens locked or vesting
- Wide distribution (1000+ unique holders)
- Active trading volume

Analysis Tools:

- Etherscan: Token Tracker, Holders tab
- CoinGecko: Market cap, volume, price
- DeFiLlama: TVL across protocols

Key Metric: Concentration ratio = % owned by top N holders.

Token Due Diligence Checklist

Before Interacting:

1. Contract verified on Etherscan?
2. Check owner privileges (mint, pause, blacklist)
3. Review holder distribution
4. Verify team tokens are vesting
5. Check trading volume vs market cap
6. Multiple sources confirm contract address

Warning: High market cap does not guarantee safety!

Analysis Tools Overview

Etherscan (etherscan.io):

- Contract verification, source code, holders
- Transaction history, internal transactions

CoinGecko (coingecko.com):

- Market cap, 24h volume, liquidity
- Exchange listings, historical prices

DeFiLlama (defillama.com):

- TVL across DeFi protocols
- Protocol comparison and analytics

Key Takeaways

1. **Verification:** Always verify contract source code before interacting
2. **Distribution:** Check holder concentration for manipulation risk
3. **Red Flags:** Hidden fees, unlimited minting, unverified code
4. **Multiple Sources:** Cross-validate with Etherscan, CoinGecko, DeFiLlama
5. **Contract Address:** Always verify exact address from official source

Lab Goal: Analyze a token and produce risk assessment report.

Token Analysis in Practice

Token Analysis

Research Tools

Data Analytics

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What does verified contract on Etherscan indicate?
A) Token is safe B) Source code matches bytecode C) Cannot be hacked D) Owner is trustworthy

Quiz (1/2)

Q1. What does verified contract on Etherscan indicate?
A) Token is safe B) Source code matches bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification proves source matches deployed contract.

Q2. High centralization risk indicator?
A) Supply over 1B B) Top 10 holders own 80% C) 18 decimals D) Listed on exchanges

Quiz (1/2)

Q1. What does verified contract on Etherscan indicate?
A) Token is safe B) Source code matches bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification proves source matches deployed contract.

Q2. High centralization risk indicator?
A) Supply over 1B B) Top 10 holders own 80% C) 18 decimals D) Listed on exchanges
Answer: B – High concentration = manipulation risk.

Q3. Major red flag in token contract?
A) SafeMath library B) Owner can mint unlimited C) Transfer events D) ERC-20 standard

Quiz (1/2)

Q1. What does verified contract on Etherscan indicate?
A) Token is safe B) Source code matches bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification proves source matches deployed contract.

Q2. High centralization risk indicator?
A) Supply over 1B B) Top 10 holders own 80% C) 18 decimals D) Listed on exchanges
Answer: B – High concentration = manipulation risk.

Q3. Major red flag in token contract?
A) SafeMath library B) Owner can mint unlimited C) Transfer events D) ERC-20 standard
Answer: B – Unlimited minting allows supply inflation.

Q4. Where to find holder distribution on Etherscan?
A) Read Contract B) Transactions C) Holders tab D) Analytics

(c) Joerg Osterrieder 2025

Quiz (1/2)

Q1. What does verified contract on Etherscan indicate?
A) Token is safe B) Source code matches bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification proves source matches deployed contract.

Q2. High centralization risk indicator?
A) Supply over 1B B) Top 10 holders own 80% C) 18 decimals D) Listed on exchanges
Answer: B – High concentration = manipulation risk.

Q3. Major red flag in token contract?
A) SafeMath library B) Owner can mint unlimited C) Transfer events D) ERC-20 standard
Answer: B – Unlimited minting allows supply inflation.

Q4. Where to find holder distribution on Etherscan?
A) Read Contract B) Transactions C) Holders tab D) Analytics
Answer: C – Holders tab shows top holders and percentages.

Q5. What does "decimals" parameter specify?
A) Price precision B) Divisible units C) Max supply D) Fee percentage

Quiz (1/2)

Q1. What does verified contract on Etherscan indicate?
A) Token is safe B) Source code matches bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification proves source matches deployed contract.

Q2. High centralization risk indicator?
A) Supply over 1B B) Top 10 holders own 80% C) 18 decimals D) Listed on exchanges
Answer: B – High concentration = manipulation risk.

Q3. Major red flag in token contract?
A) SafeMath library B) Owner can mint unlimited C) Transfer events D) ERC-20 standard
Answer: B – Unlimited minting allows supply inflation.

Q4. Where to find holder distribution on Etherscan?
A) Read Contract B) Transactions C) Holders tab D) Analytics
Answer: C – Holders tab shows top holders and percentages.

Q5. What does "decimals" parameter specify?
A) Price precision B) Divisible units C) Max supply D) Fee percentage
Answer: B – Decimals defines smallest unit divisibility.

Quiz (2/2)

Q6. Best tool for comparing DeFi protocol metrics?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub

Quiz (2/2)

Q6. Best tool for comparing DeFi protocol metrics?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across protocols.

Q7. Why check if team tokens are vesting?
A) Cannot dump immediately B) Calculate market cap C) Verify deployment D) Check gas costs

Quiz (2/2)

Q6. Best tool for comparing DeFi protocol metrics?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across protocols.

Q7. Why check if team tokens are vesting?
A) Cannot dump immediately B) Calculate market cap C) Verify deployment D) Check gas costs
Answer: A – Vesting prevents team from selling all at once.

Q8. What is a proxy pattern?
A) Hidden fees B) Upgradeable contract architecture C) Immutable contract D) NFT standard

Quiz (2/2)

Q6. Best tool for comparing DeFi protocol metrics?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across protocols.

Q7. Why check if team tokens are vesting?
A) Cannot dump immediately B) Calculate market cap C) Verify deployment D) Check gas costs
Answer: A – Vesting prevents team from selling all at once.

Q8. What is a proxy pattern?
A) Hidden fees B) Upgradeable contract architecture C) Immutable contract D) NFT standard
Answer: B – Proxy allows upgrading contract logic.

Q9. Issue with blacklist functionality?
A) Improves security B) Owner can freeze addresses without governance C) Required by ERC-20 D) Reduces gas

Quiz (2/2)

Q6. Best tool for comparing DeFi protocol metrics?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across protocols.

Q7. Why check if team tokens are vesting?
A) Cannot dump immediately B) Calculate market cap C) Verify deployment D) Check gas costs
Answer: A – Vesting prevents team from selling all at once.

Q8. What is a proxy pattern?
A) Hidden fees B) Upgradeable contract architecture C) Immutable contract D) NFT standard
Answer: B – Proxy allows upgrading contract logic.

Q9. Issue with blacklist functionality?
A) Improves security B) Owner can freeze addresses without governance C) Required by ERC-20 D) Reduces gas
Answer: B – Centralized power to freeze funds.

Q10. Before adding token to wallet, verify?
A) Check logo only B) Contract address matches official source C) Search by name D) Trust any listing

Quiz (2/2)

Q6. Best tool for comparing DeFi protocol metrics?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across protocols.

Q7. Why check if team tokens are vesting?
A) Cannot dump immediately B) Calculate market cap C) Verify deployment D) Check gas costs
Answer: A – Vesting prevents team from selling all at once.

Q8. What is a proxy pattern?
A) Hidden fees B) Upgradeable contract architecture C) Immutable contract D) NFT standard
Answer: B – Proxy allows upgrading contract logic.

Q9. Issue with blacklist functionality?
A) Improves security B) Owner can freeze addresses without governance C) Required by ERC-20 D) Reduces gas
Answer: B – Centralized power to freeze funds.

Q10. Before adding token to wallet, verify?
A) Check logo only B) Contract address matches official source C) Search by name D) Trust any listing
Answer: B – Scam tokens use similar names; verify exact address.

Thank you

Questions?

Next: L21 – NFT Technology Deep Dive

Quiz: Lab Token Analysis

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe to invest in B) Source code matches deployed bytecode C) Cannot be hacked D) Owner is trustworthy

Quiz (1–5)

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe to invest in B) Source code matches deployed bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification only proves source matches bytecode, not safety.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% C) Contract has 18 decimals D) Token listed on exchanges

Quiz (1–5)

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe to invest in B) Source code matches deployed bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification only proves source matches bytecode, not safety.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% C) Contract has 18 decimals D) Token listed on exchanges
Answer: B – High concentration in few wallets indicates centralization risk.

Q3. What is a major red flag in token contract code?
A) Using SafeMath library B) Owner can mint unlimited tokens C) Emitting Transfer events D) Implementing ERC-20 standard

Quiz (1–5)

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe to invest in B) Source code matches deployed bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification only proves source matches bytecode, not safety.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% C) Contract has 18 decimals D) Token listed on exchanges
Answer: B – High concentration in few wallets indicates centralization risk.

Q3. What is a major red flag in token contract code?
A) Using SafeMath library B) Owner can mint unlimited tokens C) Emitting Transfer events D) Implementing ERC-20 standard
Answer: B – Unlimited minting power allows owner to inflate supply.

Q4. What does the decimals parameter specify in ERC-20?
A) Token price precision B) Number of divisible units C) Maximum supply D) Transfer fee percentage

Quiz (1–5)

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe to invest in B) Source code matches deployed bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification only proves source matches bytecode, not safety.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% C) Contract has 18 decimals D) Token listed on exchanges
Answer: B – High concentration in few wallets indicates centralization risk.

Q3. What is a major red flag in token contract code?
A) Using SafeMath library B) Owner can mint unlimited tokens C) Emitting Transfer events D) Implementing ERC-20 standard
Answer: B – Unlimited minting power allows owner to inflate supply.

Q4. What does the decimals parameter specify in ERC-20?
A) Token price precision B) Number of divisible units C) Maximum supply D) Transfer fee percentage
Answer: B – Decimals defines smallest unit (18 = wei-like precision).

Q5. Why check if team tokens are vesting?
A) Prevent immediate dump B) Calculate market cap C) Verify contract deployment D) Check gas costs

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What does a verified contract on Etherscan indicate?
A) Token is safe to invest in B) Source code matches deployed bytecode C) Cannot be hacked D) Owner is trustworthy
Answer: B – Verification only proves source matches bytecode, not safety.

Q2. Which metric indicates high centralization risk?
A) Total supply over 1 billion B) Top 10 holders own 80% C) Contract has 18 decimals D) Token listed on exchanges
Answer: B – High concentration in few wallets indicates centralization risk.

Q3. What is a major red flag in token contract code?
A) Using SafeMath library B) Owner can mint unlimited tokens C) Emitting Transfer events D) Implementing ERC-20 standard
Answer: B – Unlimited minting power allows owner to inflate supply.

Q4. What does the decimals parameter specify in ERC-20?
A) Token price precision B) Number of divisible units C) Maximum supply D) Transfer fee percentage
Answer: B – Decimals defines smallest unit (18 = wei-like precision).

Q5. Why check if team tokens are vesting?
A) Prevent immediate dump B) Calculate market cap C) Verify contract deployment D) Check gas costs
Answer: A – Vesting prevents team from selling all tokens at once.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which tool is best for comparing DeFi protocol TVL?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub

Quiz (6–10)

Q6. Which tool is best for comparing DeFi protocol TVL?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across all DeFi protocols.

Q7. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in exchange pool C) Owner controls everything D) Token cannot be traded

Quiz (6–10)

Q6. Which tool is best for comparing DeFi protocol TVL?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across all DeFi protocols.

Q7. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in exchange pool C) Owner controls everything D) Token cannot be traded
Answer: B – DEX contracts holding tokens indicates liquidity pools.

Q8. What is a proxy pattern in smart contracts?
A) Token with hidden fees B) Upgradeable contract architecture C) Contract that cannot be changed D) Token standard for NFTs

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which tool is best for comparing DeFi protocol TVL?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across all DeFi protocols.

Q7. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in exchange pool C) Owner controls everything D) Token cannot be traded
Answer: B – DEX contracts holding tokens indicates liquidity pools.

Q8. What is a proxy pattern in smart contracts?
A) Token with hidden fees B) Upgradeable contract architecture C) Contract that cannot be changed D) Token standard for NFTs
Answer: B – Proxy pattern allows upgrading contract logic post-deployment.

Q9. What is concentration ratio in holder analysis?
A) Number of exchanges listing token B) Percentage owned by top N holders C) Total supply divided by decimals D) Average transaction size

Quiz (6–10)

Q6. Which tool is best for comparing DeFi protocol TVL?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across all DeFi protocols.

Q7. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in exchange pool C) Owner controls everything D) Token cannot be traded
Answer: B – DEX contracts holding tokens indicates liquidity pools.

Q8. What is a proxy pattern in smart contracts?
A) Token with hidden fees B) Upgradeable contract architecture C) Contract that cannot be changed D) Token standard for NFTs
Answer: B – Proxy pattern allows upgrading contract logic post-deployment.

Q9. What is concentration ratio in holder analysis?
A) Number of exchanges listing token B) Percentage owned by top N holders C) Total supply divided by decimals D) Average transaction size
Answer: B – Measures how much supply top holders control.

Q10. What should you verify before adding a token to your wallet?
A) Only check if it has a logo B) Verify contract address matches official source C) Just search by name
D) Trust any Etherscan listing

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which tool is best for comparing DeFi protocol TVL?
A) Etherscan only B) CoinGecko only C) DeFiLlama D) GitHub
Answer: C – DeFiLlama aggregates TVL across all DeFi protocols.

Q7. What does it mean if top holder is a DEX contract?
A) Token is a scam B) Liquidity locked in exchange pool C) Owner controls everything D) Token cannot be traded
Answer: B – DEX contracts holding tokens indicates liquidity pools.

Q8. What is a proxy pattern in smart contracts?
A) Token with hidden fees B) Upgradeable contract architecture C) Contract that cannot be changed D) Token standard for NFTs
Answer: B – Proxy pattern allows upgrading contract logic post-deployment.

Q9. What is concentration ratio in holder analysis?
A) Number of exchanges listing token B) Percentage owned by top N holders C) Total supply divided by decimals D) Average transaction size
Answer: B – Measures how much supply top holders control.

Q10. What should you verify before adding a token to your wallet?
A) Only check if it has a logo B) Verify contract address matches official source C) Just search by name D) Trust any Etherscan listing
Answer: B – Scam tokens use similar names; verify exact contract address.

(c) Joerg Osterrieder 2025

L21: NFT Technology Deep Dive

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Describe the complete NFT technology stack from blockchain to application layer
- Implement and compare different tokenURI patterns for metadata management
- Analyze minting strategies and their gas cost implications
- Apply gas optimization techniques including ERC-721A and lazy minting
- Evaluate NFT market metrics and adoption trends
- Identify common NFT security vulnerabilities and best practices

The Problem: What makes digital art scarce?

The Challenge
Digital files can be copied infinitely at zero cost. How can digital art or collectibles have scarcity when anyone can make a perfect copy by right-clicking and saving?

Why It Matters

- Digital creators had no way to monetize scarcity or prove authenticity before NFTs
- Beeple sold a JPEG for $69M (2021) – impossible without proof of uniqueness
- CryptoPunks, Art Blocks, and other early projects demonstrated demand for verifiable digital ownership

What We Need

- Value creation and capture
- Verifiable proof of authenticity and ownership recorded on-chain
- Immutable provenance tracking (who owned it, when, for how much)

The Cryptoeconomics Question
Creating and distributing economic value

Today's lesson: How NFT Technology addresses this challenge

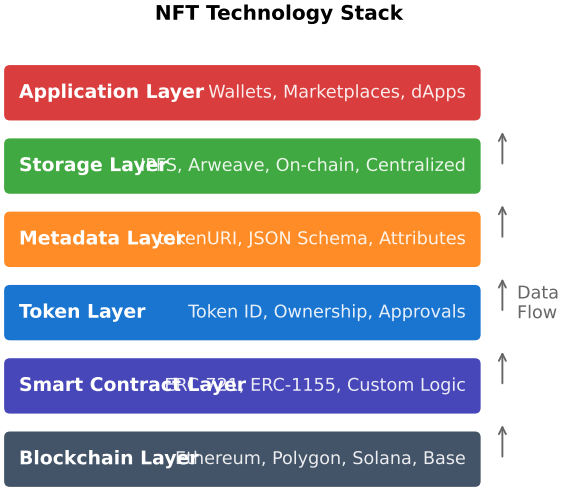
NFT Technology Stack Overview

Six-Layer Architecture:

1. **Blockchain Layer:** Ethereum, Polygon, Solana, Base
2. **Smart Contract Layer:** ERC-721, ERC-1155, custom logic
3. **Token Layer:** Token IDs, ownership mapping, approvals
4. **Metadata Layer:** tokenURI, JSON schema, attributes
5. **Storage Layer:** IPFS, Arweave, on-chain, centralized
6. **Application Layer:** Wallets, marketplaces, dApps

Key Insight: Each layer has tradeoffs between decentralization, cost, and flexibility

NFT Architecture Layers



Data flows upward; each layer adds functionality

TokenURI: The Metadata Gateway

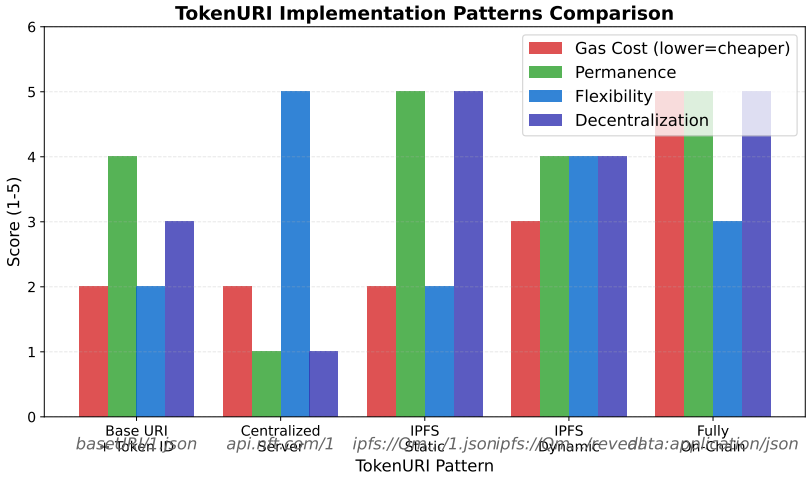
Core Function: Maps token ID to metadata location

```
// ERC-721 Metadata Extension
function tokenURI(uint256 tokenId) public view returns (string memory) {
    require(_exists(tokenId), "Token does not exist");

    string memory baseURI = _baseURI();
    return bytes(baseURI).length > 0
        ? string(abi.encodePacked(baseURI, tokenId.toString(), ".json"))
        : "";
}
```

Common Patterns:

- **Base URI + Token ID:** `ipfs://Qm.../{id}.json`
- **Centralized API:** `https://api.project.com/token/{id}`
- **Fully On-Chain:** `data:application/json; base64,...`

TokenURI Implementation Patterns



IPFS static offers best balance of cost, permanence, and decentralization

On-Chain Metadata: Fully Decentralized

Advantage: No external dependencies, truly permanent

```
function tokenURI(uint256 tokenId) public view returns (string memory) {
    string memory json = Base64.encode(bytes(string(abi.encodePacked(
        '{"name": "NFT #', tokenId.toString(),
        '", "description": "Fully on-chain NFT",
        '", "image": "', generateSVG(tokenId), '"}'
    ))));
    return string(abi.encodePacked("data:application/json; base64,", json));
}
```

Examples:

- **Loot:** Text-based adventure gear stored on-chain
- **Nouns:** Daily auctions with on-chain SVG artwork
- **Autoglyphs:** Generative art, code and output on-chain

Cost: 640,000+ gas per KB (expensive but permanent)

Ownership and Transfer Mechanics

Core State Variables:

- `_owners[tokenId] => address`: Maps each token to owner
- `_balances[owner] => uint256`: Tracks balance per address
- `_tokenApprovals[tokenId] => address`: Single-token approval
- `_operatorApprovals[owner][operator] => bool`: Operator approval

Transfer Flow:

1. Verify caller is owner, approved, or operator
2. Clear existing token approvals
3. Update `_owners` mapping
4. Update `_balances` for sender and recipient
5. Emit `Transfer` event
6. (Safe transfer) Check recipient can receive NFTs

Gas Cost: Approximately 65,000 gas per transfer

Minting Strategies Overview

Common Approaches:

Standard Mint:

- One transaction per NFT
- Creator pays gas
- Simple implementation
- Cost: 90K gas each

Batch Mint (ERC-721A):

- Multiple NFTs per transaction
- 80% gas savings
- Deferred ownership updates
- Azuki's innovation (2022)

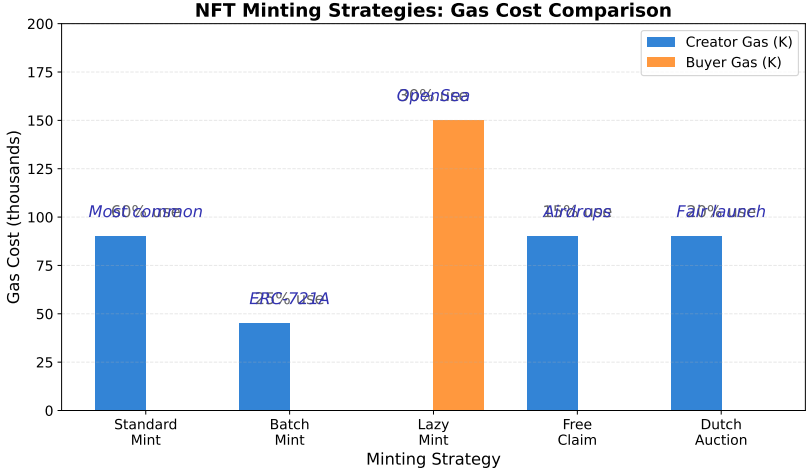
Lazy Mint:

- Creator signs voucher off-chain
- Buyer pays mint gas on purchase
- Zero upfront creator cost
- OpenSea, Rarible support

Dutch Auction:

- Price starts high, decreases
- Fair price discovery
- Reduces gas wars
- Paradigm popularized (2021)

Minting Strategies: Gas Comparison



Lazy minting shifts gas cost to buyer; ERC-721A batch minting saves 80% on bulk mints

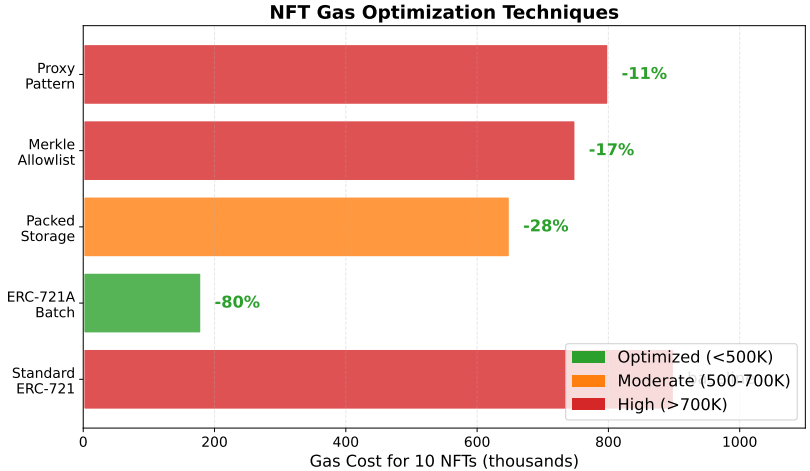
ERC-721A: Batch Optimization

Key Innovation: Deferred ownership updates

```
// Standard ERC-721: Updates storage for EACH token
function _mint(address to, uint256 tokenId) internal {
    _balances[to] += 1;              // SSTORE (20,000 gas)
    _owners[tokenId] = to;           // SSTORE (20,000 gas)
    emit Transfer(address(0), to, tokenId);
}

// ERC-721A: Single update for batch
function _mintBatch(address to, uint256 quantity) internal {
    _balances[to] += quantity;       // One SSTORE
    _owners[startTokenId] = to;      // One SSTORE (others inferred)
    // Emit events...
}
```

Trade-off: First transfer of token in batch costs extra gas (must write ownership)

Gas Optimization Techniques



ERC-721A provides 80% savings for batch mints; packed storage saves 28% for metadata

Additional Gas Optimizations

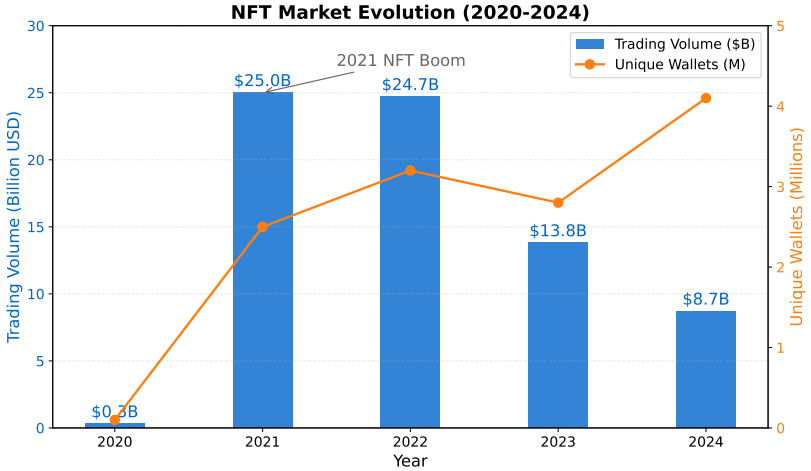
1. **Packed Storage:**
   - Store multiple values in single 256-bit slot
   - Example: Owner (160 bits) + aux data (96 bits)
   - Saves cold SLOAD costs on reads

2. **Merkle Allowlist:**
   - Store Merkle root instead of full allowlist
   - Verify membership via proof (log n hashes)
   - Saves 50% vs storing addresses on-chain

3. **Minimal Proxy Pattern (EIP-1167):**
   - Deploy lightweight clones of master contract
   - Reduces deployment cost by 90%
   - OpenSea Seaport uses this pattern

4. **Unchecked Math:**
   - Skip overflow checks where safe (Solidity 0.8+)
   - Saves 50-100 gas per operation

NFT Market Overview



Source: DappRadar, NonFungible.com. 2021 boom driven by PFPs and speculation

Market Evolution: 2020-2024

Key Milestones:

- **2020:** DeFi summer, early NFT experiments ($300M volume)
- **2021:** Beeple $69M sale, BAYC launch, $25B peak volume
- **2022:** Blur launches, royalty wars begin, volume steady
- **2023:** Market correction, focus on utility NFTs
- **2024:** Bitcoin Ordinals, gaming NFTs, RWA tokenization

Current Landscape (Dec 2024):

- OpenSea: $300M monthly volume, 2.5% fee
- Blur: $400M monthly volume, 0% fee (token incentives)
- Magic Eden: Multi-chain (Solana, Bitcoin, Ethereum)
- 4.1M unique active wallets interacting with NFTs

(c) Joerg Osterrieder 2025

NFT Security Vulnerabilities

Common Attack Vectors:

1. **Reentrancy in Minting:**
   - Attack: Callback during mint to re-enter and mint more
   - Defense: Use checks-effects-interactions, ReentrancyGuard
2. **Signature Replay:**
   - Attack: Reuse signed voucher for multiple mints
   - Defense: Include nonce, track used signatures
3. **Unlimited Approval Exploits:**
   - Attack: Malicious contract drains approved NFTs
   - Defense: Approve specific tokens, revoke unused approvals
4. **Metadata Manipulation:**
   - Attack: Owner changes tokenURI to different artwork
   - Defense: Use immutable metadata, renounce ownership

Security Best Practices

For Developers:

- Use OpenZeppelin audited contracts as base
- Implement `nonReentrant` modifier on mint functions
- Include signature expiry and nonce in signed messages
- Freeze metadata after reveal (remove `setTokenURI`)
- Use Merkle proofs for allowlists (gas + security)

For Users:

- Verify contract is verified on Etherscan
- Check for `setTokenURI` or owner functions
- Use hardware wallets for high-value NFTs
- Revoke approvals after marketplace interactions
- Verify IPFS/Arweave storage (not centralized servers)

Resources: OpenZeppelin Defender, Slither, Mythril for automated analysis

Problem Solved? NFT Technology

The Original Problem

What makes digital art scarce?

How NFT Technology Solves It

- Token ID uniquely identifies each NFT – only one owner can hold tokenId 1 at any time
- Blockchain provides immutable ownership history (provenance) that cannot be altered
- Smart contracts enforce scarcity by limiting total supply (e.g., 10,000 NFTs max)

Remaining Limitations

- The artwork itself usually isn't on-chain (IPFS or centralized servers host images)
- Metadata can be changed by contract owner if not frozen (mutable tokenURI)
- Scarcity is enforced by code trust, not physical impossibility

Open Questions

- Is provenance and social consensus enough to create lasting value?
- What happens when IPFS pinning services shut down or contract owners manipulate metadata?
- Risk: Extractive tokenomics, unsustainable yields

NFT Technology partially solves "What makes digital art scarce" but introduces new trade-offs

(c) Joerg Osterrieder 2025

NFT Enumeration: ERC-721Enumerable

Optional Extension: Enables token enumeration

Additional Functions:

- `totalSupply()`: Total tokens minted
- `tokenByIndex(index)`: Get token ID at global index
- `tokenOfOwnerByIndex(owner, index)`: Get owner's nth token

Gas Considerations:

- Adds 50% gas overhead to transfers (extra storage updates)
- Maintains arrays for enumeration (expensive writes)
- Alternative: Off-chain indexing via The Graph or events

When to Use:

- Small collections (¡1000 tokens) where on-chain queries needed
- Avoid for large collections (use event-based indexing instead)

Key Takeaways

1. NFTs operate across a six-layer technology stack from blockchain to application
2. TokenURI patterns range from centralized APIs to fully on-chain data
3. ERC-721A batch minting saves up to 80% gas for multiple mints
4. Lazy minting shifts gas costs from creator to buyer (zero upfront cost)
5. NFT market peaked at $25B in 2021, now stabilized around $8-10B annually
6. Security requires attention to reentrancy, signature replay, and metadata immutability
7. Enumerable extension adds functionality but increases gas costs significantly

(c) Joerg Osterrieder 2025

Discussion Questions

1. When is fully on-chain metadata worth the gas cost premium?
2. How should projects balance gas optimization with code simplicity?
3. What role will Layer 2 solutions play in NFT gas economics?
4. Is lazy minting fair to buyers who pay higher gas than batch minters?
5. How can the industry address metadata permanence without centralization?

Next Lesson Preview

L22: NFT Metadata and IPFS

We will explore:

- JSON metadata format standards (OpenSea schema)
- IPFS content addressing and CID structure
- Pinning services and availability guarantees
- Arweave permanent storage economics
- Metadata permanence challenges and solutions

Preparation: Explore IPFS by uploading a file to Pinata (free tier)

Quiz Questions (1–5)

Q1. How many layers comprise the complete NFT technology stack?
A) 3 B) 4 C) 5 D) 6
Answer: D – The six layers are: Blockchain, Smart Contract, Token, Metadata, Storage, and Application.

Q2. What does the tokenURI function return?
A) Token owner address B) Token price C) URI pointing to metadata D) Token approval status
Answer: C – tokenURI returns a URI (IPFS, HTTP, or data URI) pointing to the token's metadata JSON.

Q3. Which tokenURI pattern offers the best decentralization and permanence?
A) Centralized server B) IPFS static C) Base URI pattern D) Dynamic API
Answer: B – IPFS static provides content-addressed, decentralized, and immutable storage.

Q4. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – On-chain storage costs 20,000 gas per 32 bytes, so 1 KB = 640,000 gas.

Q5. Which mapping tracks individual token ownership in ERC-721?
A) _balances B) _owners C) _tokenApprovals D) _operatorApprovals
Answer: B – _owners[tokenId] maps each token ID to its current owner address.

Quiz Questions (6–10)

Q6. How much gas does a standard ERC-721 transfer cost?
A) 21,000 gas B) 45,000 gas C) 65,000 gas D) 90,000 gas
Answer: C – A standard ERC-721 transfer costs approximately 65,000 gas.

Q7. What is the key innovation of ERC-721A?
A) On-chain metadata B) Deferred ownership updates C) Royalty enforcement D) Cross-chain transfers
Answer: B – ERC-721A defers ownership updates, writing only the first token in a batch to save gas.

Q8. How much gas can ERC-721A save on batch minting?
A) 20% B) 40% C) 60% D) 80%
Answer: D – ERC-721A provides up to 80% gas savings for batch minting operations.

Q9. In lazy minting, who pays the minting gas cost?
A) Creator B) Buyer C) Marketplace D) No one (gasless)
Answer: B – Lazy minting defers gas to the buyer who mints on first purchase.

Q10. What was the peak NFT trading volume year?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: B – 2021 saw peak NFT volume of approximately $25 billion.

Quiz Questions (11–15)

Q11. Which project pioneered ERC-721A batch optimization?
A) Bored Ape Yacht Club B) CryptoPunks C) Azuki D) Nouns
Answer: C – Azuki introduced ERC-721A in 2022 for gas-optimized batch minting.

Q12. What is a Dutch auction in NFT minting?
A) Fixed price sale B) Price starts high and decreases C) Sealed bid auction D) Free mint with gas only
Answer: B – Dutch auctions start at a high price that decreases until someone buys.

Q13. What security vulnerability involves re-entering during minting?
A) Signature replay B) Reentrancy attack C) Front-running D) Overflow attack
Answer: B – Reentrancy attacks exploit callbacks to re-enter mint functions for extra tokens.

Q14. How can signature replay attacks be prevented?
A) Use reentrancy guards B) Include nonce in signed message C) Freeze metadata D) Use IPFS storage
Answer: B – Including a nonce and tracking used signatures prevents replay attacks.

Q15. What does the ERC-721Enumerable extension add?
A) Royalty support B) Token enumeration functions C) Batch transfers D) Metadata standards
Answer: B – Enumerable adds totalSupply(), tokenByIndex(), and tokenOfOwnerByIndex() functions.

Quiz Questions (16–20)

Q16. What is the gas overhead of ERC-721Enumerable on transfers?
A) 10% B) 25% C) 50% D) 100%
Answer: C – Enumerable adds approximately 50% gas overhead to maintain enumeration arrays.

Q17. What is packed storage in NFT contracts?
A) Compressing IPFS files B) Storing multiple values in one 256-bit slot C) Batch transferring tokens D) Off-chain metadata
Answer: B – Packed storage fits multiple values (e.g., owner + aux data) in a single storage slot.

Q18. How much can Merkle allowlists save compared to on-chain address storage?
A) 10% B) 25% C) 50% D) 75%
Answer: C – Merkle proofs save approximately 50% by storing only the root hash on-chain.

Q19. Which NFT project stores artwork fully on-chain as SVG?
A) Bored Ape Yacht Club B) Nouns C) CryptoPunks D) Azuki
Answer: B – Nouns generates and stores SVG artwork entirely on-chain.

Q20. What is the recommended alternative to Enumerable for large collections?
A) More gas B) Fewer tokens C) Event-based indexing (The Graph) D) Centralized database
Answer: C – The Graph or event-based indexing provides enumeration without on-chain gas overhead.

L21: NFT Technology Deep Dive

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Why pay for a JPEG?

[COMIC: placeholder]

A skeptic right-clicking to save a $500k NFT image, smugly saying "I own it now too!" while the actual owner's wallet shows provenance, royalties, and community access the skeptic will never have.

The Real Question

- Anyone can copy the image file
- But only one wallet holds the token
- Ownership = provenance + access + status

What We'll Explore

- How NFT technology creates scarcity
- The 6-layer stack from blockchain to app
- Why tokenURI matters for authenticity

The image is just the surface—the token is the ownership layer

Learning Objectives

By the end of this lesson, you will be able to:

- Describe the complete NFT technology stack from blockchain to application layer
- Implement and compare different tokenURI patterns for metadata management
- Analyze minting strategies and their gas cost implications
- Apply gas optimization techniques including ERC-721A and lazy minting
- Evaluate NFT market metrics and adoption trends
- Identify common NFT security vulnerabilities and best practices

Building on L20: Lab: Token Analysis

The Problem: What makes digital art scarce?

The Challenge
Digital files can be copied infinitely at zero cost. How can digital art or collectibles have scarcity when anyone can make a perfect copy by right-clicking and saving?

Why It Matters

- Digital creators had no way to monetize scarcity or prove authenticity before NFTs
- Beeple sold a JPEG for $69M (2021) – impossible without proof of uniqueness
- CryptoPunks, Art Blocks, and other early projects demonstrated demand for verifiable digital ownership

What We Need

- Value creation and capture
- Verifiable proof of authenticity and ownership recorded on-chain
- Immutable provenance tracking (who owned it, when, for how much)

The Cryptoeconomics Question
Creating and distributing economic value

Today's lesson: How NFT Technology addresses this challenge

How Do NFTs Actually Work?

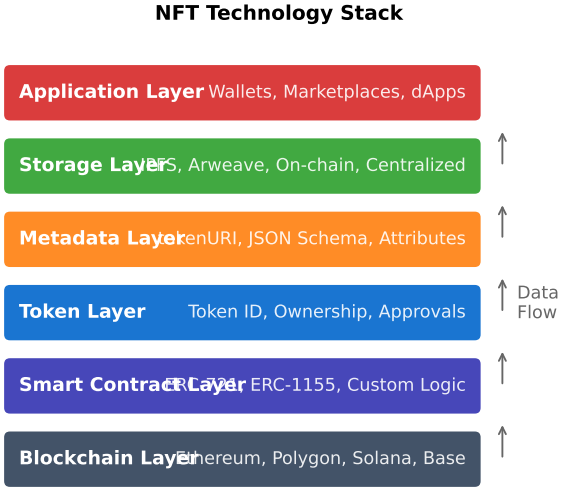
Six-Layer Architecture:

1. **Blockchain Layer:** Ethereum, Polygon, Solana, Base
2. **Smart Contract Layer:** ERC-721, ERC-1155, custom logic
3. **Token Layer:** Token IDs, ownership mapping, approvals
4. **Metadata Layer:** tokenURI, JSON schema, attributes
5. **Storage Layer:** IPFS, Arweave, on-chain, centralized
6. **Application Layer:** Wallets, marketplaces, dApps

Key Insight: Each layer has tradeoffs between decentralization, cost, and flexibility

Problem: What makes digital art scarce? — The 6-layer stack creates scarcity: blockchain ensures only one owner per tokenId, smart contracts enforce supply limits, metadata links to the actual artwork

How Does NFT Architecture Layer Up?



Data flows upward; each layer adds functionality

What is TokenURI and Why Does It Matter?

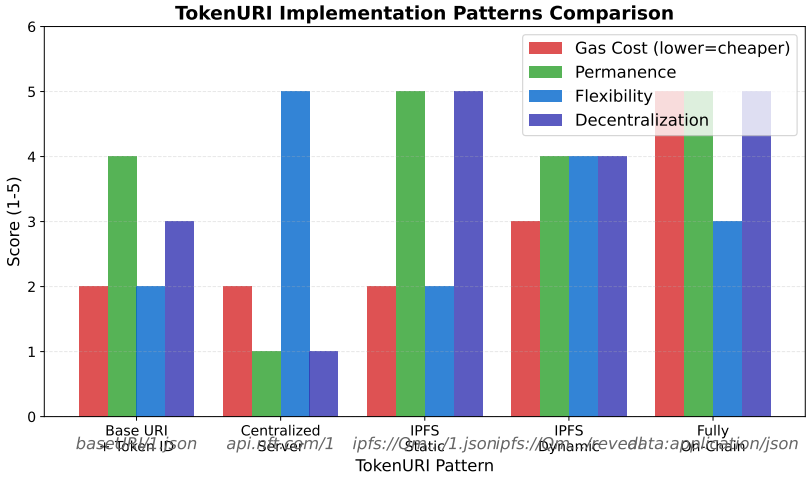
Core Function: Maps token ID to metadata location

```
// ERC-721 Metadata Extension
function tokenURI(uint256 tokenId) public view returns (string memory) {
    require(_exists(tokenId), "Token does not exist");

    string memory baseURI = _baseURI();
    return bytes(baseURI).length > 0
        ? string(abi.encodePacked(baseURI, tokenId.toString(), ".json"))
        : "";
}
```

Common Patterns:

- **Base URI + Token ID:** `ipfs://Qm.../{id}.json`
- **Centralized API:** `https://api.project.com/token/{id}`
- **Fully On-Chain:** `data:application/json; base64,...`

How Can TokenURIs Be Implemented?



Problem: What makes digital art scarce? — tokenURI links the scarce token (on blockchain) to its artwork (off-chain); IPFS ensures the artwork cannot be swapped without changing the URL

How Does Fully On-Chain Metadata Work?

Advantage: No external dependencies, truly permanent

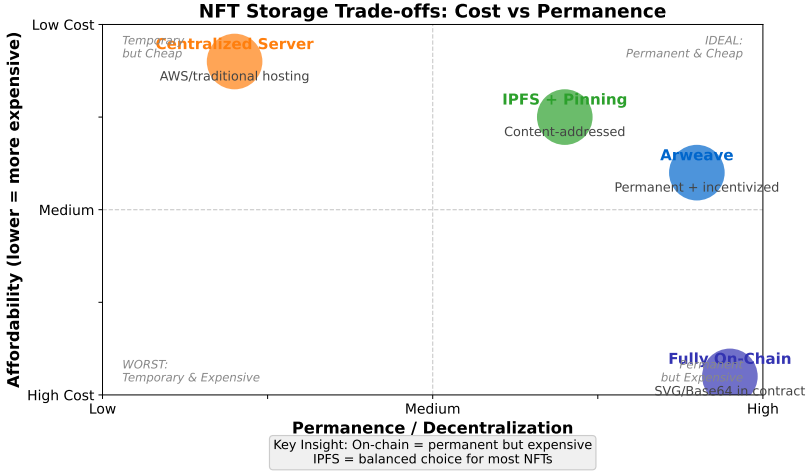
```
function tokenURI(uint256 tokenId) public view returns (string memory) {
    string memory json = Base64.encode(bytes(string(abi.encodePacked(
        '{"name": "NFT #', tokenId.toString(),
        '", "description": "Fully on-chain NFT",
        '", "image": "', generateSVG(tokenId), '"}'
    ))));
    return string(abi.encodePacked("data:application/json; base64,", json));
}
```

Examples:

- **Loot:** Text-based adventure gear stored on-chain
- **Nouns:** Daily auctions with on-chain SVG artwork
- **Autoglyphs:** Generative art, code and output on-chain

Cost: 640,000+ gas per KB (expensive but permanent)

How Do Storage Options Compare?



Each storage option represents a different trade-off between cost, permanence, and decentralization

How Do NFT Transfers Work?

Core State Variables:

- `_owners[tokenId] => address`: Maps each token to owner
- `_balances[owner] => uint256`: Tracks balance per address
- `_tokenApprovals[tokenId] => address`: Single-token approval
- `_operatorApprovals[owner][operator] => bool`: Operator approval

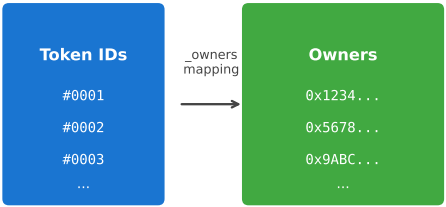
Transfer Flow:

1. Verify caller is owner, approved, or operator
2. Clear existing token approvals
3. Update `_owners` mapping
4. Update `_balances` for sender and recipient
5. Emit `Transfer` event
6. (Safe transfer) Check recipient can receive NFTs

Gas Cost: Approximately 65,000 gas per transfer

How Does NFT Provenance Build On-Chain?

NFT Ownership Mechanics: Mapping & Provenance



Provenance

(Transfer Events)

Minted

`0x0000 -> 0x1234`

Transfer

`0x1234 -> 0x5678`

Transfer

`0x5678 -> 0x9ABC`

Current

`Owner: 0x9ABC`

Token IDs map to owners; transfer events create immutable provenance trail

What Minting Strategies Exist for NFTs?

Common Approaches:

Standard Mint:

- One transaction per NFT
- Creator pays gas
- Simple implementation
- Cost: 90K gas each

Batch Mint (ERC-721A):

- Multiple NFTs per transaction
- 80% gas savings
- Deferred ownership updates
- Azuki's innovation (2022)

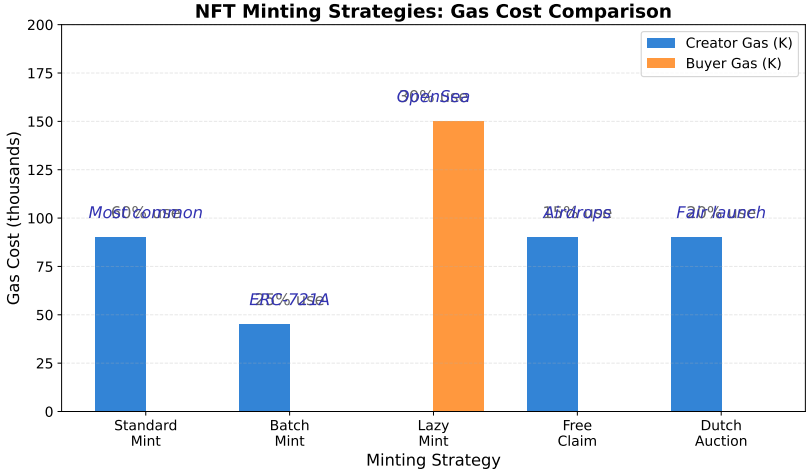
Lazy Mint:

- Creator signs voucher off-chain
- Buyer pays mint gas on purchase
- Zero upfront creator cost
- OpenSea, Rarible support

Dutch Auction:

- Price starts high, decreases
- Fair price discovery
- Reduces gas wars
- Paradigm popularized (2021)

How Do Minting Strategies Compare by Gas Cost?



Problem: What makes digital art scarce? — Minting creates new NFTs; different strategies affect who pays gas and how efficiently, but all enforce the same scarcity via MAX_SUPPLY limits

Problem Check-In: NFT Technology

Recall Our Problem

What makes digital art scarce?

What We've Learned So Far

- The 6-layer NFT stack: blockchain provides immutability, smart contracts enforce rules, tokenURI links to artwork
- tokenURI patterns range from centralized servers (risky) to fully on-chain data (expensive but permanent)
- Scarcity comes from the blockchain token (unique tokenId), not the image file which anyone can copy

Still to Address

- Gas optimization techniques (ERC-721A), market metrics, and security vulnerabilities
- If anyone can copy the image, what exactly makes an NFT valuable? (Answer: provable provenance and ownership)

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "What makes digital art scarce?"?

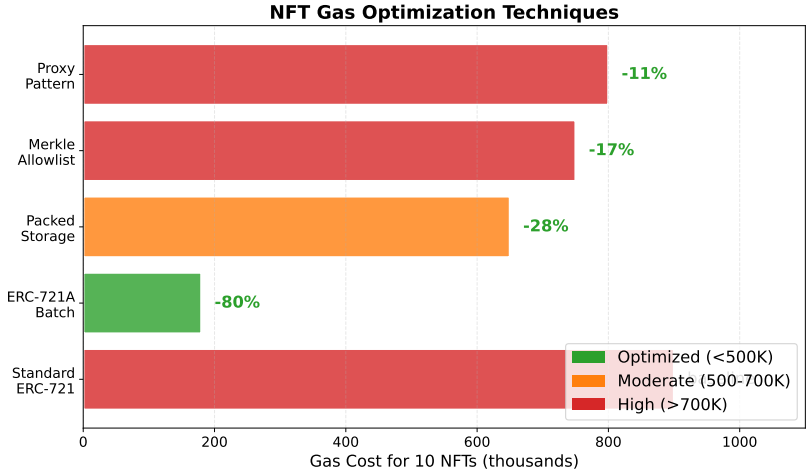
How Does ERC-721A Optimize Batch Minting?

Key Innovation: Deferred ownership updates

```
// Standard ERC-721: Updates storage for EACH token
function _mint(address to, uint256 tokenId) internal {
    _balances[to] += 1;              // SSTORE (20,000 gas)
    _owners[tokenId] = to;           // SSTORE (20,000 gas)
    emit Transfer(address(0), to, tokenId);
}

// ERC-721A: Single update for batch
function _mintBatch(address to, uint256 quantity) internal {
    _balances[to] += quantity;       // One SSTORE
    _owners[startTokenId] = to;      // One SSTORE (others inferred)
    // Emit events...
}
```

Trade-off: First transfer of token in batch costs extra gas (must write ownership)

How Much Gas Can Optimization Techniques Save?

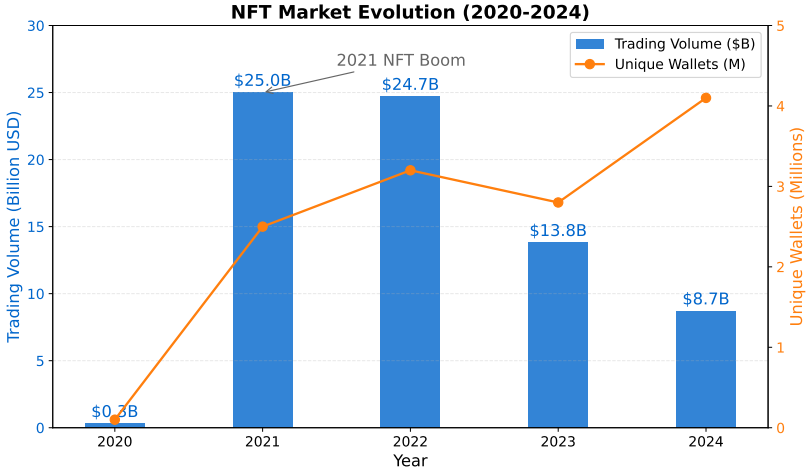


ERC-721A provides 80% savings for batch mints; packed storage saves 28% for metadata

What Other Gas Optimizations Are Available?

1. **Packed Storage:**
   - Store multiple values in single 256-bit slot
   - Example: Owner (160 bits) + aux data (96 bits)
   - Saves cold SLOAD costs on reads
2. **Merkle Allowlist:**
   - Store Merkle root instead of full allowlist
   - Verify membership via proof (log n hashes)
   - Saves 50% vs storing addresses on-chain
3. **Minimal Proxy Pattern (EIP-1167):**
   - Deploy lightweight clones of master contract
   - Reduces deployment cost by 90%
   - OpenSea Seaport uses this pattern
4. **Unchecked Math:**
   - Skip overflow checks where safe (Solidity 0.8+)
   - Saves 50-100 gas per operation

How Big is the NFT Market?



Problem: What makes digital art scarce? — Market size shows demand for digital scarcity; high prices prove buyers value provable uniqueness even for copyable images (Beeple's $69M JPEG)

How Has the NFT Market Evolved?

Key Milestones:

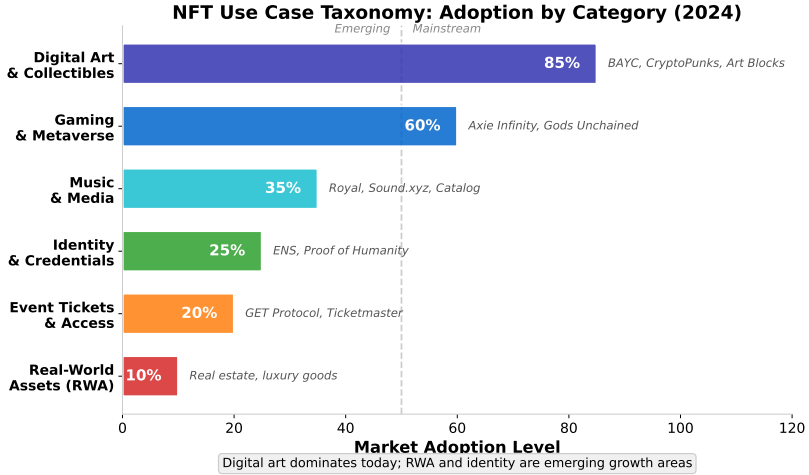
- **2020:** DeFi summer, early NFT experiments ($300M volume)
- **2021:** Beeple $69M sale, BAYC launch, $25B peak volume
- **2022:** Blur launches, royalty wars begin, volume steady
- **2023:** Market correction, focus on utility NFTs
- **2024:** Bitcoin Ordinals, gaming NFTs, RWA tokenization

Current Landscape (Dec 2024):

- OpenSea: $300M monthly volume, 2.5% fee
- Blur: $400M monthly volume, 0% fee (token incentives)
- Magic Eden: Multi-chain (Solana, Bitcoin, Ethereum)
- 4.1M unique active wallets interacting with NFTs

(c) Joerg Osterrieder 2025

Which NFT Use Cases Are Most Popular?



Digital art dominates; RWA and identity are emerging growth areas with high potential

What Are the Main NFT Security Risks?

Common Attack Vectors:

1. **Reentrancy in Minting:**
   - Attack: Callback during mint to re-enter and mint more
   - Defense: Use checks-effects-interactions, ReentrancyGuard
2. **Signature Replay:**
   - Attack: Reuse signed voucher for multiple mints
   - Defense: Include nonce, track used signatures
3. **Unlimited Approval Exploits:**
   - Attack: Malicious contract drains approved NFTs
   - Defense: Approve specific tokens, revoke unused approvals
4. **Metadata Manipulation:**
   - Attack: Owner changes tokenURI to different artwork
   - Defense: Use immutable metadata, renounce ownership

How Can NFTs Be Secured?

For Developers:

- Use OpenZeppelin audited contracts as base
- Implement `nonReentrant` modifier on mint functions
- Include signature expiry and nonce in signed messages
- Freeze metadata after reveal (remove `setTokenURI`)
- Use Merkle proofs for allowlists (gas + security)

For Users:

- Verify contract is verified on Etherscan
- Check for `setTokenURI` or owner functions
- Use hardware wallets for high-value NFTs
- Revoke approvals after marketplace interactions
- Verify IPFS/Arweave storage (not centralized servers)

Resources: OpenZeppelin Defender, Slither, Mythril for automated analysis

Problem Solved? NFT Technology

The Original Problem

What makes digital art scarce?

How NFT Technology Solves It

- Token ID uniquely identifies each NFT – only one owner can hold tokenId 1 at any time
- Blockchain provides immutable ownership history (provenance) that cannot be altered
- Smart contracts enforce scarcity by limiting total supply (e.g., 10,000 NFTs max)

Remaining Limitations

- The artwork itself usually isn't on-chain (IPFS or centralized servers host images)
- Metadata can be changed by contract owner if not frozen (mutable tokenURI)
- Scarcity is enforced by code trust, not physical impossibility

Open Questions

- Is provenance and social consensus enough to create lasting value?
- What happens when IPFS pinning services shut down or contract owners manipulate metadata?
- Risk: Extractive tokenomics, unsustainable yields

NFT Technology partially solves "What makes digital art scarce" but introduces new trade-offs

(c) Joerg Osterrieder 2025

What Does ERC-721Enumerable Add?

Optional Extension: Enables token enumeration

Additional Functions:

- `totalSupply()`: Total tokens minted
- `tokenByIndex(index)`: Get token ID at global index
- `tokenOfOwnerByIndex(owner, index)`: Get owner's nth token

Gas Considerations:

- Adds 50% gas overhead to transfers (extra storage updates)
- Maintains arrays for enumeration (expensive writes)
- Alternative: Off-chain indexing via The Graph or events

When to Use:

- Small collections (¡1000 tokens) where on-chain queries needed
- Avoid for large collections (use event-based indexing instead)

The Economics of NFT Technology

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: NFT Technology

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: NFT Technology

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Where Should NFT Data Live?

[COMIC: placeholder]

Two NFT collectors: one proudly shows a fully on-chain Noun (permanent, expensive), the other nervously watches their centralized server NFT slowly fade as the company shuts down—"Error 404: Your Art Not Found."

The Trade-off Revealed

- On-chain: Permanent but expensive (640k gas/KB)
- IPFS: Decentralized but requires pinning
- Centralized: Cheap but single point of failure

Key Insight

- Scarcity lives on-chain (tokenId)
- Art often lives off-chain (risk!)
- Best practice: IPFS + freeze metadata

Where your NFT's data lives determines whether it survives

Key Takeaways

1. NFTs operate across a six-layer technology stack from blockchain to application
2. TokenURI patterns range from centralized APIs to fully on-chain data
3. ERC-721A batch minting saves up to 80% gas for multiple mints
4. Lazy minting shifts gas costs from creator to buyer (zero upfront cost)
5. NFT market peaked at $25B in 2021, now stabilized around $8-10B annually
6. Security requires attention to reentrancy, signature replay, and metadata immutability
7. Enumerable extension adds functionality but increases gas costs significantly

Next Lesson: L22 – NFT Metadata and IPFS

Discussion Questions

1. When is fully on-chain metadata worth the gas cost premium?
2. How should projects balance gas optimization with code simplicity?
3. What role will Layer 2 solutions play in NFT gas economics?
4. Is lazy minting fair to buyers who pay higher gas than batch minters?
5. How can the industry address metadata permanence without centralization?

Next Lesson Preview

L22: NFT Metadata and IPFS

We will explore:

- JSON metadata format standards (OpenSea schema)
- IPFS content addressing and CID structure
- Pinning services and availability guarantees
- Arweave permanent storage economics
- Metadata permanence challenges and solutions

Preparation: Explore IPFS by uploading a file to Pinata (free tier)

Quiz Questions (1–5)

Q1. How many layers comprise the complete NFT technology stack?
A) 3 B) 4 C) 5 D) 6
Answer: D – The six layers are: Blockchain, Smart Contract, Token, Metadata, Storage, and Application.

Q2. What does the tokenURI function return?
A) Token owner address B) Token price C) URI pointing to metadata D) Token approval status
Answer: C – tokenURI returns a URI (IPFS, HTTP, or data URI) pointing to the token's metadata JSON.

Q3. Which tokenURI pattern offers the best decentralization and permanence?
A) Centralized server B) IPFS static C) Base URI pattern D) Dynamic API
Answer: B – IPFS static provides content-addressed, decentralized, and immutable storage.

Q4. What is the approximate gas cost to store 1 KB of data on-chain?
A) 20,000 gas B) 160,000 gas C) 640,000 gas D) 1,000,000 gas
Answer: C – On-chain storage costs 20,000 gas per 32 bytes, so 1 KB = 640,000 gas.

Q5. Which mapping tracks individual token ownership in ERC-721?
A) _balances B) _owners C) _tokenApprovals D) _operatorApprovals
Answer: B – _owners[tokenId] maps each token ID to its current owner address.

Quiz Questions (6–10)

Q6. How much gas does a standard ERC-721 transfer cost?
A) 21,000 gas B) 45,000 gas C) 65,000 gas D) 90,000 gas
Answer: C – A standard ERC-721 transfer costs approximately 65,000 gas.

Q7. What is the key innovation of ERC-721A?
A) On-chain metadata B) Deferred ownership updates C) Royalty enforcement D) Cross-chain transfers
Answer: B – ERC-721A defers ownership updates, writing only the first token in a batch to save gas.

Q8. How much gas can ERC-721A save on batch minting?
A) 20% B) 40% C) 60% D) 80%
Answer: D – ERC-721A provides up to 80% gas savings for batch minting operations.

Q9. In lazy minting, who pays the minting gas cost?
A) Creator B) Buyer C) Marketplace D) No one (gasless)
Answer: B – Lazy minting defers gas to the buyer who mints on first purchase.

Q10. What was the peak NFT trading volume year?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: B – 2021 saw peak NFT volume of approximately $25 billion.

Quiz Questions (11–15)

Q11. Which project pioneered ERC-721A batch optimization?
A) Bored Ape Yacht Club B) CryptoPunks C) Azuki D) Nouns
Answer: C – Azuki introduced ERC-721A in 2022 for gas-optimized batch minting.

Q12. What is a Dutch auction in NFT minting?
A) Fixed price sale B) Price starts high and decreases C) Sealed bid auction D) Free mint with gas only
Answer: B – Dutch auctions start at a high price that decreases until someone buys.

Q13. What security vulnerability involves re-entering during minting?
A) Signature replay B) Reentrancy attack C) Front-running D) Overflow attack
Answer: B – Reentrancy attacks exploit callbacks to re-enter mint functions for extra tokens.

Q14. How can signature replay attacks be prevented?
A) Use reentrancy guards B) Include nonce in signed message C) Freeze metadata D) Use IPFS storage
Answer: B – Including a nonce and tracking used signatures prevents replay attacks.

Q15. What does the ERC-721Enumerable extension add?
A) Royalty support B) Token enumeration functions C) Batch transfers D) Metadata standards
Answer: B – Enumerable adds totalSupply(), tokenByIndex(), and tokenOfOwnerByIndex() functions.

Quiz Questions (16–20)

Q16. What is the gas overhead of ERC-721Enumerable on transfers?
A) 10% B) 25% C) 50% D) 100%
Answer: C – Enumerable adds approximately 50% gas overhead to maintain enumeration arrays.

Q17. What is packed storage in NFT contracts?
A) Compressing IPFS files B) Storing multiple values in one 256-bit slot C) Batch transferring tokens D) Off-chain metadata
Answer: B – Packed storage fits multiple values (e.g., owner + aux data) in a single storage slot.

Q18. How much can Merkle allowlists save compared to on-chain address storage?
A) 10% B) 25% C) 50% D) 75%
Answer: C – Merkle proofs save approximately 50% by storing only the root hash on-chain.

Q19. Which NFT project stores artwork fully on-chain as SVG?
A) Bored Ape Yacht Club B) Nouns C) CryptoPunks D) Azuki
Answer: B – Nouns generates and stores SVG artwork entirely on-chain.

Q20. What is the recommended alternative to Enumerable for large collections?
A) More gas B) Fewer tokens C) Event-based indexing (The Graph) D) Centralized database
Answer: C – The Graph or event-based indexing provides enumeration without on-chain gas overhead.

L22: NFT Metadata and IPFS

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the JSON metadata format standard for NFTs
- Explain how IPFS content addressing works
- Describe the role of pinning services in NFT permanence
- Compare IPFS and Arweave for decentralized storage
- Evaluate metadata permanence and availability challenges

(c) Joerg Osterrieder 2025

The Problem: How do we store NFT data permanently?

The Challenge
When you buy an NFT, you own a token on the blockchain—but the image, metadata, and attributes live off-chain. Storing this data directly on Ethereum costs thousands of dollars per NFT. We need a way to store rich media permanently without breaking the bank.

Why It Matters

- If metadata disappears, the NFT becomes a worthless pointer to nothing
- Historical failures: Centralized servers shut down, leaving NFTs as broken links
- Mutable metadata enables "rug pulls"—owners changing artwork after sale

What We Need

- System design principles
- Content-addressed storage (same content = same identifier)
- Decentralized hosting (no single point of failure)
- Economic incentives for long-term data availability

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How NFT Metadata & IPFS addresses this challenge

NFT Metadata: The JSON Standard

Metadata Structure: OpenSea standard (widely adopted)

Core Fields:

- `name` – Display name of the NFT
- `description` – Human-readable description
- `image` – URI to primary visual asset (IPFS, HTTP)
- `external_url` – Link to project website
- `attributes` – Array of trait objects

Example Metadata JSON:

```
{
  "name": "Bored Ape #1234",
  "image": "ipfs://QmXyZ.../1234.png",
  "attributes": [{"trait_type": "Background", "value": "Blue"}]
}
```

Attributes: Defining Rarity

Attributes Array: Defines traits and properties

Attribute Object Structure:

- `trait_type` – Category name (e.g., "Hat", "Eyes")
- `value` – Specific value (e.g., "Beanie", "Laser Eyes")
- `display_type` (optional) – How to render (number, date, boost)

Rarity Calculation:

- Each trait has a frequency distribution in the collection
- Rarer traits (low frequency) increase NFT value
- Tools like Rarity Sniper calculate rarity scores

Example Rarity Analysis:

- Background: Blue (20% frequency) vs. Gold (2% frequency)
- Laser Eyes: 1% frequency (highly rare)

IPFS: The InterPlanetary File System

IPFS: Decentralized peer-to-peer file storage protocol

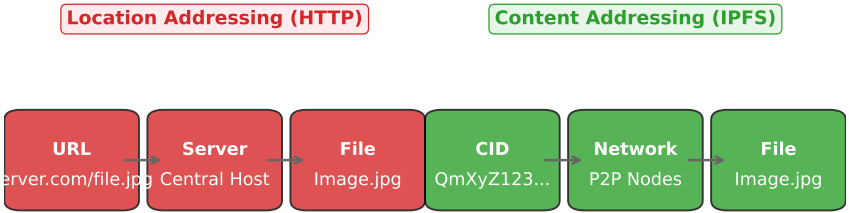
Key Concepts:

- **Content Addressing:** Files identified by cryptographic hash
- **CID (Content Identifier):** Unique hash of file content
- **Immutability:** Same content always produces same CID
- **Distributed:** Files stored across multiple nodes

Example IPFS URI:

- `ipfs://QmXyZ123abc...` (CID)
- Gateway URL: `https://ipfs.io/ipfs/QmXyZ123abc...`

Content Addressing vs Location Addressing



IPFS: Same content always produces same CID, retrievable from any node

Pinning: Ensuring Availability

IPFS Garbage Collection: Nodes delete unpinned files to save space

Without Pinning:

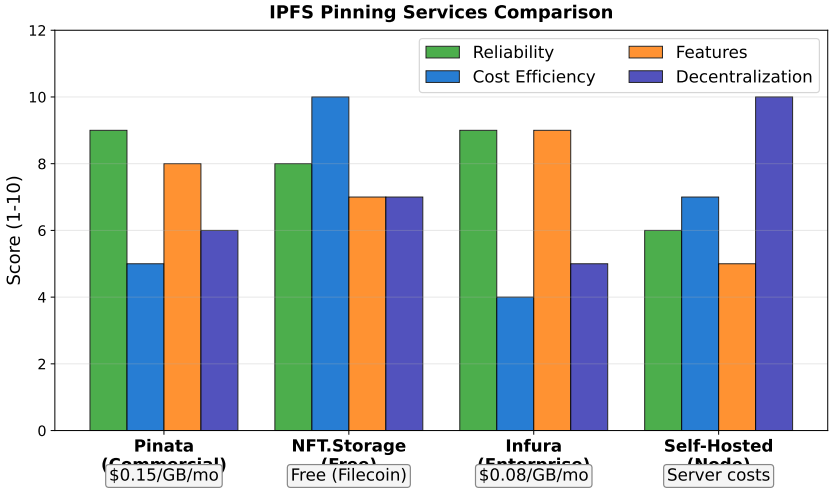
- File may be removed from all nodes (lost)
- NFT metadata/images become unavailable
- Broken image links in wallets and marketplaces

Pinning Services:

- **Pinata:** Popular commercial pinning service
- **NFT.Storage:** Free pinning for NFT data (funded by Filecoin)
- **Infura IPFS:** Enterprise-grade IPFS infrastructure
- **Self-hosting:** Run your own IPFS node and pin files

Critical Issue: If all pinning stops, files may disappear from IPFS

Pinning Services Comparison



NFT.Storage offers free pinning backed by Filecoin; Pinata is most popular commercial option

IPFS Gateways

Gateway: HTTP bridge to access IPFS content

Public Gateways:

- `https://ipfs.io/ipfs/[CID]`
- `https://gateway.pinata.cloud/ipfs/[CID]`
- `https://cloudflare-ipfs.com/ipfs/[CID]`

Why Gateways Matter:

- Browsers do not natively support `ipfs://` protocol
- Wallets and marketplaces use gateways to display NFTs
- Gateway downtime = NFTs appear broken

Centralization Risk:

- Most users rely on centralized gateways (ipfs.io, Cloudflare)
- Solution: Native IPFS support in browsers (IPFS Companion extension)

Arweave: Permanent Decentralized Storage

Arweave: Blockchain designed for permanent data storage

Key Differences from IPFS:

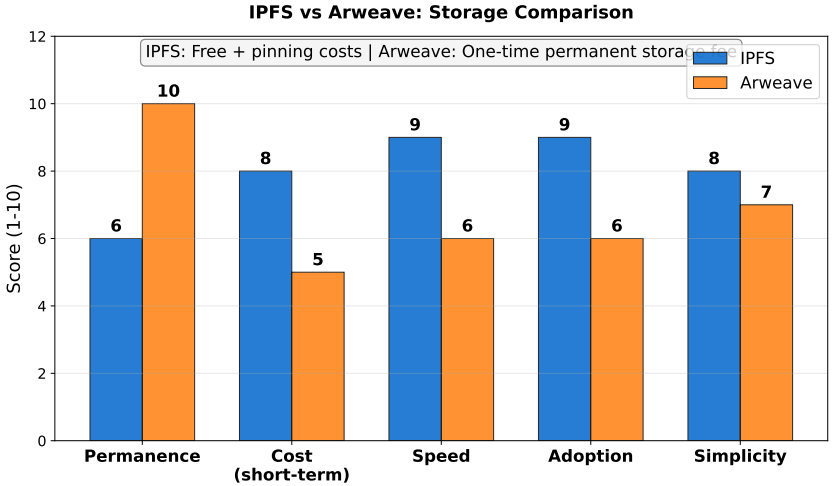
- **Permanence:** One-time payment for perpetual storage
- **Blockchain-based:** Data stored on Arweave blockchain
- **Economic model:** Storage endowment fund pays miners forever
- **No pinning needed:** Data guaranteed to persist

Arweave URI:

- `ar://[Transaction ID]`
- Gateway: `https://arweave.net/[Transaction ID]`

Use Cases: High-value NFTs requiring guaranteed permanence

IPFS vs Arweave Comparison



IPFS for most projects; Arweave for premium NFTs requiring guaranteed permanence

Metadata Permanence Challenges

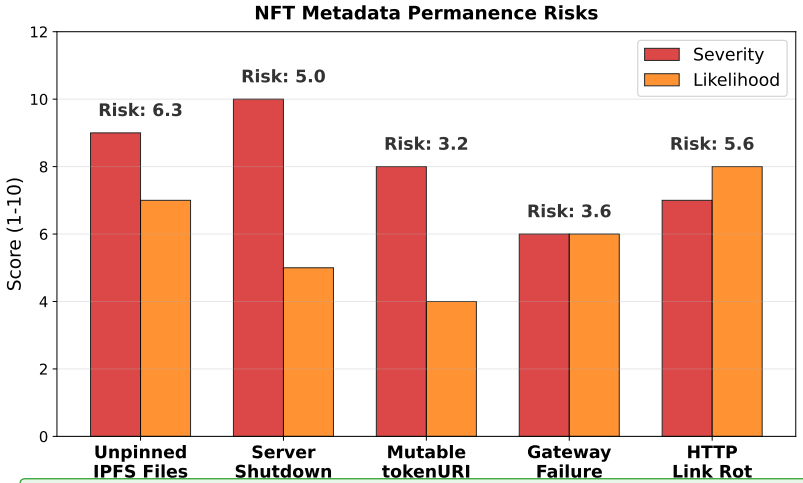
Real-World Issues:

1. **Unpinned IPFS files:** Project abandons pinning, files lost
2. **Centralized metadata servers:** Company shuts down, NFTs break
3. **Mutable tokenURI:** Smart contract allows owner to change metadata
4. **Gateway failures:** IPFS gateways go offline, NFTs appear broken
5. **Link rot:** HTTP URLs stop working (404 errors)

Case Study: Nifty Gateway (2021):

- Platform used centralized servers for metadata
- Outage caused all NFTs to display broken images
- Community backlash led to IPFS migration

Metadata Permanence Risks



Mitigation: Pin to multiple services, use immutable tokenURI, prefer IPFS/Arweave over HTTP

Server shutdown has highest severity; HTTP link rot is most likely to occur

Mutable vs. Immutable Metadata

Mutable Metadata:

- Smart contract owner can update `tokenURI`
- Allows bug fixes and metadata improvements
- Risk: Owner could change artwork or traits (rug pull)

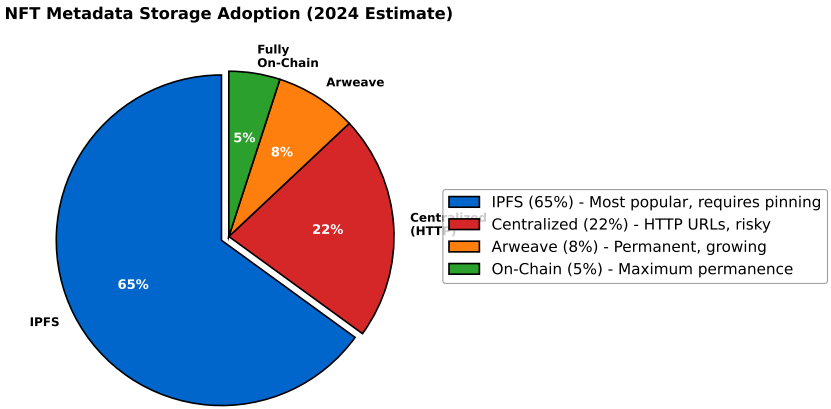
Immutable Metadata:

- `tokenURI` frozen after minting (contract locked)
- Guarantees metadata cannot be altered
- Standard for high-value collections (e.g., CryptoPunks)

Verification:

- Check smart contract code for `setTokenURI()` functions
- Verify contract ownership is renounced (no admin control)
- Use Etherscan to audit contract mutability

NFT Storage Adoption



IPFS dominates NFT storage; Arweave growing for premium projects

Best Practices for NFT Metadata

For NFT Projects:

1. **Use IPFS or Arweave:** Avoid centralized servers
2. **Pin all files:** Use reputable pinning services (Pinata, NFT.Storage)
3. **Freeze metadata:** Make `tokenURI` immutable after reveal
4. **Redundancy:** Pin to multiple services (IPFS + Arweave)
5. **Document storage:** Inform buyers where metadata is hosted

For NFT Buyers:

- Verify metadata is on IPFS/Arweave (not HTTP)
- Check if `tokenURI` is immutable
- Confirm pinning service reputation

Problem Solved? NFT Metadata & IPFS

The Original Problem

How do we store NFT data permanently?

How NFT Metadata & IPFS Solves It

- IPFS provides content-addressed storage—same content always produces same CID
- Pinning services (Pinata, NFT.Storage) ensure files remain available
- Arweave offers permanent storage with one-time payment and endowment fund
- Immutable `tokenURI` prevents metadata manipulation after minting

Remaining Limitations

- IPFS requires ongoing pinning—if all pinning stops, files disappear
- Arweave has upfront cost; neither is truly fully decentralized
- Gateway reliance creates centralization risk (most users depend on ipfs.io, Cloudflare)

Open Questions

- What storage layer best balances cost, permanence, and decentralization?
- Risk: Pinning service failures, gateway censorship, long-term economic viability

NFT Metadata & IPFS partially solves permanent storage but introduces trade-offs around cost and decentralization

(c) Joerg Osterrieder 2025

Key Takeaways

1. NFT metadata follows a JSON standard (name, description, image, attributes)
2. IPFS uses content addressing (CIDs) for decentralized, immutable storage
3. Pinning is critical for IPFS file permanence (unpinned files can be lost)
4. Arweave provides guaranteed permanent storage for a one-time fee
5. Metadata permanence challenges include unpinned files and mutable URIs
6. Best practice: Use IPFS/Arweave, pin to multiple services, freeze metadata

Discussion Questions

1. What are the trade-offs between IPFS and Arweave for NFT metadata storage?
2. Should NFT metadata be immutable, or is mutability acceptable for bug fixes?
3. How can the NFT community ensure long-term metadata availability?
4. Is fully on-chain metadata the ideal, or are off-chain solutions sufficient?
5. What happens to NFT value if metadata becomes unavailable?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L23: NFT Marketplaces

We will explore:

- OpenSea, Blur, and Rarible business models
- Listing mechanics and order book systems
- Marketplace fees and royalty enforcement
- Wash trading and market manipulation detection
- Aggregators and cross-marketplace trading

Preparation: Create a wallet and browse NFT collections on OpenSea

Quiz Questions (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media
Answer: B – The `image` field stores the URI to the primary visual asset (IPFS or HTTP).

Q3. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index Data D) Content Index Database
Answer: A – CID is the Content Identifier, a unique hash of file content in IPFS.

Q4. How does IPFS identify files?
A) By file name B) By server location C) By cryptographic hash D) By timestamp
Answer: C – IPFS uses content addressing where files are identified by their cryptographic hash.

Q5. What happens to unpinned files on IPFS?
A) They are encrypted B) They may be deleted C) They become public D) Nothing changes
Answer: B – IPFS nodes delete unpinned files during garbage collection to save space.

Quiz Questions (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks
Answer: B – Gateways are HTTP bridges that allow browsers to access IPFS content.

Q8. What is Arweave's key advantage over IPFS?
A) Faster speeds B) Permanent storage guarantee C) Free storage D) Better encryption
Answer: B – Arweave provides guaranteed permanent storage for a one-time payment.

Q9. What does the `trait_type` field define in NFT attributes?
A) Rarity score B) Category name C) Token ID D) Price range
Answer: B – `trait_type` defines the category name (e.g., "Hat", "Eyes").

Q10. Which storage protocol requires pinning to ensure file availability?
A) Arweave B) IPFS C) HTTP servers D) FTP
Answer: B – IPFS requires pinning to prevent garbage collection from removing files.

Quiz Questions (11–15)

Q11. What does "immutable metadata" mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug
Answer: B – They used centralized servers; an outage caused NFTs to display broken images.

Q13. How does Arweave achieve permanent storage?
A) Annual fees B) Storage endowment fund C) Volunteer nodes D) Government subsidy
Answer: B – A storage endowment fund pays miners perpetually to store data.

Q14. What is the primary centralization risk with IPFS gateways?
A) High costs B) Slow speeds C) Gateway downtime breaks NFTs D) Privacy leaks
Answer: C – Most users rely on centralized gateways; downtime makes NFTs appear broken.

Q15. What determines rarity in NFT collections?
A) Token ID number B) Mint date C) Trait frequency D) File size
Answer: C – Rarity is determined by trait frequency distribution; rarer traits increase value.

Quiz Questions (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss
Answer: C – Mutable metadata allows owners to update `tokenURI`, risking rug pulls.

Q18. How can buyers verify if metadata is immutable?
A) Check file size B) Audit smart contract code C) Ask on Discord D) Check token price
Answer: B – Review contract code for `setTokenURI()` functions and verify ownership is renounced.

Q19. What best practice ensures metadata redundancy?
A) Multiple wallets B) Pin to multiple services C) Daily backups D) Cloud storage
Answer: B – Pin to multiple services (e.g., IPFS + Arweave) for redundancy.

Q20. What happens if all pinning services stop hosting an IPFS file?
A) File becomes encrypted B) File may disappear C) File moves to Arweave D) File is cached
Answer: B – Without any node pinning the file, it can be garbage collected and lost forever.

L22: NFT Metadata and IPFS

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Where is my image stored?

[COMIC: placeholder]

A new NFT buyer excitedly showing off their $10k NFT, then zooming out to reveal the image is hosted on a random startup's AWS server with a "Free Trial Expires in 30 Days" warning.

The Hidden Truth

- You own the token on Ethereum
- But the image lives... somewhere else
- That "somewhere" matters enormously

What We'll Explore

- How IPFS content addressing works
- Why pinning is essential
- Arweave's permanent storage model

Your NFT is only as permanent as its weakest storage layer

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the JSON metadata format standard for NFTs
- Explain how IPFS content addressing works
- Describe the role of pinning services in NFT permanence
- Compare IPFS and Arweave for decentralized storage
- Evaluate metadata permanence and availability challenges

Building on L21: NFT Technology Deep Dive

The Problem: How do we store NFT data permanently?

The Challenge
When you buy an NFT, you own a token on the blockchain—but the image, metadata, and attributes live off-chain. Storing this data directly on Ethereum costs thousands of dollars per NFT. We need a way to store rich media permanently without breaking the bank.

Why It Matters

- If metadata disappears, the NFT becomes a worthless pointer to nothing
- Historical failures: Centralized servers shut down, leaving NFTs as broken links
- Mutable metadata enables "rug pulls"—owners changing artwork after sale

What We Need

- System design principles
- Content-addressed storage (same content = same identifier)
- Decentralized hosting (no single point of failure)
- Economic incentives for long-term data availability

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How NFT Metadata & IPFS addresses this challenge

What is the JSON Standard for NFT Metadata?

Metadata Structure: OpenSea standard (widely adopted)

Core Fields:

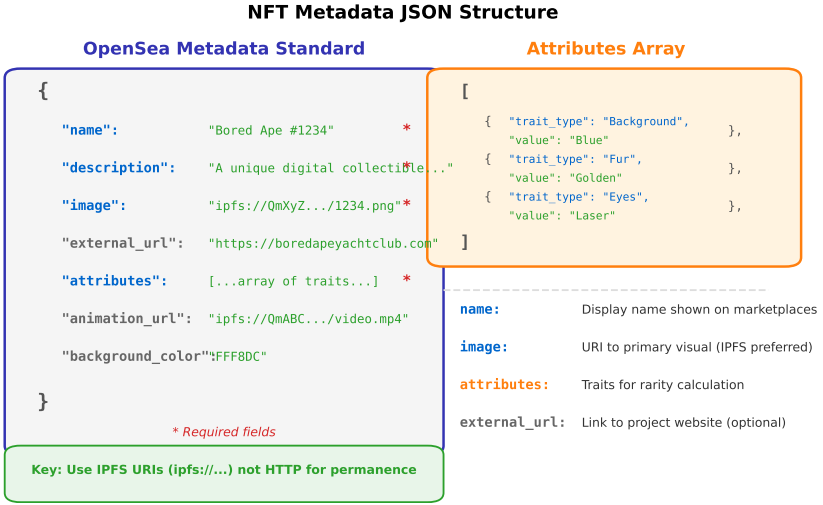
- `name` – Display name of the NFT
- `description` – Human-readable description
- `image` – URI to primary visual asset (IPFS, HTTP)
- `external_url` – Link to project website
- `attributes` – Array of trait objects

Example Metadata JSON:

```
{
  "name": "Bored Ape #1234",
  "image": "ipfs://QmXyZ.../1234.png",
  "attributes": [{"trait_type": "Background", "value": "Blue"}]
}
```

Problem: How do we store NFT data permanently? — JSON metadata lives off-chain (too expensive on-chain), linked via tokenURI; if this file disappears, your NFT becomes a pointer to nothing

How is NFT Metadata Structured?



OpenSea standard: Required fields (name, image, attributes) + optional fields (external_url, animation_url)

How Do Attributes Define NFT Rarity?

Attributes Array: Defines traits and properties

Attribute Object Structure:

- `trait_type` – Category name (e.g., "Hat", "Eyes")
- `value` – Specific value (e.g., "Beanie", "Laser Eyes")
- `display_type` (optional) – How to render (number, date, boost)

Rarity Calculation:

- Each trait has a frequency distribution in the collection
- Rarer traits (low frequency) increase NFT value
- Tools like Rarity Sniper calculate rarity scores

Example Rarity Analysis:

- Background: Blue (20% frequency) vs. Gold (2% frequency)
- Laser Eyes: 1% frequency (highly rare)

How Does IPFS Work for NFT Storage?

IPFS: Decentralized peer-to-peer file storage protocol

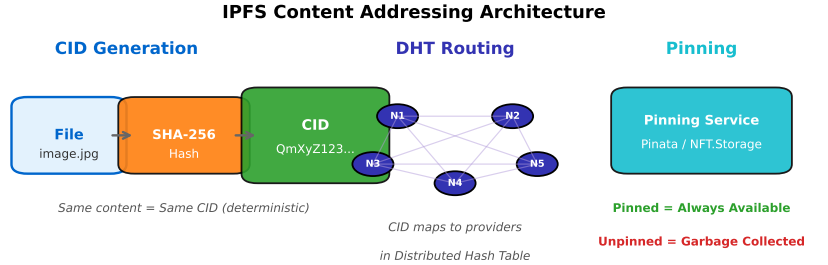
Key Concepts:

- **Content Addressing:** Files identified by cryptographic hash
- **CID (Content Identifier):** Unique hash of file content
- **Immutability:** Same content always produces same CID
- **Distributed:** Files stored across multiple nodes

Example IPFS URI:

- `ipfs://QmXyZ123abc...` (CID)
- Gateway URL: `https://ipfs.io/ipfs/QmXyZ123abc...`

How Does IPFS Content Addressing Work?



Complete workflow: Upload file, hash to CID, announce to DHT, pin for persistence, retrieve via any node

Why Use Content Addressing Instead of Location Addressing?

Content Addressing vs Location Addressing

Location Addressing (HTTP)

Content Addressing (IPFS)

Server down = 404 Error

Any node can serve file

Content can change at URL

Single point of failure

No integrity guarantee

Same content = Same CID

Distributed retrieval

Cryptographic verification

Problem: How do we store NFT data permanently? — Content addressing (IPFS) means if anyone hosts the same file, it's available; location addressing (HTTP) breaks when one server dies

Why Is Pinning Critical for NFT Permanence?

IPFS Garbage Collection: Nodes delete unpinned files to save space

Without Pinning:

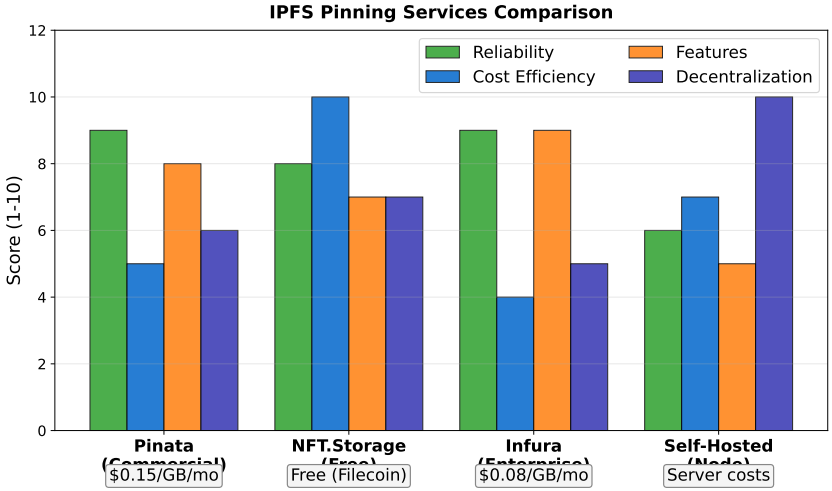
- File may be removed from all nodes (lost)
- NFT metadata/images become unavailable
- Broken image links in wallets and marketplaces

Pinning Services:

- **Pinata:** Popular commercial pinning service
- **NFT.Storage:** Free pinning for NFT data (funded by Filecoin)
- **Infura IPFS:** Enterprise-grade IPFS infrastructure
- **Self-hosting:** Run your own IPFS node and pin files

Critical Issue: If all pinning stops, files may disappear from IPFS

Which Pinning Services Are Best for NFTs?



NFT.Storage offers free pinning backed by Filecoin; Pinata is most popular commercial option

What Are IPFS Gateways and Why Do They Matter?

Gateway: HTTP bridge to access IPFS content

Public Gateways:

- `https://ipfs.io/ipfs/[CID]`
- `https://gateway.pinata.cloud/ipfs/[CID]`
- `https://cloudflare-ipfs.com/ipfs/[CID]`

Why Gateways Matter:

- Browsers do not natively support `ipfs://` protocol
- Wallets and marketplaces use gateways to display NFTs
- Gateway downtime = NFTs appear broken

Centralization Risk:

- Most users rely on centralized gateways (ipfs.io, Cloudflare)
- Solution: Native IPFS support in browsers (IPFS Companion extension)

(c) Joerg Osterrieder 2025

How Does Arweave Provide Permanent Storage?

Arweave: Blockchain designed for permanent data storage

Key Differences from IPFS:

- **Permanence:** One-time payment for perpetual storage
- **Blockchain-based:** Data stored on Arweave blockchain
- **Economic model:** Storage endowment fund pays miners forever
- **No pinning needed:** Data guaranteed to persist

Arweave URI:

- `ar://[Transaction ID]`
- Gateway: `https://arweave.net/[Transaction ID]`

Use Cases: High-value NFTs requiring guaranteed permanence

Problem: How do we store NFT data permanently? — Arweave's one-time-payment model creates permanent storage via an endowment fund that pays miners forever, unlike IPFS which requires ongoing pinning

Problem Check-In: NFT Metadata & IPFS

Recall Our Problem

How do we store NFT data permanently?

What We've Learned So Far

- IPFS uses content addressing: same file always produces same CID (Content Identifier), a cryptographic hash
- Pinning keeps files available; without pinning, IPFS nodes delete files during garbage collection
- Content addressing ensures immutability (can't swap artwork without changing CID), but pinning is required for availability

Still to Address

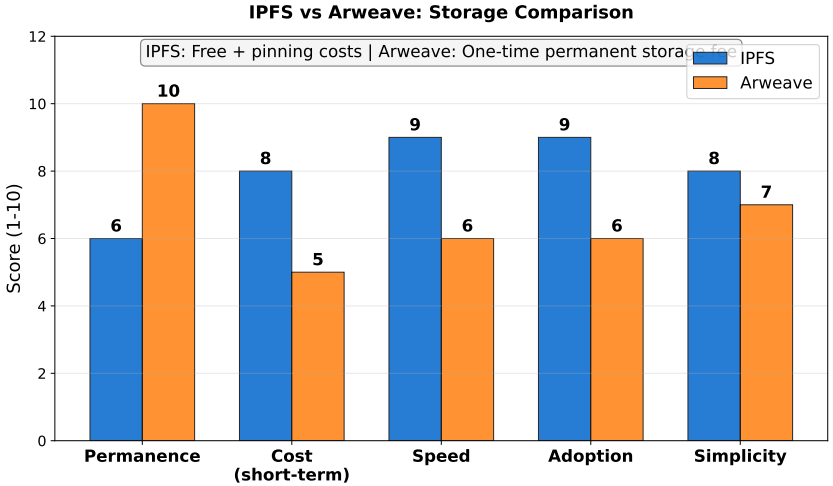
- Arweave permanent storage, metadata permanence challenges, and mutable vs immutable tokenURI
- Who pays for perpetual pinning, and what happens when projects abandon their NFT collections?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we store NFT data permanently?"?

How Do IPFS and Arweave Compare?



IPFS for most projects; Arweave for premium NFTs requiring guaranteed permanence

What Can Go Wrong with NFT Metadata?

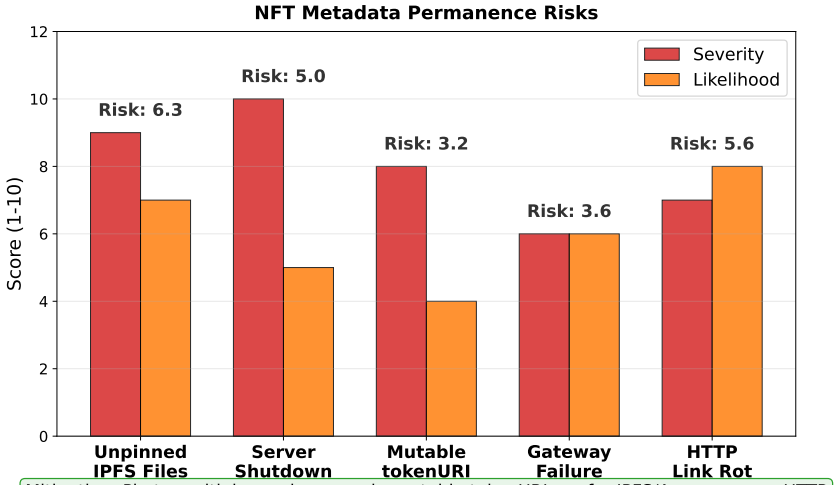
Real-World Issues:

1. **Unpinned IPFS files:** Project abandons pinning, files lost
2. **Centralized metadata servers:** Company shuts down, NFTs break
3. **Mutable tokenURI:** Smart contract allows owner to change metadata
4. **Gateway failures:** IPFS gateways go offline, NFTs appear broken
5. **Link rot:** HTTP URLs stop working (404 errors)

Case Study: Nifty Gateway (2021):

- Platform used centralized servers for metadata
- Outage caused all NFTs to display broken images
- Community backlash led to IPFS migration

What Risks Threaten NFT Metadata Permanence?



Mitigation: Pin to multiple services, use immutable tokenURI, prefer IPFS/Arweave over HTTP

Problem: How do we store NFT data permanently? — Every storage option has failure modes; best practice is redundancy (IPFS + Arweave) and freezing tokenURI to prevent owner manipulation

Should NFT Metadata Be Mutable or Immutable?

Mutable Metadata:

- Smart contract owner can update `tokenURI`
- Allows bug fixes and metadata improvements
- Risk: Owner could change artwork or traits (rug pull)

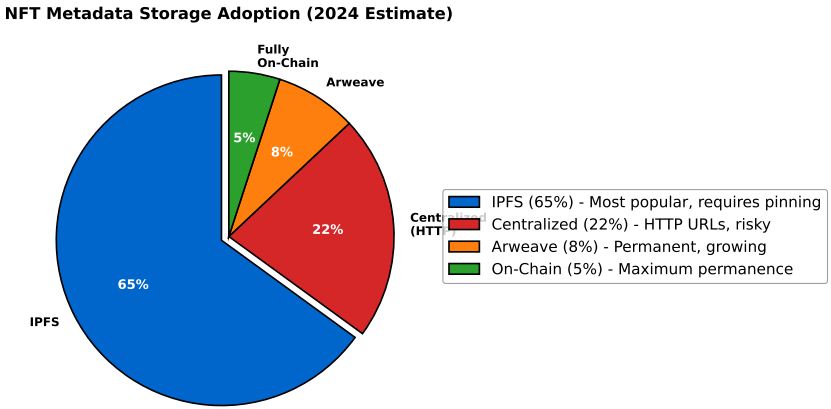
Immutable Metadata:

- `tokenURI` frozen after minting (contract locked)
- Guarantees metadata cannot be altered
- Standard for high-value collections (e.g., CryptoPunks)

Verification:

- Check smart contract code for `setTokenURI()` functions
- Verify contract ownership is renounced (no admin control)
- Use Etherscan to audit contract mutability

Which Storage Solutions Are Most Widely Adopted?



IPFS dominates NFT storage; Arweave growing for premium projects

What Are the Best Practices for NFT Metadata?

For NFT Projects:

1. **Use IPFS or Arweave:** Avoid centralized servers
2. **Pin all files:** Use reputable pinning services (Pinata, NFT.Storage)
3. **Freeze metadata:** Make `tokenURI` immutable after reveal
4. **Redundancy:** Pin to multiple services (IPFS + Arweave)
5. **Document storage:** Inform buyers where metadata is hosted

For NFT Buyers:

- Verify metadata is on IPFS/Arweave (not HTTP)
- Check if `tokenURI` is immutable
- Confirm pinning service reputation

(c) Joerg Osterrieder 2025

Problem Solved? NFT Metadata & IPFS

The Original Problem

How do we store NFT data permanently?

How NFT Metadata & IPFS Solves It

- IPFS provides content-addressed storage—same content always produces same CID
- Pinning services (Pinata, NFT.Storage) ensure files remain available
- Arweave offers permanent storage with one-time payment and endowment fund
- Immutable `tokenURI` prevents metadata manipulation after minting

Remaining Limitations

- IPFS requires ongoing pinning—if all pinning stops, files disappear
- Arweave has upfront cost; neither is truly fully decentralized
- Gateway reliance creates centralization risk (most users depend on ipfs.io, Cloudflare)

Open Questions

- What storage layer best balances cost, permanence, and decentralization?
- Risk: Pinning service failures, gateway censorship, long-term economic viability

NFT Metadata & IPFS partially solves permanent storage but introduces trade-offs around cost and decentralization

(c) Joerg Osterrieder 2025

The Economics of NFT Metadata & IPFS

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: NFT Metadata & IPFS

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: NFT Metadata & IPFS

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

IPFS pinning responsibility

[COMIC: placeholder]

A project founder driving away in a Lambo while their NFT collection's pinning subscription expires. Behind them, thousands of NFTs slowly turn into broken image icons, with holders asking "Who's paying for storage?"

The Responsibility Gap

- IPFS is decentralized, but pinning isn't free
- Someone must pay for long-term storage
- When projects abandon, who keeps pinning?

Buyer Beware

- Check: Who controls the pinning?
- Better: Arweave for permanent storage
- Best: On-chain for critical data

Decentralized storage requires centralized payment—someone always foots the bill

Key Takeaways

1. NFT metadata follows a JSON standard (name, description, image, attributes)
2. IPFS uses content addressing (CIDs) for decentralized, immutable storage
3. Pinning is critical for IPFS file permanence (unpinned files can be lost)
4. Arweave provides guaranteed permanent storage for a one-time fee
5. Metadata permanence challenges include unpinned files and mutable URIs
6. Best practice: Use IPFS/Arweave, pin to multiple services, freeze metadata

Next Lesson: L23 – NFT Marketplaces

(c) Joerg Osterrieder 2025

Discussion Questions

1. What are the trade-offs between IPFS and Arweave for NFT metadata storage?
2. Should NFT metadata be immutable, or is mutability acceptable for bug fixes?
3. How can the NFT community ensure long-term metadata availability?
4. Is fully on-chain metadata the ideal, or are off-chain solutions sufficient?
5. What happens to NFT value if metadata becomes unavailable?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L23: NFT Marketplaces

We will explore:

- OpenSea, Blur, and Rarible business models
- Listing mechanics and order book systems
- Marketplace fees and royalty enforcement
- Wash trading and market manipulation detection
- Aggregators and cross-marketplace trading

Preparation: Create a wallet and browse NFT collections on OpenSea

Quiz Questions (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media
Answer: B – The `image` field stores the URI to the primary visual asset (IPFS or HTTP).

Q3. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index Data D) Content Index Database
Answer: A – CID is the Content Identifier, a unique hash of file content in IPFS.

Q4. How does IPFS identify files?
A) By file name B) By server location C) By cryptographic hash D) By timestamp
Answer: C – IPFS uses content addressing where files are identified by their cryptographic hash.

Q5. What happens to unpinned files on IPFS?
A) They are encrypted B) They may be deleted C) They become public D) Nothing changes
Answer: B – IPFS nodes delete unpinned files during garbage collection to save space.

Quiz Questions (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks
Answer: B – Gateways are HTTP bridges that allow browsers to access IPFS content.

Q8. What is Arweave's key advantage over IPFS?
A) Faster speeds B) Permanent storage guarantee C) Free storage D) Better encryption
Answer: B – Arweave provides guaranteed permanent storage for a one-time payment.

Q9. What does the `trait_type` field define in NFT attributes?
A) Rarity score B) Category name C) Token ID D) Price range
Answer: B – `trait_type` defines the category name (e.g., "Hat", "Eyes").

Q10. Which storage protocol requires pinning to ensure file availability?
A) Arweave B) IPFS C) HTTP servers D) FTP
Answer: B – IPFS requires pinning to prevent garbage collection from removing files.

Quiz Questions (11–15)

Q11. What does "immutable metadata" mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug
Answer: B – They used centralized servers; an outage caused NFTs to display broken images.

Q13. How does Arweave achieve permanent storage?
A) Annual fees B) Storage endowment fund C) Volunteer nodes D) Government subsidy
Answer: B – A storage endowment fund pays miners perpetually to store data.

Q14. What is the primary centralization risk with IPFS gateways?
A) High costs B) Slow speeds C) Gateway downtime breaks NFTs D) Privacy leaks
Answer: C – Most users rely on centralized gateways; downtime makes NFTs appear broken.

Q15. What determines rarity in NFT collections?
A) Token ID number B) Mint date C) Trait frequency D) File size
Answer: C – Rarity is determined by trait frequency distribution; rarer traits increase value.

Quiz Questions (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss
Answer: C – Mutable metadata allows owners to update `tokenURI`, risking rug pulls.

Q18. How can buyers verify if metadata is immutable?
A) Check file size B) Audit smart contract code C) Ask on Discord D) Check token price
Answer: B – Review contract code for `setTokenURI()` functions and verify ownership is renounced.

Q19. What best practice ensures metadata redundancy?
A) Multiple wallets B) Pin to multiple services C) Daily backups D) Cloud storage
Answer: B – Pin to multiple services (e.g., IPFS + Arweave) for redundancy.

Q20. What happens if all pinning services stop hosting an IPFS file?
A) File becomes encrypted B) File may disappear C) File moves to Arweave D) File is cached
Answer: B – Without any node pinning the file, it can be garbage collected and lost forever.

L22: NFT Metadata and IPFS

Mini-Lecture — Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Understand the JSON metadata standard for NFTs
- Explain how IPFS content addressing works
- Describe the role of pinning services in NFT permanence
- Compare IPFS and Arweave for decentralized storage

(c) Joerg Osterrieder 2025

NFT Metadata: The JSON Standard

OpenSea Standard (widely adopted):

- `name` – Display name of the NFT
- `description` – Human-readable description
- `image` – URI to primary visual asset (IPFS, HTTP)
- `attributes` – Array of trait objects defining rarity

Example JSON:

```
{
  "name": "Bored Ape #1234",
  "image": "ipfs://QmXyZ.../1234.png",
  "attributes": [{"trait_type": "Background", "value": "Blue"}]
}
```

Attributes determine rarity; rarer traits (low frequency) increase NFT value

IPFS: The InterPlanetary File System

Key Concepts:

- **Content Addressing:** Files identified by cryptographic hash (not location)
- **CID (Content Identifier):** Unique hash of file content
- **Immutability:** Same content always produces same CID
- **Distributed:** Files stored across multiple nodes worldwide

Example IPFS URI:

- Native: `ipfs://QmXyZ123abc...`
- Gateway: `https://ipfs.io/ipfs/QmXyZ123abc...`

Unlike HTTP (location-based), IPFS addresses content by what it is, not where it is

Content Addressing vs Location Addressing

Aspect	HTTP (Location)	IPFS (Content)
Addressing	Server URL	Cryptographic hash
File identity	Depends on server	Content determines ID
If content changes	Same URL, different file	New CID generated
Server dependency	Single point of failure	Any node can serve
Censorship	Easy to block	Difficult to block

IPFS: Same content always produces same CID, retrievable from any node

Pinning: Ensuring Availability

IPFS Garbage Collection: Nodes delete unpinned files to save space

Without Pinning:

- Files may be removed from all nodes (permanently lost)
- NFT metadata/images become unavailable
- Broken image links in wallets and marketplaces

Popular Pinning Services:

- **Pinata:** Commercial pinning service (most popular)
- **NFT.Storage:** Free pinning backed by Filecoin
- **Infura IPFS:** Enterprise-grade infrastructure

Critical: If all pinning stops, files may disappear from IPFS forever

Arweave: Permanent Decentralized Storage

Key Differences from IPFS:

- **Permanence:** One-time payment for perpetual storage
- **Blockchain-based:** Data stored on Arweave blockchain
- **Economic model:** Storage endowment fund pays miners forever
- **No pinning needed:** Data guaranteed to persist

Arweave URI:

- Native: `ar://[Transaction ID]`
- Gateway: `https://arweave.net/[Transaction ID]`

Use case: High-value NFTs requiring guaranteed permanence

IPFS vs Arweave: When to Use Which?

Feature	IPFS	Arweave
Cost model	Ongoing (pinning fees)	One-time payment
Permanence	Requires active pinning	Guaranteed permanent
Network type	P2P file sharing	Blockchain storage
Best for	Most NFT projects	Premium/high-value NFTs
Risk	Pin abandonment	Protocol risk

Best practice: Use IPFS + Arweave redundancy for important NFT collections

Metadata Permanence Challenges

Real-World Issues:

1. **Unpinned IPFS files:** Project abandons pinning, files lost
2. **Centralized servers:** Company shuts down, NFTs break
3. **Mutable tokenURI:** Owner can change metadata (rug pull risk)
4. **Gateway failures:** IPFS gateways go offline, NFTs appear broken

Case Study – Nifty Gateway (2021):

- Platform used centralized servers for metadata
- Outage caused all NFTs to display broken images
- Community backlash led to IPFS migration

Lesson: Always verify storage method before purchasing NFTs

Best Practices for NFT Metadata

For NFT Projects:

1. Use IPFS or Arweave – avoid centralized servers
2. Pin all files to reputable services (Pinata, NFT.Storage)
3. Freeze metadata after reveal (make tokenURI immutable)
4. Use redundancy: Pin to IPFS + store on Arweave

For NFT Buyers:

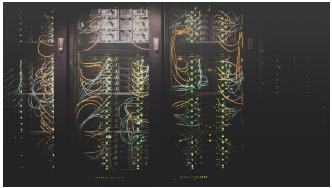
- Verify metadata is on IPFS/Arweave (not HTTP)
- Check if tokenURI is immutable (audit smart contract)
- Confirm pinning service reputation

Due diligence on storage can prevent buying NFTs that may break

Visual Summary: NFT Metadata Ecosystem

Metadata
JSON structure with
name, image, attributes

Storage
IPFS (pinning) or
Arweave (permanent)



Distribution
Decentralized nodes
serve content globally

Images: Unsplash (CC0) — Metadata lives on-chain, assets live off-chain on IPFS/Arweave

Quiz Questions (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML **C) JSON** D) CSV
OpenSea JSON standard is widely adopted for NFT metadata.

Q2. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index D) Content Index
CID is the unique hash of file content in IPFS.

Q3. What happens to unpinned files on IPFS?
A) Encrypted **B) May be deleted** C) Become public D) Nothing
Nodes delete unpinned files during garbage collection.

Q4. Which service offers free NFT storage backed by Filecoin?
A) Pinata **B) NFT.Storage** C) Infura D) Cloudflare
NFT.Storage provides free pinning funded by Filecoin.

Q5. What is Arweave's key advantage over IPFS?
A) Faster **B) Permanent storage** C) Free D) Better encryption
Arweave guarantees permanent storage for a one-time payment.

Quiz Questions (6–10)

Q6. How does IPFS identify files?
A) File name B) Server location **C) Cryptographic hash** D) Timestamp
IPFS uses content addressing where files are identified by hash.

Q7. What is the risk of mutable metadata in NFTs?
A) Higher gas B) Slow transactions **C) Owner can change artwork** D) Privacy
Mutable tokenURI allows owners to alter NFT artwork (rug pull risk).

Q8. What was the 2021 Nifty Gateway issue?
A) Hack **B) Centralized metadata outage** C) High fees D) Contract bug
Centralized servers caused all NFTs to display broken images.

Q9. What ensures metadata redundancy?
A) Multiple wallets **B) Pin to multiple services** C) Daily backups D) Cloud
Pin to IPFS + store on Arweave for redundancy.

Q10. What field in metadata contains the visual asset URI?
A) asset **B) image** C) visual D) media
The `image` field stores the URI to the primary visual asset.

Quiz: NFT Metadata and IPFS

Instructions: Multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV

Quiz (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media

Quiz (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media
Answer: B – The `image` field stores the URI to the primary visual asset (IPFS or HTTP).

Q3. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index Data D) Content Index Database

Quiz (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media
Answer: B – The `image` field stores the URI to the primary visual asset (IPFS or HTTP).

Q3. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index Data D) Content Index Database
Answer: A – CID is the Content Identifier, a unique hash of file content in IPFS.

Q4. How does IPFS identify files?
A) By file name B) By server location C) By cryptographic hash D) By timestamp

Quiz (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media
Answer: B – The `image` field stores the URI to the primary visual asset (IPFS or HTTP).

Q3. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index Data D) Content Index Database
Answer: A – CID is the Content Identifier, a unique hash of file content in IPFS.

Q4. How does IPFS identify files?
A) By file name B) By server location C) By cryptographic hash D) By timestamp
Answer: C – IPFS uses content addressing where files are identified by their cryptographic hash.

Q5. What happens to unpinned files on IPFS?
A) They are encrypted B) They may be deleted C) They become public D) Nothing changes

Quiz (1–5)

Q1. What is the standard metadata format used for NFTs?
A) XML B) YAML C) JSON D) CSV
Answer: C – The OpenSea JSON standard is widely adopted for NFT metadata structure.

Q2. Which field in NFT metadata contains the URI to the visual asset?
A) asset B) image C) visual D) media
Answer: B – The `image` field stores the URI to the primary visual asset (IPFS or HTTP).

Q3. What does CID stand for in IPFS?
A) Content Identifier B) Cryptographic ID C) Chain Index Data D) Content Index Database
Answer: A – CID is the Content Identifier, a unique hash of file content in IPFS.

Q4. How does IPFS identify files?
A) By file name B) By server location C) By cryptographic hash D) By timestamp
Answer: C – IPFS uses content addressing where files are identified by their cryptographic hash.

Q5. What happens to unpinned files on IPFS?
A) They are encrypted B) They may be deleted C) They become public D) Nothing changes
Answer: B – IPFS nodes delete unpinned files during garbage collection to save space.

Quiz (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare

Quiz (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks
Answer: B – Gateways are HTTP bridges that allow browsers to access IPFS content.

Q8. What is Arweave's key advantage over IPFS?
A) Faster speeds B) Permanent storage guarantee C) Free storage D) Better encryption

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks
Answer: B – Gateways are HTTP bridges that allow browsers to access IPFS content.

Q8. What is Arweave's key advantage over IPFS?
A) Faster speeds B) Permanent storage guarantee C) Free storage D) Better encryption
Answer: B – Arweave provides guaranteed permanent storage for a one-time payment.

Q9. What does the `trait_type` field define in NFT attributes?
A) Rarity score B) Category name C) Token ID D) Price range

Quiz (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks
Answer: B – Gateways are HTTP bridges that allow browsers to access IPFS content.

Q8. What is Arweave's key advantage over IPFS?
A) Faster speeds B) Permanent storage guarantee C) Free storage D) Better encryption
Answer: B – Arweave provides guaranteed permanent storage for a one-time payment.

Q9. What does the `trait_type` field define in NFT attributes?
A) Rarity score B) Category name C) Token ID D) Price range
Answer: B – `trait_type` defines the category name (e.g., "Hat", "Eyes").

Q10. Which storage protocol requires pinning to ensure file availability?
A) Arweave B) IPFS C) HTTP servers D) FTP

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which pinning service offers free NFT storage backed by Filecoin?
A) Pinata B) NFT.Storage C) Infura IPFS D) Cloudflare
Answer: B – NFT.Storage provides free pinning for NFT data, funded by Filecoin.

Q7. What is the purpose of an IPFS gateway?
A) Encrypt files B) Provide HTTP access to IPFS C) Store private keys D) Mine blocks
Answer: B – Gateways are HTTP bridges that allow browsers to access IPFS content.

Q8. What is Arweave's key advantage over IPFS?
A) Faster speeds B) Permanent storage guarantee C) Free storage D) Better encryption
Answer: B – Arweave provides guaranteed permanent storage for a one-time payment.

Q9. What does the `trait_type` field define in NFT attributes?
A) Rarity score B) Category name C) Token ID D) Price range
Answer: B – `trait_type` defines the category name (e.g., "Hat", "Eyes").

Q10. Which storage protocol requires pinning to ensure file availability?
A) Arweave B) IPFS C) HTTP servers D) FTP
Answer: B – IPFS requires pinning to prevent garbage collection from removing files.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What does “immutable metadata” mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage

Quiz (11–15)

Q11. What does “immutable metadata” mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug

Quiz (11–15)

Q11. What does "immutable metadata" mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug
Answer: B – They used centralized servers; an outage caused NFTs to display broken images.

Q13. How does Arweave achieve permanent storage?
A) Annual fees B) Storage endowment fund C) Volunteer nodes D) Government subsidy

Quiz (11–15)

Q11. What does "immutable metadata" mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug
Answer: B – They used centralized servers; an outage caused NFTs to display broken images.

Q13. How does Arweave achieve permanent storage?
A) Annual fees B) Storage endowment fund C) Volunteer nodes D) Government subsidy
Answer: B – A storage endowment fund pays miners perpetually to store data.

Q14. What is the primary centralization risk with IPFS gateways?
A) High costs B) Slow speeds C) Gateway downtime breaks NFTs D) Privacy leaks

Quiz (11–15)

Q11. What does "immutable metadata" mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug
Answer: B – They used centralized servers; an outage caused NFTs to display broken images.

Q13. How does Arweave achieve permanent storage?
A) Annual fees B) Storage endowment fund C) Volunteer nodes D) Government subsidy
Answer: B – A storage endowment fund pays miners perpetually to store data.

Q14. What is the primary centralization risk with IPFS gateways?
A) High costs B) Slow speeds C) Gateway downtime breaks NFTs D) Privacy leaks
Answer: C – Most users rely on centralized gateways; downtime makes NFTs appear broken.

Q15. What determines rarity in NFT collections?
A) Token ID number B) Mint date C) Trait frequency D) File size

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What does "immutable metadata" mean for an NFT?
A) Metadata stored on-chain B) tokenURI cannot be changed C) IPFS pinned D) Encrypted storage
Answer: B – Immutable metadata means the `tokenURI` is frozen and cannot be altered.

Q12. What was the issue with Nifty Gateway in 2021?
A) Hacked wallets B) Centralized metadata outage C) Gas fees too high D) Contract bug
Answer: B – They used centralized servers; an outage caused NFTs to display broken images.

Q13. How does Arweave achieve permanent storage?
A) Annual fees B) Storage endowment fund C) Volunteer nodes D) Government subsidy
Answer: B – A storage endowment fund pays miners perpetually to store data.

Q14. What is the primary centralization risk with IPFS gateways?
A) High costs B) Slow speeds C) Gateway downtime breaks NFTs D) Privacy leaks
Answer: C – Most users rely on centralized gateways; downtime makes NFTs appear broken.

Q15. What determines rarity in NFT collections?
A) Token ID number B) Mint date C) Trait frequency D) File size
Answer: C – Rarity is determined by trait frequency distribution; rarer traits increase value.

Quiz (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]

Quiz (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss

Quiz (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss
Answer: C – Mutable metadata allows owners to update `tokenURI`, risking rug pulls.

Q18. How can buyers verify if metadata is immutable?
A) Check file size B) Audit smart contract code C) Ask on Discord D) Check token price

Quiz (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss
Answer: C – Mutable metadata allows owners to update `tokenURI`, risking rug pulls.

Q18. How can buyers verify if metadata is immutable?
A) Check file size B) Audit smart contract code C) Ask on Discord D) Check token price
Answer: B – Review contract code for `setTokenURI()` functions and verify ownership is renounced.

Q19. What best practice ensures metadata redundancy?
A) Multiple wallets B) Pin to multiple services C) Daily backups D) Cloud storage

Quiz (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss
Answer: C – Mutable metadata allows owners to update `tokenURI`, risking rug pulls.

Q18. How can buyers verify if metadata is immutable?
A) Check file size B) Audit smart contract code C) Ask on Discord D) Check token price
Answer: B – Review contract code for `setTokenURI()` functions and verify ownership is renounced.

Q19. What best practice ensures metadata redundancy?
A) Multiple wallets B) Pin to multiple services C) Daily backups D) Cloud storage
Answer: B – Pin to multiple services (e.g., IPFS + Arweave) for redundancy.

Q20. What happens if all pinning services stop hosting an IPFS file?
A) File becomes encrypted B) File may disappear C) File moves to Arweave D) File is cached

Quiz (16–20)

Q16. Which URI format is used for Arweave storage?
A) ipfs://[CID] B) ar://[Transaction ID] C) http://arweave.com/[ID] D) aws://[Bucket]
Answer: B – Arweave uses `ar://[Transaction ID]` format for permanent storage.

Q17. What is the risk of mutable metadata in NFTs?
A) Higher gas fees B) Slower transactions C) Owner can change artwork D) Privacy loss
Answer: C – Mutable metadata allows owners to update `tokenURI`, risking rug pulls.

Q18. How can buyers verify if metadata is immutable?
A) Check file size B) Audit smart contract code C) Ask on Discord D) Check token price
Answer: B – Review contract code for `setTokenURI()` functions and verify ownership is renounced.

Q19. What best practice ensures metadata redundancy?
A) Multiple wallets B) Pin to multiple services C) Daily backups D) Cloud storage
Answer: B – Pin to multiple services (e.g., IPFS + Arweave) for redundancy.

Q20. What happens if all pinning services stop hosting an IPFS file?
A) File becomes encrypted B) File may disappear C) File moves to Arweave D) File is cached
Answer: B – Without any node pinning the file, it can be garbage collected and lost forever.

L23: NFT Marketplaces

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Compare business models of major NFT marketplaces (OpenSea, Blur, Rarible)
- Explain listing mechanics and order book systems
- Analyze marketplace fees and royalty enforcement debates
- Detect wash trading and market manipulation patterns
- Evaluate the role of aggregators in NFT trading

NFT Marketplace Landscape

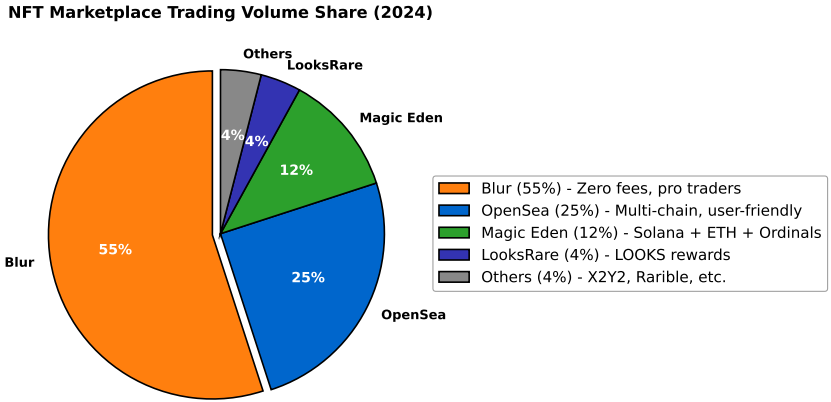
Major Platforms (by Volume, 2024):

1. **OpenSea:** Largest NFT marketplace, multi-chain support
2. **Blur:** Pro trader-focused, zero marketplace fees
3. **Magic Eden:** Solana-native, expanding to Ethereum
4. **Rarible:** Community-governed, aggregator model

Market Consolidation:

- OpenSea and Blur dominate Ethereum NFT trading (¿80% volume)
- Smaller marketplaces compete on fees, rewards, and niche communities

Marketplace Market Share (2024)



Blur overtook OpenSea in 2023 via zero fees and trader incentives

OpenSea: The Market Leader

Founded: 2017, valued at $13.3B (2022 peak)

Key Features:

- Multi-chain support (Ethereum, Polygon, Arbitrum, Optimism)
- User-friendly interface for creators and collectors
- Lazy minting (create NFTs without upfront gas costs)

Business Model:

- **Marketplace fee:** 2.5% historically, now optional 0.5%
- **Creator royalties:** Optional enforcement (formerly mandatory)
- **Revenue:** $2.7B cumulative fees (as of 2024)

(c) Joerg Osterrieder 2025

Blur: The Pro Trader Platform

Launched: October 2022, rapid growth via airdrop incentives

Key Features:

- **Zero marketplace fees:** No commission on trades
- **Advanced trading tools:** Portfolio management, sweeping, sniping
- **Bid pools:** Aggregated liquidity for collection-wide offers
- **Airdrop rewards:** BLUR token distributed to active traders

Impact: Surpassed OpenSea in volume during 2023, forced industry fee reductions

Listing Mechanics: Fixed Price vs. Auction

Fixed Price Listings:

- Seller sets a “Buy Now” price
- Instant settlement (no waiting period)
- Most common listing type (¿90% of listings)

Auction Listings:

- **English Auction:** Ascending bids, highest bidder wins
- **Dutch Auction:** Descending price until buyer accepts
- Used for high-value or uncertain pricing

Offer System:

- Buyers submit offers below listing price
- Common for negotiation and floor sniping

(c) Joerg Osterrieder 2025

Order Book and Off-Chain Matching

Traditional Order Book:

- Centralized database of buy/sell orders
- Matching engine pairs buyers and sellers
- Settlement on-chain when trade executes

OpenSea Seaport Protocol:

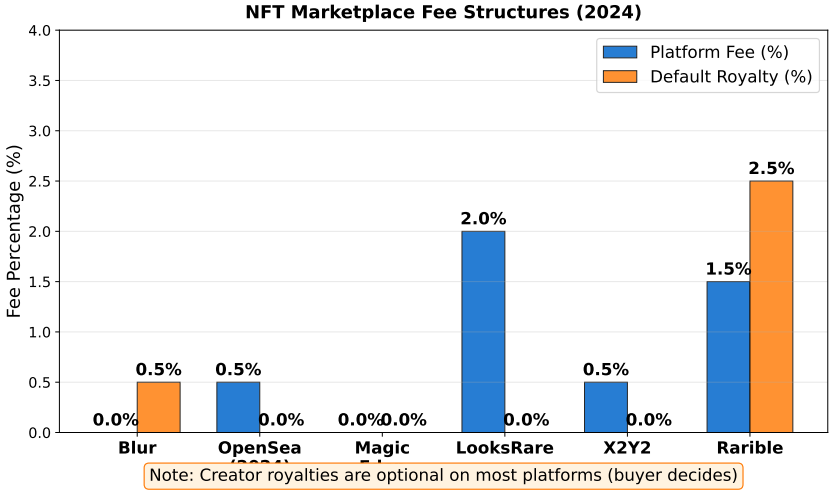
- **Off-chain orders:** Listings signed off-chain (no gas cost)
- **On-chain settlement:** Trade executes when matched
- **Gas savings:** Sellers pay no gas until sale completes

Blur's Bid Pools:

- Aggregated collection-wide offers
- Sellers can accept best available bid instantly

(c) Joerg Osterrieder 2025

Marketplace Fee Comparison



Race to zero fees to attract volume; creator royalties now optional

The Royalty Enforcement Debate

Creator Royalties: Percentage paid to original creator on secondary sales

Historical Model (2017-2022):

- Marketplaces enforced creator-set royalties (2-10% typical)
- Revenue stream for artists and projects

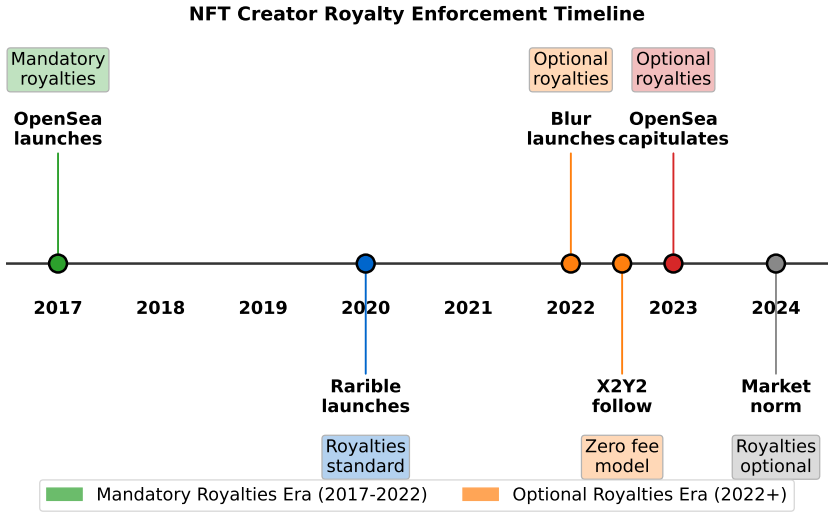
Shift to Optional Royalties (2022+):

- Blur launched with optional royalties (0.5% default)
- OpenSea capitulated in 2023 (optional royalties)

Arguments:

- **For optional:** Buyer freedom, lower transaction costs
- **Against:** Undermines creator compensation model

Royalty Enforcement Timeline



2022 marked the shift from mandatory to optional creator royalties

On-Chain Royalty Enforcement

Technical Challenge: Smart contracts cannot force royalty payments

Why Royalties Are Not Enforceable:

- ERC-721 standard has no royalty mechanism
- Buyers can transfer NFTs directly (peer-to-peer) without marketplace
- Marketplaces voluntarily honor royalties (not protocol-enforced)

ERC-2981 Royalty Standard:

- On-chain royalty information (creator address, percentage)
- Marketplaces can query but not forced to enforce

Experimental Solutions:

- **Operator Filter Registry:** Blocks transfers via non-compliant marketplaces
- **ERC-721C:** Programmable transfer restrictions in contract

Wash Trading: Artificial Volume

Wash Trading: Buyer and seller are the same entity (self-trading)

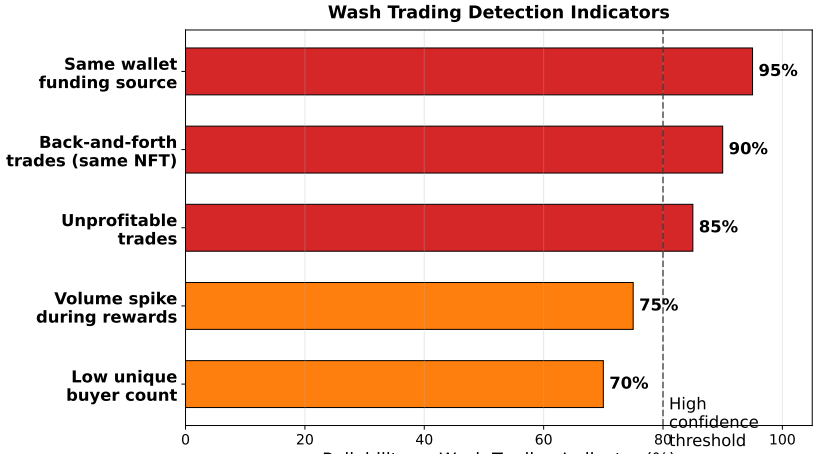
Motivation:

- Inflate collection volume and visibility
- Manipulate floor price upward
- Farm marketplace reward tokens (e.g., LooksRare, X2Y2)

Mechanics:

1. Trader owns NFT in Wallet A
2. Trader buys own NFT using Wallet B
3. Net cost: Marketplace fees + gas (often subsidized by rewards)

Wash Trading Detection



Tools: Nansen wallet analysis, Dune Analytics SQL queries, Chainalysis forensics

Wallet clustering and funding source analysis are most reliable indicators

Wash Trading Case Study: LooksRare (2022)

LooksRare Launch Strategy:

- Reward traders with LOOKS tokens based on volume
- Incentivize switching from OpenSea (vampire attack)

Unintended Consequence:

- Traders wash traded to farm LOOKS rewards
- Daily volume surged to $400M+ (mostly wash trading)
- Organic volume remained low (¡10% of reported volume)

Analysis (Chainalysis, 2022):

- Estimated 95% of LooksRare volume was wash trading
- Single wallet traded $23M in one day (same NFT repeatedly)

Lesson: Volume-based rewards create perverse incentives for manipulation

NFT Aggregators

Aggregator: Platform that sources listings from multiple marketplaces

Major Aggregators:

- **Gem (acquired by OpenSea):** Multi-marketplace sweeping
- **Genie (acquired by Uniswap):** NFT shopping cart
- **Blur:** Hybrid marketplace/aggregator

Benefits:

- Best price discovery (compare across platforms)
- Batch buying (sweep floor listings efficiently)
- Single interface for multiple marketplaces

Impact: Reduces marketplace lock-in, pressures fees downward

Floor Price Dynamics

Floor Price: Lowest listed price for any NFT in a collection

Why Floor Price Matters:

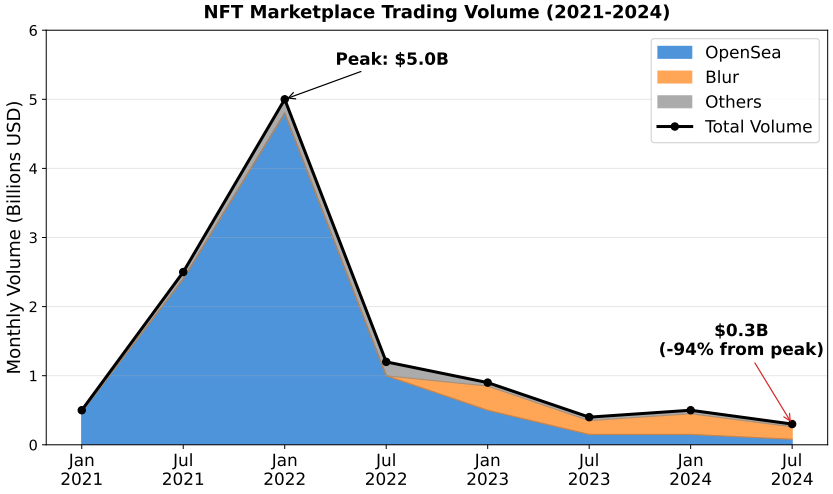
- Proxy for collection value and market sentiment
- Entry point for new buyers ("buying the floor")
- Psychological support level (panic selling if broken)

Floor Price Manipulation:

- **Artificial support:** Whales buy floor listings to prevent drops
- **Floor sweeping:** Coordinated buying to create FOMO

Healthier Metrics: Median price, 7-day sales volume, unique holder count

NFT Trading Volume Trends



Market down 90%+ from 2021 peak; Blur dominant since late 2022

Marketplace Security and Scams

Common NFT Marketplace Scams:

1. **Phishing sites:** Fake marketplace clones steal wallet signatures
2. **Malicious approvals:** Trick users into approving scam contracts
3. **Fake collections:** Counterfeit versions of popular NFTs
4. **Airdrop scams:** Fake NFTs with malicious links

Protection Measures:

- Verify marketplace URL (bookmark official sites)
- Check collection verification badge
- Review smart contract permissions before signing
- Revoke unused approvals (revoke.cash)

Cross-Chain NFT Trading

Multi-Chain Expansion:

- **Ethereum:** Dominant NFT ecosystem (70%+ market share)
- **Solana:** Low fees, fast transactions (Magic Eden)
- **Polygon:** Ethereum sidechain (gasless minting on OpenSea)
- **Base:** Coinbase L2 (emerging NFT activity)

Challenges:

- Fragmented liquidity across chains
- Bridge risks (cross-chain NFT transfers)
- Ecosystem lock-in (wallets, tools, communities)

(c) Joerg Osterrieder 2025

OpenSea Seaport: Open Protocol

Seaport (2022): Open-source NFT marketplace protocol

Key Features:

- **Permissionless:** Anyone can build marketplace frontends
- **Advanced order types:** Criteria-based, partial fills, bundles
- **Gas optimization:** Efficient settlement mechanisms
- **No protocol fees:** Frontends set their own fees

Strategic Intent:

- Commoditize marketplace infrastructure
- Compete on UX and features (not protocol lock-in)

Adoption: Coinbase NFT, GameStop NFT use Seaport protocol

Key Takeaways

1. NFT marketplaces compete on fees, features, and trader incentives
2. Blur dominates (55%+ volume) via zero fees and pro trader tools
3. Marketplace fees dropped to 0-2.5%; creator royalties now mostly optional
4. Wash trading inflates volume for rewards (detection via wallet analysis)
5. NFT market down 90%+ from peak; focus shifting to utility NFTs
6. Aggregators commoditize marketplaces, forcing fee competition

(c) Joerg Osterrieder 2025

Discussion Questions

1. Should NFT marketplaces enforce creator royalties, or should they be optional?
2. How can platforms balance trader incentives (low fees) with sustainability?
3. What measures can effectively prevent wash trading without harming legitimate users?
4. Will aggregators eventually commoditize all NFT marketplaces?
5. How does the shift to zero fees impact the long-term viability of NFT marketplaces?

Next Lesson Preview

L24: Lab – OpenSea Analysis

Hands-on activities:

- Browse and analyze NFT collections on OpenSea
- Extract and decode metadata from IPFS
- Track floor price movements and sales volume
- Use rarity tools to evaluate NFT traits
- Develop investment evaluation framework

Preparation: Create MetaMask wallet, explore OpenSea collections

Quiz Questions (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees (down from mandatory 2.5%).

Q4. Which listing type represents over 90% of NFT marketplace listings?
A) English auction B) Dutch auction C) Fixed price D) Offer system
Answer: C – Fixed price "Buy Now" listings are most common for instant settlement.

Q5. What is the main advantage of off-chain order matching in Seaport protocol?
A) Faster transactions B) No gas cost for listings C) Higher security D) Lower fees
Answer: B – Off-chain orders save gas; sellers only pay gas when sale completes.

Quiz Questions (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards (e.g., LooksRare LOOKS tokens).

Q9. What percentage of LooksRare's initial volume was estimated to be wash trading?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% of LooksRare volume was wash trading in 2022.

Q10. Which detection method is most reliable for identifying wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading; funding source analysis confirms links.

Quiz Questions (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools
Answer: B – Bid pools aggregate collection-wide offers for instant seller acceptance.

Q14. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base
Answer: C – Ethereum maintains 70%+ NFT market share despite multi-chain expansion.

Q15. What is the ERC-2981 standard designed for?
A) NFT metadata B) Royalty information C) Auction mechanics D) Cross-chain transfers
Answer: B – ERC-2981 provides on-chain royalty info, but enforcement remains optional.

Quiz Questions (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors
Answer: C – Seaport commoditizes marketplace infrastructure to compete on UX, not protocol lock-in.

Q19. How much has the NFT market declined from its 2021 peak?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – NFT trading volume is down over 90% from 2021 peak levels.

Q20. Which tool can users use to revoke unused smart contract approvals?
A) Etherscan B) MetaMask C) revoke.cash D) OpenSea
Answer: C – revoke.cash allows users to revoke unnecessary token/NFT approvals for security.

L23: NFT Marketplaces

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Compare business models of major NFT marketplaces (OpenSea, Blur, Rarible)
- Explain listing mechanics and order book systems
- Analyze marketplace fees and royalty enforcement debates
- Detect wash trading and market manipulation patterns
- Evaluate the role of aggregators in NFT trading

The Problem: How do marketplace economics work?

The Challenge
How do marketplaces create and capture value in a permissionless system where users can trade peer-to-peer without intermediaries? NFT marketplaces must balance platform sustainability with competitive pressure.

Why It Matters

- Marketplaces extract value through fees but can censor or deplatform
- 2022–2023: Blur's zero-fee model forced OpenSea to drop fees from 2.5% to 0.5%
- Royalty enforcement collapsed – creators lost recurring revenue streams

What We Need

- Sustainable revenue model without platform lock-in
- Fair value distribution between platform, creators, and traders
- Credible commitment to enforce creator royalties

The Cryptoeconomics Question
How can marketplaces align platform incentives with creator and user interests when competition drives fees to zero?

Today's lesson: How NFT Marketplaces addresses this challenge

NFT Marketplace Landscape

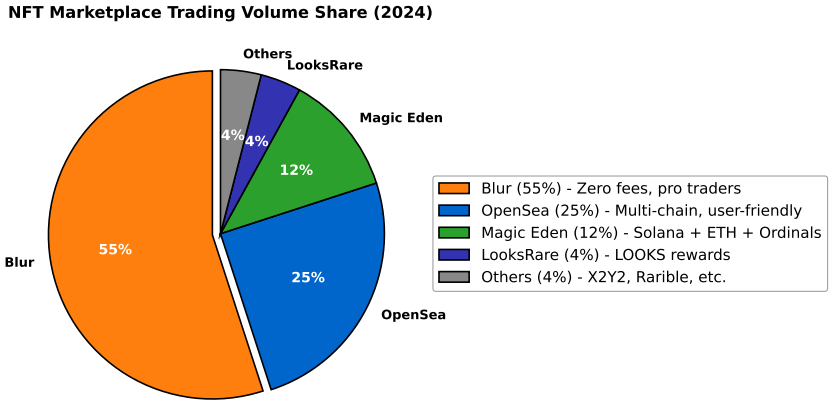
Major Platforms (by Volume, 2024):

1. **OpenSea:** Largest NFT marketplace, multi-chain support
2. **Blur:** Pro trader-focused, zero marketplace fees
3. **Magic Eden:** Solana-native, expanding to Ethereum
4. **Rarible:** Community-governed, aggregator model

Market Consolidation:

- OpenSea and Blur dominate Ethereum NFT trading (¿80% volume)
- Smaller marketplaces compete on fees, rewards, and niche communities

Marketplace Market Share (2024)



Blur overtook OpenSea in 2023 via zero fees and trader incentives

OpenSea: The Market Leader

Founded: 2017, valued at $13.3B (2022 peak)

Key Features:

- Multi-chain support (Ethereum, Polygon, Arbitrum, Optimism)
- User-friendly interface for creators and collectors
- Lazy minting (create NFTs without upfront gas costs)

Business Model:

- **Marketplace fee:** 2.5% historically, now optional 0.5%
- **Creator royalties:** Optional enforcement (formerly mandatory)
- **Revenue:** $2.7B cumulative fees (as of 2024)

(c) Joerg Osterrieder 2025

Blur: The Pro Trader Platform

Launched: October 2022, rapid growth via airdrop incentives

Key Features:

- **Zero marketplace fees:** No commission on trades
- **Advanced trading tools:** Portfolio management, sweeping, sniping
- **Bid pools:** Aggregated liquidity for collection-wide offers
- **Airdrop rewards:** BLUR token distributed to active traders

Impact: Surpassed OpenSea in volume during 2023, forced industry fee reductions

Listing Mechanics: Fixed Price vs. Auction

Fixed Price Listings:

- Seller sets a “Buy Now” price
- Instant settlement (no waiting period)
- Most common listing type (¿90% of listings)

Auction Listings:

- **English Auction:** Ascending bids, highest bidder wins
- **Dutch Auction:** Descending price until buyer accepts
- Used for high-value or uncertain pricing

Offer System:

- Buyers submit offers below listing price
- Common for negotiation and floor sniping

(c) Joerg Osterrieder 2025

Order Book and Off-Chain Matching

Traditional Order Book:

- Centralized database of buy/sell orders
- Matching engine pairs buyers and sellers
- Settlement on-chain when trade executes

OpenSea Seaport Protocol:

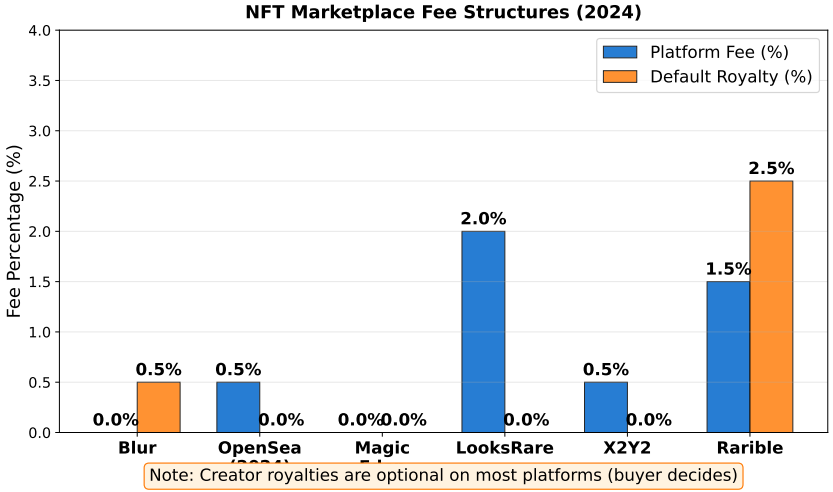
- **Off-chain orders:** Listings signed off-chain (no gas cost)
- **On-chain settlement:** Trade executes when matched
- **Gas savings:** Sellers pay no gas until sale completes

Blur's Bid Pools:

- Aggregated collection-wide offers
- Sellers can accept best available bid instantly

(c) Joerg Osterrieder 2025

Marketplace Fee Comparison



Race to zero fees to attract volume; creator royalties now optional

The Royalty Enforcement Debate

Creator Royalties: Percentage paid to original creator on secondary sales

Historical Model (2017-2022):

- Marketplaces enforced creator-set royalties (2-10% typical)
- Revenue stream for artists and projects

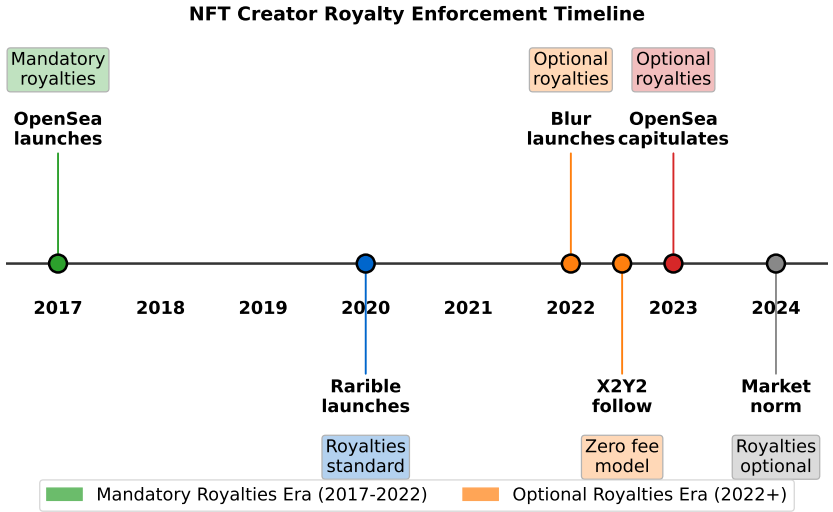
Shift to Optional Royalties (2022+):

- Blur launched with optional royalties (0.5% default)
- OpenSea capitulated in 2023 (optional royalties)

Arguments:

- **For optional:** Buyer freedom, lower transaction costs
- **Against:** Undermines creator compensation model

Royalty Enforcement Timeline



2022 marked the shift from mandatory to optional creator royalties

On-Chain Royalty Enforcement

Technical Challenge: Smart contracts cannot force royalty payments

Why Royalties Are Not Enforceable:

- ERC-721 standard has no royalty mechanism
- Buyers can transfer NFTs directly (peer-to-peer) without marketplace
- Marketplaces voluntarily honor royalties (not protocol-enforced)

ERC-2981 Royalty Standard:

- On-chain royalty information (creator address, percentage)
- Marketplaces can query but not forced to enforce

Experimental Solutions:

- **Operator Filter Registry:** Blocks transfers via non-compliant marketplaces
- **ERC-721C:** Programmable transfer restrictions in contract

Wash Trading: Artificial Volume

Wash Trading: Buyer and seller are the same entity (self-trading)

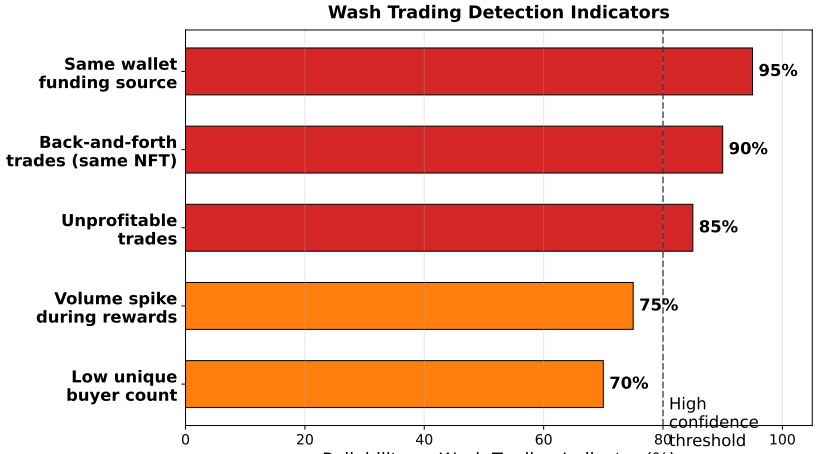
Motivation:

- Inflate collection volume and visibility
- Manipulate floor price upward
- Farm marketplace reward tokens (e.g., LooksRare, X2Y2)

Mechanics:

1. Trader owns NFT in Wallet A
2. Trader buys own NFT using Wallet B
3. Net cost: Marketplace fees + gas (often subsidized by rewards)

Wash Trading Detection



Tools: Nansen wallet analysis, Dune Analytics SQL queries, Chainalysis forensics

Wallet clustering and funding source analysis are most reliable indicators

Wash Trading Case Study: LooksRare (2022)

LooksRare Launch Strategy:

- Reward traders with LOOKS tokens based on volume
- Incentivize switching from OpenSea (vampire attack)

Unintended Consequence:

- Traders wash traded to farm LOOKS rewards
- Daily volume surged to $400M+ (mostly wash trading)
- Organic volume remained low (¡10% of reported volume)

Analysis (Chainalysis, 2022):

- Estimated 95% of LooksRare volume was wash trading
- Single wallet traded $23M in one day (same NFT repeatedly)

Lesson: Volume-based rewards create perverse incentives for manipulation

NFT Aggregators

Aggregator: Platform that sources listings from multiple marketplaces

Major Aggregators:

- **Gem (acquired by OpenSea):** Multi-marketplace sweeping
- **Genie (acquired by Uniswap):** NFT shopping cart
- **Blur:** Hybrid marketplace/aggregator

Benefits:

- Best price discovery (compare across platforms)
- Batch buying (sweep floor listings efficiently)
- Single interface for multiple marketplaces

Impact: Reduces marketplace lock-in, pressures fees downward

Floor Price Dynamics

Floor Price: Lowest listed price for any NFT in a collection

Why Floor Price Matters:

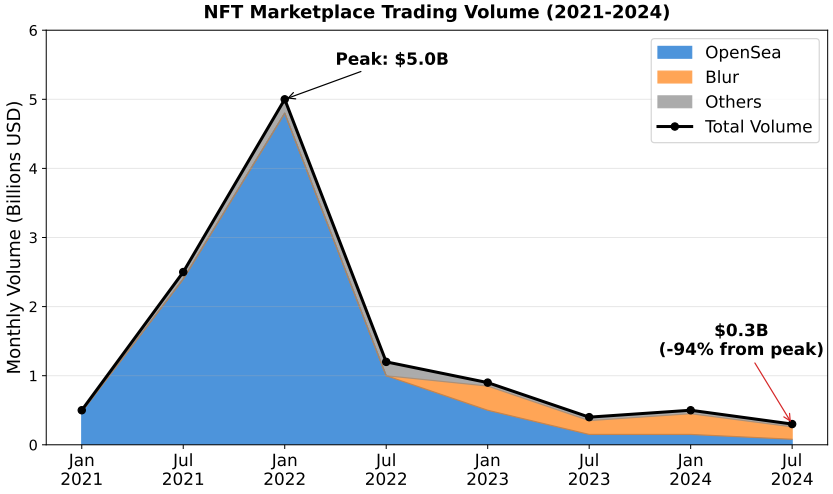
- Proxy for collection value and market sentiment
- Entry point for new buyers ("buying the floor")
- Psychological support level (panic selling if broken)

Floor Price Manipulation:

- **Artificial support:** Whales buy floor listings to prevent drops
- **Floor sweeping:** Coordinated buying to create FOMO

Healthier Metrics: Median price, 7-day sales volume, unique holder count

NFT Trading Volume Trends



Market down 90%+ from 2021 peak; Blur dominant since late 2022

Marketplace Security and Scams

Common NFT Marketplace Scams:

1. **Phishing sites:** Fake marketplace clones steal wallet signatures
2. **Malicious approvals:** Trick users into approving scam contracts
3. **Fake collections:** Counterfeit versions of popular NFTs
4. **Airdrop scams:** Fake NFTs with malicious links

Protection Measures:

- Verify marketplace URL (bookmark official sites)
- Check collection verification badge
- Review smart contract permissions before signing
- Revoke unused approvals (revoke.cash)

Cross-Chain NFT Trading

Multi-Chain Expansion:

- **Ethereum:** Dominant NFT ecosystem (70%+ market share)
- **Solana:** Low fees, fast transactions (Magic Eden)
- **Polygon:** Ethereum sidechain (gasless minting on OpenSea)
- **Base:** Coinbase L2 (emerging NFT activity)

Challenges:

- Fragmented liquidity across chains
- Bridge risks (cross-chain NFT transfers)
- Ecosystem lock-in (wallets, tools, communities)

(c) Joerg Osterrieder 2025

OpenSea Seaport: Open Protocol

Seaport (2022): Open-source NFT marketplace protocol

Key Features:

- **Permissionless:** Anyone can build marketplace frontends
- **Advanced order types:** Criteria-based, partial fills, bundles
- **Gas optimization:** Efficient settlement mechanisms
- **No protocol fees:** Frontends set their own fees

Strategic Intent:

- Commoditize marketplace infrastructure
- Compete on UX and features (not protocol lock-in)

Adoption: Coinbase NFT, GameStop NFT use Seaport protocol

Problem Solved? NFT Marketplaces

The Original Problem

How do marketplace economics work in a permissionless system?

How NFT Marketplaces Solves It

- **Auction mechanisms:** English, Dutch, and reserve auctions enable price discovery
- **Off-chain order matching:** Seaport protocol reduces gas costs for listings
- **Royalty standards (EIP-2981):** On-chain royalty information for creator compensation

Remaining Limitations

- **Royalty enforcement:** Not enforceable on-chain; buyers can bypass marketplaces
- **Wash trading:** Volume-based rewards create perverse incentives for self-trading
- **Fee competition:** Race to zero fees undermines platform sustainability

Open Questions

- Will decentralized marketplaces (e.g., sudoswap AMMs) displace centralized ones?
- Can programmable transfer restrictions (ERC-721C) enforce royalties without compromising composability?

NFT Marketplaces partially solves marketplace economics but introduces sustainability and enforcement trade-offs

Key Takeaways

1. NFT marketplaces compete on fees, features, and trader incentives
2. Blur dominates (55%+ volume) via zero fees and pro trader tools
3. Marketplace fees dropped to 0-2.5%; creator royalties now mostly optional
4. Wash trading inflates volume for rewards (detection via wallet analysis)
5. NFT market down 90%+ from peak; focus shifting to utility NFTs
6. Aggregators commoditize marketplaces, forcing fee competition

(c) Joerg Osterrieder 2025

Discussion Questions

1. Should NFT marketplaces enforce creator royalties, or should they be optional?
2. How can platforms balance trader incentives (low fees) with sustainability?
3. What measures can effectively prevent wash trading without harming legitimate users?
4. Will aggregators eventually commoditize all NFT marketplaces?
5. How does the shift to zero fees impact the long-term viability of NFT marketplaces?

Next Lesson Preview

L24: Lab – OpenSea Analysis

Hands-on activities:

- Browse and analyze NFT collections on OpenSea
- Extract and decode metadata from IPFS
- Track floor price movements and sales volume
- Use rarity tools to evaluate NFT traits
- Develop investment evaluation framework

Preparation: Create MetaMask wallet, explore OpenSea collections

Quiz Questions (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees (down from mandatory 2.5%).

Q4. Which listing type represents over 90% of NFT marketplace listings?
A) English auction B) Dutch auction C) Fixed price D) Offer system
Answer: C – Fixed price "Buy Now" listings are most common for instant settlement.

Q5. What is the main advantage of off-chain order matching in Seaport protocol?
A) Faster transactions B) No gas cost for listings C) Higher security D) Lower fees
Answer: B – Off-chain orders save gas; sellers only pay gas when sale completes.

Quiz Questions (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards (e.g., LooksRare LOOKS tokens).

Q9. What percentage of LooksRare's initial volume was estimated to be wash trading?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% of LooksRare volume was wash trading in 2022.

Q10. Which detection method is most reliable for identifying wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading; funding source analysis confirms links.

Quiz Questions (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools
Answer: B – Bid pools aggregate collection-wide offers for instant seller acceptance.

Q14. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base
Answer: C – Ethereum maintains 70%+ NFT market share despite multi-chain expansion.

Q15. What is the ERC-2981 standard designed for?
A) NFT metadata B) Royalty information C) Auction mechanics D) Cross-chain transfers
Answer: B – ERC-2981 provides on-chain royalty info, but enforcement remains optional.

Quiz Questions (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors
Answer: C – Seaport commoditizes marketplace infrastructure to compete on UX, not protocol lock-in.

Q19. How much has the NFT market declined from its 2021 peak?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – NFT trading volume is down over 90% from 2021 peak levels.

Q20. Which tool can users use to revoke unused smart contract approvals?
A) Etherscan B) MetaMask C) revoke.cash D) OpenSea
Answer: C – revoke.cash allows users to revoke unnecessary token/NFT approvals for security.

L23: NFT Marketplaces

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Marketplace fee comparison

[COMIC: placeholder]

Two NFT marketplaces as competing storefronts: OpenSea with a "2.5% Fee" sign being frantically crossed out and replaced with "0.5%!!" while Blur next door smugly displays "0% FEES + FREE TOKENS" with a line of traders rushing in.

The Fee Race to Zero

- OpenSea: 2.5% $\rightarrow$ 0.5% (forced by competition)
- Blur: 0% fees + token incentives
- Who pays when fees hit zero?

What We'll Explore

- Marketplace business models
- Royalty enforcement collapse
- Wash trading and manipulation

When fees go to zero, value extraction shifts elsewhere

Learning Objectives

By the end of this lesson, you will be able to:

- Compare business models of major NFT marketplaces (OpenSea, Blur, Rarible)
- Explain listing mechanics and order book (list matching buy and sell orders) systems
- Analyze marketplace fees and royalty enforcement debates
- Detect wash trading (self-trading to fake volume) and market manipulation patterns
- Evaluate the role of aggregators (platforms combining multiple marketplaces) in NFT trading

Building on L22: NFT Metadata and IPFS

The Problem: How do marketplace economics work?

The Challenge
How do marketplaces create and capture value in a permissionless system where users can trade peer-to-peer without intermediaries? NFT marketplaces must balance platform sustainability with competitive pressure.

Why It Matters

- Marketplaces extract value through fees but can censor or deplatform
- 2022–2023: Blur's zero-fee model (no commission on trades) forced OpenSea to drop fees from 2.5% to 0.5%
- Royalty enforcement collapsed – creators lost recurring revenue streams

What We Need

- Sustainable revenue model without platform lock-in
- Fair value distribution between platform, creators, and traders
- Credible commitment to enforce creator royalties

The Cryptoeconomics Question
How can marketplaces align platform incentives with creator and user interests when competition drives fees to zero?

Today's lesson: How NFT Marketplaces addresses this challenge

Which NFT Marketplaces Dominate Trading?

Major Platforms (by Volume, 2024):

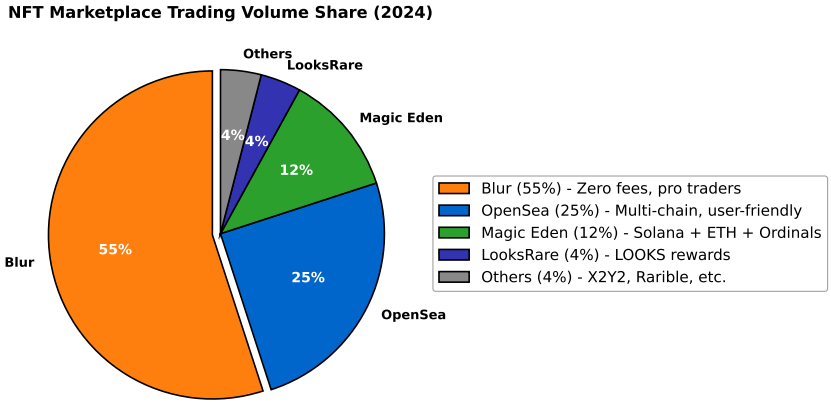
1. **OpenSea:** Largest NFT marketplace, multi-chain support
2. **Blur:** Pro trader-focused, zero marketplace fees
3. **Magic Eden:** Solana-native, expanding to Ethereum
4. **Rarible:** Community-governed, aggregator model

Market Consolidation:

- OpenSea and Blur dominate Ethereum NFT trading (¿80% volume)
- Smaller marketplaces compete on fees, rewards, and niche communities

→ *Problem: How do marketplace economics work? — NFT Marketplace Landscape: Marketplaces compete by reducing fees, but zero fees are unsustainable—who pays for development?*

Marketplace Market Share (2024)



Blur overtook OpenSea in 2023 via zero fees and trader incentives

What Makes OpenSea the Market Leader?

Founded: 2017, valued at $13.3B (2022 peak)

Key Features:

- Multi-chain support (Ethereum, Polygon, Arbitrum, Optimism)
- User-friendly interface for creators and collectors
- Lazy minting (NFT creation without upfront gas) (create NFTs without upfront gas costs)

Business Model:

- **Marketplace fee:** 2.5% historically, now optional 0.5%
- **Creator royalties:** Optional enforcement (formerly mandatory)
- **Revenue:** $2.7B cumulative fees (as of 2024)

Why Did Blur Overtake OpenSea?

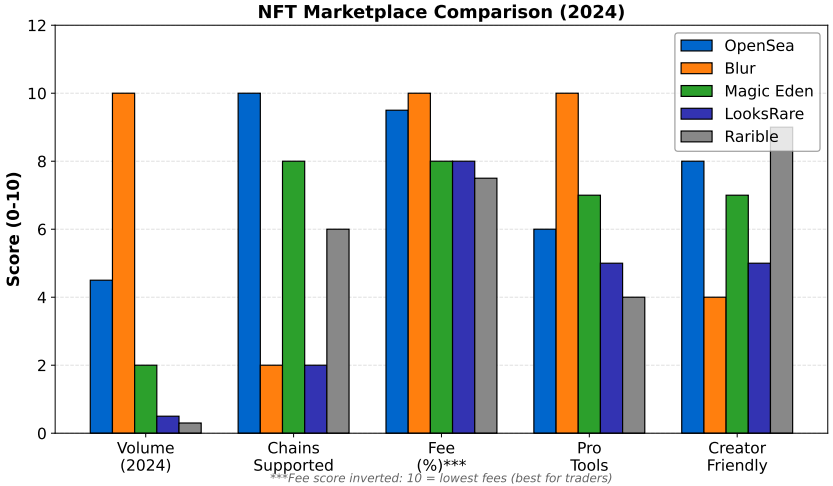
Launched: October 2022, rapid growth via airdrop incentives

Key Features:

- **Zero marketplace fees:** No commission on trades
- **Advanced trading tools:** Portfolio management, sweeping (bulk-buying floor-priced NFTs), sniping
- **Bid pools (aggregated buyer offers):** Aggregated liquidity for collection-wide offers
- **Airdrop rewards:** BLUR token distributed to active traders

Impact: Surpassed OpenSea in volume during 2023, forced industry fee reductions

How Do OpenSea and Blur Compare?



Blur leads on volume and fees; OpenSea leads on multi-chain and creator support

How Do Listing Mechanisms Work?

Fixed Price Listings:

- Seller sets a "Buy Now" price
- Instant settlement (no waiting period)
- Most common listing type (¿90% of listings)

Auction Listings:

- **English Auction:** Ascending bids, highest bidder wins
- **Dutch Auction (price drops until sold):** Descending price until buyer accepts
- Used for high-value or uncertain pricing

Offer System:

- Buyers submit offers below listing price
- Common for negotiation and floor sniping

→ *Problem: How do marketplace economics work? — Listing Mechanics: Fixed Price vs. Auction: Fixed prices favor sellers; auctions favor price discovery—marketplaces must balance both.*

How Do Marketplaces Match Buyers and Sellers?

Traditional Order Book:

- Centralized database of buy/sell orders
- Matching engine pairs buyers and sellers
- Settlement on-chain when trade executes

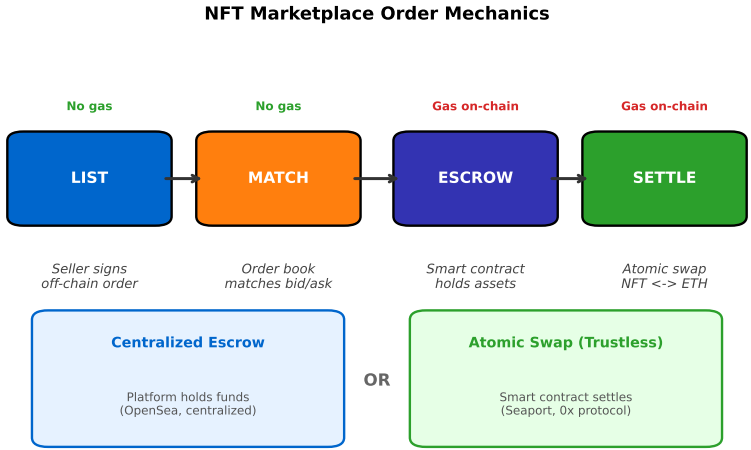
OpenSea Seaport Protocol (OpenSea's trading contracts):

- **Off-chain orders (stored off blockchain):** Listings signed off-chain (no gas cost)
- **On-chain settlement:** Trade executes when matched
- **Gas savings:** Sellers pay no gas until sale completes

Blur's Bid Pools:

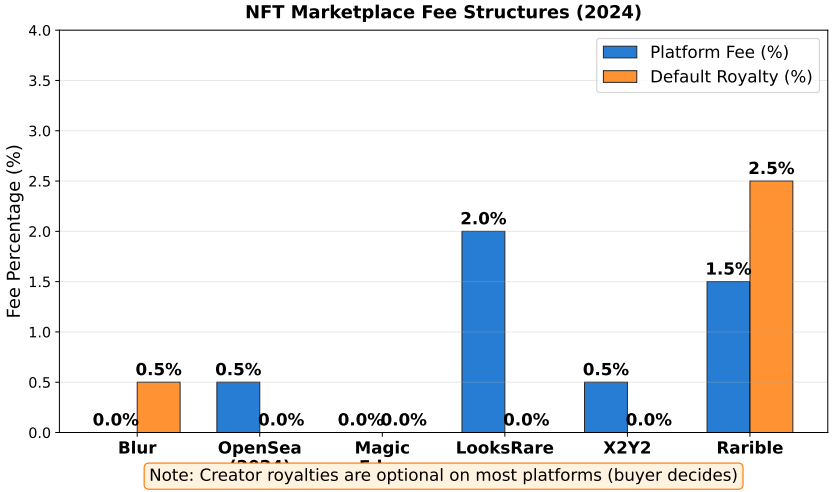
- Aggregated collection-wide offers
- Sellers can accept best available bid instantly

How Does an NFT Sale Execute?



Off-chain listings save gas; settlement uses escrow or atomic swaps

What Fees Do Marketplaces Charge?



Race to zero fees to attract volume; creator royalties now optional

Why Did Royalty Enforcement Collapse?

Creator Royalties: Percentage paid to original creator on secondary sales

Historical Model (2017-2022):

- Marketplaces enforced creator-set royalties (2-10% typical)
- Revenue stream for artists and projects

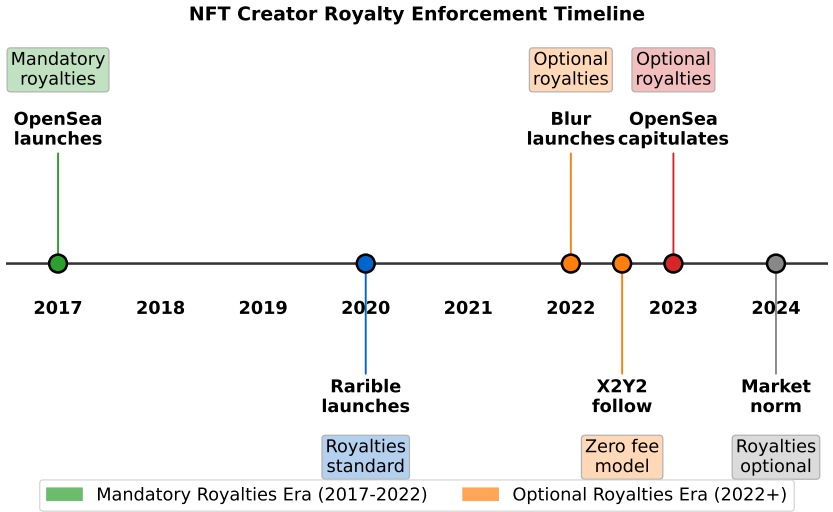
Shift to Optional Royalties (2022+):

- Blur launched with optional royalties (0.5% default)
- OpenSea capitulated in 2023 (optional royalties)

Arguments:

- **For optional:** Buyer freedom, lower transaction costs
- **Against:** Undermines creator compensation model

Royalty Enforcement Timeline



2022 marked the shift from mandatory to optional creator royalties

Problem Check-In: NFT Marketplaces

Recall Our Problem

How do marketplace economics work?

What We've Learned So Far

- Marketplaces earn revenue through fees (0-2.5%), but fee competition drives prices to zero
- Aggregators like Blur combine listings from multiple marketplaces, intensifying competition
- Zero-fee models are unsustainable; marketplaces must find alternative revenue (tokens, premium features)

Still to Address

- Royalty enforcement mechanisms and their marketplace adoption
- How can marketplaces survive long-term when fees approach zero?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do marketplace economics work?"?

Can Royalties Be Enforced On-Chain?

Technical Challenge: Smart contracts cannot force royalty payments

Why Royalties Are Not Enforceable:

- ERC-721 standard has no royalty mechanism
- Buyers can transfer NFTs directly (peer-to-peer) without marketplace
- Marketplaces voluntarily honor royalties (not protocol-enforced)

ERC-2981 Royalty Standard:

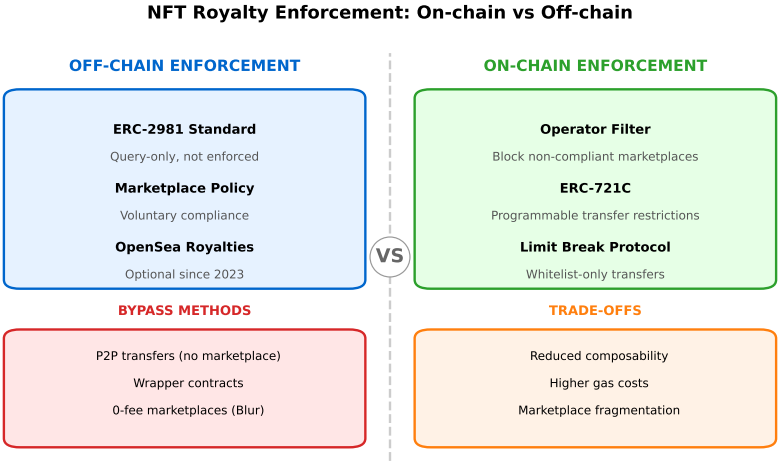
- On-chain royalty information (creator address, percentage)
- Marketplaces can query but not forced to enforce

Experimental Solutions:

- **Operator Filter (blocklist for non-royalty marketplaces) Registry:** Blocks transfers via non-compliant marketplaces
- **ERC-721C:** Programmable transfer restrictions in contract

→ *Problem: How do marketplace economics work? — On-Chain Royalty Enforcement: Royalty enforcement creates tension: creators want income, marketplaces want volume.*

How Do Royalty Enforcement Mechanisms Work?



On-chain enforcement protects creators but reduces NFT composability

How Do Traders Fake NFT Volume?

Wash Trading: Buyer and seller are the same entity (self-trading)

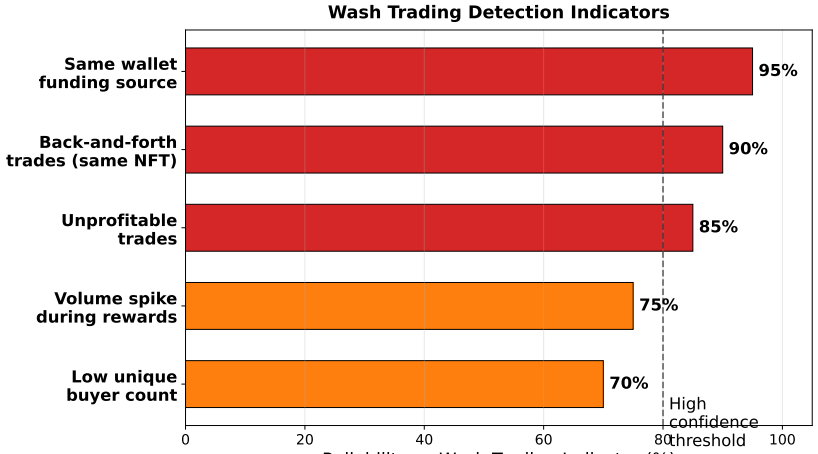
Motivation:

- Inflate collection volume and visibility
- Manipulate floor price upward
- Farm marketplace reward tokens (e.g., LooksRare, X2Y2)

Mechanics:

1. Trader owns NFT in Wallet A
2. Trader buys own NFT using Wallet B
3. Net cost: Marketplace fees + gas (often subsidized by rewards)

How Can We Detect Wash Trading?



Tools: Nansen wallet analysis, Dune Analytics SQL queries, Chainalysis forensics

Wallet clustering and funding source analysis are most reliable indicators

What Happened with LooksRare's Wash Trading?

LooksRare Launch Strategy:

- Reward traders with LOOKS tokens based on volume
- Incentivize switching from OpenSea (vampire attack - luring users with rewards)

Unintended Consequence:

- Traders wash traded to farm LOOKS rewards
- Daily volume surged to $400M+ (mostly wash trading)
- Organic volume remained low (¡10% of reported volume)

Analysis (Chainalysis, 2022):

- Estimated 95% of LooksRare volume was wash trading
- Single wallet traded $23M in one day (same NFT repeatedly)

Lesson: Volume-based rewards create perverse incentives for manipulation

How Do NFT Aggregators Work?

Aggregator: Platform that sources listings from multiple marketplaces

Major Aggregators:

- **Gem (acquired by OpenSea):** Multi-marketplace sweeping
- **Genie (acquired by Uniswap):** NFT shopping cart
- **Blur:** Hybrid marketplace/aggregator

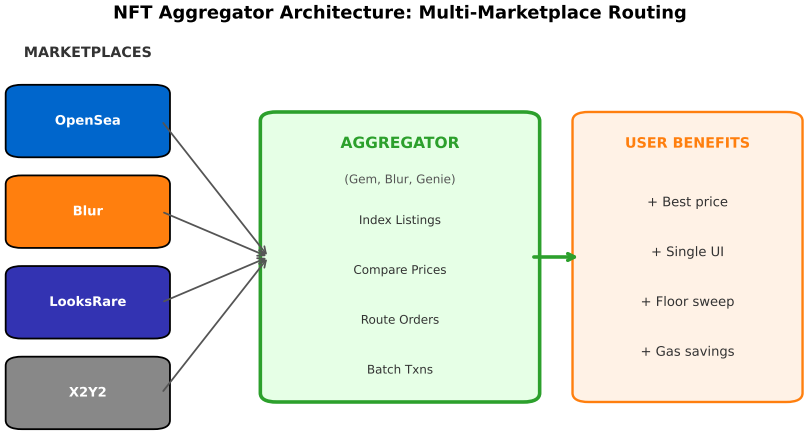
Benefits:

- Best price discovery (compare across platforms)
- Batch buying (sweep floor listings efficiently)
- Single interface for multiple marketplaces

Impact: Reduces marketplace lock-in, pressures fees downward

(c) Joerg Osterrieder 2025

How Do Aggregators Route Orders?



Example: Floor sweep finds cheapest NFTs across ALL marketplaces in one transaction

Aggregators enable best-price discovery across fragmented marketplaces

What Does Floor Price Tell You?

Floor Price: Lowest listed price for any NFT in a collection

Why Floor Price Matters:

- Proxy for collection value and market sentiment
- Entry point for new buyers ("buying the floor")
- Psychological support level (panic selling if broken)

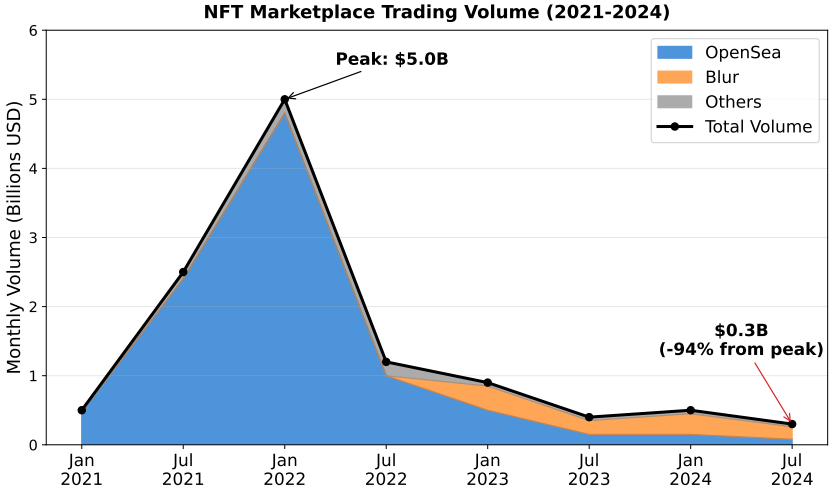
Floor Price Manipulation:

- **Artificial support:** Whales buy floor listings to prevent drops
- **Floor sweeping:** Coordinated buying to create FOMO

Healthier Metrics: Median price, 7-day sales volume, unique holder count

→ *Problem: How do marketplace economics work? — Floor Price Dynamics: Floor prices signal collection health; wash trading inflates them artificially.*

How Has NFT Trading Volume Changed?



Market down 90%+ from 2021 peak; Blur dominant since late 2022

What Scams Target NFT Marketplaces?

Common NFT Marketplace Scams:

1. **Phishing sites:** Fake marketplace clones steal wallet signatures
2. **Malicious approvals:** Trick users into approving scam contracts
3. **Fake collections:** Counterfeit versions of popular NFTs
4. **Airdrop scams:** Fake NFTs with malicious links

Protection Measures:

- Verify marketplace URL (bookmark official sites)
- Check collection verification badge
- Review smart contract permissions before signing
- Revoke unused approvals (revoke.cash)

How Does Cross-Chain NFT Trading Work?

Multi-Chain Expansion:

- **Ethereum:** Dominant NFT ecosystem (70%+ market share)
- **Solana:** Low fees, fast transactions (Magic Eden)
- **Polygon:** Ethereum sidechain (gasless minting on OpenSea)
- **Base:** Coinbase L2 (emerging NFT activity)

Challenges:

- Fragmented liquidity across chains
- Bridge risks (cross-chain NFT transfers)
- Ecosystem lock-in (wallets, tools, communities)

(c) Joerg Osterrieder 2025

What Is OpenSea Seaport?

Seaport (2022): Open-source NFT marketplace protocol

Key Features:

- **Permissionless:** Anyone can build marketplace frontends
- **Advanced order types:** Criteria-based, partial fills, bundles
- **Gas optimization:** Efficient settlement mechanisms
- **No protocol fees:** Frontends set their own fees

Strategic Intent:

- Commoditize marketplace infrastructure
- Compete on UX and features (not protocol lock-in)

Adoption: Coinbase NFT, GameStop NFT use Seaport protocol

Problem Solved? NFT Marketplaces

The Original Problem

How do marketplace economics work in a permissionless system?

How NFT Marketplaces Solves It

- **Auction mechanisms:** English, Dutch, and reserve auctions enable price discovery
- **Off-chain order matching:** Seaport protocol reduces gas costs for listings
- **Royalty standards (EIP-2981):** On-chain royalty information for creator compensation

Remaining Limitations

- **Royalty enforcement:** Not enforceable on-chain; buyers can bypass marketplaces
- **Wash trading:** Volume-based rewards create perverse incentives for self-trading
- **Fee competition:** Race to zero fees undermines platform sustainability

Open Questions

- Will decentralized marketplaces (e.g., sudoswap AMMs) displace centralized ones?
- Can programmable transfer restrictions (ERC-721C) enforce royalties without compromising composability?

NFT Marketplaces partially solves marketplace economics but introduces sustainability and enforcement trade-offs

The Economics of NFT Marketplaces

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: NFT Marketplaces

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: NFT Marketplaces

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

! Unusual economic behavior

! Incentive misalignment

! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Royalty bypass controversy

[COMIC: placeholder]

An NFT artist watching their royalty income graph plummet from "Mandatory 10%" to "Optional 0.5%" while traders celebrate "More profit for us!" The artist's thought bubble: "I created this... why don't I get paid?"

The Creator's Dilemma

- 2021: Royalties enforced (creator revenue)
- 2023: Royalties optional (trader savings)
- ERC-721 has no on-chain enforcement

The Trade-off

- Buyers: Lower costs, more flexibility
- Creators: Lost recurring revenue
- Market: Race to bottom on fees

When code can't enforce royalties, economic pressure wins

Key Takeaways

1. NFT marketplaces compete on fees, features, and trader incentives
2. Blur dominates (55%+ volume) via zero fees and pro trader tools
3. Marketplace fees dropped to 0-2.5%; creator royalties now mostly optional
4. Wash trading inflates volume for rewards (detection via wallet analysis)
5. NFT market down 90%+ from peak; focus shifting to utility NFTs
6. Aggregators commoditize marketplaces, forcing fee competition

Next Lesson: L24 – Lab: OpenSea Analysis

Discussion Questions

1. Should NFT marketplaces enforce creator royalties, or should they be optional?
2. How can platforms balance trader incentives (low fees) with sustainability?
3. What measures can effectively prevent wash trading without harming legitimate users?
4. Will aggregators eventually commoditize all NFT marketplaces?
5. How does the shift to zero fees impact the long-term viability of NFT marketplaces?

Next Lesson Preview

L24: Lab – OpenSea Analysis

Hands-on activities:

- Browse and analyze NFT collections on OpenSea
- Extract and decode metadata from IPFS
- Track floor price movements and sales volume
- Use rarity tools to evaluate NFT traits
- Develop investment evaluation framework

Preparation: Create MetaMask wallet, explore OpenSea collections

Quiz Questions (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees (down from mandatory 2.5%).

Q4. Which listing type represents over 90% of NFT marketplace listings?
A) English auction B) Dutch auction C) Fixed price D) Offer system
Answer: C – Fixed price "Buy Now" listings are most common for instant settlement.

Q5. What is the main advantage of off-chain order matching in Seaport protocol?
A) Faster transactions B) No gas cost for listings C) Higher security D) Lower fees
Answer: B – Off-chain orders save gas; sellers only pay gas when sale completes.

Quiz Questions (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards (e.g., LooksRare LOOKS tokens).

Q9. What percentage of LooksRare's initial volume was estimated to be wash trading?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% of LooksRare volume was wash trading in 2022.

Q10. Which detection method is most reliable for identifying wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading; funding source analysis confirms links.

Quiz Questions (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools
Answer: B – Bid pools aggregate collection-wide offers for instant seller acceptance.

Q14. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base
Answer: C – Ethereum maintains 70%+ NFT market share despite multi-chain expansion.

Q15. What is the ERC-2981 standard designed for?
A) NFT metadata B) Royalty information C) Auction mechanics D) Cross-chain transfers
Answer: B – ERC-2981 provides on-chain royalty info, but enforcement remains optional.

Quiz Questions (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors
Answer: C – Seaport commoditizes marketplace infrastructure to compete on UX, not protocol lock-in.

Q19. How much has the NFT market declined from its 2021 peak?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – NFT trading volume is down over 90% from 2021 peak levels.

Q20. Which tool can users use to revoke unused smart contract approvals?
A) Etherscan B) MetaMask C) revoke.cash D) OpenSea
Answer: C – revoke.cash allows users to revoke unnecessary token/NFT approvals for security.

L23: NFT Marketplaces (Condensed)

Module C: NFTs & Digital Assets – Mini-Lecture

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Compare business models of major NFT marketplaces (OpenSea, Blur)
- Understand marketplace fees and royalty enforcement debates
- Detect wash trading and market manipulation patterns
- Evaluate the impact of aggregators on NFT trading

NFT Marketplace Landscape

Major Platforms (by Volume, 2024):

1. **OpenSea:** Largest NFT marketplace, multi-chain support
2. **Blur:** Pro trader-focused, zero marketplace fees
3. **Magic Eden:** Solana-native, expanding to Ethereum

Market Consolidation:

- OpenSea and Blur dominate Ethereum NFT trading (¿80% volume)
- Smaller marketplaces compete on fees, rewards, and niche communities

Blur overtook OpenSea in 2023 via zero fees and trader incentives

OpenSea vs Blur: Key Differences

OpenSea (2017)

- Multi-chain (ETH, Polygon, Arbitrum)
- User-friendly for creators
- Lazy minting (no upfront gas)
- Fee: Optional 0.5% (was 2.5%)
- Cumulative fees: $2.7B

Blur (Oct 2022)

- Zero marketplace fees
- Advanced trading tools
- Bid pools for collection offers
- BLUR token airdrops
- 55%+ market volume

Blur's launch forced industry-wide fee reductions

Listing Mechanics: How NFT Sales Work

Fixed Price Listings (¿90% of listings):

- Seller sets "Buy Now" price; instant settlement

Auction Listings:

- English: Ascending bids, highest wins
- Dutch: Descending price until buyer accepts

Off-Chain Matching (Seaport Protocol):

- Listings signed off-chain (no gas cost for listing)
- On-chain settlement only when trade executes
- Sellers pay gas only after successful sale

Off-chain orders save significant gas costs for sellers

The Royalty Enforcement Debate

Creator Royalties: Percentage paid to original creator on secondary sales

Historical Model (2017-2022):

- Marketplaces enforced creator-set royalties (2-10%)
- Key revenue stream for artists and projects

Shift to Optional Royalties (2022+):

- Blur launched with 0.5% default; OpenSea followed in 2023
- ERC-721 has no native royalty mechanism (not enforceable on-chain)
- ERC-2981 provides royalty info, but enforcement remains optional

Technical reality: royalties are voluntary, not protocol-enforced

Wash Trading: Artificial Volume

Definition: Buyer and seller are the same entity (self-trading)

Motivation:

- Farm marketplace reward tokens (e.g., LooksRare LOOKS)
- Inflate collection volume and visibility
- Manipulate floor price upward

LooksRare Case Study (2022):

- Rewarded traders with LOOKS tokens based on volume
- Chainalysis estimated 95% of volume was wash trading
- Single wallet traded $23M in one day (same NFT repeatedly)

Detection: Wallet clustering and funding source analysis

Aggregators and Floor Price Dynamics

NFT Aggregators: Platforms sourcing listings from multiple marketplaces

- Gem (acquired by OpenSea), Genie (acquired by Uniswap)
- Benefits: Best price discovery, batch buying, single interface
- Impact: Reduces marketplace lock-in, pressures fees downward

Floor Price: Lowest listed price in a collection

- Proxy for collection value and market sentiment
- Manipulation: Whales buy floor to prevent drops ("floor sweeping")
- Better metrics: Median price, 7-day volume, unique holders

Aggregators commoditize marketplaces, forcing fee competition

Marketplace Security and Cross-Chain Trading

Common NFT Scams:

- Phishing sites (fake marketplace clones)
- Malicious approvals (trick users into signing scam contracts)
- Fake collections and airdrop scams

Protection: Verify URLs, check verification badges, use revoke.cash

Multi-Chain NFT Ecosystem:

- Ethereum: 70%+ market share (dominant ecosystem)
- Solana: Low fees, fast transactions (Magic Eden)
- L2s: Polygon, Base, Arbitrum for lower gas costs

Always review contract permissions before signing

NFT Marketplace Ecosystem

Marketplace Interface

Trading Activity

Digital Art NFTs

Images: Unsplash (CC0 License)

Key Takeaways

1. NFT marketplaces compete on fees, features, and trader incentives
2. Blur dominates (55%+ volume) via zero fees and pro trader tools
3. Creator royalties shifted from mandatory to optional (2022-2023)
4. Wash trading inflates volume for rewards – detect via wallet analysis
5. NFT market down 90%+ from 2021 peak; focus shifting to utility NFTs
6. Aggregators commoditize marketplaces, forcing fee competition

Quiz Questions (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees.

Q2. What percentage of Ethereum NFT volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of volume.

Q3. Why are creator royalties NOT technically enforceable on-chain?
A) Gas costs B) No royalty mechanism in ERC-721 C) Legal issues D) Speed
Answer: B – ERC-721 has no native royalty mechanism.

Q4. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards.

Q5. Which tool helps users revoke unused smart contract approvals?
A) Etherscan B) MetaMask C) revoke.cash D) OpenSea
Answer: C – revoke.cash allows users to revoke unnecessary approvals.

Quiz Questions (6–10)

Q6. What percentage of LooksRare's initial volume was estimated wash trading?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% was wash trading in 2022.

Q7. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale
Answer: B – Floor price is the lowest listed price for any NFT.

Q8. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base
Answer: C – Ethereum maintains 70%+ NFT market share.

Q9. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees.

Q10. What is the main advantage of off-chain order matching?
A) Faster transactions B) No gas cost for listings C) Higher security D) Lower fees
Answer: B – Off-chain orders save gas; sellers pay only when sale completes.

Further Resources

Platforms to Explore:

- OpenSea: `https://opensea.io`
- Blur: `https://blur.io`
- Magic Eden: `https://magiceden.io`

Analytics and Tools:

- Dune Analytics NFT dashboards
- revoke.cash for approval management
- NFT Floor for price tracking

Next Lesson: L24 Lab – OpenSea Analysis (hands-on exploration)

(c) Joerg Osterrieder 2025

L23: NFT Marketplaces

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

January 2026

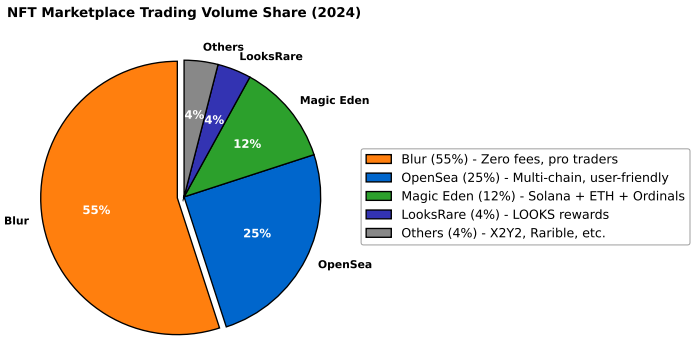
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Compare business models of major NFT marketplaces
- Explain listing mechanics and order matching
- Analyze the royalty enforcement debate
- Detect wash trading and manipulation patterns

NFT Marketplace Market Share (2024)



Blur overtook OpenSea in 2023 via zero fees and trader incentives.

Major NFT Marketplaces

OpenSea:

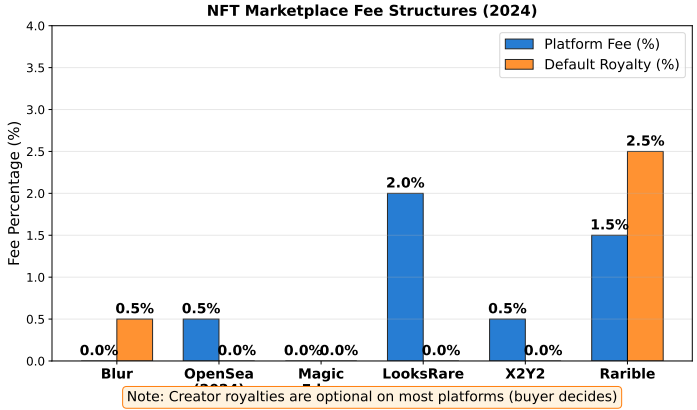
- Founded 2017, valued $13.3B (2022 peak)
- Multi-chain support, lazy minting
- Fee: Optional 0.5% (down from 2.5%)

Blur:

- Launched October 2022, pro trader-focused
- Zero marketplace fees, advanced trading tools
- Airdrop rewards (BLUR token)

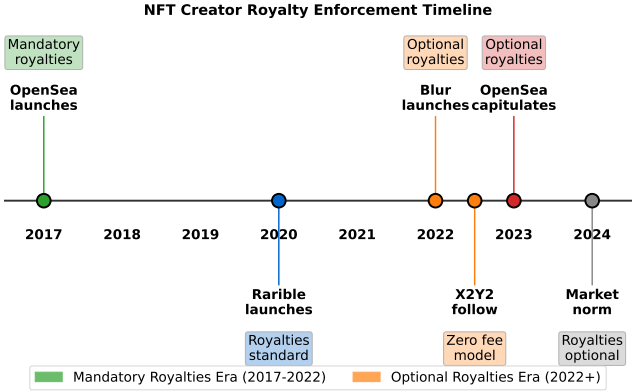
OpenSea + Blur: Control 80%+ of Ethereum NFT volume.

Marketplace Fee Comparison



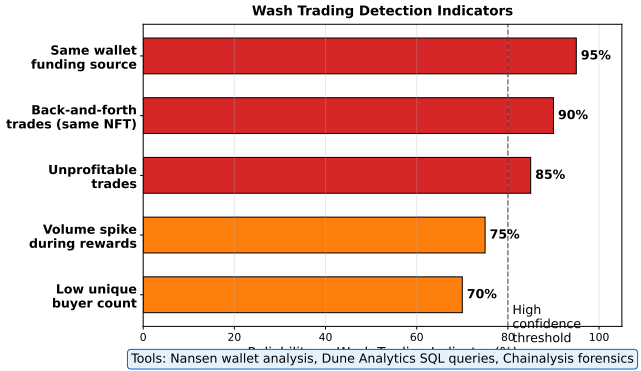
Race to zero fees to attract volume; creator royalties now optional.

The Royalty Enforcement Debate



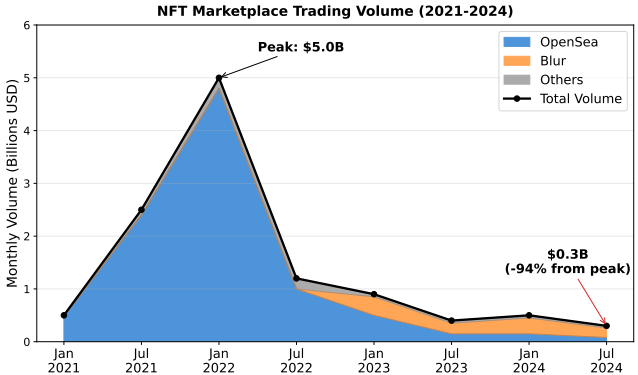
2022-2023: Shift from mandatory to optional creator royalties.

Wash Trading Detection



Case Study: LooksRare 2022 – 95% of volume was wash trading.

NFT Trading Volume Trends



Market down 90%+ from 2021 peak; focus shifting to utility NFTs.

OpenSea Seaport: Open Protocol

Key Features:

- Off-chain orders: Listings signed off-chain (no gas cost)
- On-chain settlement: Trade executes when matched
- Permissionless: Anyone can build marketplace frontends

Strategic Intent:

- Commoditize marketplace infrastructure
- Compete on UX and features (not protocol lock-in)

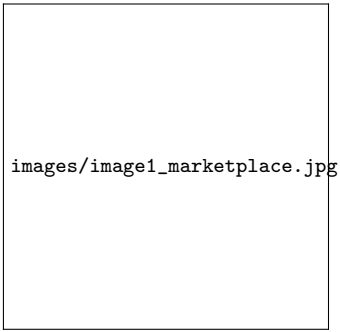
Adoption: Coinbase NFT, GameStop NFT use Seaport.

Key Takeaways

1. **Market Leaders:** Blur (55%+) and OpenSea dominate via fees and features
2. **Fee Race:** Marketplace fees dropped to 0-2.5%
3. **Royalties:** Optional enforcement since 2023 (EIP-2981 not on-chain)
4. **Wash Trading:** Farm rewards via self-trading (95% LooksRare volume)
5. **Market Decline:** NFT market down 90%+ from 2021 peak

Trend: Aggregators commoditize marketplaces, forcing fee competition.

NFT Marketplaces in Practice



NFT Marketplace

Trading Interface

Collection View

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Which marketplace launched with zero fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden

Quiz (1/2)

Q1. Which marketplace launched with zero fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched Oct 2022 with zero fees and advanced tools.

Q2. What % of Ethereum NFT volume do OpenSea and Blur control?
A) 40% B) 60% C) 80%+ D) 95%

Quiz (1/2)

Q1. Which marketplace launched with zero fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched Oct 2022 with zero fees and advanced tools.

Q2. What % of Ethereum NFT volume do OpenSea and Blur control?
A) 40% B) 60% C) 80%+ D) 95%
Answer: C – Together they dominate over 80% of Ethereum NFT volume.

Q3. When did OpenSea shift to optional royalties?
A) 2020 B) 2021 C) 2022 D) 2023

Quiz (1/2)

Q1. Which marketplace launched with zero fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched Oct 2022 with zero fees and advanced tools.

Q2. What % of Ethereum NFT volume do OpenSea and Blur control?
A) 40% B) 60% C) 80%+ D) 95%
Answer: C – Together they dominate over 80% of Ethereum NFT volume.

Q3. When did OpenSea shift to optional royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur's optional royalty launch.

Q4. What % of LooksRare volume was wash trading (2022)?
A) 25% B) 50% C) 75% D) 95%

Quiz (1/2)

Q1. Which marketplace launched with zero fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched Oct 2022 with zero fees and advanced tools.

Q2. What % of Ethereum NFT volume do OpenSea and Blur control?
A) 40% B) 60% C) 80%+ D) 95%
Answer: C – Together they dominate over 80% of Ethereum NFT volume.

Q3. When did OpenSea shift to optional royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur's optional royalty launch.

Q4. What % of LooksRare volume was wash trading (2022)?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% was wash trading.

Q5. Main advantage of off-chain order matching in Seaport?
A) Faster B) No gas cost for listings C) Higher security D) Lower fees

Quiz (1/2)

Q1. Which marketplace launched with zero fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched Oct 2022 with zero fees and advanced tools.

Q2. What % of Ethereum NFT volume do OpenSea and Blur control?
A) 40% B) 60% C) 80%+ D) 95%
Answer: C – Together they dominate over 80% of Ethereum NFT volume.

Q3. When did OpenSea shift to optional royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur's optional royalty launch.

Q4. What % of LooksRare volume was wash trading (2022)?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% was wash trading.

Q5. Main advantage of off-chain order matching in Seaport?
A) Faster B) No gas cost for listings C) Higher security D) Lower fees
Answer: B – Off-chain orders save gas; sellers pay only when sale completes.

Quiz (2/2)

Q6. Why are royalties NOT enforceable on-chain for ERC-721?
A) Gas costs B) No royalty mechanism in standard C) Legal issues D) Monopoly

Quiz (2/2)

Q6. Why are royalties NOT enforceable on-chain for ERC-721?
A) Gas costs B) No royalty mechanism in standard C) Legal issues D) Monopoly
Answer: B – ERC-721 has no native royalty mechanism.

Q7. What is floor price?
A) Average price B) Lowest listed price C) Median price D) Highest sale

Quiz (2/2)

Q6. Why are royalties NOT enforceable on-chain for ERC-721?
A) Gas costs B) No royalty mechanism in standard C) Legal issues D) Monopoly
Answer: B – ERC-721 has no native royalty mechanism.

Q7. What is floor price?
A) Average price B) Lowest listed price C) Median price D) Highest sale
Answer: B – Floor price is the lowest listed price in a collection.

Q8. Which detection method is most reliable for wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age

Quiz (2/2)

Q6. Why are royalties NOT enforceable on-chain for ERC-721?
A) Gas costs B) No royalty mechanism in standard C) Legal issues D) Monopoly
Answer: B – ERC-721 has no native royalty mechanism.

Q7. What is floor price?
A) Average price B) Lowest listed price C) Median price D) Highest sale
Answer: B – Floor price is the lowest listed price in a collection.

Q8. Which detection method is most reliable for wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading.

Q9. What is OpenSea's current fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees

Quiz (2/2)

Q6. Why are royalties NOT enforceable on-chain for ERC-721?
A) Gas costs B) No royalty mechanism in standard C) Legal issues D) Monopoly
Answer: B – ERC-721 has no native royalty mechanism.

Q7. What is floor price?
A) Average price B) Lowest listed price C) Median price D) Highest sale
Answer: B – Floor price is the lowest listed price in a collection.

Q8. Which detection method is most reliable for wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading.

Q9. What is OpenSea's current fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – Optional 0.5% (down from mandatory 2.5%).

Q10. How much has NFT market declined from 2021 peak?
A) 30% B) 50% C) 70% D) 90%+

Quiz (2/2)

Q6. Why are royalties NOT enforceable on-chain for ERC-721?
A) Gas costs B) No royalty mechanism in standard C) Legal issues D) Monopoly
Answer: B – ERC-721 has no native royalty mechanism.

Q7. What is floor price?
A) Average price B) Lowest listed price C) Median price D) Highest sale
Answer: B – Floor price is the lowest listed price in a collection.

Q8. Which detection method is most reliable for wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading.

Q9. What is OpenSea's current fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – Optional 0.5% (down from mandatory 2.5%).

Q10. How much has NFT market declined from 2021 peak?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – NFT trading volume is down over 90% from 2021 peak.

Thank you

Questions?

Next: L24 Lab – OpenSea Analysis

Quiz: NFT Marketplaces

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden

Quiz (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%

Quiz (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees

Quiz (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees (down from mandatory 2.5%).

Q4. Which listing type represents over 90% of NFT marketplace listings?
A) English auction B) Dutch auction C) Fixed price D) Offer system

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees (down from mandatory 2.5%).

Q4. Which listing type represents over 90% of NFT marketplace listings?
A) English auction B) Dutch auction C) Fixed price D) Offer system
Answer: C – Fixed price "Buy Now" listings are most common for instant settlement.

Q5. What is the main advantage of off-chain order matching in Seaport protocol?
A) Faster transactions B) No gas cost for listings C) Higher security D) Lower fees

Quiz (1–5)

Q1. Which NFT marketplace launched with zero marketplace fees to attract pro traders?
A) OpenSea B) Rarible C) Blur D) Magic Eden
Answer: C – Blur launched in October 2022 with zero fees and advanced trading tools.

Q2. What percentage of combined Ethereum NFT trading volume do OpenSea and Blur control?
A) 40% B) 60% C) 80% D) 95%
Answer: C – OpenSea and Blur dominate with over 80% of Ethereum NFT volume.

Q3. What is OpenSea's current marketplace fee structure?
A) Fixed 2.5% B) Optional 0.5% C) 1% mandatory D) Zero fees
Answer: B – OpenSea moved to optional 0.5% fees (down from mandatory 2.5%).

Q4. Which listing type represents over 90% of NFT marketplace listings?
A) English auction B) Dutch auction C) Fixed price D) Offer system
Answer: C – Fixed price "Buy Now" listings are most common for instant settlement.

Q5. What is the main advantage of off-chain order matching in Seaport protocol?
A) Faster transactions B) No gas cost for listings C) Higher security D) Lower fees
Answer: B – Off-chain orders save gas; sellers only pay gas when sale completes.

Quiz (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023

Quiz (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly

Quiz (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity

Quiz (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards (e.g., LooksRare LOOKS tokens).

Q9. What percentage of LooksRare's initial volume was estimated to be wash trading?
A) 25% B) 50% C) 75% D) 95%

Quiz (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards (e.g., LooksRare LOOKS tokens).

Q9. What percentage of LooksRare's initial volume was estimated to be wash trading?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% of LooksRare volume was wash trading in 2022.

Q10. Which detection method is most reliable for identifying wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age

Quiz (6–10)

Q6. When did OpenSea shift from mandatory to optional creator royalties?
A) 2020 B) 2021 C) 2022 D) 2023
Answer: D – OpenSea capitulated in 2023 after Blur launched with optional royalties.

Q7. Why are royalties NOT technically enforceable on-chain for ERC-721 NFTs?
A) Gas costs too high B) No royalty mechanism in standard C) Legal restrictions D) Marketplace monopoly
Answer: B – ERC-721 has no native royalty mechanism; buyers can transfer peer-to-peer.

Q8. What is the primary motivation for wash trading on NFT marketplaces?
A) Tax evasion B) Farm reward tokens C) Hide ownership D) Test liquidity
Answer: B – Wash trading inflates volume to earn marketplace rewards (e.g., LooksRare LOOKS tokens).

Q9. What percentage of LooksRare's initial volume was estimated to be wash trading?
A) 25% B) 50% C) 75% D) 95%
Answer: D – Chainalysis estimated 95% of LooksRare volume was wash trading in 2022.

Q10. Which detection method is most reliable for identifying wash trading?
A) Transaction speed B) Wallet clustering analysis C) Price patterns D) Collection age
Answer: B – Wallet clustering reveals same-entity trading; funding source analysis confirms links.

Quiz (11–15)

Q11. What is the definition of “floor price” in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price

Quiz (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools
Answer: B – Bid pools aggregate collection-wide offers for instant seller acceptance.

Q14. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools
Answer: B – Bid pools aggregate collection-wide offers for instant seller acceptance.

Q14. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base
Answer: C – Ethereum maintains 70%+ NFT market share despite multi-chain expansion.

Q15. What is the ERC-2981 standard designed for?
A) NFT metadata B) Royalty information C) Auction mechanics D) Cross-chain transfers

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the definition of "floor price" in NFT collections?
A) Average price B) Lowest listed price C) Median price D) Highest sale price
Answer: B – Floor price is the lowest listed price for any NFT in the collection.

Q12. Which NFT aggregator was acquired by OpenSea?
A) Genie B) Blur C) Gem D) Rarible
Answer: C – OpenSea acquired Gem; Uniswap acquired Genie.

Q13. What is Blur's key innovation for collection-wide offers?
A) Auction pools B) Bid pools C) Liquidity pools D) Staking pools
Answer: B – Bid pools aggregate collection-wide offers for instant seller acceptance.

Q14. Which blockchain dominates NFT market share at approximately 70%?
A) Solana B) Polygon C) Ethereum D) Base
Answer: C – Ethereum maintains 70%+ NFT market share despite multi-chain expansion.

Q15. What is the ERC-2981 standard designed for?
A) NFT metadata B) Royalty information C) Auction mechanics D) Cross-chain transfers
Answer: B – ERC-2981 provides on-chain royalty info, but enforcement remains optional.

Quiz (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B

Quiz (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas

Quiz (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors

Quiz (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors
Answer: C – Seaport commoditizes marketplace infrastructure to compete on UX, not protocol lock-in.

Q19. How much has the NFT market declined from its 2021 peak?
A) 30% B) 50% C) 70% D) 90%+

Quiz (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors
Answer: C – Seaport commoditizes marketplace infrastructure to compete on UX, not protocol lock-in.

Q19. How much has the NFT market declined from its 2021 peak?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – NFT trading volume is down over 90% from 2021 peak levels.

Q20. Which tool can users use to revoke unused smart contract approvals?
A) Etherscan B) MetaMask C) revoke.cash D) OpenSea

Quiz (16–20)

Q16. What was OpenSea's peak valuation during the 2022 bull market?
A) $1.3B B) $5.5B C) $13.3B D) $25B
Answer: C – OpenSea reached a $13.3 billion valuation at its 2022 peak.

Q17. Which feature does OpenSea offer to reduce upfront costs for creators?
A) Free listings B) Lazy minting C) Batch minting D) Subsidized gas
Answer: B – Lazy minting allows creating NFTs without paying gas until first sale.

Q18. What is the main strategic intent behind OpenSea's Seaport protocol?
A) Lock in users B) Increase fees C) Commoditize infrastructure D) Block competitors
Answer: C – Seaport commoditizes marketplace infrastructure to compete on UX, not protocol lock-in.

Q19. How much has the NFT market declined from its 2021 peak?
A) 30% B) 50% C) 70% D) 90%+
Answer: D – NFT trading volume is down over 90% from 2021 peak levels.

Q20. Which tool can users use to revoke unused smart contract approvals?
A) Etherscan B) MetaMask C) revoke.cash D) OpenSea
Answer: C – revoke.cash allows users to revoke unnecessary token/NFT approvals for security.

Lab Session: OpenSea Collection Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module C: NFTs & Digital Assets

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Navigate OpenSea marketplace effectively
- Analyze NFT collection metrics
- Evaluate rarity using trait analysis
- Identify legitimate vs suspicious collections
- Use third-party rarity tools

The Problem: Hands-on NFT Marketplace Evaluation

The Challenge
You want to invest in NFTs but face information asymmetry: sellers know their assets' true quality, you see only public metrics. How do you distinguish genuine collections from manipulated markets when floor prices, volumes, and rarity rankings can all be gamed?

Why It Matters

- Billions lost to rug pulls and fake collections (e.g., Evolved Apes $2.7M exit scam 2021)
- Wash trading inflates volumes by 40-80% on average (Chainalysis 2022)

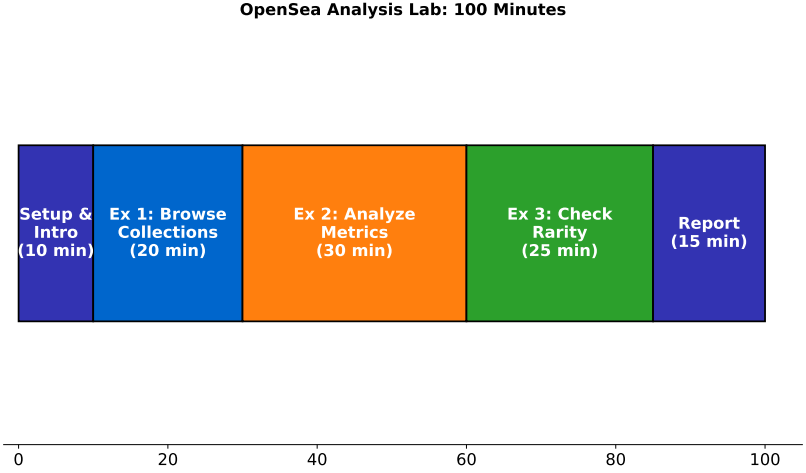
What You'll Explore

- Collection analysis (floor price dynamics, owner distribution)
- Trait rarity evaluation using third-party tools
- Wash trading detection patterns
- Contract verification and creator legitimacy

The Cryptoeconomics Question
How do market mechanisms reveal true demand when participants have incentives to manipulate signals?

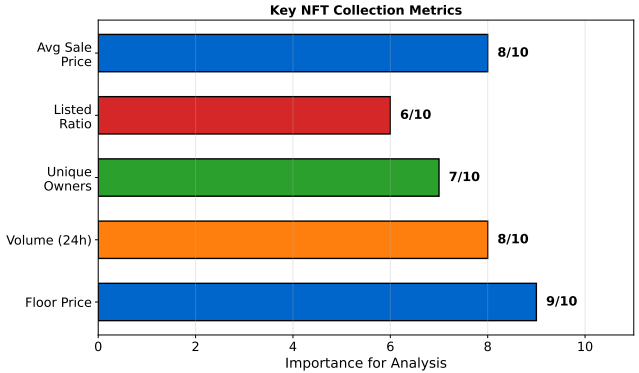
Today's lab: Hands-on skills to analyze NFT markets and avoid common pitfalls

Lab Session Structure



Focus on analysis skills, not purchasing

Key Collection Metrics



Floor price and volume are the most watched metrics

Exercise 1: Browse Collections

Navigate OpenSea:

1. Visit: `https://opensea.io`
2. Explore Rankings: Top collections by volume
3. Select a collection (e.g., Bored Apes, Azuki, Pudgy Penguins)
4. Note: floor price, total volume, owner count

Collection Stats to Record:

- Total items and unique owners
- Floor price and 7-day volume
- Creator royalty percentage
- Contract verification status

Exercise 2: Metric Analysis

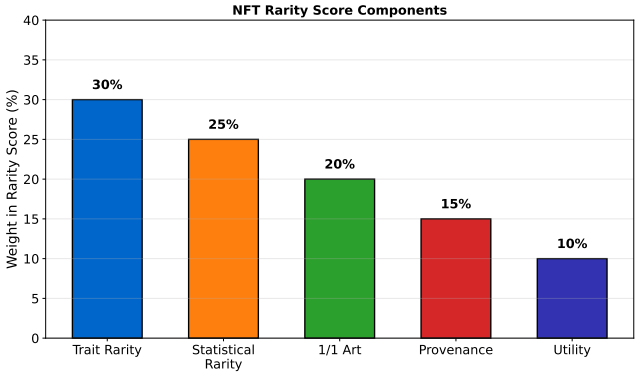
Key Metrics Explained:

- **Floor Price**: Lowest listed price
- **Volume**: Total trading activity (ETH)
- **Listed Ratio**: % of collection for sale
- **Unique Owners**: Distribution measure

Analysis Questions:

1. Is floor price stable or volatile?
2. High volume with low owners = wash trading?
3. What % of collection is listed? (High = bearish)

Rarity Score Components



Trait rarity is typically the largest factor in NFT valuation

Exercise 3: Rarity Analysis

Tools:

- Rarity.tools
- Trait Sniper
- OpenSea trait filters

Tasks:

1. Select an item from your chosen collection
2. List all traits and their rarity percentages
3. Calculate approximate rarity rank
4. Compare price to similar rarity items

Lab Deliverables

Submit:

1. **Collection Analysis (2 pages):**
   - Collection name and contract address
   - Key metrics summary
   - Rarity analysis of one item
   - Market health assessment
2. **Screenshots:**
   - Collection stats page
   - Individual item with traits
   - Price history chart

Problem Solved? NFT Market Analysis

The Original Problem

Distinguishing genuine NFT collections from manipulated markets

How Analysis Tools Help

- **Metric correlation**: Cross-check volume vs unique owners to detect wash trading
- **Rarity verification**: Use third-party tools (Rarity.tools) to validate trait claims
- **On-chain forensics**: Verify contract code and transaction patterns on Etherscan

Remaining Limitations

- Rarity tools can be gamed through metadata manipulation
- No substitute for due diligence on creator reputation and roadmap

The Economic Trade-off

- **Cost**: Time investment in research, risk of buying illiquid assets
- **Reward**: Better investment decisions, avoid scams and rug pulls
- **Risk**: Sophisticated manipulation (fake volume, sybil owner accounts) still hard to detect

Market data reveals patterns, but informed judgment requires combining multiple signals

Key Takeaways

- Floor price is the key metric for collection health
- High unique owner count indicates strong distribution
- Rarity drives individual NFT pricing
- Watch for wash trading (high volume, few owners)
- Verify contract and creator reputation

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit, indicating bearish market sentiment.

Q3. Which metric best indicates distribution quality of an NFT collection?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners mean better distribution and less centralization risk.

Q4. What is wash trading in NFT markets?
A) Trading across blockchains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales
Answer: B – Wash trading is when the same entity trades to create fake volume signals.

Q5. On OpenSea, what does the verified checkmark indicate?
A) High value collection B) Authentic creator account C) No scams D) Guaranteed profits
Answer: B – Verification confirms the account belongs to the authentic creator or project team.

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners with high volume indicates potential self-trading to manipulate metrics.

Q8. Which tool is commonly used for NFT rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores based on trait frequency.

Q9. What does a decreasing floor price over 7 days typically signal?
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity
Answer: C – Falling floor price suggests sellers lowering prices due to reduced demand.

Q10. Why is contract verification status important when analyzing NFT collections?
A) Affects rarity B) Determines gas fees C) Confirms code legitimacy D) Sets floor price
Answer: C – Verified contracts allow users to review code and confirm no malicious functions exist.

Quiz Questions (11–15)

Q11. What percentage metric indicates seller supply pressure?
A) Unique owners B) Listed ratio C) Royalty rate D) Volume growth
Answer: B – Listed ratio shows what percentage of the collection is for sale.

Q12. On OpenSea, where can you find the creator royalty percentage?
A) Collection stats page B) Item page C) User profile D) Transaction history
Answer: A – Collection details page displays creator royalty settings.

Q13. What is the best indicator of active trading for a collection?
A) Floor price B) 7-day volume C) Total items D) Owner count
Answer: B – Recent trading volume shows current market activity and liquidity.

Q14. If an NFT has a trait present in only 2% of the collection, it is:
A) Common B) Rare C) Average D) Verified
Answer: B – Low trait frequency (2%) makes the NFT rare and typically more valuable.

Q15. What should you compare to assess if an NFT is fairly priced?
A) Floor price only B) Items with similar rarity C) Total volume D) Creator's other works
Answer: B – Compare prices of NFTs with similar rarity scores for fair valuation.

Quiz Questions (16–20)

Q16. What does "total items" refer to in collection metrics?
A) Number listed B) Number sold C) Total supply of NFTs D) Active traders
Answer: C – Total items is the complete supply/size of the NFT collection.

Q17. Which scenario suggests a healthy NFT market for a collection?
A) 50% listed, falling floor B) 5% listed, stable volume C) 80% listed, no trades D) High volume, 10 owners
Answer: B – Low listing percentage with consistent volume indicates holder confidence and demand.

Q18. What information can you extract from an NFT's contract address?
A) Rarity score B) Blockchain verification C) Floor price D) Owner profits
Answer: B – Contract address allows verification on block explorers like Etherscan.

Q19. Why are trait filters useful on OpenSea?
A) Calculate royalties B) Find NFTs with specific attributes C) Verify contracts D) Set floor price
Answer: B – Trait filters help locate NFTs with desired characteristics for rarity analysis.

Q20. What is a red flag when evaluating a new NFT collection?
A) Verified contract B) Many unique owners C) Anonymous team with no roadmap D) Creator royalty set
Answer: C – Anonymous teams without clear plans increase rug pull and scam risk.

Lab Session: OpenSea Collection Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module C: NFTs & Digital Assets

(c) Joerg Osterrieder 2025

How Do Floor Prices Signal Market Health?

[COMIC: placeholder]

An investor staring at an NFT collection dashboard showing "Floor: 10 ETH, Volume: 500 ETH/day" and thinking "Great investment!" Meanwhile, a detective with magnifying glass reveals the fine print: "Unique Owners: 12, Same wallet bought it 50 times."

Numbers Can Lie

- Floor price shows lowest listing
- Volume shows trading activity
- But who is actually trading?

What We'll Practice

- Reading collection metrics critically
- Spotting manipulation red flags
- Using rarity tools for valuation

Due diligence means looking beyond the headline numbers

Learning Objectives

By the end of this lab session, you will be able to:

- Navigate OpenSea marketplace effectively
- Analyze NFT collection metrics
- Evaluate rarity using trait analysis
- Identify legitimate vs suspicious collections
- Use third-party rarity tools

Building on L23: NFT Marketplaces

The Problem: Hands-on NFT Marketplace Evaluation

The Challenge
You want to invest in NFTs but face information asymmetry (sellers know more): sellers know their assets' true quality, you see only public metrics. How do you distinguish genuine collections from manipulated markets when floor prices, volumes, and rarity rankings can all be gamed?

Why It Matters

- Billions lost to rug pulls (creators abandon after collecting funds) and fake collections (e.g., Evolved Apes $2.7M exit scam 2021)
- Wash trading (self-trading to inflate volume) inflates volumes by 40-80% on average (Chainalysis 2022)

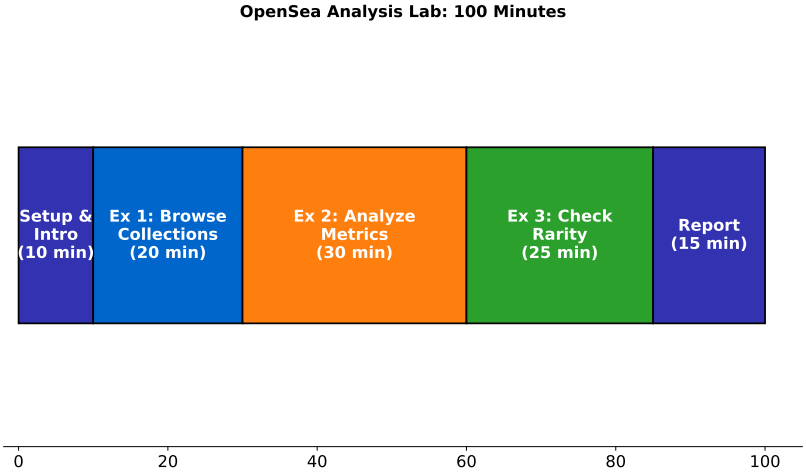
What You'll Explore

- Collection analysis (floor price dynamics, owner distribution)
- Trait rarity evaluation using third-party tools
- Wash trading detection patterns
- Contract verification and creator legitimacy

The Cryptoeconomics Question
How do market mechanisms reveal true demand when participants have incentives to manipulate signals?

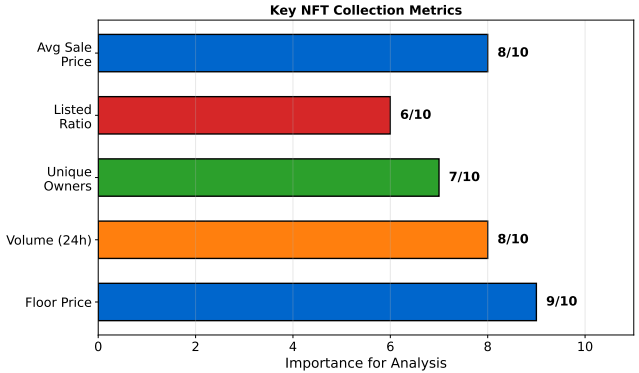
Today's lab: Hands-on skills to analyze NFT markets and avoid common pitfalls

How Will We Navigate This Lab?



Focus on analysis skills, not purchasing

What Metrics Matter Most for Collections?



Floor price and volume are the most watched metrics

How Do You Explore Top Collections?

Navigate OpenSea:

1. Visit: `https://opensea.io`
2. Explore Rankings: Top collections by volume
3. Select a collection (e.g., Bored Apes, Azuki, Pudgy Penguins)
4. Note: floor price, total volume, owner count

Collection Stats to Record:

- Total items and unique owners
- Floor price and 7-day volume
- Creator royalty percentage
- Contract verification status

What Do These Metrics Tell You?

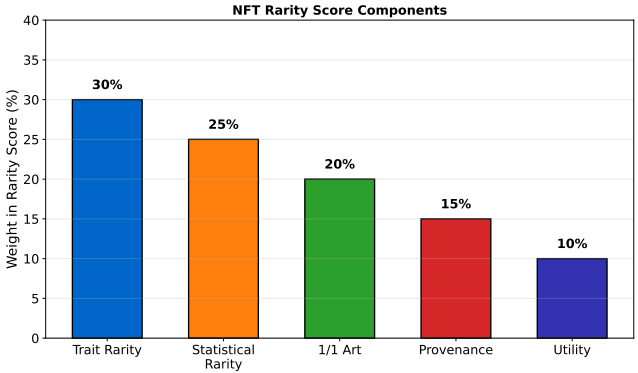
Key Metrics Explained:

- **Floor Price (lowest asking price)**: Lowest listed price
- **Volume**: Total trading activity (ETH)
- **Listed Ratio (percent for sale)**: % of collection for sale
- **Unique Owners**: Distribution measure

Analysis Questions:

1. Is floor price stable or volatile?
2. High volume with low owners = wash trading?
3. What % of collection is listed? (High = bearish)

How Is Rarity Calculated?



Trait rarity (how uncommon) is typically the largest factor in NFT valuation

How Do You Analyze Individual NFT Rarity?

Tools:

- rarity.tools (NFT rarity calculator)
- Trait Sniper
- OpenSea trait filters

Tasks:

1. Select an item from your chosen collection
2. List all traits and their rarity percentages
3. Calculate approximate rarity rank
4. Compare price to similar rarity items

What Should You Submit for This Lab?

Submit:

1. **Collection Analysis (2 pages):**
   - Collection name and contract address
   - Key metrics summary
   - Rarity analysis of one item
   - Market health assessment
2. **Screenshots:**
   - Collection stats page
   - Individual item with traits
   - Price history chart

Problem Solved? NFT Market Analysis

The Original Problem

Distinguishing genuine NFT collections from manipulated markets

How Analysis Tools Help

- **Metric correlation**: Cross-check volume vs unique owners to detect wash trading
- **Rarity verification**: Use third-party tools (Rarity.tools) to validate trait claims
- **On-chain forensics (blockchain analysis)**: Verify contract code and transaction patterns on Etherscan

Remaining Limitations

- Rarity tools can be gamed through metadata manipulation
- No substitute for due diligence on creator reputation and roadmap

The Economic Trade-off

- **Cost**: Time investment in research, risk of buying illiquid assets
- **Reward**: Better investment decisions, avoid scams and rug pulls
- **Risk**: Sophisticated manipulation (fake volume, sybil accounts (fake accounts by one person)) still hard to detect

Market data reveals patterns, but informed judgment requires combining multiple signals

The Economics of OpenSea Analysis

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: OpenSea Analysis

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: OpenSea Analysis

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

! Unusual economic behavior

! Incentive misalignment

! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

(c) Joerg Osterrieder 2025

How Do You Spot Wash Trading?

[COMIC: placeholder]

A blockchain detective following a trail of NFT sales that all lead back to the same wallet wearing different disguises (Wallet A, Wallet B, Wallet C). The detective's notepad shows: "Same funding source, circular trades, reward farming detected."

Red Flags to Watch

- High volume + few unique owners
- Circular trading patterns
- Same funding source for multiple wallets

Your Detection Toolkit

- Check unique owner count vs. volume
- Use wallet clustering analysis
- Cross-reference with on-chain data

Volume-based rewards create incentives for manipulation—always verify

Key Takeaways

- Floor price is the key metric for collection health
- High unique owner count indicates strong distribution
- Rarity drives individual NFT pricing
- Watch for wash trading (high volume, few owners)
- Verify contract and creator reputation

Next Lesson: L25 – Digital Art and Collectibles

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit, indicating bearish market sentiment.

Q3. Which metric best indicates distribution quality of an NFT collection?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners mean better distribution and less centralization risk.

Q4. What is wash trading in NFT markets?
A) Trading across blockchains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales
Answer: B – Wash trading is when the same entity trades to create fake volume signals.

Q5. On OpenSea, what does the verified checkmark indicate?
A) High value collection B) Authentic creator account C) No scams D) Guaranteed profits
Answer: B – Verification confirms the account belongs to the authentic creator or project team.

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners with high volume indicates potential self-trading to manipulate metrics.

Q8. Which tool is commonly used for NFT rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores based on trait frequency.

Q9. What does a decreasing floor price over 7 days typically signal?
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity
Answer: C – Falling floor price suggests sellers lowering prices due to reduced demand.

Q10. Why is contract verification status important when analyzing NFT collections?
A) Affects rarity B) Determines gas fees C) Confirms code legitimacy D) Sets floor price
Answer: C – Verified contracts allow users to review code and confirm no malicious functions exist.

Quiz Questions (11–15)

Q11. What percentage metric indicates seller supply pressure?
A) Unique owners B) Listed ratio C) Royalty rate D) Volume growth
Answer: B – Listed ratio shows what percentage of the collection is for sale.

Q12. On OpenSea, where can you find the creator royalty percentage?
A) Collection stats page B) Item page C) User profile D) Transaction history
Answer: A – Collection details page displays creator royalty settings.

Q13. What is the best indicator of active trading for a collection?
A) Floor price B) 7-day volume C) Total items D) Owner count
Answer: B – Recent trading volume shows current market activity and liquidity.

Q14. If an NFT has a trait present in only 2% of the collection, it is:
A) Common B) Rare C) Average D) Verified
Answer: B – Low trait frequency (2%) makes the NFT rare and typically more valuable.

Q15. What should you compare to assess if an NFT is fairly priced?
A) Floor price only B) Items with similar rarity C) Total volume D) Creator's other works
Answer: B – Compare prices of NFTs with similar rarity scores for fair valuation.

Quiz Questions (16–20)

Q16. What does "total items" refer to in collection metrics?
A) Number listed B) Number sold C) Total supply of NFTs D) Active traders
Answer: C – Total items is the complete supply/size of the NFT collection.

Q17. Which scenario suggests a healthy NFT market for a collection?
A) 50% listed, falling floor B) 5% listed, stable volume C) 80% listed, no trades D) High volume, 10 owners
Answer: B – Low listing percentage with consistent volume indicates holder confidence and demand.

Q18. What information can you extract from an NFT's contract address?
A) Rarity score B) Blockchain verification C) Floor price D) Owner profits
Answer: B – Contract address allows verification on block explorers like Etherscan.

Q19. Why are trait filters useful on OpenSea?
A) Calculate royalties B) Find NFTs with specific attributes C) Verify contracts D) Set floor price
Answer: B – Trait filters help locate NFTs with desired characteristics for rarity analysis.

Q20. What is a red flag when evaluating a new NFT collection?
A) Verified contract B) Many unique owners C) Anonymous team with no roadmap D) Creator royalty set
Answer: C – Anonymous teams without clear plans increase rug pull and scam risk.

L24: Lab – OpenSea Collection Analysis

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

January 2026

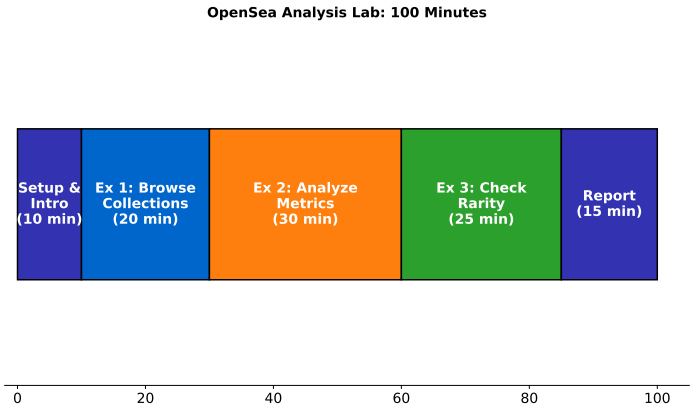
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

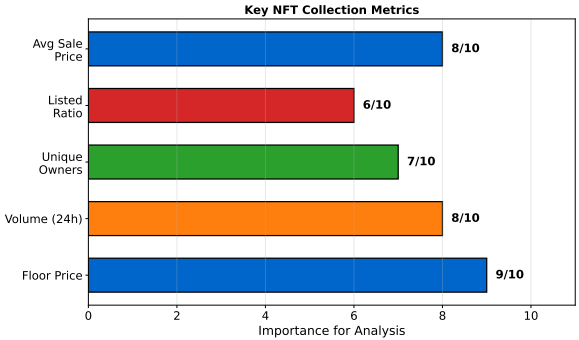
- Navigate OpenSea marketplace effectively
- Analyze NFT collection metrics
- Evaluate rarity using trait analysis
- Identify legitimate vs suspicious collections

OpenSea Analysis Workflow



Focus: Analysis skills, not purchasing.

Key Collection Metrics



Floor price and volume are the most watched metrics.

Understanding Collection Metrics

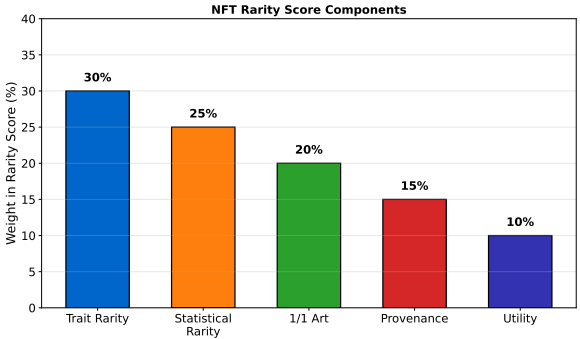
Key Metrics:

- **Floor Price:** Lowest listed price in collection
- **Volume:** Total trading activity (ETH)
- **Listed Ratio:** % of collection for sale (high = bearish)
- **Unique Owners:** Distribution measure (more = healthier)

Analysis Questions:

1. Is floor price stable or volatile?
2. High volume with few owners = wash trading?
3. What % is listed? (High listing = seller pressure)

Rarity Score Components



Trait rarity is typically the largest factor in NFT valuation.

Rarity Analysis Tools

Tools:

- Rarity.tools
- Trait Sniper
- OpenSea trait filters

Analysis Steps:

1. Select an item from chosen collection
2. List all traits and their rarity percentages
3. Calculate approximate rarity rank
4. Compare price to similar rarity items

Key: 2% trait frequency = rare and more valuable.

Healthy vs Unhealthy Market Signs

Healthy Signs:

- Wide distribution (many unique owners)
- Low listing percentage ($<10\%$)
- Stable/growing floor price
- Organic trading patterns

Red Flags:

- High volume, few owners (wash trading)
- 30%+ listed (bearish sentiment)
- Declining floor price
- Anonymous team, no roadmap

(c) Joerg Osterrieder 2025

Contract Verification

Why Verification Matters:

- Verified checkmark = authentic creator account
- Contract verification on Etherscan = code transparency
- Allows security review of smart contract

Never interact with unverified contracts:

- Check contract address on Etherscan
- Look for verified badge on OpenSea
- Cross-reference with official project channels

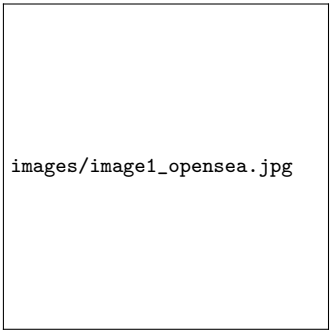
(c) Joerg Osterrieder 2025

Key Takeaways

1. **Floor Price:** Key metric for collection health
2. **Unique Owners:** High count indicates strong distribution
3. **Rarity:** Trait frequency drives individual NFT pricing
4. **Wash Trading:** High volume + few owners = suspicious
5. **Verification:** Always verify contract and creator reputation

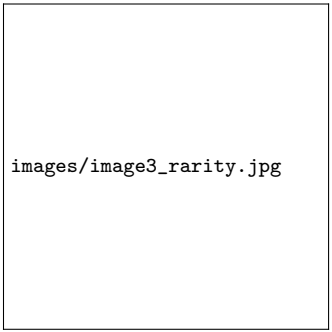
Lab Goal: Analyze a collection with metrics, rarity, and health assessment.

OpenSea Analysis in Practice



OpenSea Interface

Collection Stats



Rarity Analysis

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is floor price in an NFT collection?
A) Average price B) Lowest listed price C) Highest sale D) Creator's set price

Quiz (1/2)

Q1. What is floor price in an NFT collection?
A) Average price B) Lowest listed price C) Highest sale D) Creator's set price
Answer: B – Floor price is minimum price currently listed.

Q2. What does high listed ratio (30%) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity

Quiz (1/2)

Q1. What is floor price in an NFT collection?
A) Average price B) Lowest listed price C) Highest sale D) Creator's set price
Answer: B – Floor price is minimum price currently listed.

Q2. What does high listed ratio (30%) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit.

Q3. Which metric best indicates distribution quality?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty

Quiz (1/2)

Q1. What is floor price in an NFT collection?
A) Average price B) Lowest listed price C) Highest sale D) Creator's set price
Answer: B – Floor price is minimum price currently listed.

Q2. What does high listed ratio (30%) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit.

Q3. Which metric best indicates distribution quality?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners = better distribution.

Q4. What is wash trading?
A) Trading across chains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales

Quiz (1/2)

Q1. What is floor price in an NFT collection?
A) Average price B) Lowest listed price C) Highest sale D) Creator's set price
Answer: B – Floor price is minimum price currently listed.

Q2. What does high listed ratio (30%) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit.

Q3. Which metric best indicates distribution quality?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners = better distribution.

Q4. What is wash trading?
A) Trading across chains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales
Answer: B – Same entity trades to create fake volume.

Q5. What does verified checkmark indicate on OpenSea?
A) High value B) Authentic creator account C) No scams D) Guaranteed profits

(c) Joerg Osterrieder 2025

Quiz (1/2)

Q1. What is floor price in an NFT collection?
A) Average price B) Lowest listed price C) Highest sale D) Creator's set price
Answer: B – Floor price is minimum price currently listed.

Q2. What does high listed ratio (30%) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit.

Q3. Which metric best indicates distribution quality?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners = better distribution.

Q4. What is wash trading?
A) Trading across chains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales
Answer: B – Same entity trades to create fake volume.

Q5. What does verified checkmark indicate on OpenSea?
A) High value B) Authentic creator account C) No scams D) Guaranteed profits
Answer: B – Verification confirms authentic creator.

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. Primary factor determining an NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price

Quiz (2/2)

Q6. Primary factor determining an NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations = lower frequency.

Q7. High volume with few unique owners suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution

Quiz (2/2)

Q6. Primary factor determining an NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations = lower frequency.

Q7. High volume with few unique owners suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners + high volume = suspicious.

Q8. Which tool is commonly used for rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask

Quiz (2/2)

Q6. Primary factor determining an NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations = lower frequency.

Q7. High volume with few unique owners suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners + high volume = suspicious.

Q8. Which tool is commonly used for rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores.

Q9. Decreasing floor price over 7 days signals:
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. Primary factor determining an NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations = lower frequency.

Q7. High volume with few unique owners suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners + high volume = suspicious.

Q8. Which tool is commonly used for rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores.

Q9. Decreasing floor price over 7 days signals:
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity
Answer: C – Falling floor = reduced demand.

Q10. Why is contract verification important?
A) Affects rarity B) Determines gas C) Confirms code legitimacy D) Sets floor price

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. Primary factor determining an NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations = lower frequency.

Q7. High volume with few unique owners suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners + high volume = suspicious.

Q8. Which tool is commonly used for rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores.

Q9. Decreasing floor price over 7 days signals:
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity
Answer: C – Falling floor = reduced demand.

Q10. Why is contract verification important?
A) Affects rarity B) Determines gas C) Confirms code legitimacy D) Sets floor price
Answer: C – Verified contracts allow security review.

Thank you

Questions?

Next: L25 – Digital Art and Collectibles

Quiz: Lab OpenSea Analysis

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price

Quiz (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit, indicating bearish market sentiment.

Q3. Which metric best indicates distribution quality of an NFT collection?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit, indicating bearish market sentiment.

Q3. Which metric best indicates distribution quality of an NFT collection?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners mean better distribution and less centralization risk.

Q4. What is wash trading in NFT markets?
A) Trading across blockchains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit, indicating bearish market sentiment.

Q3. Which metric best indicates distribution quality of an NFT collection?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners mean better distribution and less centralization risk.

Q4. What is wash trading in NFT markets?
A) Trading across blockchains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales
Answer: B – Wash trading is when the same entity trades to create fake volume signals.

Q5. On OpenSea, what does the verified checkmark indicate?
A) High value collection B) Authentic creator account C) No scams D) Guaranteed profits

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the floor price in an NFT collection?
A) The average price of all NFTs B) The lowest listed price C) The highest sale price D) The creator's set price
Answer: B – Floor price is the minimum price at which an NFT is currently listed for sale.

Q2. What does a high listed ratio (e.g., 30% of collection) typically indicate?
A) Strong demand B) Bullish sentiment C) Bearish sentiment D) High rarity
Answer: C – Many listings suggest sellers trying to exit, indicating bearish market sentiment.

Q3. Which metric best indicates distribution quality of an NFT collection?
A) Floor price B) Total volume C) Unique owner count D) Creator royalty
Answer: C – More unique owners mean better distribution and less centralization risk.

Q4. What is wash trading in NFT markets?
A) Trading across blockchains B) Self-trading to inflate volume C) Bulk buying D) Liquidation sales
Answer: B – Wash trading is when the same entity trades to create fake volume signals.

Q5. On OpenSea, what does the verified checkmark indicate?
A) High value collection B) Authentic creator account C) No scams D) Guaranteed profits
Answer: B – Verification confirms the account belongs to the authentic creator or project team.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price

Quiz (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners with high volume indicates potential self-trading to manipulate metrics.

Q8. Which tool is commonly used for NFT rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask

Quiz (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners with high volume indicates potential self-trading to manipulate metrics.

Q8. Which tool is commonly used for NFT rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores based on trait frequency.

Q9. What does a decreasing floor price over 7 days typically signal?
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners with high volume indicates potential self-trading to manipulate metrics.

Q8. Which tool is commonly used for NFT rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores based on trait frequency.

Q9. What does a decreasing floor price over 7 days typically signal?
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity
Answer: C – Falling floor price suggests sellers lowering prices due to reduced demand.

Q10. Why is contract verification status important when analyzing NFT collections?
A) Affects rarity B) Determines gas fees C) Confirms code legitimacy D) Sets floor price

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the primary factor that determines an individual NFT's rarity?
A) Age B) Trait frequency C) Owner history D) Floor price
Answer: B – Rarer trait combinations have lower frequency, making the NFT more valuable.

Q7. If a collection has high volume but very few unique owners, this suggests:
A) Healthy market B) High demand C) Possible wash trading D) Strong distribution
Answer: C – Few owners with high volume indicates potential self-trading to manipulate metrics.

Q8. Which tool is commonly used for NFT rarity analysis?
A) Uniswap B) Rarity.tools C) Aave D) MetaMask
Answer: B – Rarity.tools calculates rarity scores based on trait frequency.

Q9. What does a decreasing floor price over 7 days typically signal?
A) Increasing demand B) Market strength C) Weakening interest D) Rising rarity
Answer: C – Falling floor price suggests sellers lowering prices due to reduced demand.

Q10. Why is contract verification status important when analyzing NFT collections?
A) Affects rarity B) Determines gas fees C) Confirms code legitimacy D) Sets floor price
Answer: C – Verified contracts allow users to review code and confirm no malicious functions exist.

(c) Joerg Osterrieder 2025

L25: Digital Art and Collectibles

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Distinguish between 1/1 art, editions, and generative art NFTs
- Explain generative art platforms and on-chain algorithms (Art Blocks)
- Analyze PFP collections and their cultural significance (BAYC, CryptoPunks)
- Apply valuation frameworks to digital art NFTs
- Evaluate the impact of high-profile sales (Beeple $69M)

(c) Joerg Osterrieder 2025

The Problem: Why do some NFTs hold value?

The Challenge
In a market with millions of NFT collections, most digital assets go to zero while a select few trade at life-changing prices. What separates valuable NFTs from worthless JPEGs?

Why It Matters

- Over $40 billion traded in NFTs (2021-2023), yet 95% of collections are worthless
- CryptoPunks floor price: $100k+ while thousands of PFP projects collapsed

What We Need

- Value creation and capture mechanisms
- Framework for evaluating NFT value propositions beyond speculation

The Cryptoeconomics Question
Creating and distributing economic value in digital collectibles

Today's lesson: How digital art and collectibles address this challenge

NFT Art Categories

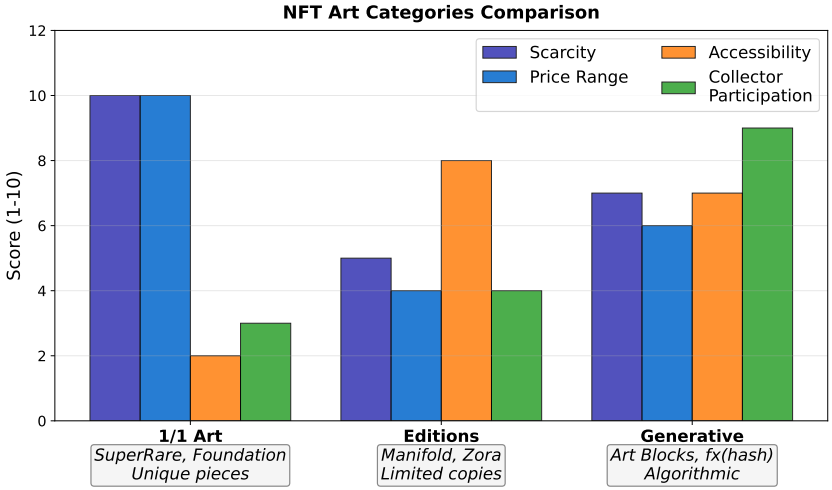
Three Primary Categories:

1. **1/1 Digital Art** – Unique, single-edition artwork (SuperRare, Foundation)
2. **Editions** – Multiple identical copies (Manifold, Zora)
3. **Generative Art** – Algorithm-created unique outputs (Art Blocks)

Key Differences:

- Scarcity: 1/1 highest, editions moderate, generative varies
- Price: 1/1 premium, editions accessible, generative mid-range
- Collector participation: Generative highest (mint reveals)

NFT Art Categories Comparison



1/1 art commands highest prices; generative art offers collector participation

1/1 Digital Art: Unique Creations

Characteristics:

- Single NFT per artwork (no duplicates)
- Artist-signed and authenticated on-chain
- Direct artist-to-collector relationship

Leading 1/1 Platforms:

- **SuperRare:** Curated marketplace, invitation-only artists
- **Foundation:** Auction-based, community-curated
- **Nifty Gateway:** Drops from celebrity artists (Beeple, Pak)

Valuation Factors:

- Artist reputation and exhibition history
- Aesthetic quality and cultural relevance
- Provenance (ownership history)

(c) Joerg Osterrieder 2025

Case Study: Beeple's "Everydays" ($69M)

Event: March 2021, Christie's auction

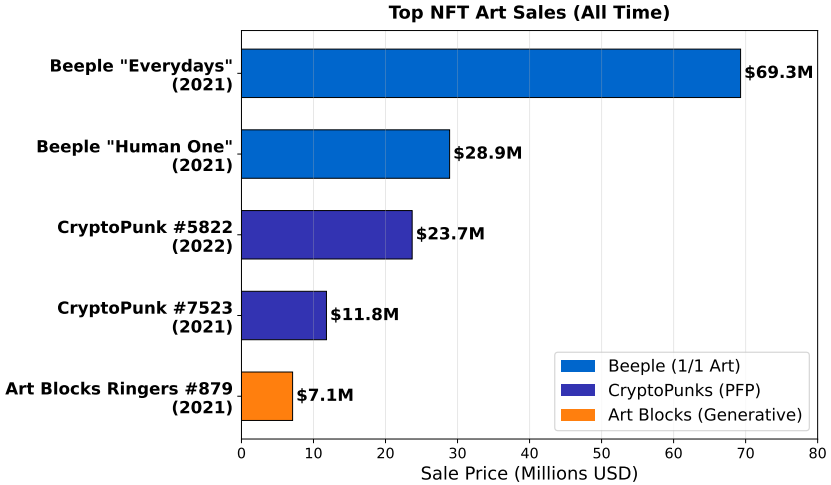
Artwork Details:

- Title: "Everydays: The First 5000 Days"
- Artist: Beeple (Mike Winkelmann)
- Format: Collage of 5,000 daily digital artworks (2007-2021)
- Sale price: $69.3 million (42,329 ETH at time)

Significance:

- Third-highest price for living artist (after Koons, Hockney)
- Legitimized NFTs in traditional art world
- Catalyzed NFT bull market (2021 peak)

High-Profile NFT Art Sales



Beeple's $69M sale remains the highest NFT art price; CryptoPunks dominate PFP sales

Generative Art: Code as Artist

Definition: Artwork generated by algorithmic code with controlled randomness

How It Works:

1. Artist writes generative algorithm (JavaScript, p5.js)
2. Algorithm uses random seed (from transaction hash)
3. Each NFT mint produces unique output from same code

Appeal:

- Each piece is unique (seed-based randomness)
- Collector participates in creation (mint reveals outcome)
- On-chain code storage (true permanence)
- Lower price than 1/1s (algorithmic scalability)

Art Blocks: Premier Generative Platform

Founded: 2020 by Erick Calderon (Snowfro)

How Art Blocks Works:

1. Artist submits generative algorithm (JavaScript)
2. Collector mints NFT (pays ETH + gas)
3. Transaction hash seeds random number generator
4. Algorithm runs, generates unique output

Project Tiers:

- **Curated:** Highly selective, premium (Fidenza, Ringers)
- **Playground:** Emerging artists, experimental
- **Factory:** Open submissions, lower curation bar

(c) Joerg Osterrieder 2025

Iconic Generative Projects

Fidenza by Tyler Hobbs (2021):

- 999 unique outputs, flow field algorithm
- Mint: 0.17 ETH, Floor peak: 140 ETH ($500k+)

Ringers by Dmitri Cherniak (2021):

- 1,000 outputs, wrapped strings around pegs
- Mint: 0 ETH (free + gas), Floor peak: 25 ETH

Chromie Squiggle (2020):

- Art Blocks' first project (Snowfro)
- 10,000 outputs, "genesis" Art Blocks NFT

Rarity: Certain outputs extremely rare (algorithmic traits)

PFP Collections: Profile Pictures as Identity

PFP: Profile Picture NFTs, avatar-style collectibles

Characteristics:

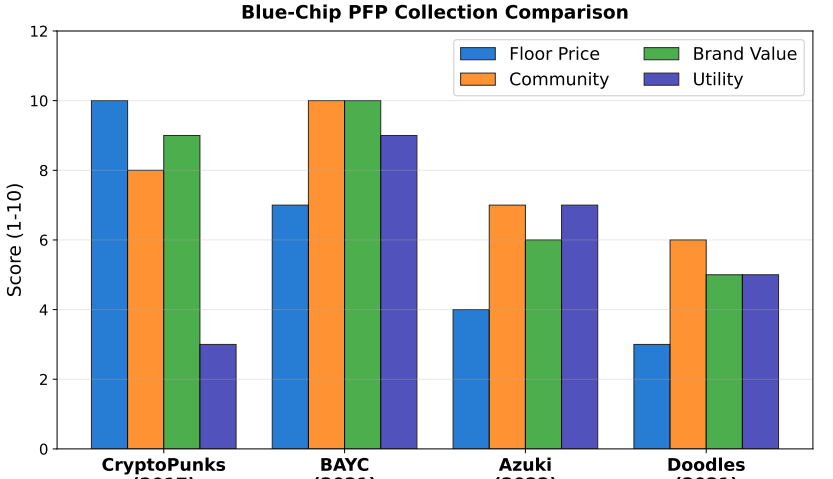
- 10,000-item collections (standard size)
- Trait-based variation (hat, eyes, background)
- Social signaling (Twitter/Discord avatars)
- Community membership and status

Leading PFP Collections:

- **CryptoPunks (2017):** 10,000 pixel art characters
- **Bored Ape Yacht Club (2021):** 10,000 apes, Yuga Labs
- **Azuki (2022):** 10,000 anime-style characters

Value Drivers: Brand recognition, community, utility, celebrities

Blue-Chip PFP Collection Comparison



Floor prices (2024): CryptoPunks ~50 ETH, BAYC ~25 ETH, Azuki ~3 ETH, Doodles ~2 ETH

BAYC leads in utility and community; CryptoPunks maintain highest floor prices

CryptoPunks: The OG NFT Collection

Created: June 2017 by Larva Labs

Technical Details:

- 10,000 unique 24x24 pixel art characters
- Originally free to claim (gas only)
- Pre-dates ERC-721 standard (custom contract)

Rarity Breakdown:

- 6,039 Male — 3,840 Female — 88 Zombie
- 24 Ape — 9 Alien (rarest, ¿10,000 ETH peak)

Cultural Impact: Inspired entire PFP category, held by Jay-Z, Snoop Dogg

Bored Ape Yacht Club: Community and Utility

Created: April 2021 by Yuga Labs

Key Innovations:

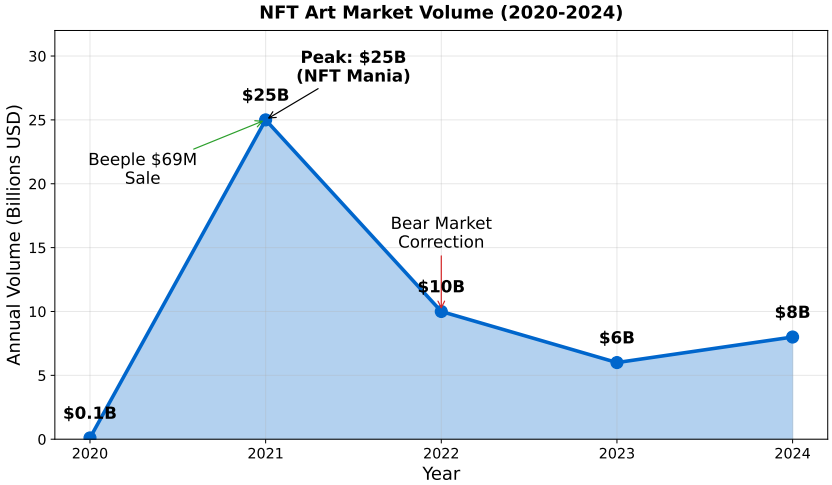
- **IP rights:** Holders own commercial rights to their ape
- **Community events:** Exclusive parties, metaverse experiences
- **Airdrops:** Free Mutant Apes, ApeCoin tokens

Valuation Milestones:

- Mint price: 0.08 ETH (April 2021)
- Floor peak: 153 ETH ($500k+, April 2022)
- Current floor (2024): 20-30 ETH range

Celebrity Holders: Eminem, Stephen Curry, Paris Hilton

NFT Art Market Trends



2021 peak driven by Beeple sale and mainstream adoption; market stabilizing post-correction

The Social Capital Thesis

Argument: NFTs represent digital social capital and identity

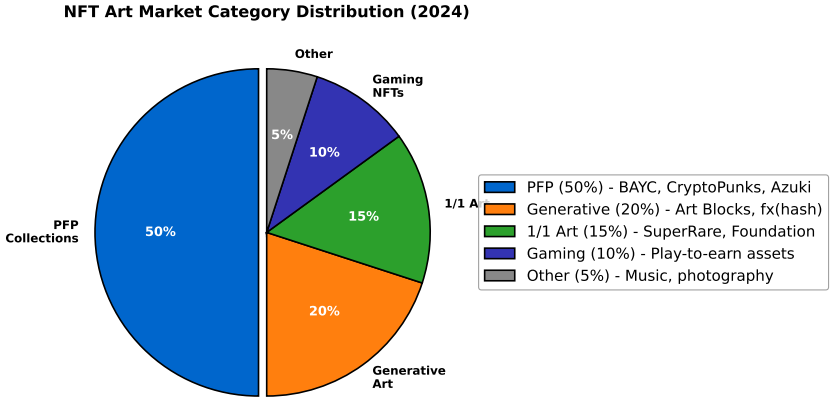
Mechanisms:

- **Signaling:** PFP shows wealth, taste, community affiliation
- **Access:** Token-gated Discord channels, events, alpha groups
- **Status:** Owning rare/expensive NFTs confers prestige
- **Network effects:** Value increases with community size

Comparison to Luxury Goods:

- Rolex watch: $10k+ for timekeeping (social signal)
- Bored Ape: $100k+ for pixel art (social signal)
- Both: Functional value ¡¡ social signaling value

NFT Art Category Distribution



PFP collections dominate volume; generative art growing among collectors

Valuation Framework for Digital Art

Key Criteria:

1. **Artist reputation:** Exhibition history, awards, following
2. **Scarcity:** 1/1 vs. edition size
3. **Provenance:** Ownership history (celebrity collectors)
4. **Cultural significance:** Historical impact, media coverage
5. **Technical quality:** Metadata storage (IPFS)
6. **Market comparables:** Similar artist sales

Example Valuation:

- Established artist, 1/1 artwork, IPFS storage
- Recent comparable: 5 ETH $\rightarrow$ Range: 4-6 ETH

(c) Joerg Osterrieder 2025

Blue-Chip NFT Collections

Blue-Chip: Established collections with sustained demand and liquidity

Criteria:

- 2+ years of trading history
- Consistent floor price support (bear market resilience)
- Strong community and holder base
- Cultural significance and brand recognition

Current Blue-Chips (2024):

- CryptoPunks (50+ ETH floor)
- Bored Ape Yacht Club (20-30 ETH floor)
- Autoglyphs (on-chain generative, 100+ ETH floor)
- Art Blocks Curated projects (Fidenza, Ringers)

(c) Joerg Osterrieder 2025

Problem Solved? Digital Art & Collectibles

The Original Problem

Why do some NFTs hold value?

How Digital Art & Collectibles Solve It

- Community and cultural significance create sustained demand (BAYC, CryptoPunks)
- Utility (access, governance, IP rights) adds tangible value beyond aesthetics
- Provenance and scarcity mechanisms differentiate blue-chip collections

Remaining Limitations

- Highly speculative with subjective value determination
- Illiquid markets with volatile floor prices

Open Questions

- What makes digital collectibles a lasting asset class vs. temporary speculation?
- Can NFT value persist without constant community engagement and hype?

Digital art partially solves "Why do some NFTs hold value" through community and utility, but introduces volatility

Key Takeaways

1. NFT art includes 1/1 unique pieces, limited editions, and generative algorithmic art
2. Generative platforms (Art Blocks) create unique outputs from code using randomness
3. PFP collections (BAYC, CryptoPunks) derive value from community and social capital
4. Beeple's $69M sale catalyzed mainstream NFT adoption but raised speculation concerns
5. Valuation combines traditional art criteria with on-chain metrics and community factors
6. Blue-chip NFTs show resilience through market cycles due to cultural significance

(c) Joerg Osterrieder 2025

Discussion Questions

1. Is digital art fundamentally different from physical art in terms of value and ownership?
2. What distinguishes a blue-chip NFT collection from a speculative project?
3. How should generative art be valued compared to artist-created 1/1 pieces?
4. Will PFP collections retain value long-term, or are they a temporary trend?
5. Should NFT marketplaces curate art quality, or remain open platforms?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L26: Gaming NFTs and Metaverse

We will explore:

- Play-to-earn gaming model and tokenomics
- Case study: Axie Infinity rise and collapse
- Virtual land NFTs (Decentraland, The Sandbox)
- Interoperability and cross-game asset portability
- Sustainability challenges of blockchain gaming

Preparation: Explore Decentraland or The Sandbox metaverse platforms

Quiz Questions (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper than generative art
B) Generative art uses algorithms with controlled randomness; 1/1 art is unique artist-created pieces
C) 1/1 art has multiple editions; generative art does not
D) Generative art cannot be stored on-chain
Answer: B – Generative art is created by code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9 million B) $69.3 million C) $6.9 billion D) $693 million
Answer: B – Sold for $69.3 million at Christie's in March 2021.

Q3. Which platform is the premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in generative art using on-chain code.

Q4. How does Art Blocks generate unique artwork for each NFT?
A) Artists manually create each piece
B) Random images are selected from a database
C) Transaction hash seeds a random number generator in the algorithm
D) Collectors upload their own designs
Answer: C – Transaction hash seeds the RNG for unique outputs.

Q5. What does PFP stand for in the context of NFT collections?
A) Proof of Purchase B) Profile Picture C) Public Financial Protocol D) Permanently Fixed Price
Answer: B – PFP refers to Profile Picture NFTs used as avatars.

Quiz Questions (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – Larva Labs created 10,000 unique 24x24 pixel art CryptoPunks in June 2017.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88 total) B) Ape (24 total) C) Alien (9 total) D) Female (3,840 total)
Answer: C – Only 9 Alien CryptoPunks exist with peak values over 10,000 ETH.

Q8. What was the mint price of Bored Ape Yacht Club NFTs in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – BAYC minted at 0.08 ETH before reaching a floor peak of 153 ETH.

Q9. Which innovative feature did Bored Ape Yacht Club introduce?
A) Free minting for all users
B) Commercial IP rights for NFT holders
C) Physical artwork redemption
D) Automatic price appreciation
Answer: B – BAYC holders own full commercial rights to their ape.

Q10. What is the standard collection size for most PFP NFT projects?
A) 1,000 items B) 5,000 items C) 10,000 items D) 100,000 items
Answer: C – Most PFP collections have 10,000 items as the standard size.

Quiz Questions (11–15)

Q11. Which generative art project was Art Blocks' first release?
A) Fidenza B) Ringers C) Chromie Squiggle D) Autoglyphs
Answer: C – Chromie Squiggle by Snowfro was the first project with 10,000 outputs.

Q12. What programming language is commonly used for Art Blocks generative algorithms?
A) Python B) Solidity C) JavaScript (p5.js) D) Rust
Answer: C – Artists use JavaScript with the p5.js library for generative algorithms.

Q13. According to the social capital thesis, why do NFTs have value?
A) They generate passive income
B) They can be exchanged for physical goods
C) They signal wealth, taste, and community affiliation
D) They are backed by government guarantees
Answer: C – NFTs represent digital social capital through signaling and status.

Q14. Which criterion is NOT part of the digital art valuation framework?
A) Artist reputation and exhibition history
B) Number of Twitter followers
C) Provenance (ownership history)
D) Scarcity (1/1 vs. edition size)
Answer: B – Twitter followers are not a formal valuation criterion.

Q15. What is a "blue-chip" NFT collection?
A) Collections themed around the color blue
B) Established collections with sustained demand and liquidity
C) NFTs that only appreciate in value
D) Collections created by verified artists only
Answer: B – Blue-chip NFTs have 2+ years of trading history and bear market resilience.

Quiz Questions (16–20)

Q16. What was significant about CryptoPunks' creation in 2017?
A) They were the first NFTs ever created
B) They pre-dated the ERC-721 standard
C) They cost 1 ETH to mint
D) They were created by Yuga Labs
Answer: B – CryptoPunks used a custom contract before ERC-721 existed.

Q17. Which of the following is an example of a 1/1 digital art platform?
A) Art Blocks B) OpenSea (any category) C) SuperRare D) Axie Infinity
Answer: C – SuperRare is a curated marketplace for unique 1/1 digital artworks.

Q18. What determines the uniqueness of each generative art piece in a collection?
A) The artist manually selects traits
B) The algorithm uses a random seed (from transaction hash)
C) Collectors vote on the design
D) Time of day when minted
Answer: B – Transaction hash provides a unique random seed for the algorithm.

Q19. What was the peak floor price of Bored Ape Yacht Club in April 2022?
A) 15.3 ETH B) 53 ETH C) 153 ETH D) 1,530 ETH
Answer: C – BAYC reached a floor price of 153 ETH (approximately $500k+).

Q20. Which factor is most important for generative art valuation?
A) Physical gallery exhibitions
B) On-chain code storage and algorithmic rarity
C) Number of social media likes
D) Government art certifications
Answer: B – Generative art value depends on on-chain permanence and trait rarity.

L25: Digital Art and Collectibles

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Beeple $69M sale shock

[COMIC: placeholder]

A Christie's auctioneer in shock as the hammer falls on "Everydays" for $69.3M. Traditional art collectors fainting while crypto whales in hoodies casually bid on their phones. One whale: "That's only 42,329 ETH, I'll take it."

The Moment Everything Changed

- March 2021: Christie's sells a JPEG
- Third-highest price for living artist
- Traditional art world meets crypto

What We'll Explore

- 1/1 art vs. editions vs. generative
- PFP collections and social capital
- Valuation frameworks for digital art

Beeple's sale legitimized NFT art—and raised questions about what makes it valuable

Learning Objectives

By the end of this lesson, you will be able to:

- Distinguish between 1/1 art (single unique artwork), editions, and generative art (algorithm-created) NFTs
- Explain generative art (algorithm-created) platforms and on-chain algorithms (Art Blocks)
- Analyze PFP collections (Profile Picture avatars) and their cultural significance (BAYC, CryptoPunks)
- Apply valuation frameworks to digital art NFTs
- Evaluate the impact of high-profile sales (Beeple $69M)

Building on L24: Lab: OpenSea Analysis

The Problem: Why do some NFTs hold value?

The Challenge
In a market with millions of NFT collections, most digital assets go to zero while a select few trade at life-changing prices. What separates valuable NFTs from worthless JPEGs?

Why It Matters

- Over $40 billion traded in NFTs (2021-2023), yet 95% of collections are worthless
- CryptoPunks floor price: $100k+ while thousands of PFP projects collapsed

What We Need

- Value creation and capture mechanisms
- Framework for evaluating NFT value propositions beyond speculation

The Cryptoeconomics Question
Creating and distributing economic value in digital collectibles

Today's lesson: How digital art and collectibles address this challenge

What Are the Three Types of NFT Art?

Three Primary Categories:

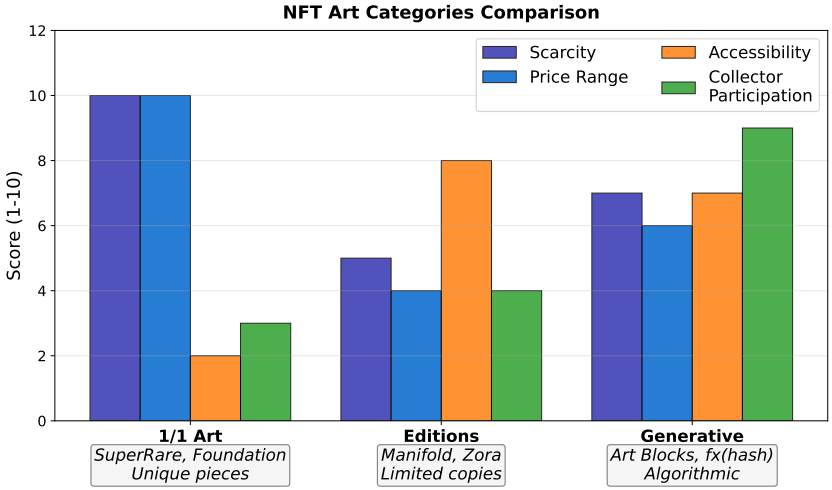
1. **1/1 Digital Art** – Unique, single-edition artwork (SuperRare, Foundation)
2. **Editions** – Multiple identical copies (Manifold, Zora)
3. **Generative Art** – Algorithm-created unique outputs (Art Blocks)

Key Differences:

- Scarcity: 1/1 highest, editions moderate, generative varies
- Price: 1/1 premium, editions accessible, generative mid-range
- Collector participation: Generative highest (mint reveals (random traits at purchase))

→ *Problem: Why do some NFTs hold value? — NFT Art Categories: 1/1 art has scarcity by definition; editions require creator reputation to hold value.*

NFT Art Categories Comparison



1/1 art commands highest prices; generative art offers collector participation

What Makes 1/1 Digital Art Unique?

Characteristics:

- Single NFT per artwork (no duplicates)
- Artist-signed and authenticated on-chain
- Direct artist-to-collector relationship

Leading 1/1 Platforms:

- **SuperRare (curated art marketplace):** Curated marketplace, invitation-only artists
- **Foundation:** Auction-based, community-curated
- **Nifty Gateway (celebrity art drops):** Drops from celebrity artists (Beeple, Pak)

Valuation Factors:

- Artist reputation and exhibition history
- Aesthetic quality and cultural relevance
- Provenance (ownership history)

(c) Joerg Osterrieder 2025

Case Study: Beeple's "Everydays" ($69M)

Event: March 2021, Christie's auction

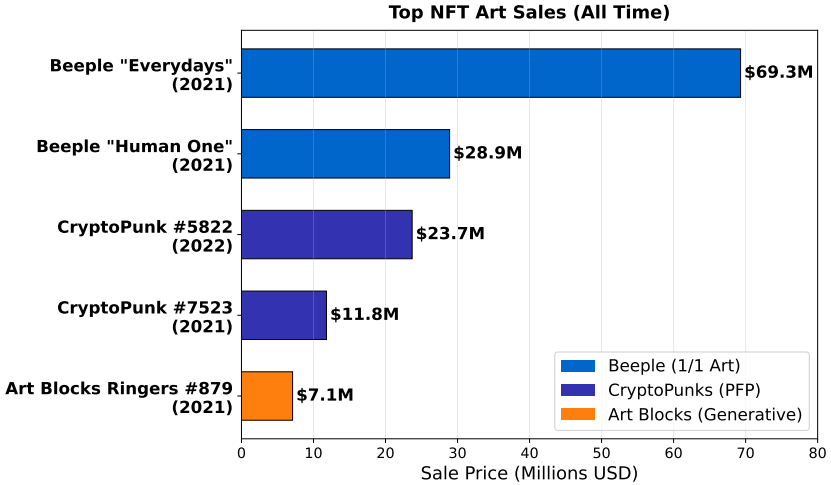
Artwork Details:

- Title: "Everydays: The First 5000 Days"
- Artist: Beeple (Mike Winkelmann)
- Format: Collage of 5,000 daily digital artworks (2007-2021)
- Sale price: $69.3 million (42,329 ETH at time)

Significance:

- Third-highest price for living artist (after Koons, Hockney)
- Legitimized NFTs in traditional art world
- Catalyzed NFT bull market (2021 peak)

High-Profile NFT Art Sales



Beeple's $69M sale remains the highest NFT art price; CryptoPunks dominate PFP sales | → Problem: Why do some NFTs hold value? — High-Profile NFT Art Sales: Generative art derives value from algorithm uniqueness and output rarity—not just visual appeal.

How Does Generative Art Create Unique Pieces?

Definition: Artwork generated by algorithmic code with controlled randomness

How It Works:

1. Artist writes generative algorithm (JavaScript, p5.js (JavaScript art library))
2. Algorithm uses random seed (algorithm starting number) (from transaction hash)
3. Each NFT mint produces unique output from same code

Appeal:

- Each piece is unique (seed-based randomness)
- Collector participates in creation (mint reveals outcome)
- On-chain code storage (true permanence)
- Lower price than 1/1s (algorithmic scalability)

How Does Art Blocks Generate On-Chain Art?

Founded: 2020 by Erick Calderon (Snowfro)

How Art Blocks Works:

1. Artist submits generative algorithm (JavaScript)
2. Collector mints NFT (pays ETH + gas)
3. Transaction hash seeds random number generator
4. Algorithm runs, generates unique output

Project Tiers:

- **Curated:** Highly selective, premium (Fidenza, Ringers)
- **Playground:** Emerging artists, experimental
- **Factory:** Open submissions, lower curation bar

Which Generative Projects Became Blue-Chip?

Fidenza by Tyler Hobbs (2021):

- 999 unique outputs, Flow field (code creating patterns) algorithm
- Mint: 0.17 ETH, Floor peak: 140 ETH ($500k+)

Ringers by Dmitri Cherniak (2021):

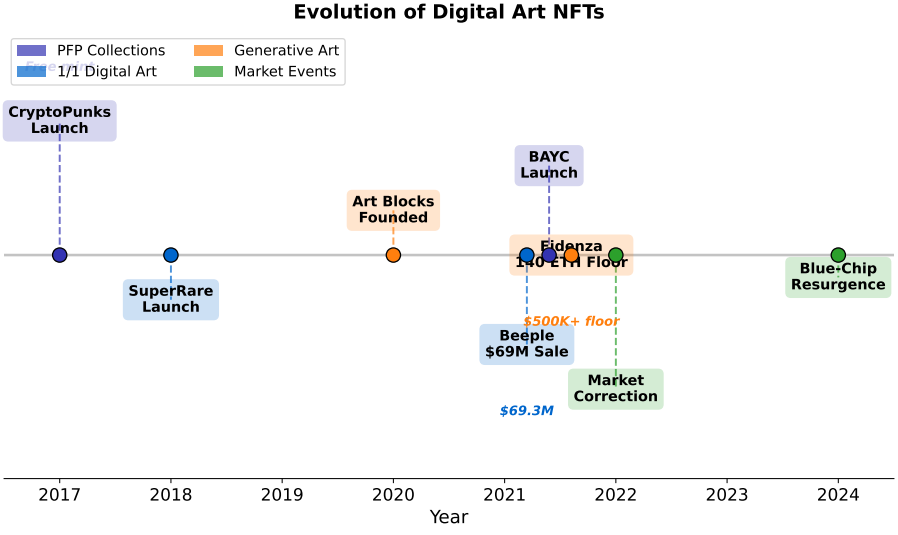
- 1,000 outputs, wrapped strings around pegs
- Mint: 0 ETH (free + gas), Floor peak: 25 ETH

Chromie Squiggle (2020):

- Art Blocks' first project (Snowfro)
- 10,000 outputs, "genesis" Art Blocks NFT

Rarity: Certain outputs extremely rare (algorithmic traits)

Evolution of Digital Art NFTs



From CryptoPunks (2017) to blue-chip resurgence: key milestones in NFT art history

PFP Collections: Profile Pictures as Identity

PFP: Profile Picture NFTs, avatar-style collectibles

Characteristics:

- 10,000-item collections (standard size)
- Trait-based variation (hat, eyes, background)
- Social signaling (Twitter/Discord avatars)
- Community membership and status

Leading PFP Collections:

- **CryptoPunks (2017):** 10,000 pixel art characters
- **Bored Ape Yacht Club (2021):** 10,000 apes, Yuga Labs
- **Azuki (2022):** 10,000 anime-style characters

Value Drivers: Brand recognition, community, utility, celebrities

→ *Problem: Why do some NFTs hold value? — PFP Collections: Profile Pictures as Identity: PFP value comes from community (club membership) not just image aesthetics.*

Problem Check-In: Digital Art & Collectibles

Recall Our Problem

Why do some NFTs hold value?

What We've Learned So Far

- 1/1 digital art has inherent scarcity; editions (10+) require artist reputation for value
- Generative art (Art Blocks, p5.js) creates unique outputs from algorithms—rarity is mathematical
- Value comes from scarcity + provenance + community—95% of collections have none of these

Still to Address

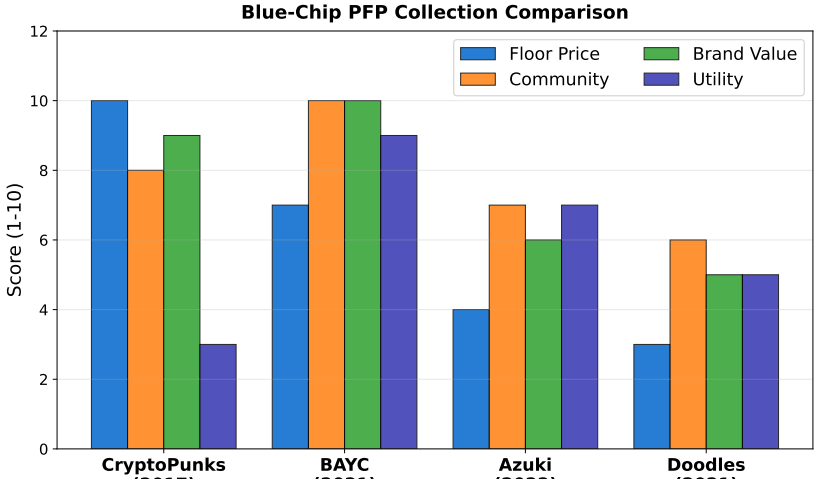
- PFP collection dynamics (CryptoPunks, BAYC) and community-driven value
- Why did Beeple's $69M sale succeed when most digital art sells for nothing?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "Why do some NFTs hold value?"?

Blue-Chip PFP Collection Comparison



Floor prices (2024): CryptoPunks ~50 ETH, BAYC ~25 ETH, Azuki ~3 ETH, Doodles ~2 ETH

BAYC leads in utility and community; CryptoPunks maintain highest floor prices

Why Are CryptoPunks Valuable?

Created: June 2017 by Larva Labs

Technical Details:

- 10,000 unique 24x24 pixel art characters
- Originally free to claim (gas only)
- Pre-dates ERC-721 standard (custom contract before standard)

Rarity Breakdown:

- 6,039 Male — 3,840 Female — 88 Zombie
- 24 Ape — 9 Alien (rarest, ¿10,000 ETH peak)

Cultural Impact: Inspired entire PFP category, held by Jay-Z, Snoop Dogg

What Made Bored Apes More Than Just Art?

Created: April 2021 by Yuga Labs

Key Innovations:

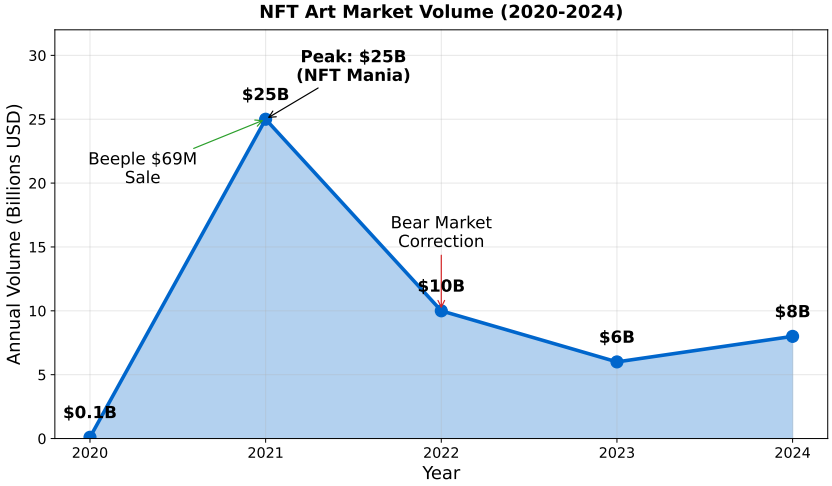
- **IP rights:** Holders own commercial rights to their ape
- **Community events:** Exclusive parties, metaverse experiences
- **Airdrops:** Free Mutant Apes, ApeCoin tokens

Valuation Milestones:

- Mint price: 0.08 ETH (April 2021)
- Floor peak: 153 ETH ($500k+, April 2022)
- Current floor (2024): 20-30 ETH range

Celebrity Holders: Eminem, Stephen Curry, Paris Hilton

NFT Art Market Trends



2021 peak driven by Beeple sale and mainstream adoption; market stabilizing post-correction | → Problem: Why do some NFTs hold value? — NFT Art Market Trends: Provenance (ownership history) creates value—a CryptoPunk owned by celebrities is worth more.

Why Do People Pay Millions for PFP NFTs?

Argument: NFTs represent digital social capital and identity

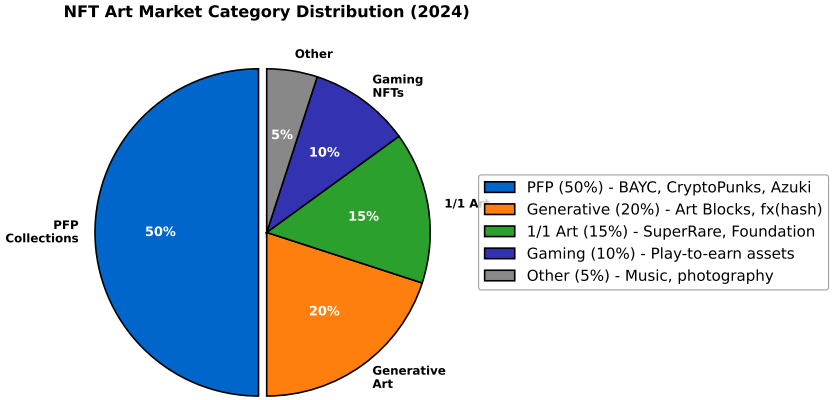
Mechanisms:

- **Signaling:** PFP shows wealth, taste, community affiliation
- **Access:** Token-gated (token holders only) Discord channels, events, alpha groups (exclusive investment info)
- **Status:** Owning rare/expensive NFTs confers prestige
- **Network effects:** Value increases with community size

Comparison to Luxury Goods:

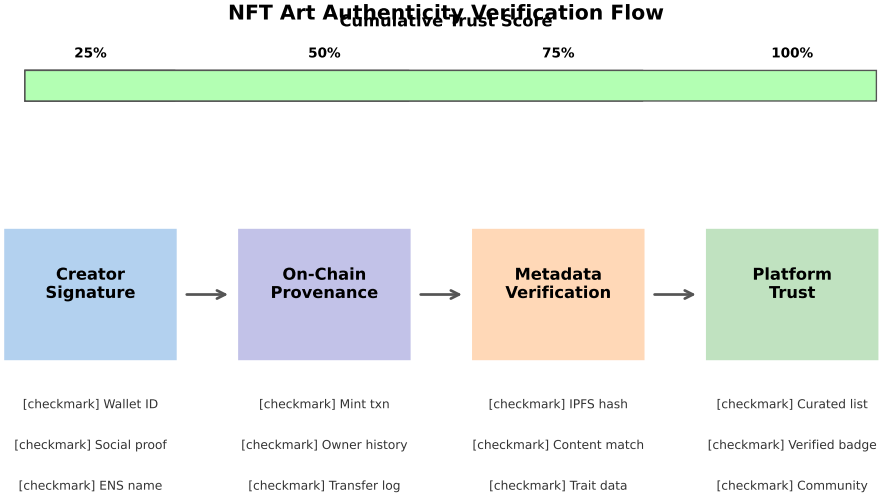
- Rolex watch: $10k+ for timekeeping (social signal)
- Bored Ape: $100k+ for pixel art (social signal)
- Both: Functional value ¡¡ social signaling value

NFT Art Category Distribution



PFP collections dominate volume; generative art growing among collectors

Art Authenticity Verification



How Do We Value Digital Art NFTs?

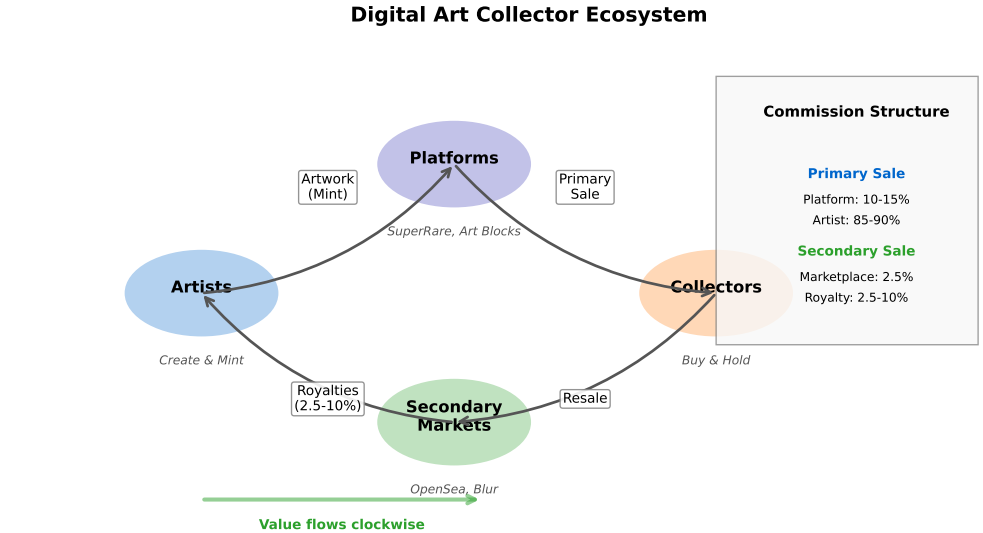
Key Criteria:

1. **Artist reputation:** Exhibition history, awards, following
2. **Scarcity:** 1/1 vs. edition size
3. **Provenance:** Ownership history (celebrity collectors)
4. **Cultural significance:** Historical impact, media coverage
5. **Technical quality:** Metadata storage (IPFS)
6. **Market comparables:** Similar artist sales

Example Valuation:

- Established artist, 1/1 artwork, IPFS storage
- Recent comparable: 5 ETH $\rightarrow$ Range: 4-6 ETH

(c) Joerg Osterrieder 2025


Digital Art Collector Ecosystem
Platforms
Artwork (Mint)
Primary Sale
SuperRare, Art Blocks
Artists
Collectors
Create & Mint
Buy & Hold
Royalties (2.5-10%)
Secondary Markets
Resale
OpenSea, Blur
Value flows clockwise
Commission Structure
Primary Sale
Platform: 10-15%
Artist: 85-90%
Secondary Sale
Marketplace: 2.5%
Royalty: 2.5-10%

What Defines a Blue-Chip NFT Collection?

Blue-Chip: Established collections with sustained demand and liquidity

Criteria:

- 2+ years of trading history
- Consistent floor price support (bear market resilience)
- Strong community and holder base
- Cultural significance and brand recognition

Current Blue-Chips (2024):

- CryptoPunks (50+ ETH floor)
- Bored Ape Yacht Club (20-30 ETH floor)
- Autoglyphs (on-chain generative, 100+ ETH floor)
- Art Blocks Curated projects (Fidenza, Ringers)

(c) Joerg Osterrieder 2025

Problem Solved? Digital Art & Collectibles

The Original Problem

Why do some NFTs hold value?

How Digital Art & Collectibles Solve It

- Community and cultural significance create sustained demand (BAYC, CryptoPunks)
- Utility (access, governance, IP rights) adds tangible value beyond aesthetics
- Provenance and scarcity mechanisms differentiate blue-chip collections

Remaining Limitations

- Highly speculative with subjective value determination
- Illiquid markets with volatile floor prices

Open Questions

- What makes digital collectibles a lasting asset class vs. temporary speculation?
- Can NFT value persist without constant community engagement and hype?

Digital art partially solves "Why do some NFTs hold value" through community and utility, but introduces volatility

The Economics of Digital Art & Collectibles

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Digital Art & Collectibles

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Digital Art & Collectibles

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

! Unusual economic behavior

! Incentive misalignment

! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

(c) Joerg Osterrieder 2025

Art authenticity verification

[COMIC: placeholder]

Two identical-looking NFTs side by side. One has a verified checkmark and provenance trail back to the original artist. The other has "DEFINITELY REAL BEEPLE" written in Comic Sans with a sketchy contract address. A buyer asks: "How do I tell which is real?"

Trust in Digital Art

- Anyone can mint an image
- Authenticity = creator signature
- Provenance = on-chain ownership trail

Verification Checklist

- Check creator's verified accounts
- Trace contract to official sources
- Review ownership history on-chain

Digital scarcity is meaningless without verified authenticity

Key Takeaways

1. NFT art includes 1/1 unique pieces, limited editions, and generative algorithmic art
2. Generative platforms (Art Blocks) create unique outputs from code using randomness
3. PFP collections (BAYC, CryptoPunks) derive value from community and social capital
4. Beeple's $69M sale catalyzed mainstream NFT adoption but raised speculation concerns
5. Valuation combines traditional art criteria with on-chain metrics and community factors
6. Blue-chip NFTs show resilience through market cycles due to cultural significance

Next Lesson: L26 – Gaming NFTs and Metaverse

(c) Joerg Osterrieder 2025

Discussion Questions

1. Is digital art fundamentally different from physical art in terms of value and ownership?
2. What distinguishes a blue-chip NFT collection from a speculative project?
3. How should generative art be valued compared to artist-created 1/1 pieces?
4. Will PFP collections retain value long-term, or are they a temporary trend?
5. Should NFT marketplaces curate art quality, or remain open platforms?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L26: Gaming NFTs and Metaverse

We will explore:

- Play-to-earn gaming model and tokenomics
- Case study: Axie Infinity rise and collapse
- Virtual land NFTs (Decentraland, The Sandbox)
- Interoperability and cross-game asset portability
- Sustainability challenges of blockchain gaming

Preparation: Explore Decentraland or The Sandbox metaverse platforms

Quiz Questions (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper than generative art
B) Generative art uses algorithms with controlled randomness; 1/1 art is unique artist-created pieces
C) 1/1 art has multiple editions; generative art does not
D) Generative art cannot be stored on-chain
Answer: B – Generative art is created by code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9 million B) $69.3 million C) $6.9 billion D) $693 million
Answer: B – Sold for $69.3 million at Christie's in March 2021.

Q3. Which platform is the premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in generative art using on-chain code.

Q4. How does Art Blocks generate unique artwork for each NFT?
A) Artists manually create each piece
B) Random images are selected from a database
C) Transaction hash seeds a random number generator in the algorithm
D) Collectors upload their own designs
Answer: C – Transaction hash seeds the RNG for unique outputs.

Q5. What does PFP stand for in the context of NFT collections?
A) Proof of Purchase B) Profile Picture C) Public Financial Protocol D) Permanently Fixed Price
Answer: B – PFP refers to Profile Picture NFTs used as avatars.

Quiz Questions (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – Larva Labs created 10,000 unique 24x24 pixel art CryptoPunks in June 2017.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88 total) B) Ape (24 total) C) Alien (9 total) D) Female (3,840 total)
Answer: C – Only 9 Alien CryptoPunks exist with peak values over 10,000 ETH.

Q8. What was the mint price of Bored Ape Yacht Club NFTs in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – BAYC minted at 0.08 ETH before reaching a floor peak of 153 ETH.

Q9. Which innovative feature did Bored Ape Yacht Club introduce?
A) Free minting for all users
B) Commercial IP rights for NFT holders
C) Physical artwork redemption
D) Automatic price appreciation
Answer: B – BAYC holders own full commercial rights to their ape.

Q10. What is the standard collection size for most PFP NFT projects?
A) 1,000 items B) 5,000 items C) 10,000 items D) 100,000 items
Answer: C – Most PFP collections have 10,000 items as the standard size.

Quiz Questions (11–15)

Q11. Which generative art project was Art Blocks' first release?
A) Fidenza B) Ringers C) Chromie Squiggle D) Autoglyphs
Answer: C – Chromie Squiggle by Snowfro was the first project with 10,000 outputs.

Q12. What programming language is commonly used for Art Blocks generative algorithms?
A) Python B) Solidity C) JavaScript (p5.js) D) Rust
Answer: C – Artists use JavaScript with the p5.js library for generative algorithms.

Q13. According to the social capital thesis, why do NFTs have value?
A) They generate passive income
B) They can be exchanged for physical goods
C) They signal wealth, taste, and community affiliation
D) They are backed by government guarantees
Answer: C – NFTs represent digital social capital through signaling and status.

Q14. Which criterion is NOT part of the digital art valuation framework?
A) Artist reputation and exhibition history
B) Number of Twitter followers
C) Provenance (ownership history)
D) Scarcity (1/1 vs. edition size)
Answer: B – Twitter followers are not a formal valuation criterion.

Q15. What is a "blue-chip" NFT collection?
A) Collections themed around the color blue
B) Established collections with sustained demand and liquidity
C) NFTs that only appreciate in value
D) Collections created by verified artists only
Answer: B – Blue-chip NFTs have 2+ years of trading history and bear market resilience.

Quiz Questions (16–20)

Q16. What was significant about CryptoPunks' creation in 2017?
A) They were the first NFTs ever created
B) They pre-dated the ERC-721 standard
C) They cost 1 ETH to mint
D) They were created by Yuga Labs
Answer: B – CryptoPunks used a custom contract before ERC-721 existed.

Q17. Which of the following is an example of a 1/1 digital art platform?
A) Art Blocks B) OpenSea (any category) C) SuperRare D) Axie Infinity
Answer: C – SuperRare is a curated marketplace for unique 1/1 digital artworks.

Q18. What determines the uniqueness of each generative art piece in a collection?
A) The artist manually selects traits
B) The algorithm uses a random seed (from transaction hash)
C) Collectors vote on the design
D) Time of day when minted
Answer: B – Transaction hash provides a unique random seed for the algorithm.

Q19. What was the peak floor price of Bored Ape Yacht Club in April 2022?
A) 15.3 ETH B) 53 ETH C) 153 ETH D) 1,530 ETH
Answer: C – BAYC reached a floor price of 153 ETH (approximately $500k+).

Q20. Which factor is most important for generative art valuation?
A) Physical gallery exhibitions
B) On-chain code storage and algorithmic rarity
C) Number of social media likes
D) Government art certifications
Answer: B – Generative art value depends on on-chain permanence and trait rarity.

L25: Digital Art and Collectibles

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

January 2026

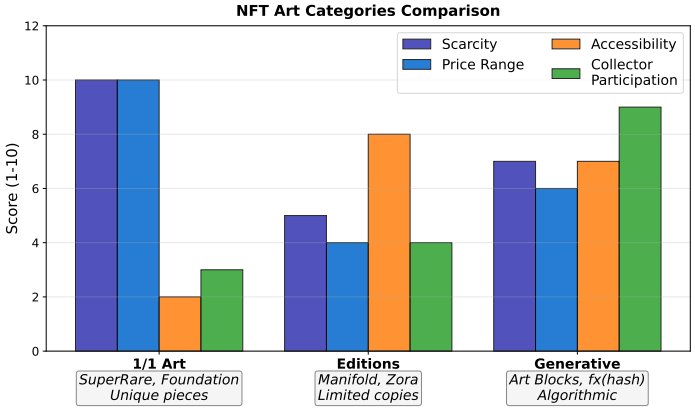
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

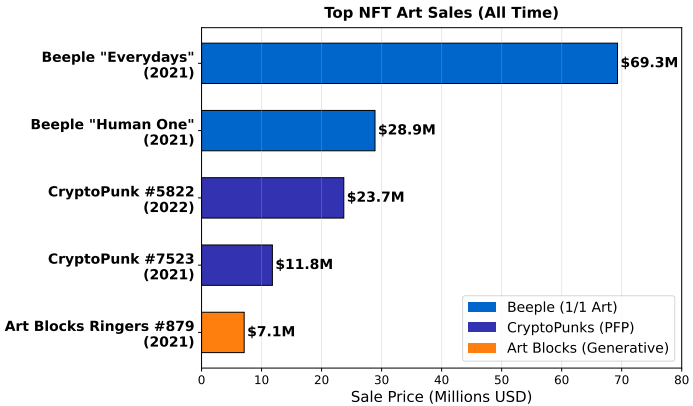
- Distinguish between 1/1 art, editions, and generative art
- Explain generative art platforms (Art Blocks)
- Analyze PFP collections and their cultural significance
- Apply valuation frameworks to digital art NFTs

NFT Art Categories Comparison



1/1 art: Highest prices — **Generative:** Collector participation in creation

High-Profile NFT Art Sales



Beeple's $69M sale (March 2021) remains the highest NFT art price.

Generative Art: Code as Artist

How It Works:

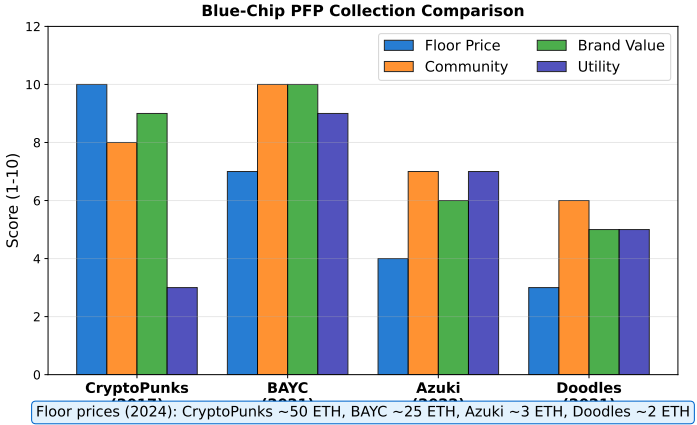
1. Artist writes generative algorithm (JavaScript, p5.js)
2. Algorithm uses random seed (from transaction hash)
3. Each NFT mint produces unique output from same code

Art Blocks (Founded 2020):

- **Curated:** Highly selective (Fidenza, Ringers)
- **Playground:** Emerging artists
- **Factory:** Open submissions

Appeal: Each piece unique, collector participates in creation, on-chain permanence.

PFP Collection Comparison



Floor prices (2024): CryptoPunks ~50 ETH, BAYC ~25 ETH, Azuki ~3 ETH, Doodles ~2 ETH

BAYC: Leads in utility — **CryptoPunks:** Highest floor prices

Blue-Chip NFT Case Studies

CryptoPunks (2017):

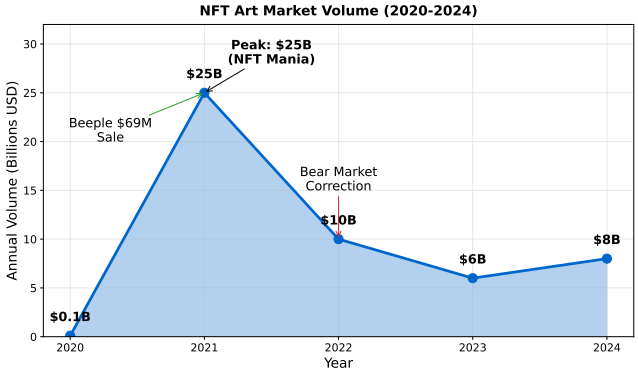
- 10,000 pixel art characters, pre-dates ERC-721
- 9 Aliens (rarest) peaked at 10,000+ ETH

Bored Ape Yacht Club (2021):

- Mint: 0.08 ETH, peak floor: 153 ETH ($500k+)
- Commercial IP rights granted to holders
- Celebrity holders: Eminem, Stephen Curry

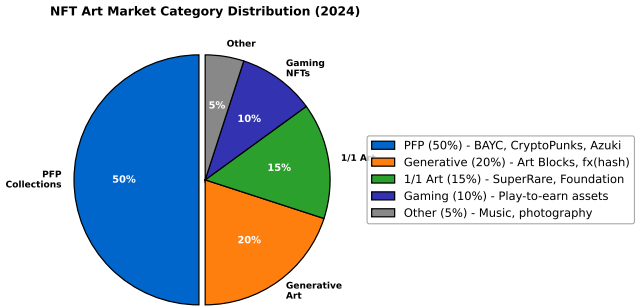
Current floors (2024-2025): CryptoPunks 50+ ETH, BAYC 20-30 ETH

NFT Art Market Trends



2021 peak: Beeple sale + mainstream adoption — **2022+:** Correction

NFT Art Category Distribution



PFP collections dominate volume; generative art growing among collectors.

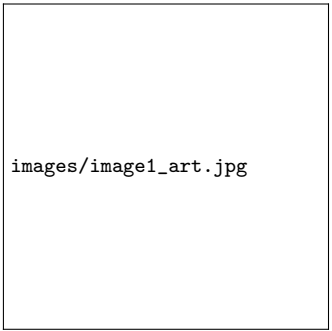
Key Takeaways

1. **Categories:** 1/1 unique, limited editions, generative algorithmic
2. **Generative Art:** Art Blocks uses code + transaction hash for unique outputs
3. **PFP Collections:** BAYC, CryptoPunks derive value from community
4. **Beeple $69M:** Catalyzed mainstream NFT adoption (March 2021)
5. **Blue-Chips:** 2+ year history, bear market resilience, cultural significance

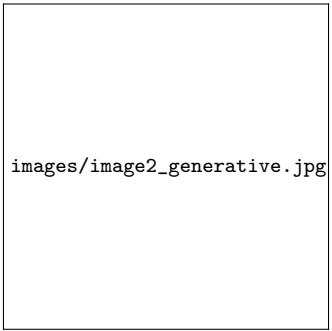
Social Capital Thesis: NFTs signal wealth, taste, and community affiliation.

(c) Joerg Osterrieder 2025

Digital Art and Collectibles in Practice



Digital Art



Generative Art

PFP Collections

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Difference between 1/1 art and generative art?
A) 1/1 cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative not on-chain

Quiz (1/2)

Q1. Difference between 1/1 art and generative art?
A) 1/1 cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative not on-chain
Answer: B – Generative art created by code with seed-based randomness.

Q2. Sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9M B) $69.3M C) $6.9B D) $693M

Quiz (1/2)

Q1. Difference between 1/1 art and generative art?
A) 1/1 cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative not on-chain
Answer: B – Generative art created by code with seed-based randomness.

Q2. Sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9M B) $69.3M C) $6.9B D) $693M
Answer: B – Sold for $69.3M at Christie's March 2021.

Q3. Premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway

(c) Joerg Osterrieder 2025

Quiz (1/2)

Q1. Difference between 1/1 art and generative art?
A) 1/1 cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative not on-chain
Answer: B – Generative art created by code with seed-based randomness.

Q2. Sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9M B) $69.3M C) $6.9B D) $693M
Answer: B – Sold for $69.3M at Christie's March 2021.

Q3. Premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in generative art.

Q4. How many CryptoPunks were created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000

Quiz (1/2)

Q1. Difference between 1/1 art and generative art?
A) 1/1 cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative not on-chain
Answer: B – Generative art created by code with seed-based randomness.

Q2. Sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9M B) $69.3M C) $6.9B D) $693M
Answer: B – Sold for $69.3M at Christie's March 2021.

Q3. Premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in generative art.

Q4. How many CryptoPunks were created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters (June 2017).

Q5. What does PFP stand for?
A) Proof of Purchase B) Profile Picture C) Public Finance D) Permanent File

Quiz (1/2)

Q1. Difference between 1/1 art and generative art?
A) 1/1 cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative not on-chain
Answer: B – Generative art created by code with seed-based randomness.

Q2. Sale price of Beeple's "Everydays: The First 5000 Days"?
A) $6.9M B) $69.3M C) $6.9B D) $693M
Answer: B – Sold for $69.3M at Christie's March 2021.

Q3. Premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in generative art.

Q4. How many CryptoPunks were created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters (June 2017).

Q5. What does PFP stand for?
A) Proof of Purchase B) Profile Picture C) Public Finance D) Permanent File
Answer: B – Profile Picture NFTs used as avatars.

Quiz (2/2)

Q6. Rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)

Quiz (2/2)

Q6. Rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens, peak values over 10,000 ETH.

Q7. BAYC mint price in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH

Quiz (2/2)

Q6. Rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens, peak values over 10,000 ETH.

Q7. BAYC mint price in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – Minted at 0.08 ETH, peak floor 153 ETH.

Q8. Innovative feature BAYC introduced?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation

Quiz (2/2)

Q6. Rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens, peak values over 10,000 ETH.

Q7. BAYC mint price in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – Minted at 0.08 ETH, peak floor 153 ETH.

Q8. Innovative feature BAYC introduced?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation
Answer: B – BAYC holders own full commercial rights.

Q9. What was Art Blocks' first project?
A) Fidenza B) Ringers C) Chromie Squiggle D) Autoglyphs

Quiz (2/2)

Q6. Rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens, peak values over 10,000 ETH.

Q7. BAYC mint price in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – Minted at 0.08 ETH, peak floor 153 ETH.

Q8. Innovative feature BAYC introduced?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation
Answer: B – BAYC holders own full commercial rights.

Q9. What was Art Blocks' first project?
A) Fidenza B) Ringers C) Chromie Squiggle D) Autoglyphs
Answer: C – Chromie Squiggle by Snowfro (10,000 outputs).

Q10. Why do NFTs have value according to social capital thesis?
A) Generate income B) Exchange for goods C) Signal wealth, taste, community D) Government backing

Quiz (2/2)

Q6. Rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens, peak values over 10,000 ETH.

Q7. BAYC mint price in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – Minted at 0.08 ETH, peak floor 153 ETH.

Q8. Innovative feature BAYC introduced?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation
Answer: B – BAYC holders own full commercial rights.

Q9. What was Art Blocks' first project?
A) Fidenza B) Ringers C) Chromie Squiggle D) Autoglyphs
Answer: C – Chromie Squiggle by Snowfro (10,000 outputs).

Q10. Why do NFTs have value according to social capital thesis?
A) Generate income B) Exchange for goods C) Signal wealth, taste, community D) Government backing
Answer: C – NFTs represent digital social capital.

Thank you

Questions?

Next: L26 – Gaming NFTs and Metaverse

Quiz: Digital Art Collectibles

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative cannot be on-chain

Quiz (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative cannot be on-chain
Answer: B – Generative art uses code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays" at Christie's?
A) $6.9M B) $69.3M C) $693M D) $6.93B

Quiz (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative cannot be on-chain
Answer: B – Generative art uses code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays" at Christie's?
A) $6.9M B) $69.3M C) $693M D) $6.93B
Answer: B – Sold for $69.3 million in March 2021.

Q3. Which platform is the premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative cannot be on-chain
Answer: B – Generative art uses code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays" at Christie's?
A) $6.9M B) $69.3M C) $693M D) $6.93B
Answer: B – Sold for $69.3 million in March 2021.

Q3. Which platform is the premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in on-chain generative art.

Q4. How does Art Blocks generate unique artwork for each NFT?
A) Artists create manually B) Random database selection C) Transaction hash seeds RNG D) Collector uploads

Quiz (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative cannot be on-chain
Answer: B – Generative art uses code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays" at Christie's?
A) $6.9M B) $69.3M C) $693M D) $6.93B
Answer: B – Sold for $69.3 million in March 2021.

Q3. Which platform is the premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in on-chain generative art.

Q4. How does Art Blocks generate unique artwork for each NFT?
A) Artists create manually B) Random database selection C) Transaction hash seeds RNG D) Collector uploads
Answer: C – Transaction hash provides unique random seed.

Q5. What does PFP stand for in NFT collections?
A) Proof of Purchase B) Profile Picture C) Public Financial Protocol D) Permanently Fixed Price

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary difference between 1/1 digital art and generative art NFTs?
A) 1/1 art is cheaper B) Generative uses algorithms with randomness C) 1/1 has editions D) Generative cannot be on-chain
Answer: B – Generative art uses code with seed-based randomness.

Q2. What was the sale price of Beeple's "Everydays" at Christie's?
A) $6.9M B) $69.3M C) $693M D) $6.93B
Answer: B – Sold for $69.3 million in March 2021.

Q3. Which platform is the premier marketplace for generative art NFTs?
A) OpenSea B) SuperRare C) Art Blocks D) Nifty Gateway
Answer: C – Art Blocks specializes in on-chain generative art.

Q4. How does Art Blocks generate unique artwork for each NFT?
A) Artists create manually B) Random database selection C) Transaction hash seeds RNG D) Collector uploads
Answer: C – Transaction hash provides unique random seed.

Q5. What does PFP stand for in NFT collections?
A) Proof of Purchase B) Profile Picture C) Public Financial Protocol D) Permanently Fixed Price
Answer: B – PFP refers to Profile Picture NFTs used as avatars.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000

Quiz (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)

Quiz (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens exist with peak values over 10,000 ETH.

Q8. What was the mint price of Bored Ape Yacht Club in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH

Quiz (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens exist with peak values over 10,000 ETH.

Q8. What was the mint price of Bored Ape Yacht Club in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – BAYC minted at 0.08 ETH before reaching 153 ETH peak.

Q9. Which innovative feature did BAYC introduce?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation

Quiz (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens exist with peak values over 10,000 ETH.

Q8. What was the mint price of Bored Ape Yacht Club in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – BAYC minted at 0.08 ETH before reaching 153 ETH peak.

Q9. Which innovative feature did BAYC introduce?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation
Answer: B – BAYC holders own full commercial rights to their ape.

Q10. What defines a "blue-chip" NFT collection?
A) Blue-themed art B) Established with 2+ years and sustained demand C) Only appreciates D) Verified artists only

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. How many CryptoPunks were originally created?
A) 1,000 B) 5,000 C) 10,000 D) 50,000
Answer: C – 10,000 unique 24x24 pixel art characters.

Q7. What is the rarest type of CryptoPunk?
A) Zombie (88) B) Ape (24) C) Alien (9) D) Female (3,840)
Answer: C – Only 9 Aliens exist with peak values over 10,000 ETH.

Q8. What was the mint price of Bored Ape Yacht Club in April 2021?
A) 0.08 ETH B) 0.8 ETH C) 8 ETH D) 80 ETH
Answer: A – BAYC minted at 0.08 ETH before reaching 153 ETH peak.

Q9. Which innovative feature did BAYC introduce?
A) Free minting B) Commercial IP rights for holders C) Physical redemption D) Auto appreciation
Answer: B – BAYC holders own full commercial rights to their ape.

Q10. What defines a "blue-chip" NFT collection?
A) Blue-themed art B) Established with 2+ years and sustained demand C) Only appreciates D) Verified artists only
Answer: B – Blue-chip NFTs have trading history and bear market resilience.

L26: Gaming NFTs and Metaverse

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the play-to-earn gaming model and tokenomics
- Analyze Axie Infinity's rise and collapse as a case study
- Evaluate virtual land NFTs in metaverse platforms
- Assess interoperability challenges for cross-game assets
- Identify sustainability issues in blockchain gaming economies

(c) Joerg Osterrieder 2025

The Problem: How do virtual economies work?

The Challenge
In traditional games, players spend billions on virtual items, but game companies control the economy. Items can't be sold or transferred. Virtual economies have no real ownership or market value outside the game ecosystem.

Why It Matters

- Global gaming market: $200B+, but players can't monetize their investments
- Historical example: Axie Infinity showed P2E potential (2.8M users), but collapsed 99%

What We Need

- Value creation and capture
- Sustainable virtual economies where players have true ownership and can earn value

The Cryptoeconomics Question
Creating and distributing economic value

Today's lesson: How Gaming NFTs & Metaverse addresses this challenge

Blockchain Gaming: Core Concepts

Traditional Gaming:

- Players pay for games and in-game items
- Items locked to game (no true ownership)
- Value accrues to game company, not players

Blockchain Gaming:

- In-game assets are NFTs (player-owned)
- Items tradable on open marketplaces
- Players can earn cryptocurrency while playing
- Potential for cross-game asset portability

Promise: Players as stakeholders, value extraction to players

Play-to-Earn (P2E) Model

Concept: Players earn tokens/NFTs through gameplay

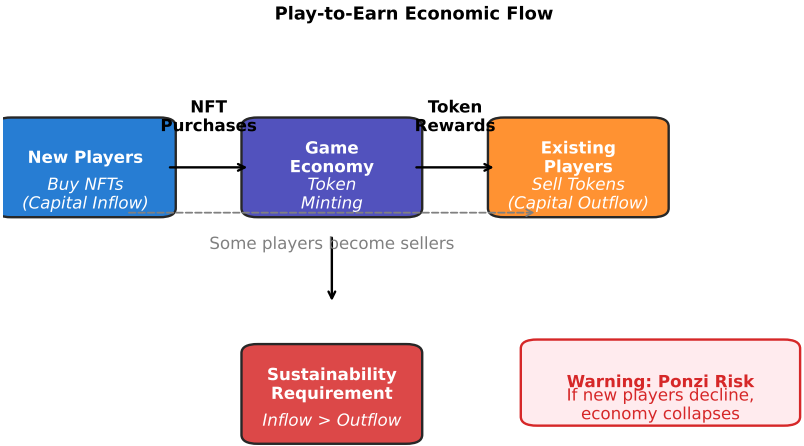
Mechanics:

1. Player acquires NFT characters/assets (upfront investment)
2. Player completes in-game tasks (battles, quests)
3. Game rewards player with tokens (cryptocurrency)
4. Player sells tokens on exchange

Economic Model:

- New players buy NFTs (inflow of capital)
- Existing players earn and sell tokens (outflow)
- Sustainability requires continuous new player demand

Play-to-Earn Economic Flow



P2E models resemble Ponzi dynamics: new player capital pays existing players

Axie Infinity: The P2E Pioneer

Game Overview:

- Creature-battling game (similar to Pokemon)
- Players collect, breed, and battle Axies (NFT creatures)
- Launched: 2018, exploded in popularity 2021

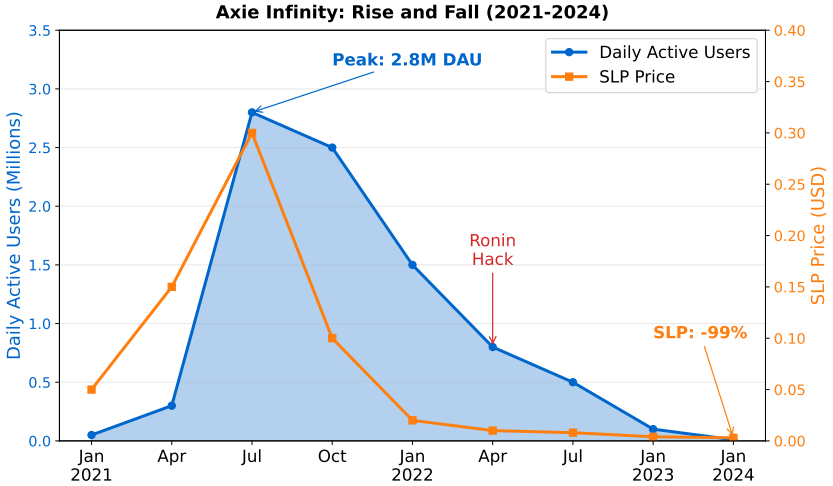
Tokenomics:

- **Axie NFTs:** Characters needed to play (3 required)
- **AXS:** Governance and staking token
- **SLP (Smooth Love Potion):** In-game reward token

Peak Stats (2021):

- 2.8 million daily active users
- Entry cost: $600-1000 (3 Axies)

Axie Infinity: Rise and Fall



SLP token collapsed 99%+; users dropped from 2.8M to ¡10K

Axie Infinity: What Went Wrong?

Fundamental Flaws:

1. **Ponzi Dynamics:** Relied on new player money to pay existing players
2. **Unlimited Inflation:** SLP had no supply cap (infinite minting)
3. **Weak Demand Sinks:** Breeding not enough to absorb SLP supply
4. **High Entry Barrier:** $600-1000 deterred new players
5. **Gameplay Quality:** Repetitive, grind-focused (not fun)

Lesson: P2E model requires genuine value creation, not just token redistribution

Ronin Bridge Hack (March 2022)

Incident: Largest DeFi hack in history

Details:

- **Target:** Ronin Network (Ethereum sidechain for Axie)
- **Amount stolen:** 173,600 ETH + 25.5M USDC = $625M
- **Attack vector:** Social engineering of validators
- **Discovery:** Hack unnoticed for 6 days

Impact:

- Player confidence shattered
- Accelerated player exodus

Lesson: Centralized bridges are critical vulnerabilities

Virtual Land NFTs: Metaverse Real Estate

Concept: Owning digital land parcels as NFTs in virtual worlds

Major Metaverse Platforms:

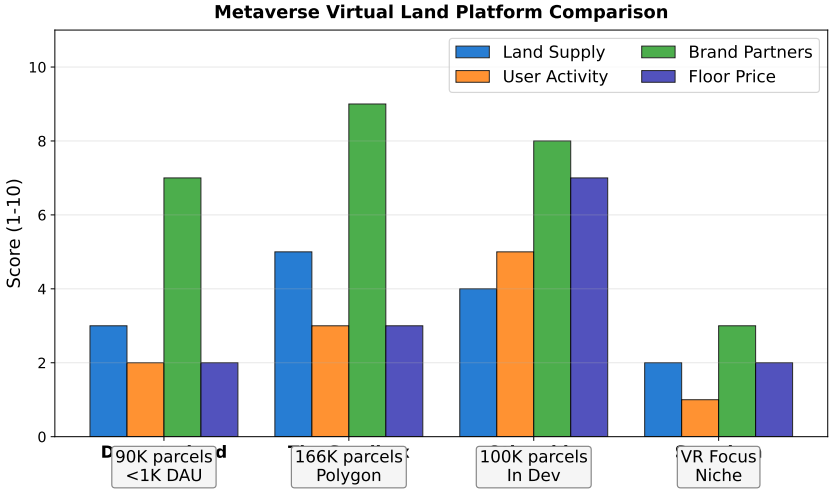
- **Decentraland:** Ethereum-based, 90,000 parcels
- **The Sandbox:** Polygon-based, 166,464 parcels
- **Otherside (Yuga Labs):** BAYC metaverse, 100,000 parcels

Value Proposition:

- Build experiences (games, galleries, events)
- Monetize through rentals or advertising
- Speculate on location value

Reality: Low usage, most land undeveloped, speculation-driven

Metaverse Platform Comparison



All platforms struggle with low daily active users; brand partnerships exceed organic activity

Decentraland: The OG Metaverse

Launched: 2020, Ethereum-based

Structure:

- 90,000 LAND parcels (16x16 meter plots)
- MANA token: Currency for buying land
- DAO governance: Landowners vote on changes

Peak Hype (2021-2022):

- Prime land sold for $2.4M
- Brands: Samsung, Adidas, Sotheby's

Current State (2024):

- Daily active users: ¡1,000
- Floor price: $500-1,000 per parcel (down 90%+)

Interoperability: The Cross-Game Asset Dream

Vision: NFT items usable across multiple games

Example Scenarios:

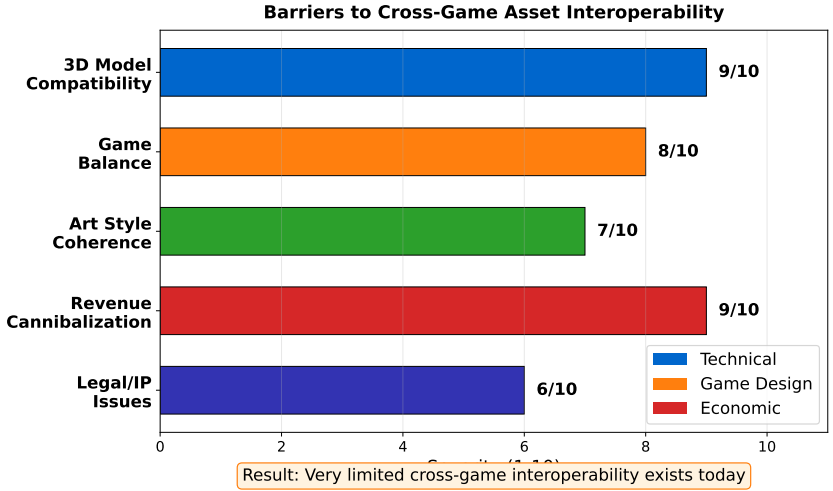
- Sword earned in Game A usable in Game B
- Avatar skin portable across virtual worlds
- Virtual real estate accessible from multiple platforms

Technical Challenges:

1. 3D model compatibility (different engines, formats)
2. Game balance (overpowered items)
3. Art style coherence
4. Legal/IP issues

Reality: Very limited interoperability today

Interoperability Barriers



Result: Very limited cross-game interoperability exists today

Economic and technical barriers make true cross-game asset portability extremely difficult

Sustainability of Blockchain Gaming

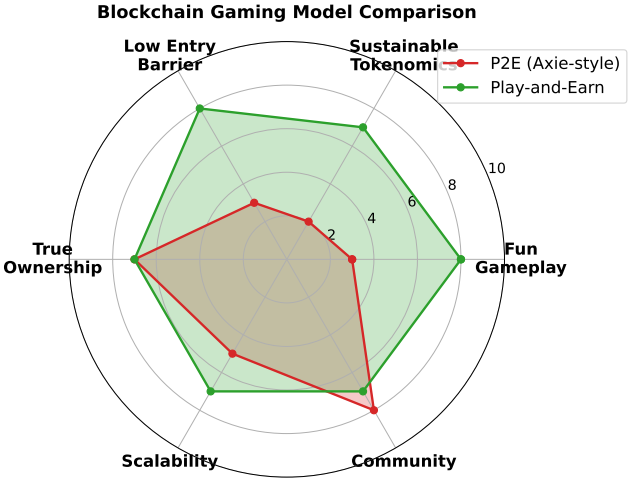
Concerns:

1. **Ponzi Tokenomics:** Most P2E models collapse without new players
2. **Gameplay Quality:** Focus on earning, not fun
3. **High Costs:** Gas fees, NFT entry barriers
4. **Regulatory Risk:** P2E may be classified as gambling

Potential Solutions:

- Shift to "play-and-earn" (fun first, earn secondary)
- Deflationary tokenomics (burning mechanisms)
- Layer 2 solutions (lower gas fees)
- Free-to-play with optional NFT purchases

Gaming Model Comparison



Play-and-Earn models score better on sustainability factors than traditional P2E

Play-and-Earn: The New Paradigm

Play-and-Earn: Prioritize gameplay quality, earnings as bonus

Contrast with P2E:

- **P2E:** Gameplay is work, earnings primary motivation
- **Play-and-Earn:** Gameplay is fun, earnings enhance experience

Examples:

- **Illuvium:** AAA-quality open-world RPG with NFT creatures
- **Ember Sword:** Free-to-play MMORPG with optional cosmetics
- **Gods Unchained:** Free-to-play card game, sustainable

Key Insight: Fun gameplay attracts organic users, reducing Ponzi dynamics

Blockchain Gaming Guilds

Guilds: Organizations that lend NFT assets to players

Scholarship Model:

1. Guild purchases NFT game assets
2. Guild lends assets to players (scholars)
3. Players earn tokens through gameplay
4. Earnings split: 70% player, 30% guild

Major Guilds:

- **Yield Guild Games (YGG):** Largest guild
- **Merit Circle:** DAO-governed

Decline: Axie collapse decimated guild revenues

Problem Solved? Gaming NFTs & Metaverse

The Original Problem

How do virtual economies work?

How Gaming NFTs & Metaverse Solves It

- Play-to-earn creates direct financial incentives for participation through token rewards
- NFT ownership enables true asset ownership and tradability on open markets
- Interoperability promises allow assets to be used across multiple games

Remaining Limitations

- Inflationary pressures from unlimited token minting (SLP case)
- Ponzi-like structures require continuous new player inflow to sustain earnings
- Fun vs. profit tension: gameplay quality suffers when earning is the primary goal

Open Questions

- Can play-to-earn be sustainable without constant new players?
- Risk: Extractive tokenomics, unsustainable yields

Gaming NFTs & Metaverse partially solves "virtual economies work" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Key Takeaways

1. Play-to-earn (P2E) models enable earning through gameplay but often resemble Ponzi schemes
2. Axie Infinity collapsed due to unsustainable tokenomics and unlimited SLP inflation
3. Virtual land NFTs (Decentraland, Sandbox) are speculation-driven with low actual usage
4. Interoperability of cross-game assets is limited by technical and economic barriers
5. Sustainable blockchain gaming requires fun-first design and balanced token economies
6. Play-and-Earn (fun primary, earning secondary) shows more promise

Discussion Questions

1. Can play-to-earn gaming models ever be sustainable without Ponzi dynamics?
2. What would make virtual land NFTs genuinely valuable beyond speculation?
3. Is true cross-game interoperability achievable, or a pipe dream?
4. Should blockchain games focus on financialization or gameplay quality?
5. How can regulators balance innovation with consumer protection in P2E gaming?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L27: Real-World Asset Tokenization

We will explore:

- RWA tokenization concept and mechanics
- Real estate tokenization platforms and legal frameworks
- Securities tokenization and compliance (Reg D, Reg S)
- Case study: BlackRock BUIDL fund ($500M+ on-chain)
- Market size: $50B on-chain, projected $18T by 2033

Preparation: Review traditional real estate investment structures (REITs)

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs
C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them
C) Players rent games from developers D) Players trade items within the game only
Answer: B – P2E allows earning cryptocurrency tokens by completing in-game tasks.

Q3. Why do P2E models often resemble Ponzi schemes?
A) They use complex technology B) New player capital pays existing players' earnings
C) They require internet connection D) They have high transaction fees
Answer: B – Requires continuous new player capital to fund existing players' earnings.

Q4. How many Axies were required to start playing Axie Infinity?
A) 1 Axie B) 2 Axies C) 3 Axies D) 5 Axies
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q5. What was Axie Infinity's peak daily active user count in 2021?
A) 500,000 B) 1.2 million C) 2.8 million D) 5 million
Answer: C – Peaked at 2.8 million users before collapsing to under 10,000.

Quiz Questions (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap
C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen (173,600 ETH + 25.5M USDC), largest DeFi hack at the time.

Q8. How long did the Ronin Bridge hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Undetected for 6 days, demonstrating critical security failures.

Q9. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q10. What is the approximate daily active user count for Decentraland in 2024?
A) Under 1,000 B) 5,000-10,000 C) 20,000-30,000 D) Over 50,000
Answer: A – Despite hype, under 1,000 daily active users in 2024.

Quiz Questions (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues
C) High gas fees D) Lack of users
Answer: B – Different engines, formats, balancing, and art style coherence issues.

Q13. What is the key difference between "play-to-earn" and "play-and-earn"?
A) Different blockchain networks B) Play-and-earn prioritizes fun gameplay, earnings as bonus
C) Play-and-earn requires more investment D) Play-to-earn uses NFTs, play-and-earn does not
Answer: B – Play-and-earn focuses on gameplay quality first, not earnings.

Q14. What was the typical earnings split in blockchain gaming guild scholarships?
A) 50% player, 50% guild B) 60% player, 40% guild
C) 70% player, 30% guild D) 80% player, 20% guild
Answer: C – 70% to players (scholars), 30% to guilds.

Q15. Which game is cited as an example of the play-and-earn model?
A) Axie Infinity B) Decentraland C) Gods Unchained D) CryptoKitties
Answer: C – Gods Unchained is a free-to-play card game with optional NFT elements.

Quiz Questions (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity
C) Metaverse NFT standard D) Layer 2 scaling solution
Answer: A – MANA is used to purchase LAND parcels in Decentraland.

Q18. What was the highest recorded sale price for prime Decentraland land?
A) $500,000 B) $1.2M C) $2.4M D) $5M
Answer: C – Prime Decentraland land sold for $2.4M during peak hype (2021-2022).

Q19. What is Yield Guild Games (YGG)?
A) A play-to-earn game B) Organization that lends NFT assets to players
C) A metaverse platform D) A DeFi protocol
Answer: B – YGG is the largest guild that lends NFT game assets to scholars.

Q20. Which solution is proposed to improve blockchain gaming sustainability?
A) Increase token inflation B) Higher entry fees
C) Shift to Layer 2 for lower gas fees D) Remove NFTs entirely
Answer: C – Layer 2 solutions reduce gas fees, improving accessibility and sustainability.

L26: Gaming NFTs and Metaverse

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Play-to-earn economics

[COMIC: placeholder]

A player in the Philippines celebrating "I'm earning $50/day playing Axies!" (2021). Next panel shows the same player in 2023 staring at a screen: "My SLP is worth $0.003 and I need 1000 new players to join so I can cash out." A Ponzi pyramid diagram forms in the background.

The P2E Promise

- Play games, earn real money
- 2.8M daily users at peak (Axie)
- Developing countries adopted it as income

What We'll Explore

- How P2E tokenomics work
- Why most models collapse
- Virtual land and metaverse economics

When earning requires new players, you're not in a game—you're in a pyramid

Learning Objectives

By the end of this lesson, you will be able to:

- Explain the play-to-earn (earning crypto via gameplay) gaming model and tokenomics (token economic design)
- Analyze Axie Infinity's rise and collapse as a case study
- Evaluate virtual land NFTs in metaverse platforms
- Assess interoperability challenges for cross-game assets
- Identify sustainability issues in blockchain gaming economies

Building on L25: Digital Art and Collectibles

The Problem: How do virtual economies work?

The Challenge
In traditional games, players spend billions on virtual items, but game companies control the economy. Items can't be sold or transferred. Virtual economies have no real ownership or market value outside the game ecosystem.

Why It Matters

- Global gaming market: $200B+, but players can't monetize their investments
- Historical example: Axie Infinity showed P2E (play-to-earn) potential (2.8M users), but collapsed 99%

What We Need

- Value creation and capture
- Sustainable virtual economies where players have true ownership and can earn value

The Cryptoeconomics Question
Creating and distributing economic value

Today's lesson: How Gaming NFTs & Metaverse addresses this challenge

How Do Blockchain Games Differ from Traditional Games?

Traditional Gaming:

- Players pay for games and in-game items
- Items locked to game (no true ownership)
- Value accrues to game company, not players

Blockchain Gaming:

- In-game assets are NFTs (player-owned)
- Items tradable on open marketplaces
- Players can earn cryptocurrency while playing
- Potential for cross-game asset portability

Promise: Players as stakeholders, value extraction to players

Traditional games keep 100% of virtual item value; NFT games let players own and trade.

What is Play-to-Earn?

Concept: Players earn tokens/NFTs through gameplay

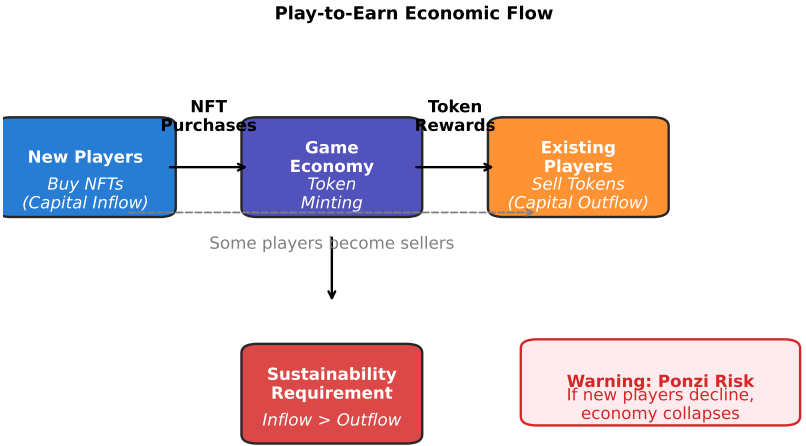
Mechanics:

1. Player acquires NFT characters/assets (upfront investment)
2. Player completes in-game tasks (battles, quests)
3. Game rewards player with tokens (cryptocurrency)
4. Player sells tokens on exchange

Economic Model:

- New players buy NFTs (inflow of capital)
- Existing players earn and sell tokens (outflow)
- Sustainability requires continuous new player demand

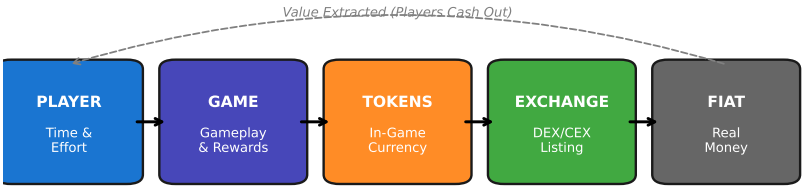
Play-to-Earn Economic Flow



P2E models resemble Ponzi dynamics (early paid by later—unsustainable): new player capital pays existing players

P2E Economic Sustainability: From Gameplay to Cash-Out

P2E Economic Flow: From Gameplay to Cash-Out



SUSTAINABILITY CONCERNS

Token Inflation	Ponzi Dynamics	Death Spiral	External Shocks
Unlimited minting devalues rewards	Early paid by later joiners	Price drop triggers mass exodus	Hack/regulation can collapse value

Critical concerns: token inflation, Ponzi dynamics, death spirals, and external shocks can collapse value

How Did Axie Infinity Work?

Game Overview:

- Creature-battling game (similar to Pokemon)
- Players collect, breed, and battle Axies (NFT creatures)
- Launched: 2018, exploded in popularity 2021

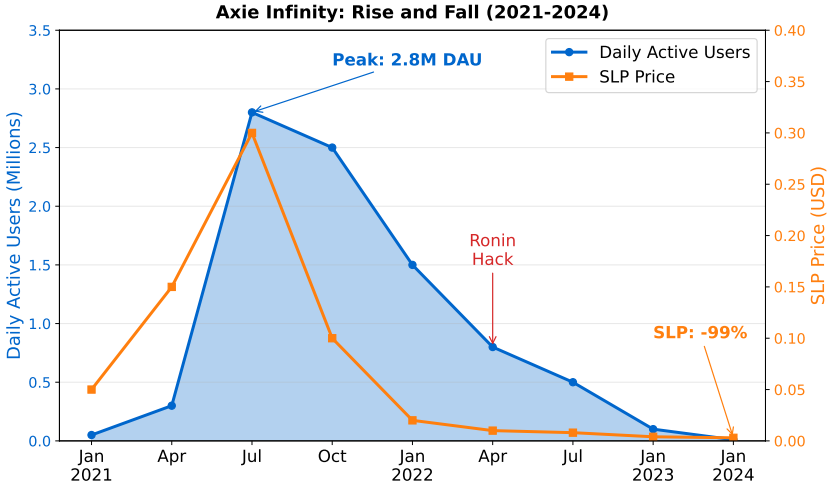
Tokenomics:

- **Axie NFTs:** Characters needed to play (3 required)
- **AXS:** Governance and staking token
- **SLP (Axie's reward token):** In-game reward token (Smooth Love Potion)

Peak Stats (2021):

- 2.8 million daily active users
- Entry cost: $600-1000 (3 Axies)

Axie Infinity: Rise and Fall



Play-to-earn sounds ideal but requires constant new players—Ponzi dynamics emerge.

Why Did Axie Infinity Collapse 99%?

Fundamental Flaws:

1. **Ponzi Dynamics:** Relied on new player money to pay existing players
2. **Unlimited Inflation:** SLP had no supply cap (infinite minting)
3. **Weak Demand Sinks (remove tokens from circulation):** Breeding not enough to absorb SLP supply
4. **High Entry Barrier:** $600-1000 deterred new players
5. **Gameplay Quality:** Repetitive, grind-focused (not fun)

Lesson: P2E model requires genuine value creation, not just token redistribution

What Happened in the Ronin Bridge Hack?

Incident: Largest DeFi hack in history

Details:

- **Target:** Ronin Network (Axie's blockchain) (Ethereum sidechain (separate lower-fee blockchain) for Axie)
- **Amount stolen:** 173,600 ETH + 25.5M USDC = $625M
- **Attack vector:** Social engineering (tricking into transactions) of validators
- **Discovery:** Hack unnoticed for 6 days

Impact:

- Player confidence shattered
- Accelerated player exodus

Lesson: Centralized bridges are critical vulnerabilities

Why Buy Virtual Land for Real Money?

Concept: Owning digital land parcels as NFTs in virtual worlds

Major Metaverse Platforms:

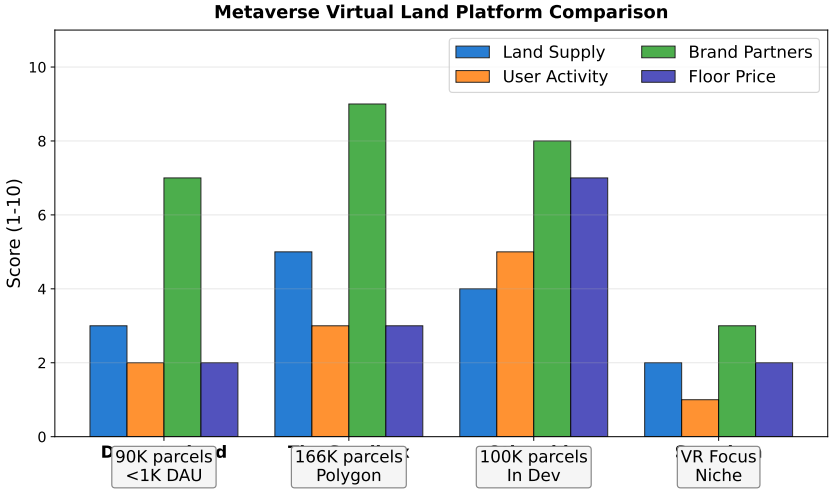
- **Decentraland (virtual world with land):** Ethereum-based, 90,000 parcels
- **The Sandbox (gaming metaverse):** Polygon-based, 166,464 parcels
- **Otherside (Yuga Labs):** BAYC metaverse, 100,000 parcels

Value Proposition:

- Build experiences (games, galleries, events)
- Monetize through rentals or advertising
- Speculate on location value

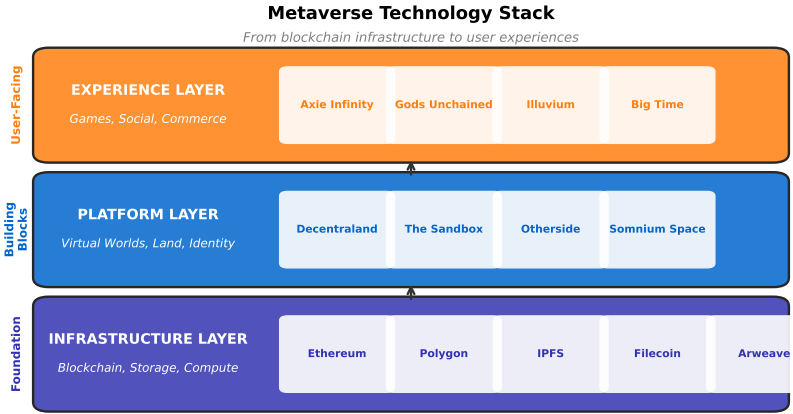
Reality: Low usage, most land undeveloped, speculation-driven

Metaverse Platform Comparison



Axie crashed because SLP had infinite supply with no demand sinks—tokenomics failure.

Metaverse Technology Stack



Experience layer apps depend on platform infrastructure, which relies on blockchain foundations

Problem Check-In: Gaming NFTs & Metaverse

Recall Our Problem

How do virtual economies work?

What We've Learned So Far

- Play-to-earn (P2E) gives players ownership of in-game items as NFTs
- Axie Infinity's SLP token had infinite inflation—price collapsed 99% when new players stopped joining
- Most P2E models are unsustainable Ponzi structures requiring constant growth

Still to Address

- Sustainable tokenomics: demand sinks, deflationary mechanisms, real utility
- Can blockchain games succeed without Ponzi dynamics? (See: Illuvium, Big Time attempts)

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do virtual economies work?"?

What is Decentraland?

Launched: 2020, Ethereum-based

Structure:

- 90,000 LAND parcels (16x16 meter plots)
- MANA token: Currency for buying land
- DAO governance (token holder voting): Landowners vote on changes

Peak Hype (2021-2022):

- Prime land sold for $2.4M
- Brands: Samsung, Adidas, Sotheby's

Current State (2024):

- Daily active users: ¡1,000
- Floor price: $500-1,000 per parcel (down 90%+)

Can NFT Assets Work Across Different Games?

Vision: NFT items usable across multiple games

Example Scenarios:

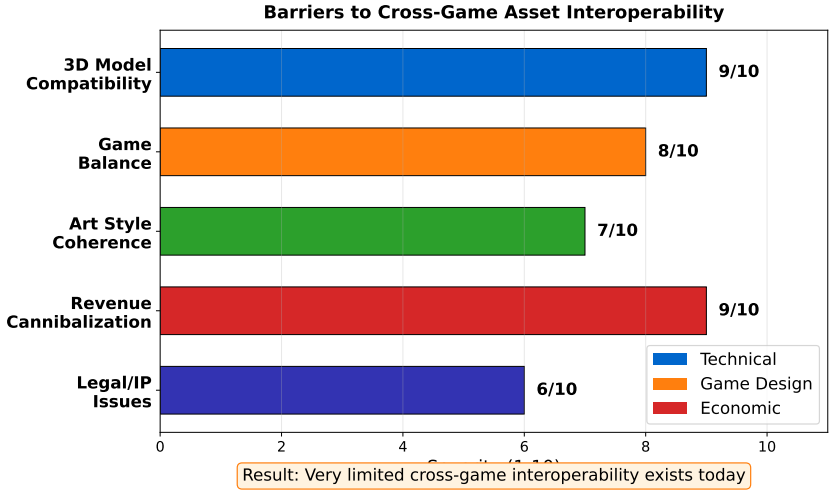
- Sword earned in Game A usable in Game B
- Avatar skin portable across virtual worlds
- Virtual real estate accessible from multiple platforms

Technical Challenges:

1. 3D model compatibility (different engines, formats)
2. Game balance (overpowered items)
3. Art style coherence
4. Legal/IP issues

Reality: Very limited interoperability today

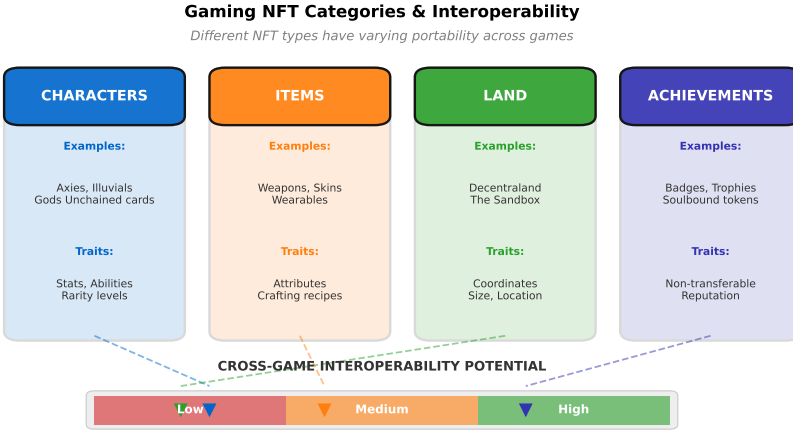
Interoperability Barriers



Result: Very limited cross-game interoperability exists today

Economic and technical barriers make true cross-game asset portability extremely difficult

Gaming NFT Categories and Interoperability



Characters and Land have low portability; Achievements (soulbound) can be highly interoperable

Can Blockchain Gaming Be Sustainable?

Concerns:

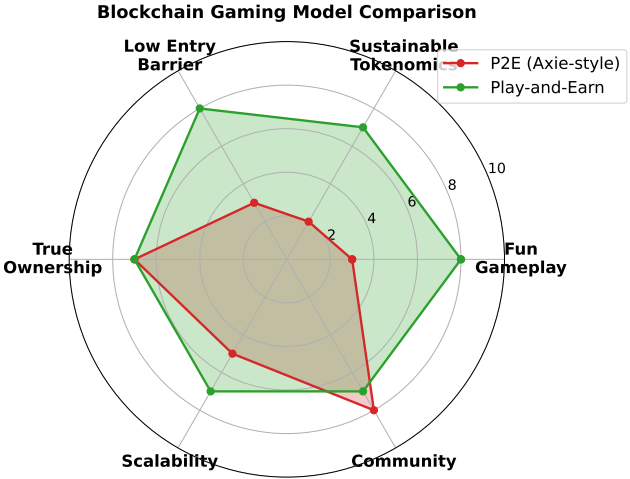
1. **Ponzi Tokenomics:** Most P2E models collapse without new players
2. **Gameplay Quality:** Focus on earning, not fun
3. **High Costs:** Gas fees, NFT entry barriers
4. **Regulatory Risk:** P2E may be classified as gambling

Potential Solutions:

- Shift to "play-and-earn" (fun first, earn secondary)
- Deflationary (reducing supply over time) tokenomics (burning (destroying tokens permanently) mechanisms)
- Layer 2 solutions (lower gas fees)
- Free-to-play with optional NFT purchases

Metaverse land speculation assumes future demand; most virtual worlds remain empty.

Gaming Model Comparison



Play-and-Earn models score better on sustainability factors than traditional P2E

What is Play-and-Earn?

Play-and-Earn: Prioritize gameplay quality, earnings as bonus

Contrast with P2E:

- **P2E:** Gameplay is work, earnings primary motivation
- **Play-and-Earn:** Gameplay is fun, earnings enhance experience

Examples:

- **Illuvium:** AAA-quality open-world RPG with NFT creatures
- **Ember Sword:** Free-to-play MMORPG (Massively Multiplayer Online RPG) with optional cosmetics
- **Gods Unchained:** Free-to-play card game, sustainable

Key Insight: Fun gameplay attracts organic users, reducing Ponzi dynamics

What Are Gaming Guilds?

Guilds: Organizations that lend NFT assets to players

Scholarship (guilds lend assets, share earnings) Model:

1. Guild purchases NFT game assets
2. Guild lends assets to players (scholars)
3. Players earn tokens through gameplay
4. Earnings split: 70% player, 30% guild

Major Guilds:

- **Yield Guild Games (YGG):** Largest guild
- **Merit Circle:** DAO-governed

Decline: Axie collapse decimated guild revenues

Problem Solved? Gaming NFTs & Metaverse

The Original Problem

How do virtual economies work?

How Gaming NFTs & Metaverse Solves It

- Play-to-earn creates direct financial incentives for participation through token rewards
- NFT ownership enables true asset ownership and tradability on open markets
- Interoperability promises allow assets to be used across multiple games

Remaining Limitations

- Inflationary pressures from unlimited token minting (SLP case)
- Ponzi-like structures require continuous new player inflow to sustain earnings
- Fun vs. profit tension: gameplay quality suffers when earning is the primary goal

Open Questions

- Can play-to-earn be sustainable without constant new players?
- Risk: Extractive tokenomics, unsustainable yields

Gaming NFTs & Metaverse partially solves "virtual economies work" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Gaming NFTs & Metaverse

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Design Space: Gaming NFTs & Metaverse

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Gaming NFTs & Metaverse

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Virtual real estate speculation

[COMIC: placeholder]

A proud "landowner" showing off their $2M Decentraland parcel: "Prime virtual real estate next to Snoop Dogg!" Pan out to reveal an empty, low-poly wasteland with a single avatar walking past. Stats overlay: "Daily Active Users: 38."

The Speculation Reality

- Peak hype: $2.4M for virtual land
- Current reality: ¡1,000 daily users
- Floor prices down 90%+

The Hard Question

- Value = scarcity + utility + demand
- Scarcity: Artificial (infinite virtual land possible)
- Utility: Limited (few experiences built)
- Demand: Where are the users?

Virtual land speculation assumed future demand that hasn't materialized

Key Takeaways

1. Play-to-earn (P2E) models enable earning through gameplay but often resemble Ponzi schemes
2. Axie Infinity collapsed due to unsustainable tokenomics and unlimited SLP inflation
3. Virtual land NFTs (Decentraland, Sandbox) are speculation-driven with low actual usage
4. Interoperability of cross-game assets is limited by technical and economic barriers
5. Sustainable blockchain gaming requires fun-first design and balanced token economies
6. Play-and-Earn (fun primary, earning secondary) shows more promise

Next Lesson: L27 – RWA Tokenization

Discussion Questions

1. Can play-to-earn gaming models ever be sustainable without Ponzi dynamics?
2. What would make virtual land NFTs genuinely valuable beyond speculation?
3. Is true cross-game interoperability achievable, or a pipe dream?
4. Should blockchain games focus on financialization or gameplay quality?
5. How can regulators balance innovation with consumer protection in P2E gaming?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L27: Real-World Asset Tokenization

We will explore:

- RWA tokenization concept and mechanics
- Real estate tokenization platforms and legal frameworks
- Securities tokenization and compliance (Reg D, Reg S)
- Case study: BlackRock BUIDL fund ($500M+ on-chain)
- Market size: $50B on-chain, projected $18T by 2033

Preparation: Review traditional real estate investment structures (REITs)

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs
C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them
C) Players rent games from developers D) Players trade items within the game only
Answer: B – P2E allows earning cryptocurrency tokens by completing in-game tasks.

Q3. Why do P2E models often resemble Ponzi schemes?
A) They use complex technology B) New player capital pays existing players' earnings
C) They require internet connection D) They have high transaction fees
Answer: B – Requires continuous new player capital to fund existing players' earnings.

Q4. How many Axies were required to start playing Axie Infinity?
A) 1 Axie B) 2 Axies C) 3 Axies D) 5 Axies
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q5. What was Axie Infinity's peak daily active user count in 2021?
A) 500,000 B) 1.2 million C) 2.8 million D) 5 million
Answer: C – Peaked at 2.8 million users before collapsing to under 10,000.

Quiz Questions (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap
C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen (173,600 ETH + 25.5M USDC), largest DeFi hack at the time.

Q8. How long did the Ronin Bridge hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Undetected for 6 days, demonstrating critical security failures.

Q9. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q10. What is the approximate daily active user count for Decentraland in 2024?
A) Under 1,000 B) 5,000-10,000 C) 20,000-30,000 D) Over 50,000
Answer: A – Despite hype, under 1,000 daily active users in 2024.

Quiz Questions (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues
C) High gas fees D) Lack of users
Answer: B – Different engines, formats, balancing, and art style coherence issues.

Q13. What is the key difference between "play-to-earn" and "play-and-earn"?
A) Different blockchain networks B) Play-and-earn prioritizes fun gameplay, earnings as bonus
C) Play-and-earn requires more investment D) Play-to-earn uses NFTs, play-and-earn does not
Answer: B – Play-and-earn focuses on gameplay quality first, not earnings.

Q14. What was the typical earnings split in blockchain gaming guild scholarships?
A) 50% player, 50% guild B) 60% player, 40% guild
C) 70% player, 30% guild D) 80% player, 20% guild
Answer: C – 70% to players (scholars), 30% to guilds.

Q15. Which game is cited as an example of the play-and-earn model?
A) Axie Infinity B) Decentraland C) Gods Unchained D) CryptoKitties
Answer: C – Gods Unchained is a free-to-play card game with optional NFT elements.

Quiz Questions (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity
C) Metaverse NFT standard D) Layer 2 scaling solution
Answer: A – MANA is used to purchase LAND parcels in Decentraland.

Q18. What was the highest recorded sale price for prime Decentraland land?
A) $500,000 B) $1.2M C) $2.4M D) $5M
Answer: C – Prime Decentraland land sold for $2.4M during peak hype (2021-2022).

Q19. What is Yield Guild Games (YGG)?
A) A play-to-earn game B) Organization that lends NFT assets to players
C) A metaverse platform D) A DeFi protocol
Answer: B – YGG is the largest guild that lends NFT game assets to scholars.

Q20. Which solution is proposed to improve blockchain gaming sustainability?
A) Increase token inflation B) Higher entry fees
C) Shift to Layer 2 for lower gas fees D) Remove NFTs entirely
Answer: C – Layer 2 solutions reduce gas fees, improving accessibility and sustainability.

L26: Gaming NFTs and Metaverse

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

January 2026

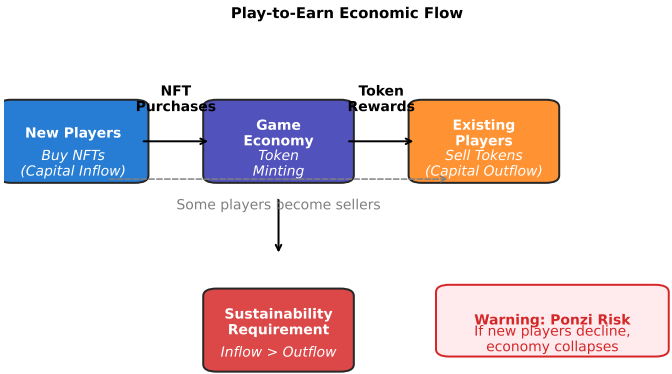
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Explain the play-to-earn (P2E) model and its Ponzi dynamics
- Analyze Axie Infinity's rise and collapse
- Evaluate virtual land NFTs and metaverse economics
- Distinguish play-to-earn from play-and-earn models

Play-to-Earn Economic Flow



Core Problem: New player capital pays existing players' earnings.

Play-to-Earn Model

Traditional Gaming:

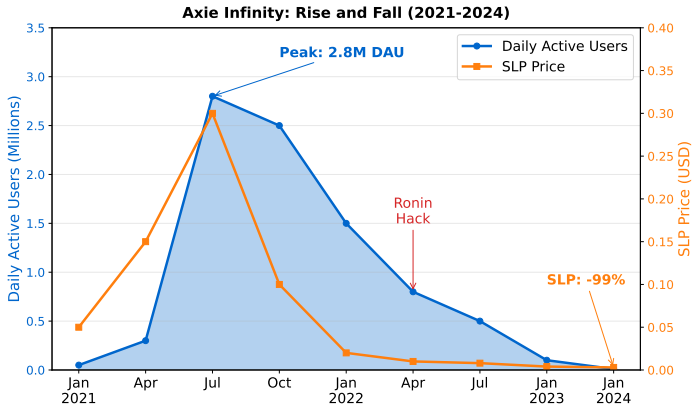
- Players pay for games and items (locked, no ownership)
- Value accrues to game company, not players

P2E Mechanics:

1. Player buys NFT characters (upfront investment)
2. Player completes tasks, earns tokens
3. Player sells tokens on exchanges

Sustainability Problem: Requires continuous new player inflow.

Axie Infinity: Rise and Fall



Peak: 2.8M daily users, $600-1000 entry cost — **Collapse:** SLP -99%+

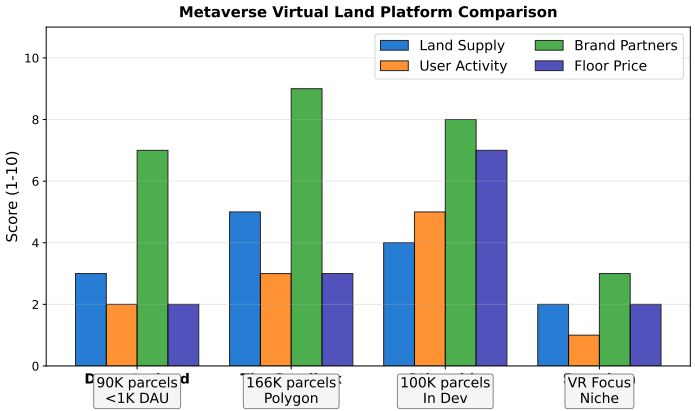
Axie Infinity: What Went Wrong?

Fatal Flaws:

1. **Ponzi Dynamics:** New player money funded existing rewards
2. **Unlimited Inflation:** SLP had no supply cap
3. **Weak Demand Sinks:** Breeding couldn't absorb supply
4. **High Entry Barrier:** $600-1000 deterred new users
5. **Poor Gameplay:** Repetitive grind, not fun

Ronin Hack (March 2022): $625M stolen, hack unnoticed for 6 days.

Metaverse Platform Comparison



Reality: Low usage (¡1000 DAU), speculation-driven, most land undeveloped.

Virtual Land NFTs

Major Platforms:

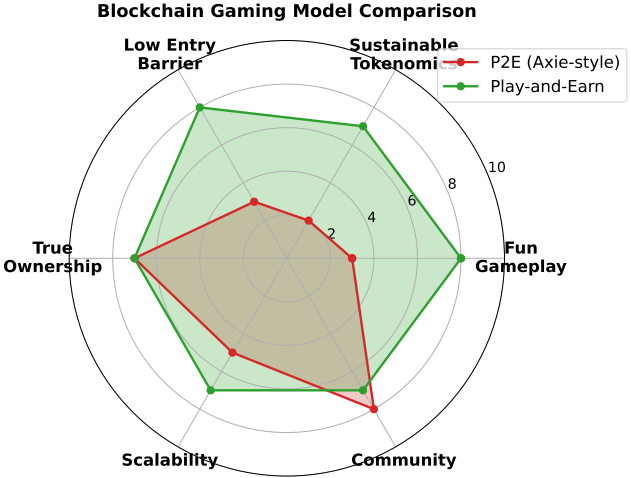
- **Decentraland:** 90,000 parcels, Ethereum, peak $2.4M sales
- **The Sandbox:** 166,464 parcels, Polygon-based
- **Otherside:** 100,000 parcels, BAYC metaverse

Current State (2024-2025):

- Decentraland: ¡1,000 daily active users
- Floor prices down 90%+ from peak
- Most land undeveloped, brand partnerships exceed organic activity

(c) Joerg Osterrieder 2025

Gaming Model Sustainability



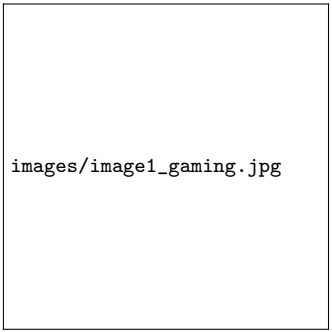
Play-and-Earn: Fun first, earnings secondary – more sustainable model.

Key Takeaways

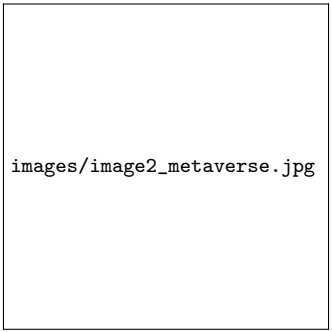
1. **P2E Model:** New player capital funds existing player earnings (Ponzi dynamics)
2. **Axie Collapse:** Unlimited SLP inflation + high entry cost + poor gameplay
3. **Ronin Hack:** $625M stolen (March 2022), largest DeFi hack at time
4. **Virtual Land:** Speculation-driven with ¡1000 daily users on major platforms
5. **Play-and-Earn:** Fun gameplay first, optional earnings – more sustainable

Lesson: P2E requires genuine value creation, not just token redistribution.

Gaming NFTs and Metaverse in Practice



Blockchain Gaming



Metaverse Land

Virtual Worlds

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Why do P2E models often resemble Ponzi schemes?
A) High technology costs B) New player capital pays existing players
C) Government restrictions D) Limited blockchain capacity

Quiz (1/2)

Q1. Why do P2E models often resemble Ponzi schemes?
A) High technology costs B) New player capital pays existing players
C) Government restrictions D) Limited blockchain capacity
Answer: B – P2E requires new player money to fund existing earnings.

Q2. How many Axies were required to start playing?
A) 1 B) 2 C) 3 D) 5

Quiz (1/2)

Q1. Why do P2E models often resemble Ponzi schemes?
A) High technology costs B) New player capital pays existing players
C) Government restrictions D) Limited blockchain capacity
Answer: B – P2E requires new player money to fund existing earnings.

Q2. How many Axies were required to start playing?
A) 1 B) 2 C) 3 D) 5
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q3. What was the peak daily active users for Axie Infinity?
A) 500K B) 1.2M C) 2.8M D) 5M

Quiz (1/2)

Q1. Why do P2E models often resemble Ponzi schemes?
A) High technology costs B) New player capital pays existing players
C) Government restrictions D) Limited blockchain capacity
Answer: B – P2E requires new player money to fund existing earnings.

Q2. How many Axies were required to start playing?
A) 1 B) 2 C) 3 D) 5
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q3. What was the peak daily active users for Axie Infinity?
A) 500K B) 1.2M C) 2.8M D) 5M
Answer: C – Peaked at 2.8 million before collapsing to under 10K.

Q4. What was the fundamental flaw with SLP tokenomics?
A) Fixed supply B) Unlimited inflation C) High fees D) Slow transactions

Quiz (1/2)

Q1. Why do P2E models often resemble Ponzi schemes?
A) High technology costs B) New player capital pays existing players
C) Government restrictions D) Limited blockchain capacity
Answer: B – P2E requires new player money to fund existing earnings.

Q2. How many Axies were required to start playing?
A) 1 B) 2 C) 3 D) 5
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q3. What was the peak daily active users for Axie Infinity?
A) 500K B) 1.2M C) 2.8M D) 5M
Answer: C – Peaked at 2.8 million before collapsing to under 10K.

Q4. What was the fundamental flaw with SLP tokenomics?
A) Fixed supply B) Unlimited inflation C) High fees D) Slow transactions
Answer: B – SLP had no supply cap, leading to infinite minting.

Q5. How much was stolen in the Ronin Bridge hack?
A) $100M B) $300M C) $625M D) $1B

Quiz (1/2)

Q1. Why do P2E models often resemble Ponzi schemes?
A) High technology costs B) New player capital pays existing players
C) Government restrictions D) Limited blockchain capacity
Answer: B – P2E requires new player money to fund existing earnings.

Q2. How many Axies were required to start playing?
A) 1 B) 2 C) 3 D) 5
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q3. What was the peak daily active users for Axie Infinity?
A) 500K B) 1.2M C) 2.8M D) 5M
Answer: C – Peaked at 2.8 million before collapsing to under 10K.

Q4. What was the fundamental flaw with SLP tokenomics?
A) Fixed supply B) Unlimited inflation C) High fees D) Slow transactions
Answer: B – SLP had no supply cap, leading to infinite minting.

Q5. How much was stolen in the Ronin Bridge hack?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen, largest DeFi hack at the time.

Quiz (2/2)

Q6. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464

Quiz (2/2)

Q6. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q7. What is Decentraland's approximate daily active users (2024)?
A) Under 1,000 B) 10,000 C) 50,000 D) 100,000

Quiz (2/2)

Q6. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q7. What is Decentraland's approximate daily active users (2024)?
A) Under 1,000 B) 10,000 C) 50,000 D) 100,000
Answer: A – Under 1,000 despite peak hype.

Q8. What is the key difference between P2E and play-and-earn?
A) Different blockchains B) Play-and-earn prioritizes fun first
C) P2E is cheaper D) Play-and-earn has no NFTs

Quiz (2/2)

Q6. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q7. What is Decentraland's approximate daily active users (2024)?
A) Under 1,000 B) 10,000 C) 50,000 D) 100,000
Answer: A – Under 1,000 despite peak hype.

Q8. What is the key difference between P2E and play-and-earn?
A) Different blockchains B) Play-and-earn prioritizes fun first
C) P2E is cheaper D) Play-and-earn has no NFTs
Answer: B – Play-and-earn: gameplay quality first, earnings secondary.

Q9. How long did the Ronin hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days

Quiz (2/2)

Q6. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q7. What is Decentraland's approximate daily active users (2024)?
A) Under 1,000 B) 10,000 C) 50,000 D) 100,000
Answer: A – Under 1,000 despite peak hype.

Q8. What is the key difference between P2E and play-and-earn?
A) Different blockchains B) Play-and-earn prioritizes fun first
C) P2E is cheaper D) Play-and-earn has no NFTs
Answer: B – Play-and-earn: gameplay quality first, earnings secondary.

Q9. How long did the Ronin hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Hack undetected for 6 days.

Q10. Which game is cited as a sustainable play-and-earn example?
A) Axie Infinity B) Decentraland C) Gods Unchained D) CryptoKitties

Quiz (2/2)

Q6. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q7. What is Decentraland's approximate daily active users (2024)?
A) Under 1,000 B) 10,000 C) 50,000 D) 100,000
Answer: A – Under 1,000 despite peak hype.

Q8. What is the key difference between P2E and play-and-earn?
A) Different blockchains B) Play-and-earn prioritizes fun first
C) P2E is cheaper D) Play-and-earn has no NFTs
Answer: B – Play-and-earn: gameplay quality first, earnings secondary.

Q9. How long did the Ronin hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Hack undetected for 6 days.

Q10. Which game is cited as a sustainable play-and-earn example?
A) Axie Infinity B) Decentraland C) Gods Unchained D) CryptoKitties
Answer: C – Free-to-play card game with optional NFT elements.

Thank you

Questions?

Next: L27 – Real-World Asset Tokenization

Quiz: Gaming NFTs Metaverse

Instructions: 21 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs C) Traditional games have better graphics D) Blockchain games are easier to play

Quiz (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them C) Players rent games from developers D) Players trade items within the game only

Quiz (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them C) Players rent games from developers D) Players trade items within the game only
Answer: B – P2E allows earning cryptocurrency tokens by completing in-game tasks.

Q3. Why do P2E models often resemble Ponzi schemes?
A) They use complex technology B) New player capital pays existing players' earnings C) They require internet connection D) They have high transaction fees

Quiz (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them C) Players rent games from developers D) Players trade items within the game only
Answer: B – P2E allows earning cryptocurrency tokens by completing in-game tasks.

Q3. Why do P2E models often resemble Ponzi schemes?
A) They use complex technology B) New player capital pays existing players' earnings C) They require internet connection D) They have high transaction fees
Answer: B – Requires continuous new player capital to fund existing players' earnings.

Q4. How many Axies were required to start playing Axie Infinity?
A) 1 Axie B) 2 Axies C) 3 Axies D) 5 Axies

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them C) Players rent games from developers D) Players trade items within the game only
Answer: B – P2E allows earning cryptocurrency tokens by completing in-game tasks.

Q3. Why do P2E models often resemble Ponzi schemes?
A) They use complex technology B) New player capital pays existing players' earnings C) They require internet connection D) They have high transaction fees
Answer: B – Requires continuous new player capital to fund existing players' earnings.

Q4. How many Axies were required to start playing Axie Infinity?
A) 1 Axie B) 2 Axies C) 3 Axies D) 5 Axies
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q5. What was Axie Infinity's peak daily active user count in 2021?
A) 500,000 B) 1.2 million C) 2.8 million D) 5 million

Quiz (1–5)

Q1. What is the fundamental difference between traditional and blockchain gaming?
A) Traditional games are more expensive B) Blockchain games offer true player ownership via NFTs C) Traditional games have better graphics D) Blockchain games are easier to play
Answer: B – In-game assets are NFTs owned by players and tradable.

Q2. What is the core mechanic of the play-to-earn (P2E) model?
A) Players pay subscription fees B) Players earn tokens through gameplay and can sell them C) Players rent games from developers D) Players trade items within the game only
Answer: B – P2E allows earning cryptocurrency tokens by completing in-game tasks.

Q3. Why do P2E models often resemble Ponzi schemes?
A) They use complex technology B) New player capital pays existing players' earnings C) They require internet connection D) They have high transaction fees
Answer: B – Requires continuous new player capital to fund existing players' earnings.

Q4. How many Axies were required to start playing Axie Infinity?
A) 1 Axie B) 2 Axies C) 3 Axies D) 5 Axies
Answer: C – 3 Axie NFTs required, costing $600-1000 at peak.

Q5. What was Axie Infinity's peak daily active user count in 2021?
A) 500,000 B) 1.2 million C) 2.8 million D) 5 million
Answer: C – Peaked at 2.8 million users before collapsing to under 10,000.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap C) Too high transaction fees D) Government regulation

Quiz (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen (173,600 ETH + 25.5M USDC), largest DeFi hack at the time.

Q8. How long did the Ronin Bridge hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days

Quiz (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen (173,600 ETH + 25.5M USDC), largest DeFi hack at the time.

Q8. How long did the Ronin Bridge hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Undetected for 6 days, demonstrating critical security failures.

Q9. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464

Quiz (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen (173,600 ETH + 25.5M USDC), largest DeFi hack at the time.

Q8. How long did the Ronin Bridge hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Undetected for 6 days, demonstrating critical security failures.

Q9. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q10. What is the approximate daily active user count for Decentraland in 2024?
A) Under 1,000 B) 5,000-10,000 C) 20,000-30,000 D) Over 50,000

Quiz (6–10)

Q6. What was the fundamental flaw with SLP (Smooth Love Potion) tokenomics?
A) Fixed supply cap B) Unlimited inflation with no supply cap C) Too high transaction fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

Q7. How much was stolen in the Ronin Bridge hack of March 2022?
A) $100M B) $300M C) $625M D) $1B
Answer: C – $625M stolen (173,600 ETH + 25.5M USDC), largest DeFi hack at the time.

Q8. How long did the Ronin Bridge hack go unnoticed?
A) 1 day B) 3 days C) 6 days D) 10 days
Answer: C – Undetected for 6 days, demonstrating critical security failures.

Q9. How many LAND parcels exist in Decentraland?
A) 30,000 B) 60,000 C) 90,000 D) 166,464
Answer: C – 90,000 LAND parcels (16x16 meter plots).

Q10. What is the approximate daily active user count for Decentraland in 2024?
A) Under 1,000 B) 5,000-10,000 C) 20,000-30,000 D) Over 50,000
Answer: A – Despite hype, under 1,000 daily active users in 2024.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity

Quiz (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues C) High gas fees D) Lack of users

Quiz (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues C) High gas fees D) Lack of users
Answer: B – Different engines, formats, balancing, and art style coherence issues.

Q13. What is the key difference between "play-to-earn" and "play-and-earn"?
A) Different blockchain networks B) Play-and-earn prioritizes fun gameplay, earnings as bonus C) Play-and-earn requires more investment D) Play-to-earn uses NFTs, play-and-earn does not

Quiz (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues C) High gas fees D) Lack of users
Answer: B – Different engines, formats, balancing, and art style coherence issues.

Q13. What is the key difference between "play-to-earn" and "play-and-earn"?
A) Different blockchain networks B) Play-and-earn prioritizes fun gameplay, earnings as bonus C) Play-and-earn requires more investment D) Play-to-earn uses NFTs, play-and-earn does not
Answer: B – Play-and-earn focuses on gameplay quality first, not earnings.

Q14. What was the typical earnings split in blockchain gaming guild scholarships?
A) 50% player, 50% guild B) 60% player, 40% guild C) 70% player, 30% guild D) 80% player, 20% guild

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues C) High gas fees D) Lack of users
Answer: B – Different engines, formats, balancing, and art style coherence issues.

Q13. What is the key difference between "play-to-earn" and "play-and-earn"?
A) Different blockchain networks B) Play-and-earn prioritizes fun gameplay, earnings as bonus C) Play-and-earn requires more investment D) Play-to-earn uses NFTs, play-and-earn does not
Answer: B – Play-and-earn focuses on gameplay quality first, not earnings.

Q14. What was the typical earnings split in blockchain gaming guild scholarships?
A) 50% player, 50% guild B) 60% player, 40% guild C) 70% player, 30% guild D) 80% player, 20% guild
Answer: C – 70% to players (scholars), 30% to guilds.

Q15. Which game is cited as an example of the play-and-earn model?
A) Axie Infinity B) Decentraland C) Gods Unchained D) CryptoKitties

Quiz (11–15)

Q11. Which metaverse platform has 166,464 land parcels?
A) Decentraland B) The Sandbox C) Otherside D) Axie Infinity
Answer: B – The Sandbox (Polygon-based) has 166,464 parcels.

Q12. What is the main challenge preventing true cross-game NFT interoperability?
A) Blockchain speed B) 3D model compatibility and game balance issues C) High gas fees D) Lack of users
Answer: B – Different engines, formats, balancing, and art style coherence issues.

Q13. What is the key difference between "play-to-earn" and "play-and-earn"?
A) Different blockchain networks B) Play-and-earn prioritizes fun gameplay, earnings as bonus C) Play-and-earn requires more investment D) Play-to-earn uses NFTs, play-and-earn does not
Answer: B – Play-and-earn focuses on gameplay quality first, not earnings.

Q14. What was the typical earnings split in blockchain gaming guild scholarships?
A) 50% player, 50% guild B) 60% player, 40% guild C) 70% player, 30% guild D) 80% player, 20% guild
Answer: C – 70% to players (scholars), 30% to guilds.

Q15. Which game is cited as an example of the play-and-earn model?
A) Axie Infinity B) Decentraland C) Gods Unchained D) CryptoKitties
Answer: C – Gods Unchained is a free-to-play card game with optional NFT elements.

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+

Quiz (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity C) Metaverse NFT standard D) Layer 2 scaling solution

Quiz (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity C) Metaverse NFT standard D) Layer 2 scaling solution
Answer: A – MANA is used to purchase LAND parcels in Decentraland.

Q18. What was the highest recorded sale price for prime Decentraland land?
A) $500,000 B) $1.2M C) $2.4M D) $5M

Quiz (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity C) Metaverse NFT standard D) Layer 2 scaling solution
Answer: A – MANA is used to purchase LAND parcels in Decentraland.

Q18. What was the highest recorded sale price for prime Decentraland land?
A) $500,000 B) $1.2M C) $2.4M D) $5M
Answer: C – Prime Decentraland land sold for $2.4M during peak hype (2021-2022).

Q19. What is Yield Guild Games (YGG)?
A) A play-to-earn game B) Organization that lends NFT assets to players C) A metaverse platform D) A DeFi protocol

Quiz (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity C) Metaverse NFT standard D) Layer 2 scaling solution
Answer: A – MANA is used to purchase LAND parcels in Decentraland.

Q18. What was the highest recorded sale price for prime Decentraland land?
A) $500,000 B) $1.2M C) $2.4M D) $5M
Answer: C – Prime Decentraland land sold for $2.4M during peak hype (2021-2022).

Q19. What is Yield Guild Games (YGG)?
A) A play-to-earn game B) Organization that lends NFT assets to players C) A metaverse platform D) A DeFi protocol
Answer: B – YGG is the largest guild that lends NFT game assets to scholars.

Q20. Which solution is proposed to improve blockchain gaming sustainability?
A) Increase token inflation B) Higher entry fees C) Shift to Layer 2 for lower gas fees D) Remove NFTs entirely

Quiz (16–20)

Q16. What was the peak entry cost to start playing Axie Infinity?
A) $100-200 B) $300-400 C) $600-1,000 D) $2,000+
Answer: C – 3 Axies cost $600-1,000 at peak, creating high barrier to entry.

Q17. What is MANA?
A) Currency token for buying land in Decentraland B) Governance token for Axie Infinity C) Metaverse NFT standard D) Layer 2 scaling solution
Answer: A – MANA is used to purchase LAND parcels in Decentraland.

Q18. What was the highest recorded sale price for prime Decentraland land?
A) $500,000 B) $1.2M C) $2.4M D) $5M
Answer: C – Prime Decentraland land sold for $2.4M during peak hype (2021-2022).

Q19. What is Yield Guild Games (YGG)?
A) A play-to-earn game B) Organization that lends NFT assets to players C) A metaverse platform D) A DeFi protocol
Answer: B – YGG is the largest guild that lends NFT game assets to scholars.

Q20. Which solution is proposed to improve blockchain gaming sustainability?
A) Increase token inflation B) Higher entry fees C) Shift to Layer 2 for lower gas fees D) Remove NFTs entirely
Answer: C – Layer 2 solutions reduce gas fees, improving accessibility and sustainability.

(c) Joerg Osterrieder 2025

Quiz (21–21)

Q21. What was the fundamental flaw with SLP tokenomics?
A) Fixed supply cap B) Unlimited inflation with no cap C) Too high fees D) Government regulation

Q21. What was the fundamental flaw with SLP tokenomics?
A) Fixed supply cap B) Unlimited inflation with no cap C) Too high fees D) Government regulation
Answer: B – SLP had no supply cap, leading to infinite minting and price collapse.

L27: Real-World Asset Tokenization

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lesson, you will be able to:

- Define real-world asset (RWA) tokenization and its benefits
- Describe real estate tokenization platforms and legal structures
- Explain securities tokenization and regulatory compliance frameworks
- Analyze BlackRock BUIDL fund as institutional RWA case study
- Evaluate market size and growth projections for tokenized assets

The Problem: How do we tokenize physical assets?

The Challenge
How do we tokenize physical assets while maintaining legal validity and enforceable ownership rights?

Why It Matters

- Trillions in illiquid assets (real estate, art, private equity) locked away from most investors
- Historical failures: Security token offerings failed to gain traction (2017-2019) due to legal uncertainty

What We Need

- Bridge between on-chain tokens and off-chain legal ownership
- Regulatory frameworks that recognize tokenized securities
- Mechanisms to fractionalize expensive assets for retail investors

The Cryptoeconomics Question
How do we create and capture value from previously illiquid assets?

Today's lesson: How Real-World Asset Tokenization addresses this challenge

(c) Joerg Osterrieder 2025

What is Real-World Asset Tokenization?

RWA Tokenization: Representing ownership of physical assets as blockchain tokens

Asset Classes:

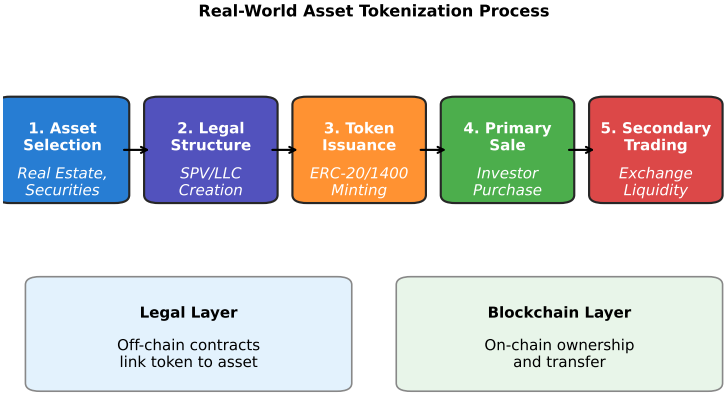
- Real estate (residential, commercial)
- Securities (stocks, bonds, funds)
- Commodities (gold, oil, carbon credits)
- Art and collectibles (paintings, wine, watches)
- Debt instruments (loans, mortgages, invoices)

Key Benefits:

- **Fractional ownership:** Divide expensive assets into affordable shares
- **Liquidity:** Trade traditionally illiquid assets 24/7
- **Transparency:** Ownership and transaction history on-chain

(c) Joerg Osterrieder 2025

RWA Tokenization Process



6-step process from asset selection to secondary market trading

Tokenization vs. Traditional Ownership

Traditional Asset Ownership:

- High minimum investment (e.g., $100k+ for real estate)
- Illiquid (weeks/months to sell)
- Paperwork-heavy (legal docs, notaries, brokers)
- Limited access (accredited investors only for many assets)

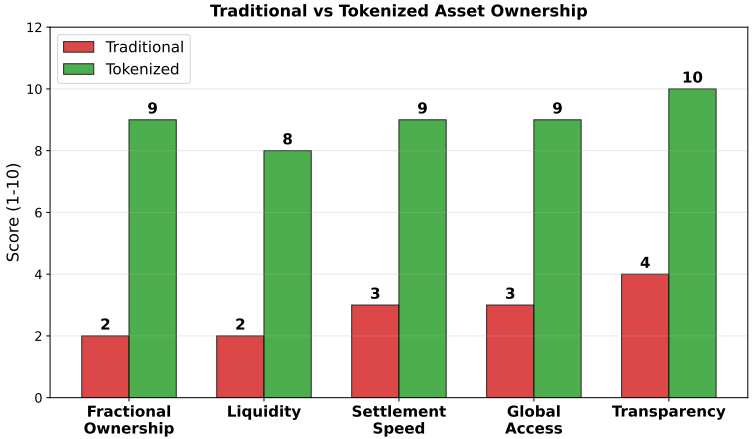
Tokenized Asset Ownership:

- Fractional shares (invest $100-$10k+)
- 24/7 trading on secondary markets
- Smart contract automation (instant settlement)
- Broader access (retail investors if compliant)

Critical Requirement: Legal framework linking token to real-world asset rights

(c) Joerg Osterrieder 2025

Traditional vs Tokenized Ownership



Tokenization dramatically improves fractional ownership, liquidity, and settlement speed

How RWA Tokenization Works

Typical Process:

1. **Asset Selection:** Identify real-world asset (e.g., building)
2. **Legal Structure:** Create SPV (Special Purpose Vehicle) to hold asset
3. **Valuation:** Independent appraisal determines asset value
4. **Token Issuance:** Mint tokens representing fractional ownership
5. **Distribution:** Sell tokens to investors (primary market)
6. **Trading:** Tokens trade on secondary markets (exchanges)

Legal Bridge: Smart contract references off-chain legal agreement

Real Estate Tokenization

Value Proposition: Make real estate investment accessible and liquid

Tokenization Models:

1. **Direct Property Ownership:** Tokens = shares in SPV owning property
2. **Debt-Backed:** Tokens represent mortgage or loan on property
3. **REIT Tokenization:** Digitize traditional REIT shares

Example: $10M commercial building

- Issue 10,000 tokens at $1,000 each
- Investors buy tokens (minimum $1,000)
- Rental income distributed pro-rata to token holders

Platforms: RealT, Propy, Lofty AI, Polymath

RealT: Fractional Real Estate

Platform: Ethereum-based real estate tokenization (USA properties)

Model:

- RealT buys US rental properties
- Property held in LLC, tokens issued on Ethereum
- Minimum investment: $50 per property
- Daily rent distribution (stablecoins to wallets)

Example Property:

- Address: 123 Main St, Detroit, MI
- Token price: $52.50 per token
- Total tokens: 5,000 (property value $262,500)
- Annual yield: 8-12% (rent minus costs)

Regulatory Compliance: Reg D (accredited investors only) or Reg A+ (retail)

(c) Joerg Osterrieder 2025

Propy: Blockchain Real Estate Transactions

Platform: End-to-end real estate transactions on blockchain

Services:

- Property listings and search
- Smart contract-based escrow
- NFT property deeds (ownership certificate)
- Cross-border transaction facilitation

First Blockchain Property Sale (2017):

- Property: Apartment in Kiev, Ukraine
- Deed issued as NFT on Ethereum
- Sale price: $60,000 (ETH payment)

Limitations:

- Legal recognition varies by jurisdiction
- Most countries require traditional deed registration

Securities Tokenization

Security Token: Digital token representing traditional security (stock, bond, fund share)

Difference from Utility Token:

- **Security Token:** Investment contract, subject to SEC regulation
- **Utility Token:** Access to product/service, may avoid securities law

Regulatory Frameworks (USA):

- **Reg D (Rule 506):** Private placement, accredited investors only
- **Reg A+:** Mini-IPO, retail investors, up to $75M raise
- **Reg S:** Offshore sales to non-US investors
- **Reg CF:** Crowdfunding, retail investors, up to $5M raise

Compliance: KYC/AML, transfer restrictions, accreditation verification

(c) Joerg Osterrieder 2025

Security Token Standards

ERC-20 Limitations for Securities:

- No built-in transfer restrictions (KYC/AML)
- Cannot enforce accredited investor rules
- No compliance checks before transfer

Enhanced Token Standards:

- **ERC-1400:** Security token standard with partitions
- **ERC-3643 (T-REX):** Transfer restrictions, compliance modules
- **DS Protocol:** Debt securities tokenization

Key Features:

- Identity verification (KYC whitelist)
- Transfer restrictions (lock-ups, accreditation checks)
- Document references (prospectus, legal agreements)

BlackRock BUIDL Fund: Institutional RWA

Fund: BlackRock USD Institutional Digital Liquidity Fund

Details:

- **Launch:** March 2024
- **AUM:** $2.9B (December 2024) – largest tokenized fund
- **Blockchain:** Ethereum, Solana, Arbitrum, Optimism, Polygon, Aptos
- **Asset backing:** US Treasury bills, cash, repos
- **Token:** BUIDL (ERC-20 security token)
- **Yield:** 5% APY (Treasury yield minus fees)

Significance:

- World's largest asset manager enters on-chain finance
- Legitimizes tokenized securities for institutions

BUIDL Fund Mechanics

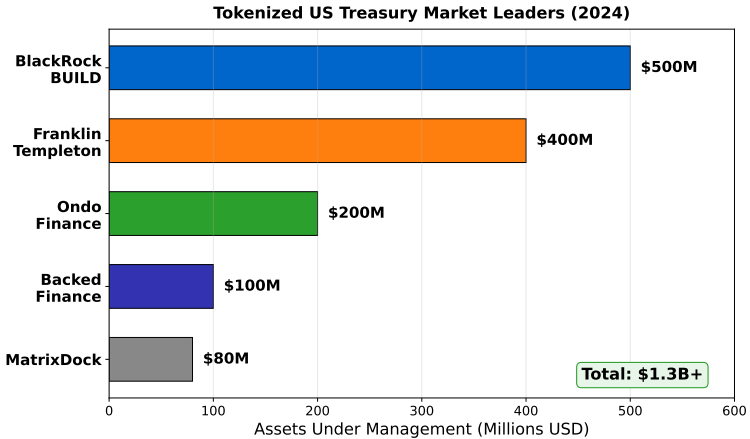
How It Works:

1. Institutional investor completes KYC/AML (accredited only)
2. Investor deposits USD (wire transfer)
3. BlackRock mints BUIDL tokens 1:1 with USD
4. Tokens represent pro-rata share of fund assets
5. Fund invests in US Treasuries and cash equivalents
6. Interest accrues daily, distributed as new BUIDL tokens
7. Investor can redeem BUIDL for USD (T+1 settlement)

Smart Contract Functions:

- Transfer restrictions (KYC whitelist)
- Dividend distribution automation

Tokenized Treasury Market Leaders



BlackRock BUIDL and Franklin Templeton dominate the tokenized Treasury market

BUIDL Impact on RWA Market

Before BUIDL:

- Tokenized Treasuries: ¡$1B total market
- Skepticism from traditional finance
- Retail-focused platforms (small scale)

After BUIDL:

- BUIDL grew to $2.9B in 9 months (largest single fund)
- Competitor launches: Franklin Templeton, Fidelity, WisdomTree
- Institutional validation ("if BlackRock does it, it's real")
- Total tokenized Treasury market: $3B+ (December 2024)

Trend: Major asset managers tokenizing money market funds and Treasuries

Commodity Tokenization

Gold Tokenization:

- **Pax Gold (PAXG):** 1 token = 1 troy oz of gold
- **Tether Gold (XAUT):** Similar model, Tether-issued
- **Backing:** Physical gold in vaults (audited)
- **Redeemability:** Can redeem for physical gold (high minimums)

Carbon Credit Tokenization:

- **Toucan Protocol:** Tokenizes verified carbon credits (TCO2)
- **KlimaDAO:** Carbon-backed currency
- **Use case:** Corporations offset emissions via token purchases

Oil and Energy:

- Tokenized oil barrels (experimental)
- Renewable energy certificates as NFTs

Art and Collectibles Tokenization

Fine Art Fractionalization:

- **Masterworks:** Tokenizes blue-chip art (Banksy, Basquiat)
- **Rally:** Fractional ownership of collectibles (cars, comics, art)
- **Model:** Platform buys asset, issues shares as tokens

Example: Banksy Artwork:

- Artwork value: $2M
- Tokenized into 10,000 shares at $200 each
- Investors earn returns if artwork appreciates and sells

Challenges:

- Storage and insurance costs
- Illiquid underlying asset (art market)
- Valuation subjectivity

Private Credit and Debt Tokenization

Tokenized Loans:

- **Centrifuge:** Real-world asset lending protocol
- **Goldfinch:** Crypto loans to non-crypto businesses
- **Maple Finance:** Institutional undercollateralized lending

How It Works:

1. Company needs loan (e.g., $1M for inventory)
2. Platform originates loan, tokenizes it
3. DeFi investors buy loan tokens (earn interest)
4. Company repays loan + interest over time

Risk: Default risk (borrower fails to repay), requires legal recourse

Legal Challenges in RWA Tokenization

Key Issues:

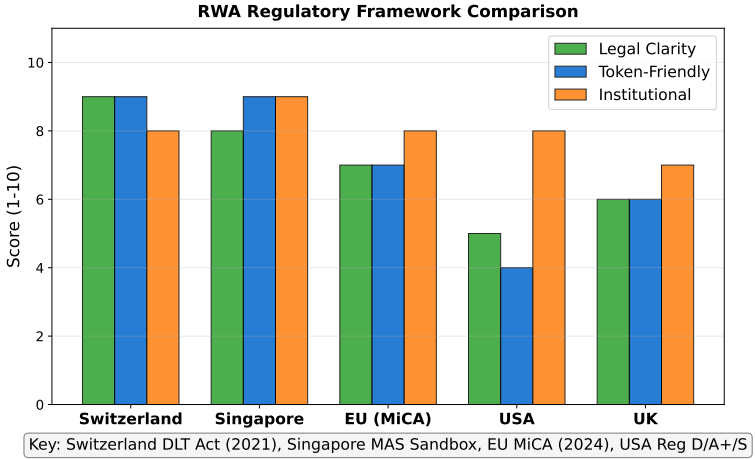
1. **Property Rights:** Does token legally represent asset ownership?
2. **Jurisdiction:** Which country's laws apply (asset vs. token location)?
3. **Enforcement:** How to enforce rights if smart contract disputes?
4. **Bankruptcy:** What happens if SPV or platform goes bankrupt?

Solutions:

- Robust legal agreements (off-chain documentation)
- Established jurisdictions (Delaware, Switzerland, Singapore)
- Regulatory engagement (work with SEC, FINMA, MAS)
- Insurance and guarantees

(c) Joerg Osterrieder 2025

Regulatory Framework Comparison



Switzerland and Singapore lead in legal clarity and token-friendliness

Regulatory Frameworks by Jurisdiction

United States:

- SEC oversight (securities laws apply)
- Reg D, Reg A+, Reg S compliance required
- State-level licensing (money transmitter laws)

Switzerland:

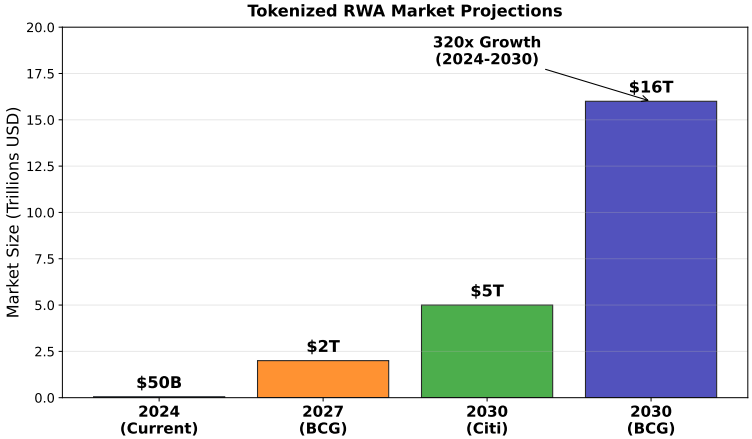
- DLT Act (2021): Legal framework for tokenized securities
- FINMA guidance on token classifications
- Crypto Valley (Zug): Hub for RWA projects

Singapore:

- MAS (Monetary Authority) sandbox for tokenization
- Payment Services Act covers digital tokens
- Project Guardian: Institutional DeFi pilot

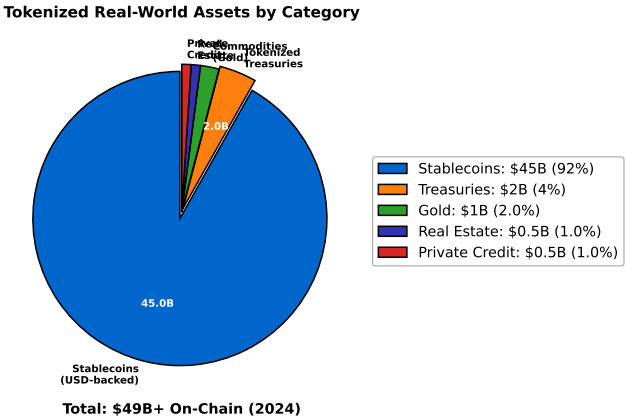
EU: MiCA (Markets in Crypto-Assets) regulation (2024)

RWA Market Projections



*BCG and Citi project **$**5-16T in tokenized assets by 2030 (320x growth)*

Current RWA Asset Distribution



Stablecoins dominate (92%), with Treasuries emerging as fastest-growing category

RWA Market Size and Projections

Current Market (December 2024):

- Total tokenized RWA (excl. stablecoins): $15.2B (up 85% YoY)
- Breakdown:
  - Tokenized Treasuries: $3B+ (BUIDL: $2.9B)
  - Private credit: $8B+
  - Real estate: $500M
  - Commodities (gold): $1B

Growth Projections:

- **BCG (2022):** $16T tokenized assets by 2030
- **Citi (2023):** $4-5T by 2030
- **BlackRock (2024):** "Next evolution of markets"

Drivers: Institutional adoption, regulatory clarity, infrastructure maturity

Benefits of RWA Tokenization

For Investors:

- Fractional access to assets
- 24/7 liquidity, global access
- Transparent ownership

For Asset Owners:

- Unlock illiquid asset value
- Lower cost of capital
- Programmable rights

For Markets:

- Instant settlement
- Financial inclusion
- Fewer intermediaries

(c) Joerg Osterrieder 2025

Risks and Limitations

Key Risks:

- Legal uncertainty (enforceability)
- Smart contract vulnerabilities
- Custody/counterparty risk
- Regulatory changes
- Liquidity illusion

Mitigation Strategies:

- Established legal jurisdictions
- Thorough smart contract audits
- Insurance for custody/assets
- Legal recourse mechanisms

(c) Joerg Osterrieder 2025

RWA vs. DeFi Integration

RWA as DeFi Collateral:

Use Cases:

- Deposit tokenized Treasuries, borrow stablecoins
- Earn DeFi yield while holding real-world assets
- Leverage real estate tokens for liquidity

Platforms:

- **MakerDAO:** Accepts RWA as collateral for DAI minting
- **Aave Arc:** Permissioned pool for institutional RWA
- **Compound:** Exploring RWA collateral integration

Advantage: Bridges traditional finance yield with DeFi composability

Problem Solved? Real-World Asset Tokenization

The Original Problem

How do we tokenize physical assets while maintaining legal validity?

How Real-World Asset Tokenization Solves It

- Legal wrappers (SPVs) connect tokens to asset ownership rights
- Oracles and custodians verify real-world asset status (gold vaults, property registries)
- Regulatory frameworks (Reg D, Reg A+, DLT Act) provide legal certainty

Remaining Limitations

- Requires legal enforcement in traditional courts (jurisdiction-dependent)
- Counterparty risk: SPV, custodian, or platform insolvency
- Liquidity illusion: tokens trade 24/7 but underlying asset remains illiquid

Open Questions

- Will RWA tokenization achieve mainstream adoption or remain a niche?
- Risk: Extractive tokenomics, unsustainable yields in private credit markets

Real-World Asset Tokenization partially solves "tokenizing physical assets" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Key Takeaways

1. RWA tokenization represents ownership of physical assets as blockchain tokens
2. Real estate tokenization enables fractional ownership and liquidity (RealT, Propy)
3. Securities tokenization requires regulatory compliance (Reg D, Reg A+, ERC-1400)
4. BlackRock BUIDL fund ($2.9B) legitimizes institutional RWA adoption
5. RWA market: $15B current (excl. stablecoins), projected $4-16T by 2030
6. Legal frameworks and custody remain critical challenges for mainstream adoption

Discussion Questions

1. What are the primary barriers to widespread RWA tokenization adoption?
2. How can legal systems ensure token holders have enforceable rights to underlying assets?
3. Should all security tokens be regulated like traditional securities, or is lighter regulation appropriate?
4. What risks does DeFi integration of RWA collateral introduce to financial stability?
5. Will RWA tokenization democratize investing, or create new forms of inequality?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L28: Lab – NFT Valuation

Hands-on activities:

- Develop comprehensive due diligence checklist
- Identify red flags and scam indicators
- Conduct rarity analysis and trait valuation
- Prepare investment recommendation report
- Practice evaluating NFT projects systematically

Preparation: Review all previous lessons on NFT technology, marketplaces, and categories

Quiz Questions (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity
C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset
C) A cryptocurrency wallet D) A type of smart contract
Answer: B – SPV is the legal structure that owns the asset while tokens represent fractional ownership.

Q3. What is the minimum investment on RealT platform?
A) $10 B) $50 C) $500 D) $5,000
Answer: B – RealT enables fractional real estate ownership with a minimum of $50 per property.

Q4. Which regulatory framework allows retail investors in the USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is a mini-IPO framework that allows retail investors (up to $75M raise).

Q5. What was the first blockchain property sale in 2017?
A) Apartment in Dubai B) Apartment in Kiev C) House in California D) Office in London
Answer: B – Propy facilitated the first blockchain property sale (Kiev apartment, $60k, NFT deed).

Quiz Questions (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks
C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B AUM in 9 months, making it the largest tokenized fund.

Q8. What assets back the BlackRock BUIDL token?
A) Bitcoin and Ethereum B) Real estate portfolios
C) US Treasury bills and cash D) Corporate bonds
Answer: C – BUIDL is backed by US Treasuries, cash, and repos, yielding 5% APY.

Q9. What does 1 PAXG token represent?
A) 1 gram of gold B) 1 troy ounce of gold C) 1 kilogram of gold D) $1 of gold
Answer: B – Pax Gold (PAXG) is backed 1:1 by physical gold (1 token = 1 troy oz).

Q10. Which platform tokenizes verified carbon credits?
A) Propy B) RealT C) Toucan Protocol D) Centrifuge
Answer: C – Toucan Protocol tokenizes carbon credits as TCO2 for corporate emissions offsetting.

Quiz Questions (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – Boston Consulting Group projects $16T in tokenized RWAs by 2030 (320x growth).

Q13. Which jurisdiction has the DLT Act (2021) for tokenized securities?
A) United States B) Singapore C) Switzerland D) United Kingdom
Answer: C – Switzerland enacted the DLT Act in 2021, providing legal framework for tokenized securities.

Q14. What protocol enables real-world asset lending on-chain?
A) Uniswap B) Centrifuge C) Aave D) Compound
Answer: B – Centrifuge tokenizes real-world loans, enabling DeFi investors to earn interest.

Q15. What is the settlement time for BUIDL token redemption?
A) Instant B) T+1 (1 business day) C) T+3 (3 days) D) T+7 (1 week)
Answer: B – BUIDL tokens can be redeemed for USD with T+1 settlement (1 business day).

Quiz Questions (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds
C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions for securities.

Q18. What percentage of current RWA market is stablecoins?
A) 50% B) 75% C) 92% D) 99%
Answer: C – Stablecoins dominate at 92%, with Treasuries as the fastest-growing non-stablecoin category.

Q19. Which platform uses NFT property deeds for real estate?
A) RealT B) Propy C) Lofty AI D) Polymath
Answer: B – Propy issues property ownership certificates as NFTs on Ethereum.

Q20. What risk does "liquidity illusion" refer to in RWA tokenization?
A) Smart contract bugs B) Tokens trade but underlying asset remains illiquid
C) Regulatory changes D) Custody failures
Answer: B – Tokens may trade 24/7, but the underlying real-world asset may still be difficult to sell.

L27: Real-World Asset Tokenization

Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Tokenizing your house

[COMIC: placeholder]

A homeowner excitedly holding a smartphone: "I tokenized my house into 10,000 NFTs!" A lawyer nearby with a stack of paperwork: "Great, now explain to the Delaware court how your smart contract interacts with property law, bankruptcy proceedings, and tenant rights."

The Promise vs. Reality

- Promise: Fractional real estate for everyone
- Reality: Legal bridges needed everywhere
- Tokens don't automatically grant property rights

What We'll Explore

- How RWA tokenization actually works
- Legal wrappers (SPVs) that make it valid
- BlackRock BUIDL: Institutions go on-chain

Blockchain creates tokens—law creates property rights

Learning Objectives

By the end of this lesson, you will be able to:

- Define real-world asset (RWA – Real-World Assets—physical items) tokenization and its benefits
- Describe real estate tokenization platforms and legal structures
- Explain securities tokenization and regulatory compliance frameworks
- Analyze BlackRock BUIDL fund as institutional RWA case study
- Evaluate market size and growth projections for tokenized assets

Building on L26: Gaming NFTs and Metaverse

The Problem: How do we tokenize physical assets?

The Challenge
How do we tokenize physical assets while maintaining legal validity and enforceable ownership rights?

Why It Matters

- Trillions in illiquid assets (real estate, art, private equity) locked away from most investors
- Historical failures: Security token offerings failed to gain traction (2017-2019) due to legal uncertainty

What We Need

- Bridge between on-chain tokens and off-chain legal ownership
- Regulatory frameworks that recognize tokenized securities
- Mechanisms to fractionalize expensive assets for retail investors

The Cryptoeconomics Question
How do we create and capture value from previously illiquid assets?

Today's lesson: How Real-World Asset Tokenization addresses this challenge

(c) Joerg Osterrieder 2025

How Do You Turn Physical Assets into Tokens?

RWA Tokenization (assets as digital tokens): Representing ownership of physical assets as blockchain tokens

Asset Classes:

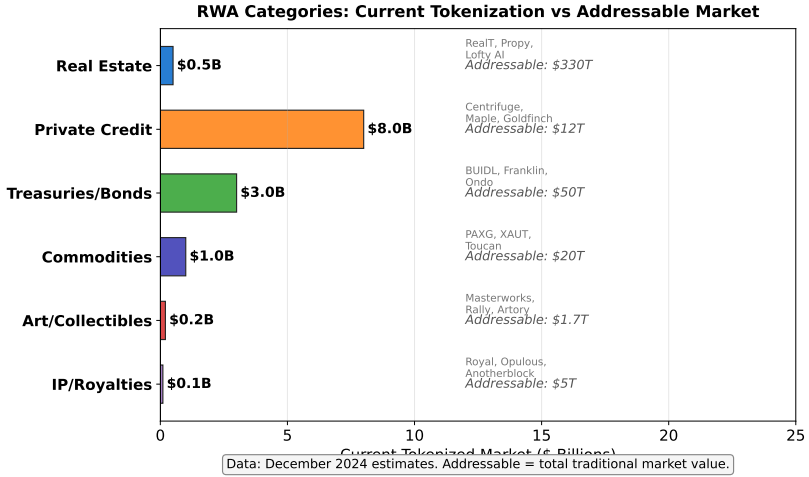
- Real estate (residential, commercial)
- Securities (stocks, bonds, funds)
- Commodities (gold, oil, carbon credits)
- Art and collectibles (paintings, wine, watches)
- Debt instruments (loans, mortgages, invoices)

Key Benefits:

- **Fractional ownership (divided into small shares):** Divide expensive assets into affordable shares
- **Liquidity:** Trade traditionally illiquid assets 24/7
- **Transparency:** Ownership and transaction history on-chain

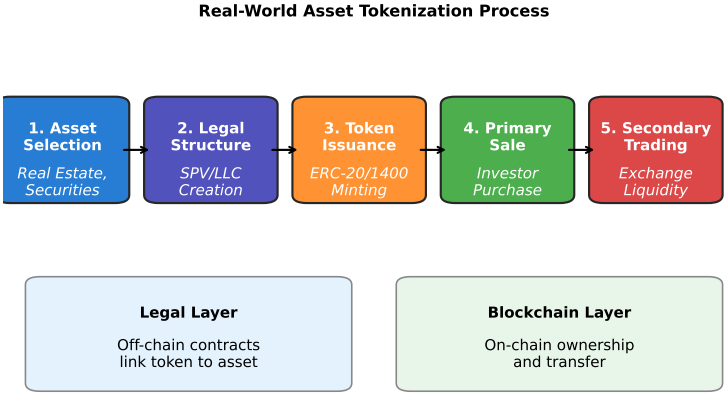
→ *Problem: How do we tokenize physical assets? — What is Real-World Asset Tokenization? Tokenization promises fractional ownership, but legal enforcement remains the hard problem.*

What Asset Categories Can Be Tokenized?



Private credit and treasuries lead current tokenization; real estate has largest addressable market

How Does the Tokenization Process Work?



6-step process from asset selection to secondary market trading

How Does Tokenization Compare to Traditional Ownership?

Traditional Asset Ownership:

- High minimum investment (e.g., $100k+ for real estate)
- Illiquid (weeks/months to sell)
- Paperwork-heavy (legal docs, notaries, brokers)
- Limited access (accredited investors only for many assets)

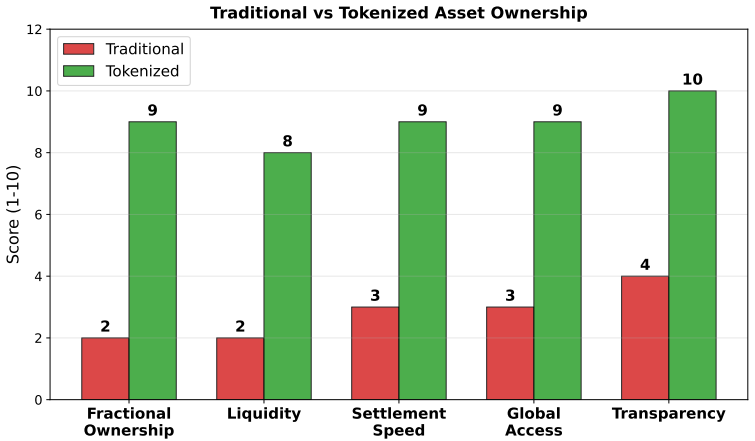
Tokenized Asset Ownership:

- Fractional shares (invest $100-$10k+)
- 24/7 trading on secondary markets
- Smart contract automation (instant settlement)
- Broader access (retail investors if compliant)

Critical Requirement: Legal framework linking token to real-world asset rights

(c) Joerg Osterrieder 2025

What Are the Key Differences Between Traditional and Tokenized Ownership?



Tokenization dramatically improves fractional ownership, liquidity, and settlement speed

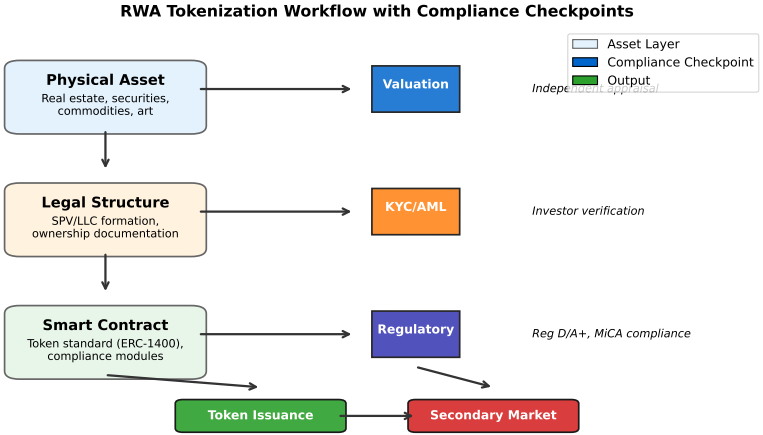
What's the Step-by-Step Tokenization Process?

Typical Process:

1. **Asset Selection:** Identify real-world asset (e.g., building)
2. **Legal Structure:** Create SPV (legal entity holding asset) to hold asset
3. **Valuation:** Independent appraisal determines asset value
4. **Token Issuance:** Mint tokens representing fractional ownership
5. **Distribution:** Sell tokens to investors (primary market)
6. **Trading:** Tokens trade on secondary markets (exchanges)

Legal Bridge: Smart contract references off-chain legal agreement

What Compliance Checkpoints Are Required?



Each stage requires compliance checkpoint: valuation, KYC/AML, and regulatory approval

How Does Real Estate Tokenization Work?

Value Proposition: Make real estate investment accessible and liquid

Tokenization Models:

1. **Direct Property Ownership:** Tokens = shares in SPV owning property
2. **Debt-Backed:** Tokens represent mortgage or loan on property
3. **REIT (Real Estate Investment Trust) Tokenization:** Digitize traditional REIT shares

Example: $10M commercial building

- Issue 10,000 tokens at $1,000 each
- Investors buy tokens (minimum $1,000)
- Rental income distributed pro-rata to token holders

Platforms: RealT, Propy, Lofty AI, Polymath

How Does RealT Enable Fractional Real Estate?

Platform: Ethereum-based real estate tokenization (USA properties)

Model:

- RealT buys US rental properties
- Property held in LLC, tokens issued on Ethereum
- Minimum investment: $50 per property
- Daily rent distribution (stablecoins to wallets)

Example Property:

- Address: 123 Main St, Detroit, MI
- Token price: $52.50 per token
- Total tokens: 5,000 (property value $262,500)
- Annual yield: 8-12% (rent minus costs)

Regulatory Compliance: Reg D (US private sales to wealthy) or Reg A+ (mini-IPO for regular investors)

→ *Problem: How do we tokenize physical assets? — RealT: Fractional Real Estate US securities law (Reg D, A+) determines who can buy—compliance is expensive.*

How Does Propy Handle Blockchain Real Estate Transactions?

Platform: End-to-end real estate transactions on blockchain

Services:

- Property listings and search
- Smart contract-based escrow
- NFT property deeds (ownership certificate)
- Cross-border transaction facilitation

First Blockchain Property Sale (2017):

- Property: Apartment in Kiev, Ukraine
- Deed issued as NFT on Ethereum
- Sale price: $60,000 (ETH payment)

Limitations:

- Legal recognition varies by jurisdiction
- Most countries require traditional deed registration

How Do Security Tokens Differ from Utility Tokens?

Security Token: Digital token representing traditional security (stock, bond, fund share)

Difference from Utility Token:

- **Security Token (regulated investment):** Investment contract, subject to SEC regulation
- **Utility Token (service access token):** Access to product/service, may avoid securities law

Regulatory Frameworks (USA):

- **Reg D (Rule 506):** Private placement, accredited investors only
- **Reg A+ (mini-IPO for regular investors):** Mini-IPO, retail investors, up to $75M raise
- **Reg S (non-US investor exemption):** Offshore sales to non-US investors
- **Reg CF:** Crowdfunding, retail investors, up to $5M raise

Compliance: KYC/AML (identity verification), transfer restrictions, accreditation verification

(c) Joerg Osterrieder 2025

What Standards Are Used for Security Tokens?

ERC-20 Limitations for Securities:

- No built-in transfer restrictions (KYC/AML)
- Cannot enforce accredited investor rules
- No compliance checks before transfer

Enhanced Token Standards:

- **ERC-1400 (security token standard):** Security token standard with partitions
- **ERC-3643 (T-REX):** Transfer restrictions, compliance modules
- **DS Protocol:** Debt securities tokenization

Key Features:

- Identity verification (KYC whitelist)
- Transfer restrictions (lock-ups, accreditation checks)
- Document references (prospectus, legal agreements)

What Is BlackRock's BUIDL Fund?

Fund: BlackRock USD Institutional Digital Liquidity Fund

Details:

- **Launch:** March 2024
- **AUM (Assets Under Management):** $2.9B (December 2024) – largest tokenized fund
- **Blockchain:** Ethereum, Solana, Arbitrum, Optimism, Polygon, Aptos
- **Asset backing:** US Treasury bills, cash, repos
- **Token:** BUIDL (ERC-20 security token)
- **Yield:** 5% APY (Treasury yield minus fees)

Significance:

- World's largest asset manager enters on-chain finance
- Legitimizes tokenized securities for institutions

How Does the BUIDL Fund Work?

How It Works:

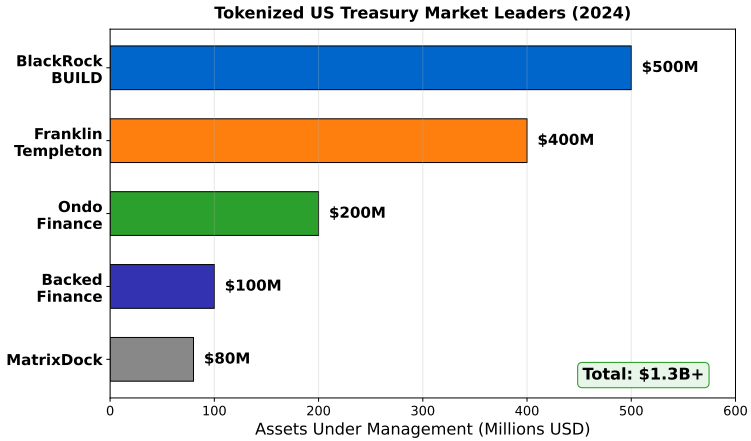
1. Institutional investor completes KYC/AML (accredited only)
2. Investor deposits USD (wire transfer)
3. BlackRock mints BUIDL tokens 1:1 with USD
4. Tokens represent pro-rata share of fund assets
5. Fund invests in US Treasuries and cash equivalents
6. Interest accrues daily, distributed as new BUIDL tokens
7. Investor can redeem BUIDL for USD (T+1 settlement)

Smart Contract Functions:

- Transfer restrictions (KYC whitelist)
- Dividend distribution automation

(c) Joerg Osterrieder 2025

Who Leads the Tokenized Treasury Market?



BlackRock BUIDL and Franklin Templeton dominate the tokenized Treasury market

Problem Check-In: Real-World Asset Tokenization

Recall Our Problem

How do we tokenize physical assets?

What We've Learned So Far

- Fractional ownership via tokens makes expensive assets (real estate, art) accessible to small investors
- SPVs (Special Purpose Vehicles) hold physical assets; tokens represent shares in the SPV
- The oracle problem: blockchain cannot verify real-world asset status—trusted intermediaries remain

Still to Address

- Regulatory frameworks: Reg D (accredited only), Reg A+ (mini-IPO), MiCA (EU)
- If tokenization requires trusted custodians anyway, what's the advantage over traditional shares?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we tokenize physical assets?"?

(c) Joerg Osterrieder 2025

How Did BUIDL Impact the RWA Market?

Before BUIDL:

- Tokenized Treasuries: ¡$1B total market
- Skepticism from traditional finance
- Retail-focused platforms (small scale)

After BUIDL:

- BUIDL grew to $2.9B in 9 months (largest single fund)
- Competitor launches: Franklin Templeton, Fidelity, WisdomTree
- Institutional validation ("if BlackRock does it, it's real")
- Total tokenized Treasury market: $3B+ (December 2024)

Trend: Major asset managers tokenizing money market funds and Treasuries

→ *Problem: How do we tokenize physical assets? — BUIDL Impact on RWA Market Real estate tokens must solve: custody, legal title, and what happens in bankruptcy.*

How Are Commodities Tokenized?

Gold Tokenization:

- **Pax Gold (PAXG – gold-backed token):** 1 token = 1 troy oz of gold
- **Tether Gold (XAUT):** Similar model, Tether-issued
- **Backing:** Physical gold in vaults (audited)
- **Redeemability:** Can redeem for physical gold (high minimums)

Carbon Credit Tokenization:

- **Toucan Protocol:** Tokenizes verified carbon credits (TCO2)
- **KlimaDAO:** Carbon-backed currency
- **Use case:** Corporations offset emissions via token purchases

Oil and Energy:

- Tokenized oil barrels (experimental)
- Renewable energy certificates as NFTs

How Are Art and Collectibles Tokenized?

Fine Art Fractionalization:

- **Masterworks:** Tokenizes blue-chip art (Banksy, Basquiat)
- **Rally:** Fractional ownership of collectibles (cars, comics, art)
- **Model:** Platform buys asset, issues shares as tokens

Example: Banksy Artwork:

- Artwork value: $2M
- Tokenized into 10,000 shares at $200 each
- Investors earn returns if artwork appreciates and sells

Challenges:

- Storage and insurance costs
- Illiquid underlying asset (art market)
- Valuation subjectivity

(c) Joerg Osterrieder 2025

How Are Private Credit and Debt Tokenized?

Tokenized Loans:

- **Centrifuge (real-world loan tokenization):** Real-world asset lending protocol
- **Goldfinch (crypto loans to businesses):** Crypto loans to non-crypto businesses
- **Maple Finance:** Institutional undercollateralized lending

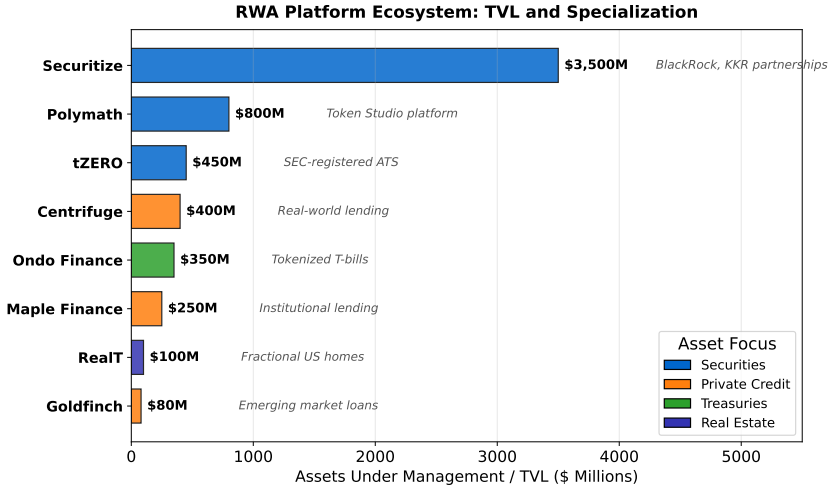
How It Works:

1. Company needs loan (e.g., $1M for inventory)
2. Platform originates loan, tokenizes it
3. DeFi investors buy loan tokens (earn interest)
4. Company repays loan + interest over time

Risk: Default risk (borrower fails to repay), requires legal recourse

(c) Joerg Osterrieder 2025

What Platforms Dominate the RWA Ecosystem?



Securitize leads with $3.5B AUM; platforms specialize in securities, credit, or real estate

What Legal Hurdles Block RWA Adoption?

Key Issues:

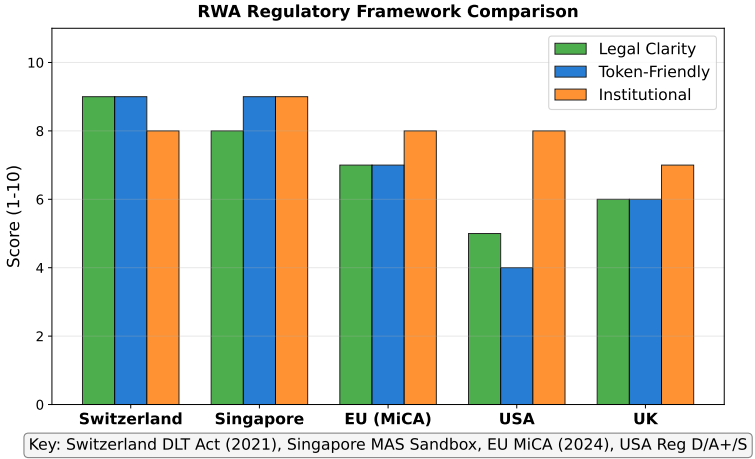
1. **Property Rights:** Does token legally represent asset ownership?
2. **Jurisdiction:** Which country's laws apply (asset vs. token location)?
3. **Enforcement:** How to enforce rights if smart contract disputes?
4. **Bankruptcy (token holders may lose investment):** What happens if SPV or platform goes bankrupt?

Solutions:

- Robust legal agreements (off-chain documentation)
- Established jurisdictions (Delaware, Switzerland, Singapore)
- Regulatory engagement (work with SEC, FINMA, MAS)
- Insurance and guarantees

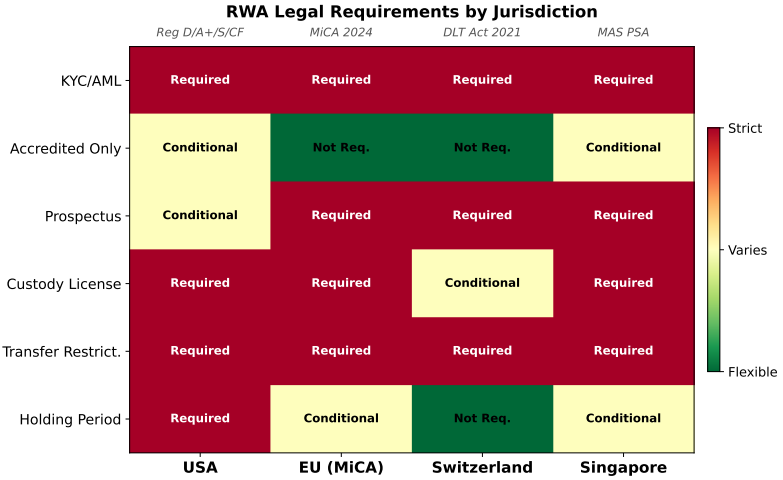
(c) Joerg Osterrieder 2025

How Do Regulatory Frameworks Compare Globally?



Switzerland and Singapore lead in legal clarity and token-friendliness

What Legal Requirements Vary by Jurisdiction?



USA most restrictive (accreditation, holding periods); Switzerland most flexible

How Do Regulatory Frameworks Differ Across Jurisdictions?

United States:

- SEC oversight (securities laws apply)
- Reg D, Reg A+, Reg S compliance required
- State-level licensing (money transmitter laws)

Switzerland:

- DLT Act (2021): Legal framework for tokenized securities
- FINMA guidance on token classifications
- Crypto Valley (Zug): Hub for RWA projects

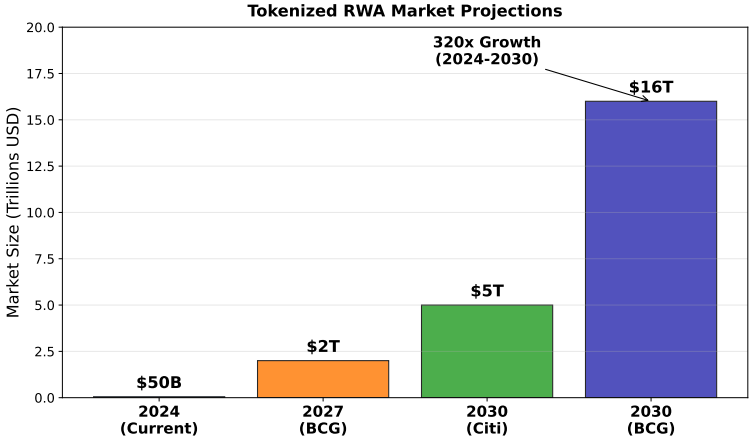
Singapore:

- MAS (Monetary Authority) sandbox for tokenization
- Payment Services Act covers digital tokens
- Project Guardian: Institutional DeFi pilot

EU: MiCA (EU crypto regulation 2024 – Markets in Crypto-Assets) regulation (2024)

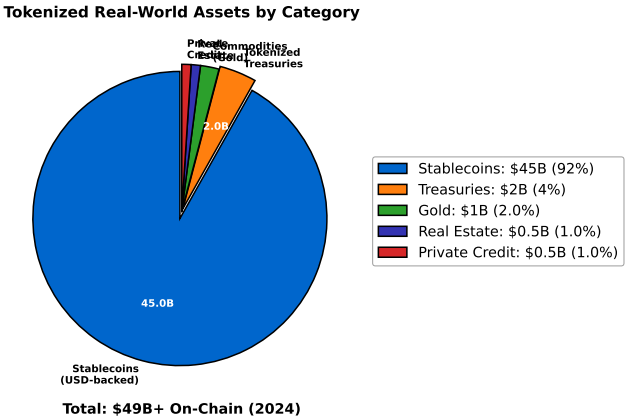
→ Problem: How do we tokenize physical assets? — Regulatory Frameworks by Jurisdiction MiCA (EU 2024) provides clearer rules than US, potentially shifting RWA activity to Europe.

What Are the RWA Market Projections for 2030?



BCG and Citi project $5-16T in tokenized assets by 2030 (320x growth)

How Are Current RWA Assets Distributed?



Stablecoins dominate (92%), with Treasuries emerging as fastest-growing category

What Is the Current RWA Market Size?

Current Market (December 2024):

- Total tokenized RWA (excl. stablecoins): $15.2B (up 85% YoY)
- Breakdown:
  - Tokenized Treasuries: $3B+ (BUIDL: $2.9B)
  - Private credit: $8B+
  - Real estate: $500M
  - Commodities (gold): $1B

Growth Projections:

- **BCG (2022):** $16T tokenized assets by 2030
- **Citi (2023):** $4-5T by 2030
- **BlackRock (2024):** "Next evolution of markets"

Drivers: Institutional adoption, regulatory clarity, infrastructure maturity

What Benefits Does RWA Tokenization Offer?

For Investors:

- Fractional access to assets
- 24/7 liquidity, global access
- Transparent ownership

For Asset Owners:

- Unlock illiquid asset value
- Lower cost of capital
- Programmable rights

For Markets:

- Instant settlement
- Financial inclusion
- Fewer intermediaries

(c) Joerg Osterrieder 2025

What Risks and Limitations Exist?

Key Risks:

- Legal uncertainty (enforceability)
- Smart contract vulnerabilities
- Custody/counterparty risk
- Regulatory changes
- Liquidity illusion

Mitigation Strategies:

- Established legal jurisdictions
- Thorough smart contract audits
- Insurance for custody/assets
- Legal recourse mechanisms

(c) Joerg Osterrieder 2025

How Do RWAs Integrate with DeFi?

RWA as DeFi Collateral:

Use Cases:

- Deposit tokenized Treasuries, borrow stablecoins
- Earn DeFi yield while holding real-world assets
- Leverage real estate tokens for liquidity

Platforms:

- **MakerDAO:** Accepts RWA as collateral for DAI minting
- **Aave Arc:** Permissioned pool for institutional RWA
- **Compound:** Exploring RWA collateral integration

Advantage: Bridges traditional finance yield with DeFi composability

Problem Solved? Real-World Asset Tokenization

The Original Problem

How do we tokenize physical assets while maintaining legal validity?

How Real-World Asset Tokenization Solves It

- Legal wrappers (SPVs) connect tokens to asset ownership rights
- Oracles and custodians verify real-world asset status (gold vaults, property registries)
- Regulatory frameworks (Reg D, Reg A+, DLT Act) provide legal certainty

Remaining Limitations

- Requires legal enforcement in traditional courts (jurisdiction-dependent)
- Counterparty risk: SPV, custodian, or platform insolvency
- Liquidity illusion: tokens trade 24/7 but underlying asset remains illiquid

Open Questions

- Will RWA tokenization achieve mainstream adoption or remain a niche?
- Risk: Extractive tokenomics, unsustainable yields in private credit markets

Real-World Asset Tokenization partially solves "tokenizing physical assets" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Real-World Asset Tokenization

Incentive Structure

- **Core Problem:** Creating and distributing economic value
- **Why act honestly?** Value capture aligned with value creation
- **Value Flow:** Creators capture value, users pay for utility

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Creators capture value, users pay for utility

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Real-World Asset Tokenization

Alternatives Considered

1. **Chosen Design:** Fee models, token distribution
2. **Alternative:** Alternative value capture mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Real-World Asset Tokenization

Critical Failure Mode

- **What breaks:** Extractive tokenomics, unsustainable yields
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

! Unusual economic behavior

! Incentive misalignment

! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Regulatory boundary crossing

[COMIC: placeholder]

A tokenized real estate investor happily trading on their phone: "24/7 global liquidity!" Meanwhile, the token crosses a digital border and multiple regulators appear: SEC (USA), FINMA (Switzerland), MAS (Singapore), each with different rulebooks. "Which laws apply here?"

The Jurisdiction Problem

- Asset in Delaware, token on Ethereum
- Buyer in Singapore, seller in Germany
- Which court handles disputes?

Current Solutions

- Reg D/A+: US accredited investor rules
- MiCA: EU harmonized framework (2024)
- Switzerland DLT Act: Token-friendly
- Compliance built into token (ERC-3643)

Global tokens meet local laws—regulatory clarity is RWA's biggest bottleneck

Key Takeaways

1. RWA tokenization represents ownership of physical assets as blockchain tokens
2. Real estate tokenization enables fractional ownership and liquidity (RealT, Propy)
3. Securities tokenization requires regulatory compliance (Reg D, Reg A+, ERC-1400)
4. BlackRock BUIDL fund ($2.9B) legitimizes institutional RWA adoption
5. RWA market: $15B current (excl. stablecoins), projected $4-16T by 2030
6. Legal frameworks and custody remain critical challenges for mainstream adoption

Next Lesson: L28 – Lab: NFT Evaluation

Discussion Questions

1. What are the primary barriers to widespread RWA tokenization adoption?
2. How can legal systems ensure token holders have enforceable rights to underlying assets?
3. Should all security tokens be regulated like traditional securities, or is lighter regulation appropriate?
4. What risks does DeFi integration of RWA collateral introduce to financial stability?
5. Will RWA tokenization democratize investing, or create new forms of inequality?

(c) Joerg Osterrieder 2025

Next Lesson Preview

L28: Lab – NFT Valuation

Hands-on activities:

- Develop comprehensive due diligence checklist
- Identify red flags and scam indicators
- Conduct rarity analysis and trait valuation
- Prepare investment recommendation report
- Practice evaluating NFT projects systematically

Preparation: Review all previous lessons on NFT technology, marketplaces, and categories

Quiz Questions (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity
C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset
C) A cryptocurrency wallet D) A type of smart contract
Answer: B – SPV is the legal structure that owns the asset while tokens represent fractional ownership.

Q3. What is the minimum investment on RealT platform?
A) $10 B) $50 C) $500 D) $5,000
Answer: B – RealT enables fractional real estate ownership with a minimum of $50 per property.

Q4. Which regulatory framework allows retail investors in the USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is a mini-IPO framework that allows retail investors (up to $75M raise).

Q5. What was the first blockchain property sale in 2017?
A) Apartment in Dubai B) Apartment in Kiev C) House in California D) Office in London
Answer: B – Propy facilitated the first blockchain property sale (Kiev apartment, $60k, NFT deed).

Quiz Questions (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks
C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B AUM in 9 months, making it the largest tokenized fund.

Q8. What assets back the BlackRock BUIDL token?
A) Bitcoin and Ethereum B) Real estate portfolios
C) US Treasury bills and cash D) Corporate bonds
Answer: C – BUIDL is backed by US Treasuries, cash, and repos, yielding 5% APY.

Q9. What does 1 PAXG token represent?
A) 1 gram of gold B) 1 troy ounce of gold C) 1 kilogram of gold D) $1 of gold
Answer: B – Pax Gold (PAXG) is backed 1:1 by physical gold (1 token = 1 troy oz).

Q10. Which platform tokenizes verified carbon credits?
A) Propy B) RealT C) Toucan Protocol D) Centrifuge
Answer: C – Toucan Protocol tokenizes carbon credits as TCO2 for corporate emissions offsetting.

Quiz Questions (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – Boston Consulting Group projects $16T in tokenized RWAs by 2030 (320x growth).

Q13. Which jurisdiction has the DLT Act (2021) for tokenized securities?
A) United States B) Singapore C) Switzerland D) United Kingdom
Answer: C – Switzerland enacted the DLT Act in 2021, providing legal framework for tokenized securities.

Q14. What protocol enables real-world asset lending on-chain?
A) Uniswap B) Centrifuge C) Aave D) Compound
Answer: B – Centrifuge tokenizes real-world loans, enabling DeFi investors to earn interest.

Q15. What is the settlement time for BUIDL token redemption?
A) Instant B) T+1 (1 business day) C) T+3 (3 days) D) T+7 (1 week)
Answer: B – BUIDL tokens can be redeemed for USD with T+1 settlement (1 business day).

Quiz Questions (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds
C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions for securities.

Q18. What percentage of current RWA market is stablecoins?
A) 50% B) 75% C) 92% D) 99%
Answer: C – Stablecoins dominate at 92%, with Treasuries as the fastest-growing non-stablecoin category.

Q19. Which platform uses NFT property deeds for real estate?
A) RealT B) Propy C) Lofty AI D) Polymath
Answer: B – Propy issues property ownership certificates as NFTs on Ethereum.

Q20. What risk does "liquidity illusion" refer to in RWA tokenization?
A) Smart contract bugs B) Tokens trade but underlying asset remains illiquid
C) Regulatory changes D) Custody failures
Answer: B – Tokens may trade 24/7, but the underlying real-world asset may still be difficult to sell.

L27: Real-World Asset Tokenization

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Define RWA tokenization and explain its key benefits
- Understand how SPVs bridge tokens to real-world assets
- Identify major RWA categories (real estate, securities, commodities)
- Analyze the BlackRock BUIDL fund as institutional case study

Condensed from full L27 lecture (27 slides to 13 slides)

What is Real-World Asset Tokenization?

Definition: Representing ownership of physical assets as blockchain tokens

Asset Classes:

- Real estate (residential, commercial properties)
- Securities (stocks, bonds, fund shares)
- Commodities (gold, carbon credits)

Key Benefits:

- **Fractional ownership:** Divide expensive assets into affordable shares
- **Liquidity:** Trade traditionally illiquid assets 24/7
- **Transparency:** Ownership and transactions recorded on-chain

Critical requirement: Legal framework linking token to real-world asset rights

How RWA Tokenization Works

The SPV (Special Purpose Vehicle) Model:

1. **Asset Selection:** Identify real-world asset (e.g., $10M building)
2. **Legal Structure:** Create SPV to hold the asset
3. **Token Issuance:** Mint tokens representing fractional ownership
4. **Distribution:** Sell tokens to investors (primary market)
5. **Trading:** Tokens trade on secondary markets

Example: $10M commercial building

- Issue 10,000 tokens at $1,000 each
- Rental income distributed pro-rata to token holders

Legal bridge: Smart contract references off-chain legal agreement

Real Estate Tokenization Platforms

RealT (Ethereum-based):

- Minimum investment: $50 per property
- Daily rent distribution (stablecoins to wallets)
- Annual yield: 8-12% (rent minus costs)
- Regulatory: Reg D (accredited) or Reg A+ (retail)

Propy (End-to-end transactions):

- Smart contract-based escrow
- NFT property deeds (ownership certificate)
- First blockchain sale: Kiev apartment, 2017 ($60k)

Other platforms: Lofty AI, Polymath

Real estate tokenization makes property investment accessible globally

Securities Tokenization

Security Token: Digital token representing traditional security

US Regulatory Frameworks:

- **Reg D:** Private placement, accredited investors only
- **Reg A+:** Mini-IPO, retail investors, up to $75M raise
- **Reg S:** Offshore sales to non-US investors

Enhanced Token Standards (vs. ERC-20):

- **ERC-1400:** Security token with partitions
- **ERC-3643:** Transfer restrictions, compliance modules

Key Features: KYC whitelist, transfer restrictions, document references

ERC-20 lacks built-in compliance – security tokens require enhanced standards

BlackRock BUIDL Fund: Institutional RWA

Fund: BlackRock USD Institutional Digital Liquidity Fund

Key Details:

- **Launch:** March 2024
- **AUM:** $2.9B (December 2024) – largest tokenized fund
- **Blockchains:** Ethereum, Solana, Arbitrum, Optimism, Polygon, Aptos
- **Asset backing:** US Treasury bills, cash, repos
- **Yield:** Approximately 5% APY

Significance:

- World's largest asset manager enters on-chain finance
- Legitimizes tokenized securities for institutions

"If BlackRock does it, it's real" – institutional validation of RWA

Commodity and Carbon Tokenization

Gold Tokenization:

- **Pax Gold (PAXG):** 1 token = 1 troy ounce of gold
- **Tether Gold (XAUT):** Similar model, Tether-issued
- Physical gold in vaults (audited), redeemable at high minimums

Carbon Credit Tokenization:

- **Toucan Protocol:** Tokenizes verified carbon credits (TCO2)
- **KlimaDAO:** Carbon-backed currency
- Corporations offset emissions via token purchases

Other: Tokenized oil barrels (experimental), renewable energy certificates as NFTs

Commodity tokens enable fractional ownership and easier trading of physical assets

RWA Market Size and Projections

Current Market (December 2024):

- Total RWA (excl. stablecoins): $15.2B (up 85% YoY)
- Tokenized Treasuries: $3B+ (BUIDL: $2.9B)
- Private credit: $8B+
- Real estate: $500M — Commodities (gold): $1B

Growth Projections:

- BCG (2022): $16T tokenized assets by 2030
- Citi (2023): $4-5T by 2030
- BlackRock (2024): "Next evolution of markets"

Drivers: Institutional adoption, regulatory clarity, infrastructure maturity

Stablecoins dominate at 92%; Treasuries are fastest-growing non-stablecoin category

Risks and Legal Challenges

Key Risks:

1. **Legal uncertainty:** Token rights may not hold in court
2. **Smart contract bugs:** Exploits can drain funds
3. **Custody risk:** Asset held by third party (trust required)
4. **Liquidity illusion:** Tokens trade, but underlying asset still illiquid

Mitigation Strategies:

- Use established jurisdictions (Delaware, Switzerland, Singapore)
- Audit smart contracts thoroughly
- Maintain legal recourse mechanisms

Critical challenge: Bridging token ownership to enforceable real-world property rights

Key Takeaways

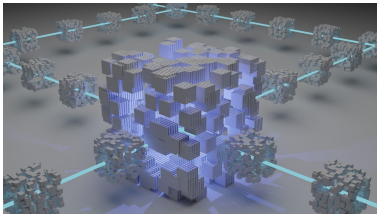
1. RWA tokenization represents ownership of physical assets as blockchain tokens
2. Real estate platforms (RealT, Propy) enable fractional ownership from $50
3. Securities tokenization requires compliance (Reg D/A+, ERC-1400/ERC-3643)
4. BlackRock BUIDL ($2.9B) legitimizes institutional RWA adoption
5. RWA market: $15B current, projected $4-16T by 2030
6. Legal frameworks and custody remain critical challenges

For full coverage, see complete L27 lecture (27 slides)

RWA Tokenization – Visual Overview

Real Estate
Fractional property ownership

Commodities
Gold and asset tokenization



Blockchain
On-chain asset representation

Images: Unsplash (CC0) – free for commercial use, no attribution required

Quiz Questions (1–5)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates legal requirements B) Enables fractional ownership and liquidity
C) Guarantees appreciation D) Removes investment risk
Answer: B – Tokenization divides expensive assets into affordable shares with 24/7 trading.

Q2. What is an SPV in RWA tokenization?
A) Blockchain protocol B) Legal entity holding the physical asset
C) Cryptocurrency wallet D) Smart contract type
Answer: B – SPV owns the asset; tokens represent fractional ownership.

Q3. What is the AUM of BlackRock BUIDL (December 2024)?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B, making it the largest tokenized fund.

Q4. What does 1 PAXG token represent?
A) 1 gram of gold B) 1 troy ounce of gold C) 1 kg of gold D) $1 of gold
Answer: B – Pax Gold is backed 1:1 by physical gold (1 token = 1 troy oz).

Q5. Which US regulation allows retail investors?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is a mini-IPO framework allowing retail investors.

Quiz Questions (6–10)

Q6. What is the current RWA market size (excl. stablecoins)?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY) in December 2024.

Q7. Which ERC standard includes compliance modules?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions.

Q8. What is the minimum investment on RealT?
A) $10 B) $50 C) $500 D) $5,000
Answer: B – RealT enables fractional real estate with $50 minimum.

Q9. What risk does "liquidity illusion" refer to?
A) Smart contract bugs B) Tokens trade but underlying asset remains illiquid
C) Regulatory changes D) Custody failures
Answer: B – Tokens may trade 24/7, but the underlying asset may be hard to sell.

Q10. Which platform tokenizes carbon credits?
A) Propy B) RealT C) Toucan Protocol D) Centrifuge
Answer: C – Toucan Protocol tokenizes carbon credits as TCO2.

L27: Real-World Asset Tokenization

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

January 2026

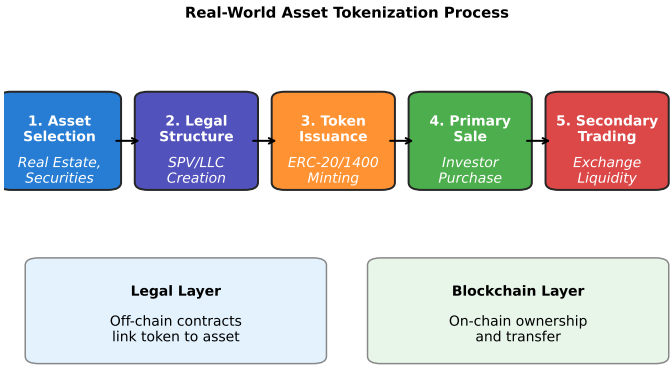
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Define real-world asset (RWA) tokenization and key benefits
- Explain securities tokenization and regulatory frameworks (Reg D, A+, S)
- Analyze BlackRock BUIDL fund as institutional case study
- Evaluate RWA market size and growth projections

RWA Tokenization Process



Key: Legal SPV (Special Purpose Vehicle) bridges token to real-world ownership.

What is RWA Tokenization?

Definition: Representing ownership of physical assets as blockchain tokens

Asset Classes:

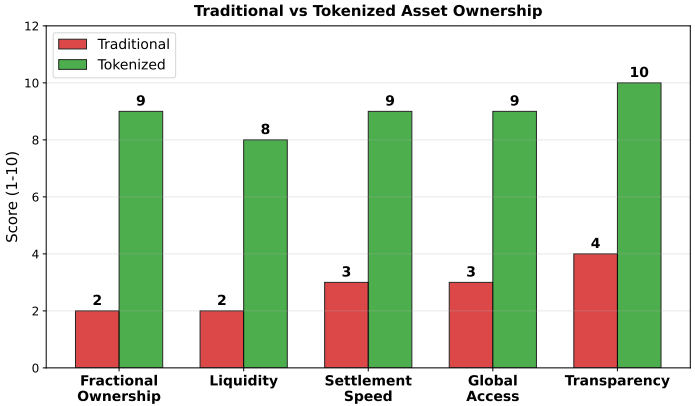
- Real estate, securities (stocks, bonds), commodities (gold, carbon)
- Art/collectibles, debt instruments (loans, mortgages)

Key Benefits:

- **Fractional ownership:** $50-100 minimums vs $100k+
- **24/7 liquidity:** Trade traditionally illiquid assets
- **Transparency:** On-chain ownership records
- **Lower fees:** Fewer intermediaries

(c) Joerg Osterrieder 2025

Traditional vs Tokenized Ownership



Tokenization: Dramatically improves fractional access, liquidity, settlement.

Securities Tokenization: Regulatory Frameworks

USA Frameworks:

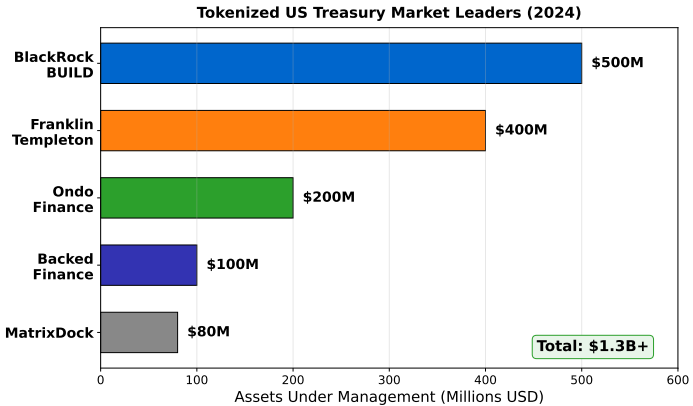
- **Reg D (506):** Private placement, accredited investors only
- **Reg A+:** Mini-IPO, retail investors, up to $75M raise
- **Reg S:** Offshore sales to non-US investors
- **Reg CF:** Crowdfunding, retail, up to $5M raise

Security Token Standards:

- **ERC-1400:** Security token with partitions
- **ERC-3643 (T-REX):** Transfer restrictions, KYC modules

ERC-20 Limitation: No built-in compliance or transfer restrictions.

Tokenized Treasury Market Leaders



BlackRock BUIDL: $2.9B AUM (Dec 2024) – largest tokenized fund.

BlackRock BUIDL Fund: Institutional RWA

Details:

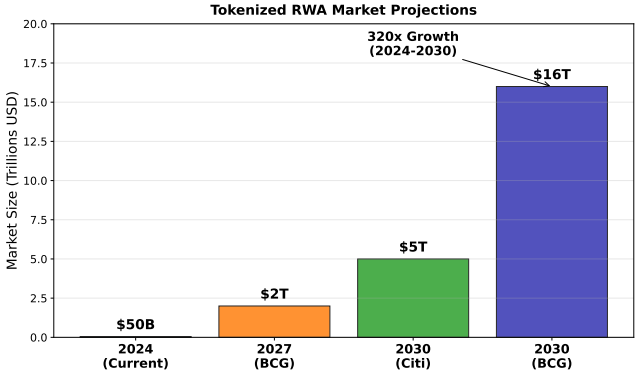
- **Launch:** March 2024, grew to $2.9B in 9 months
- **Backing:** US Treasury bills, cash, repos
- **Chains:** Ethereum, Solana, Arbitrum, Optimism, Polygon, Aptos
- **Yield:** 5% APY (Treasury yield minus fees)
- **Redemption:** T+1 settlement

Significance:

- World's largest asset manager on-chain
- Legitimizes tokenized securities for institutions
- Total tokenized Treasury market: $3B+ (December 2024)

(c) Joerg Osterrieder 2025

RWA Market Projections



BCG: $16T by 2030 — **Citi:** $4-5T by 2030 — **Current:** $15.2B (excl. stables)

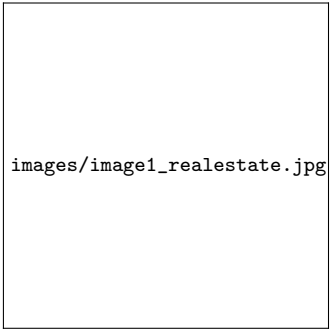
Key Takeaways

1. **RWA Tokenization:** Physical assets as blockchain tokens via SPV legal structure
2. **Benefits:** Fractional ownership ($50+), 24/7 liquidity, transparent records
3. **Regulation:** Reg D (accredited), Reg A+ (retail), ERC-3643 compliance
4. **BlackRock BUIDL:** $2.9B AUM, 5% yield, T+1 redemption
5. **Market:** $15.2B current (Dec 2024), projected $4-16T by 2030

Key Risk: Token rights must legally represent enforceable asset ownership.

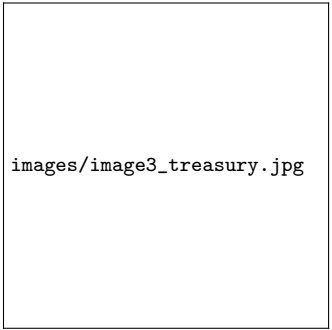
(c) Joerg Osterrieder 2025

RWA Tokenization in Practice



Real Estate

Securities



Treasury Bills

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates all risk B) Fractional ownership and liquidity
C) Guarantees returns D) No regulation needed

Quiz (1/2)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates all risk B) Fractional ownership and liquidity
C) Guarantees returns D) No regulation needed
Answer: B – Enables affordable shares and 24/7 trading.

Q2. What is an SPV in RWA tokenization?
A) Blockchain protocol B) Legal entity holding the physical asset
C) Cryptocurrency wallet D) Smart contract type

Quiz (1/2)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates all risk B) Fractional ownership and liquidity
C) Guarantees returns D) No regulation needed
Answer: B – Enables affordable shares and 24/7 trading.

Q2. What is an SPV in RWA tokenization?
A) Blockchain protocol B) Legal entity holding the physical asset
C) Cryptocurrency wallet D) Smart contract type
Answer: B – SPV owns asset; tokens represent fractional ownership.

Q3. Which regulatory framework allows retail investors in USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only

Quiz (1/2)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates all risk B) Fractional ownership and liquidity
C) Guarantees returns D) No regulation needed
Answer: B – Enables affordable shares and 24/7 trading.

Q2. What is an SPV in RWA tokenization?
A) Blockchain protocol B) Legal entity holding the physical asset
C) Cryptocurrency wallet D) Smart contract type
Answer: B – SPV owns asset; tokens represent fractional ownership.

Q3. Which regulatory framework allows retail investors in USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is mini-IPO allowing retail (up to $75M).

Q4. What is BlackRock BUIDL AUM (December 2024)?
A) $500M B) $1.5B C) $2.9B D) $5B

Quiz (1/2)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates all risk B) Fractional ownership and liquidity
C) Guarantees returns D) No regulation needed
Answer: B – Enables affordable shares and 24/7 trading.

Q2. What is an SPV in RWA tokenization?
A) Blockchain protocol B) Legal entity holding the physical asset
C) Cryptocurrency wallet D) Smart contract type
Answer: B – SPV owns asset; tokens represent fractional ownership.

Q3. Which regulatory framework allows retail investors in USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is mini-IPO allowing retail (up to $75M).

Q4. What is BlackRock BUIDL AUM (December 2024)?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – $2.9B in 9 months, largest tokenized fund.

Q5. What backs the BUIDL token?
A) Bitcoin and ETH B) Real estate C) US Treasuries and cash D) Corporate bonds

Quiz (1/2)

Q1. What is the primary benefit of RWA tokenization?
A) Eliminates all risk B) Fractional ownership and liquidity
C) Guarantees returns D) No regulation needed
Answer: B – Enables affordable shares and 24/7 trading.

Q2. What is an SPV in RWA tokenization?
A) Blockchain protocol B) Legal entity holding the physical asset
C) Cryptocurrency wallet D) Smart contract type
Answer: B – SPV owns asset; tokens represent fractional ownership.

Q3. Which regulatory framework allows retail investors in USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is mini-IPO allowing retail (up to $75M).

Q4. What is BlackRock BUIDL AUM (December 2024)?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – $2.9B in 9 months, largest tokenized fund.

Q5. What backs the BUIDL token?
A) Bitcoin and ETH B) Real estate C) US Treasuries and cash D) Corporate bonds
Answer: C – US Treasury bills, cash, repos (5% APY).

Quiz (2/2)

Q6. Why can't ERC-20 be used directly for securities?
A) Too expensive B) No transfer restrictions or KYC
C) Not compatible D) Cannot represent ownership

Quiz (2/2)

Q6. Why can't ERC-20 be used directly for securities?
A) Too expensive B) No transfer restrictions or KYC
C) Not compatible D) Cannot represent ownership
Answer: B – Lacks compliance checks and transfer restrictions.

Q7. What is the total RWA market size (excl. stablecoins) Dec 2024?
A) $5B B) $15.2B C) $50B D) $100B

Quiz (2/2)

Q6. Why can't ERC-20 be used directly for securities?
A) Too expensive B) No transfer restrictions or KYC
C) Not compatible D) Cannot represent ownership
Answer: B – Lacks compliance checks and transfer restrictions.

Q7. What is the total RWA market size (excl. stablecoins) Dec 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – $15.2B (up 85% YoY).

Q8. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T

Quiz (2/2)

Q6. Why can't ERC-20 be used directly for securities?
A) Too expensive B) No transfer restrictions or KYC
C) Not compatible D) Cannot represent ownership
Answer: B – Lacks compliance checks and transfer restrictions.

Q7. What is the total RWA market size (excl. stablecoins) Dec 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – $15.2B (up 85% YoY).

Q8. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – $16T projected (320x growth).

Q9. What ERC standard includes compliance modules?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643

Quiz (2/2)

Q6. Why can't ERC-20 be used directly for securities?
A) Too expensive B) No transfer restrictions or KYC
C) Not compatible D) Cannot represent ownership
Answer: B – Lacks compliance checks and transfer restrictions.

Q7. What is the total RWA market size (excl. stablecoins) Dec 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – $15.2B (up 85% YoY).

Q8. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – $16T projected (320x growth).

Q9. What ERC standard includes compliance modules?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes KYC and transfer restrictions.

Q10. What is BUIDL token redemption settlement time?
A) Instant B) T+1 C) T+3 D) T+7

Quiz (2/2)

Q6. Why can't ERC-20 be used directly for securities?
A) Too expensive B) No transfer restrictions or KYC
C) Not compatible D) Cannot represent ownership
Answer: B – Lacks compliance checks and transfer restrictions.

Q7. What is the total RWA market size (excl. stablecoins) Dec 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – $15.2B (up 85% YoY).

Q8. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – $16T projected (320x growth).

Q9. What ERC standard includes compliance modules?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes KYC and transfer restrictions.

Q10. What is BUIDL token redemption settlement time?
A) Instant B) T+1 C) T+3 D) T+7
Answer: B – T+1 (1 business day) for USD redemption.

Thank you

Questions?

Next: L28 Lab – NFT Project Evaluation

Quiz: RWA Tokenization

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity C) Guarantees asset appreciation D) Removes all investment risk

Quiz (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset C) A cryptocurrency wallet D) A type of smart contract

Quiz (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset C) A cryptocurrency wallet D) A type of smart contract
Answer: B – SPV is the legal structure that owns the asset while tokens represent fractional ownership.

Q3. What is the minimum investment on RealT platform?
A) $10 B) $50 C) $500 D) $5,000

Quiz (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset C) A cryptocurrency wallet D) A type of smart contract
Answer: B – SPV is the legal structure that owns the asset while tokens represent fractional ownership.

Q3. What is the minimum investment on RealT platform?
A) $10 B) $50 C) $500 D) $5,000
Answer: B – RealT enables fractional real estate ownership with a minimum of $50 per property.

Q4. Which regulatory framework allows retail investors in the USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only

Quiz (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset C) A cryptocurrency wallet D) A type of smart contract
Answer: B – SPV is the legal structure that owns the asset while tokens represent fractional ownership.

Q3. What is the minimum investment on RealT platform?
A) $10 B) $50 C) $500 D) $5,000
Answer: B – RealT enables fractional real estate ownership with a minimum of $50 per property.

Q4. Which regulatory framework allows retail investors in the USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is a mini-IPO framework that allows retail investors (up to $75M raise).

Q5. What was the first blockchain property sale in 2017?
A) Apartment in Dubai B) Apartment in Kiev C) House in California D) Office in London

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary benefit of real-world asset (RWA) tokenization?
A) Eliminates all legal requirements B) Enables fractional ownership and liquidity C) Guarantees asset appreciation D) Removes all investment risk
Answer: B – Tokenization allows expensive assets to be divided into affordable shares and traded 24/7.

Q2. What is an SPV (Special Purpose Vehicle) in RWA tokenization?
A) A blockchain protocol B) A legal entity that holds the physical asset C) A cryptocurrency wallet D) A type of smart contract
Answer: B – SPV is the legal structure that owns the asset while tokens represent fractional ownership.

Q3. What is the minimum investment on RealT platform?
A) $10 B) $50 C) $500 D) $5,000
Answer: B – RealT enables fractional real estate ownership with a minimum of $50 per property.

Q4. Which regulatory framework allows retail investors in the USA?
A) Reg D B) Reg A+ C) Reg S D) All accredited-only
Answer: B – Reg A+ is a mini-IPO framework that allows retail investors (up to $75M raise).

Q5. What was the first blockchain property sale in 2017?
A) Apartment in Dubai B) Apartment in Kiev C) House in California D) Office in London
Answer: B – Propy facilitated the first blockchain property sale (Kiev apartment, $60k, NFT deed).

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks C) Not compatible with Ethereum D) Cannot represent ownership

Quiz (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B

Quiz (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B AUM in 9 months, making it the largest tokenized fund.

Q8. What assets back the BlackRock BUIDL token?
A) Bitcoin and Ethereum B) Real estate portfolios C) US Treasury bills and cash D) Corporate bonds

Quiz (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B AUM in 9 months, making it the largest tokenized fund.

Q8. What assets back the BlackRock BUIDL token?
A) Bitcoin and Ethereum B) Real estate portfolios C) US Treasury bills and cash D) Corporate bonds
Answer: C – BUIDL is backed by US Treasuries, cash, and repos, yielding 5% APY.

Q9. What does 1 PAXG token represent?
A) 1 gram of gold B) 1 troy ounce of gold C) 1 kilogram of gold D) $1 of gold

Quiz (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B AUM in 9 months, making it the largest tokenized fund.

Q8. What assets back the BlackRock BUIDL token?
A) Bitcoin and Ethereum B) Real estate portfolios C) US Treasury bills and cash D) Corporate bonds
Answer: C – BUIDL is backed by US Treasuries, cash, and repos, yielding 5% APY.

Q9. What does 1 PAXG token represent?
A) 1 gram of gold B) 1 troy ounce of gold C) 1 kilogram of gold D) $1 of gold
Answer: B – Pax Gold (PAXG) is backed 1:1 by physical gold (1 token = 1 troy oz).

Q10. Which platform tokenizes verified carbon credits?
A) Propy B) RealT C) Toucan Protocol D) Centrifuge

Quiz (6–10)

Q6. Why can't ERC-20 tokens be used directly for security tokenization?
A) Too expensive B) No transfer restrictions or compliance checks C) Not compatible with Ethereum D) Cannot represent ownership
Answer: B – ERC-20 lacks built-in KYC/AML, accreditation verification, and transfer restrictions.

Q7. What is the AUM of BlackRock BUIDL fund as of December 2024?
A) $500M B) $1.5B C) $2.9B D) $5B
Answer: C – BUIDL reached $2.9B AUM in 9 months, making it the largest tokenized fund.

Q8. What assets back the BlackRock BUIDL token?
A) Bitcoin and Ethereum B) Real estate portfolios C) US Treasury bills and cash D) Corporate bonds
Answer: C – BUIDL is backed by US Treasuries, cash, and repos, yielding 5% APY.

Q9. What does 1 PAXG token represent?
A) 1 gram of gold B) 1 troy ounce of gold C) 1 kilogram of gold D) $1 of gold
Answer: B – Pax Gold (PAXG) is backed 1:1 by physical gold (1 token = 1 troy oz).

Q10. Which platform tokenizes verified carbon credits?
A) Propy B) RealT C) Toucan Protocol D) Centrifuge
Answer: C – Toucan Protocol tokenizes carbon credits as TCO2 for corporate emissions offsetting.

Quiz (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B

Quiz (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T

Quiz (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – Boston Consulting Group projects $16T in tokenized RWAs by 2030 (320x growth).

Q13. Which jurisdiction has the DLT Act (2021) for tokenized securities?
A) United States B) Singapore C) Switzerland D) United Kingdom

Quiz (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – Boston Consulting Group projects $16T in tokenized RWAs by 2030 (320x growth).

Q13. Which jurisdiction has the DLT Act (2021) for tokenized securities?
A) United States B) Singapore C) Switzerland D) United Kingdom
Answer: C – Switzerland enacted the DLT Act in 2021, providing legal framework for tokenized securities.

Q14. What protocol enables real-world asset lending on-chain?
A) Uniswap B) Centrifuge C) Aave D) Compound

Quiz (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – Boston Consulting Group projects $16T in tokenized RWAs by 2030 (320x growth).

Q13. Which jurisdiction has the DLT Act (2021) for tokenized securities?
A) United States B) Singapore C) Switzerland D) United Kingdom
Answer: C – Switzerland enacted the DLT Act in 2021, providing legal framework for tokenized securities.

Q14. What protocol enables real-world asset lending on-chain?
A) Uniswap B) Centrifuge C) Aave D) Compound
Answer: B – Centrifuge tokenizes real-world loans, enabling DeFi investors to earn interest.

Q15. What is the settlement time for BUIDL token redemption?
A) Instant B) T+1 (1 business day) C) T+3 (3 days) D) T+7 (1 week)

Quiz (11–15)

Q11. What is the total RWA market size (excluding stablecoins) in December 2024?
A) $5B B) $15.2B C) $50B D) $100B
Answer: B – RWA market reached $15.2B (up 85% YoY), with Treasuries and private credit dominating.

Q12. What is BCG's projection for tokenized assets by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – Boston Consulting Group projects $16T in tokenized RWAs by 2030 (320x growth).

Q13. Which jurisdiction has the DLT Act (2021) for tokenized securities?
A) United States B) Singapore C) Switzerland D) United Kingdom
Answer: C – Switzerland enacted the DLT Act in 2021, providing legal framework for tokenized securities.

Q14. What protocol enables real-world asset lending on-chain?
A) Uniswap B) Centrifuge C) Aave D) Compound
Answer: B – Centrifuge tokenizes real-world loans, enabling DeFi investors to earn interest.

Q15. What is the settlement time for BUIDL token redemption?
A) Instant B) T+1 (1 business day) C) T+3 (3 days) D) T+7 (1 week)
Answer: B – BUIDL tokens can be redeemed for USD with T+1 settlement (1 business day).

Quiz (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds C) Ensuring token legally represents asset ownership D) Limited blockchain scalability

Quiz (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions for securities.

Q18. What percentage of current RWA market is stablecoins?
A) 50% B) 75% C) 92% D) 99%

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions for securities.

Q18. What percentage of current RWA market is stablecoins?
A) 50% B) 75% C) 92% D) 99%
Answer: C – Stablecoins dominate at 92%, with Treasuries as the fastest-growing non-stablecoin category.

Q19. Which platform uses NFT property deeds for real estate?
A) RealT B) Propy C) Lofty AI D) Polymath

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions for securities.

Q18. What percentage of current RWA market is stablecoins?
A) 50% B) 75% C) 92% D) 99%
Answer: C – Stablecoins dominate at 92%, with Treasuries as the fastest-growing non-stablecoin category.

Q19. Which platform uses NFT property deeds for real estate?
A) RealT B) Propy C) Lofty AI D) Polymath
Answer: B – Propy issues property ownership certificates as NFTs on Ethereum.

Q20. What risk does "liquidity illusion" refer to in RWA tokenization?
A) Smart contract bugs B) Tokens trade but underlying asset remains illiquid C) Regulatory changes D) Custody failures

Quiz (16–20)

Q16. What is the main legal challenge in RWA tokenization?
A) High transaction fees B) Slow blockchain speeds C) Ensuring token legally represents asset ownership D) Limited blockchain scalability
Answer: C – The critical challenge is bridging token ownership to enforceable real-world property rights.

Q17. Which ERC standard includes compliance modules and transfer restrictions?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3643
Answer: D – ERC-3643 (T-REX) includes identity verification and transfer restrictions for securities.

Q18. What percentage of current RWA market is stablecoins?
A) 50% B) 75% C) 92% D) 99%
Answer: C – Stablecoins dominate at 92%, with Treasuries as the fastest-growing non-stablecoin category.

Q19. Which platform uses NFT property deeds for real estate?
A) RealT B) Propy C) Lofty AI D) Polymath
Answer: B – Propy issues property ownership certificates as NFTs on Ethereum.

Q20. What risk does "liquidity illusion" refer to in RWA tokenization?
A) Smart contract bugs B) Tokens trade but underlying asset remains illiquid C) Regulatory changes D) Custody failures
Answer: B – Tokens may trade 24/7, but the underlying real-world asset may still be difficult to sell.

Lab Session: NFT Project Evaluation

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module C: NFTs & Digital Assets

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Conduct due diligence on NFT projects
- Analyze on-chain metrics and holder behavior
- Identify red flags and rug pull indicators
- Create a comprehensive risk assessment
- Make informed evaluation decisions

Building on L27: RWA Tokenization

The Problem: Evaluating Digital Asset Value

The Challenge
You're considering investing in an NFT project, but how do you separate genuine value from hype? The market is flooded with projects - some deliver real utility, others are sophisticated scams waiting to rug pull.

Why It Matters

- $2.8B lost to NFT scams and rug pulls (2021-2024)
- 95% of NFT projects fail within 18 months

What We Need

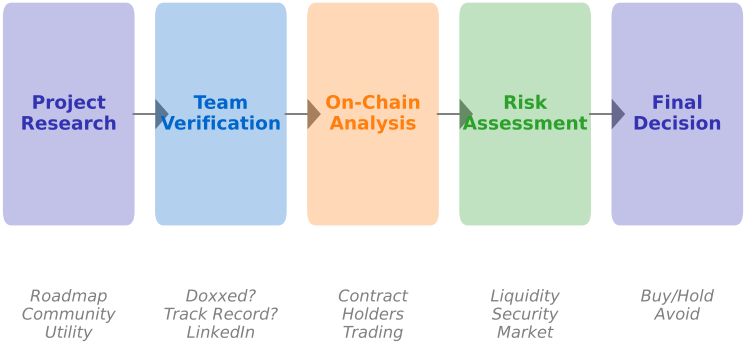
- Systematic evaluation framework for due diligence
- On-chain analysis to verify claims
- Risk assessment methodology for informed decisions

The Cryptoeconomics Question
How do we reveal true value vs marketing hype through forensic analysis?

Today's lab: Hands-on NFT project evaluation and asset tokenization analysis

Lab Session Structure

NFT Project Evaluation Workflow



Comprehensive evaluation before any NFT investment decision

Exercise 1: Project Research

Research Checklist:

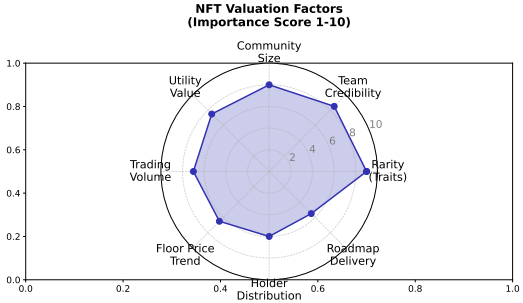
- Team: Doxxed? Track record? LinkedIn profiles?
- Roadmap: Realistic? Delivered milestones?
- Community: Discord activity? Twitter engagement?
- Partnerships: Verified? Real companies?

Red Flags:

- Anonymous team with no track record
- Unrealistic promises (guaranteed profits)
- Fake partnerships or celebrity endorsements
- Copied art or unoriginal concept

(c) Joerg Osterrieder 2025

Valuation Factors



Exercise 2: On-Chain Analysis

Etherscan Analysis:

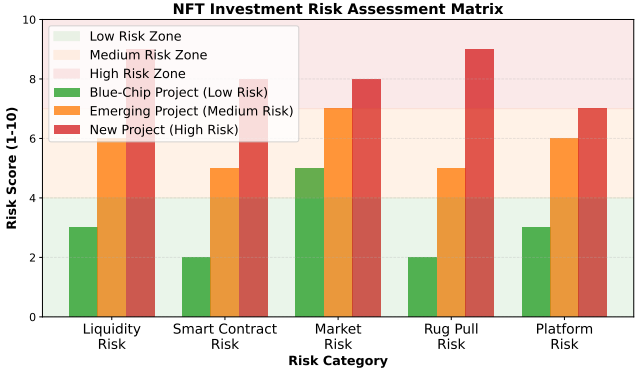
1. Contract address verification
2. Owner/admin functions review
3. Mint function (max supply enforced?)
4. Transfer restrictions

Holder Analysis:

- Distribution across wallets
- Team wallet identification
- Whale concentration
- Trading patterns (organic vs wash)

(c) Joerg Osterrieder 2025

Risk Assessment Matrix



NFT investments carry multiple risk factors - assess each carefully

Exercise 3: Risk Assessment

Risk Categories:

1. **Liquidity Risk**: Can you sell when needed?
2. **Smart Contract Risk**: Bugs, exploits, centralization
3. **Market Risk**: Volatility, bear markets
4. **Rug Pull Risk**: Team abandonment, exit scam
5. **Platform Risk**: Marketplace dependency

Create Risk Score:

- Rate each category 1-10
- Calculate weighted average
- Determine: Low (¡4), Medium (4-7), High (¿7)

(c) Joerg Osterrieder 2025

Lab Deliverables

Submit:

1. **Evaluation Report (3 pages):**
   - Project overview and team research
   - On-chain analysis findings
   - Risk assessment with scores
   - Final recommendation (Buy/Hold/Avoid)
2. **Supporting Evidence:**
   - Screenshots of research sources
   - Contract analysis snippets
   - Risk score calculation

Problem Solved? The Economics of NFT Due Diligence

The Original Problem

How do we evaluate NFT value and avoid scams?

How Systematic Evaluation Helps

- Contract verification reveals hidden admin powers and risks
- Holder analysis exposes whale concentration and wash trading
- Multi-factor risk scoring quantifies investment danger

The Economic Model

- **Incentive**: Thorough analysis protects capital from scams
- **Cost**: Research time investment (2-4 hours per project)
- **Reward**: Informed decisions, avoiding 95% failure rate

What Could Still Go Wrong?

- Hidden contract upgradability or proxy patterns
- Centralized metadata storage (IPFS vs AWS)
- False utility promises without actual implementation

Due diligence reduces risk but cannot eliminate it - allocation sizing matters

(c) Joerg Osterrieder 2025

The Economics of NFT Evaluation

Incentive Structure

- **Buyers**: Information asymmetry — sellers know more than buyers
- **Analysts**: Monetize expertise through advisory fees or early access
- **Scammers**: Exploit information gaps and FOMO

Value Flow

- Research time = insurance premium against losses
- Quality information has market value (alpha)

Security Model

- On-chain data is trustless and verifiable
- Off-chain claims (team, roadmap) require trust
- Multi-source verification reduces manipulation risk

Economic Reality

- 95% of NFT projects fail or lose value
- Position sizing is ultimate risk management
- Due diligence is necessary but not sufficient

Information asymmetry is the core economic problem in NFT markets

(c) Joerg Osterrieder 2025

Design Space: NFT Evaluation

Alternative Approaches

1. **Pure Technical**: Contract code review only
2. **Pure Social**: Team/community signals only
3. **Quantitative**: On-chain metrics scoring
4. **Holistic**: Multi-factor weighted analysis

Trade-offs

- Depth vs breadth of analysis
- Speed vs thoroughness
- False positives vs false negatives

Design Questions

- How to weight different risk factors?
- What threshold defines "high risk"?
- How often to re-evaluate held positions?

Current Best Practice

- Multi-source verification
- Contract + team + community + metrics
- Time-boxed research (2-4 hours max)
- Position sizing based on risk score

No single evaluation method is perfect — diversification applies to methodology too

(c) Joerg Osterrieder 2025

Failure Modes: NFT Evaluation

Assumptions That Can Break

- Team identity is verifiable (can be faked)
- On-chain data is complete (hidden wallets)
- Historical patterns predict future (market shifts)
- "Blue chip" status provides safety (all can fail)

Historical Failures

- Azuki creator's previous rug (reputation risk)
- Bored Ape governance attack (smart contract risk)
- Opensea insider trading (market manipulation)

Warning Signs

- Pressure tactics ("limited time", "last chance")
- Extraordinary return promises
- Defensive reaction to questions
- Locked/upgradeable contracts without justification

Risk Mitigation

- Never invest more than you can lose
- Diversify across projects and chains
- Set exit criteria before entry
- Re-evaluate regularly

Even thorough due diligence cannot prevent all losses — risk management is essential

Key Takeaways

- Always DYOR (Do Your Own Research)
- Team reputation is critical - anonymous = higher risk
- On-chain analysis reveals true holder behavior
- Multiple risk factors compound overall risk
- Most NFT projects fail - invest accordingly

Next Lesson: L29 – Token Economics

Quiz Questions (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Your Own Risks D) Deploy Your Own Records
Answer: B – Do Your Own Research is fundamental before investing in any NFT project.

Q2. Which is a major red flag for an NFT project team?
A) Active LinkedIn profiles B) Delivered roadmap milestones C) Anonymous team with no track record D) Verified partnerships
Answer: C – Anonymous teams with no verifiable history pose high rug pull risk.

Q3. What should you verify first when analyzing an NFT smart contract on Etherscan?
A) Gas price B) Contract address verification C) Transaction count D) Latest block number
Answer: B – Contract verification ensures code transparency and allows security review.

Q4. What indicates unhealthy holder distribution in an NFT collection?
A) Wide distribution across many wallets B) High whale concentration C) Organic trading patterns D) Diverse holder locations
Answer: B – High concentration in few wallets (whales) creates price manipulation risk.

Q5. Which risk score range indicates HIGH risk in the evaluation framework?
A) Less than 4 B) 4 to 7 C) Greater than 7 D) Exactly 5
Answer: C – Scores above 7 indicate high risk and warrant caution or avoidance.

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. What is a key indicator of fake partnerships in NFT projects?
A) Press releases on company websites B) Joint Twitter Spaces C) Unverified claims without proof D) Co-branded merchandise
Answer: C – Always verify partnerships through official channels of both parties.

Q7. Which on-chain metric helps identify wash trading?
A) Total supply B) Trading patterns between same wallets C) Contract creation date D) Token metadata
Answer: B – Repeated trades between related addresses indicate artificial volume.

Q8. What does liquidity risk refer to in NFT evaluation?
A) Water damage to physical art B) Ability to sell when needed C) Smart contract bugs D) Team reputation
Answer: B – Liquidity risk concerns whether you can exit your position when desired.

Q9. Which is NOT a primary risk category in the framework?
A) Liquidity Risk B) Smart Contract Risk C) Weather Risk D) Rug Pull Risk
Answer: C – Weather risk is not relevant to NFT evaluation (physical assets only).

Q10. What should be enforced in the NFT mint function?
A) Minimum price B) Maximum supply cap C) Transaction speed D) Gas limit
Answer: B – Max supply enforcement prevents unlimited minting that dilutes value.

Quiz Questions (11–15)

Q11. Which community metric is MOST important for project health?
A) Number of Discord members B) Quality of engagement and activity C) Twitter follower count D) Telegram group size
Answer: B – Genuine engagement matters more than vanity metrics (bots inflate numbers).

Q12. What is the recommended action for a project with unrealistic profit guarantees?
A) Invest immediately B) Wait and see C) Avoid - major red flag D) Invest small amount
Answer: C – Guaranteed profit promises are classic scam indicators.

Q13. Which valuation factor considers long-term project sustainability?
A) Current floor price B) Team track record and roadmap C) Short-term hype D) Celebrity endorsements
Answer: B – Proven teams with realistic roadmaps indicate sustainability potential.

Q14. What does a doxxed team mean?
A) Team uses pseudonyms B) Team identities are publicly known C) Team has no social media D) Team is anonymous
Answer: B – Doxxed means real identities are publicly disclosed and verifiable.

Q15. Which is a sign of organic vs artificial trading volume?
A) All trades same size B) Trades only during specific hours C) Diverse trade sizes and timing D) Only large trades
Answer: C – Natural trading shows variety in size, timing, and participants.

Quiz Questions (16–20)

Q16. What should you examine in the smart contract owner/admin functions?
A) Color scheme B) Centralized control and pause mechanisms C) File size D) Compilation date
Answer: B – Admin powers (pause, withdraw, modify) reveal centralization risks.

Q17. Which marketplace dependency creates platform risk?
A) Using multiple marketplaces B) Relying solely on one platform C) No marketplace presence D) Direct peer-to-peer only
Answer: B – Single platform dependency means exposure to that platform's risks.

Q18. What is the minimum content for a proper evaluation report?
A) One paragraph B) Social media screenshot C) 3 pages with research, analysis, risk assessment D) Just a recommendation
Answer: C – Comprehensive reports include overview, analysis, risk scores, and recommendation.

Q19. Which indicates a realistic roadmap?
A) Promise of 100x returns B) Achievable milestones with clear timeline C) Vague future plans D) No specific deliverables
Answer: B – Realistic roadmaps have specific, measurable, and time-bound goals.

Q20. What is the final recommendation format in the evaluation framework?
A) Maybe/Perhaps/Possibly B) Buy/Hold/Avoid C) Good/Bad D) Yes/No
Answer: B – Clear actionable recommendation: Buy (invest), Hold (monitor), or Avoid (pass).

(c) Joerg Osterrieder 2025

L28: Lab – NFT Project Evaluation

Mini-Lecture – Module C: NFTs & Digital Assets

Blockchain & Cryptocurrency Course

January 2026

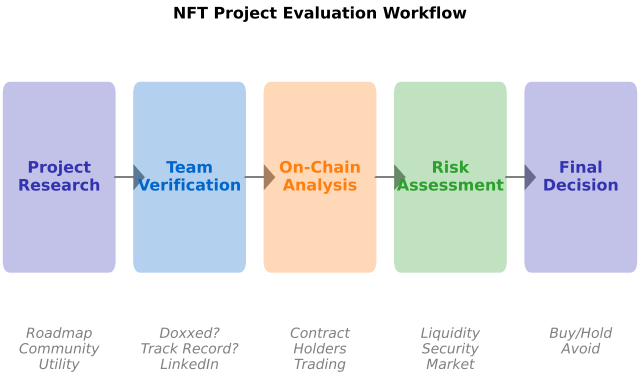
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Conduct due diligence on NFT projects
- Identify red flags and rug pull indicators
- Analyze on-chain metrics and holder behavior
- Create a comprehensive risk assessment

NFT Evaluation Workflow



DYOR (Do Your Own Research): Systematic evaluation before any investment.

Project Due Diligence Checklist

Team Research:

- Doxxed team (real identities public)?
- Track record in crypto/gaming/art?
- Verifiable LinkedIn profiles?

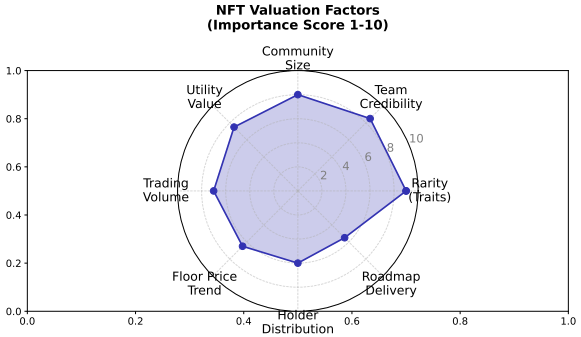
Red Flags:

- Anonymous team with no track record
- Unrealistic promises (guaranteed profits)
- Fake partnerships or celebrity endorsements
- Copied art or unoriginal concept

Roadmap: Realistic milestones? Previously delivered on promises?

(c) Joerg Osterrieder 2025

Valuation Factor Weights



Team reputation and utility are critical long-term value drivers.

On-Chain Analysis

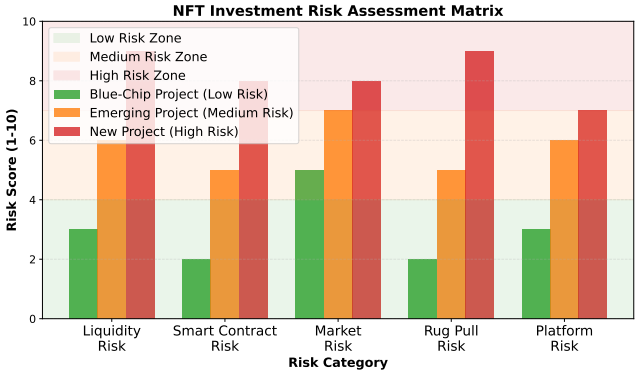
Contract Analysis (Etherscan):

1. Contract verified and source code visible?
2. Owner/admin functions (mint, pause, blacklist)?
3. Max supply enforced in mint function?
4. Transfer restrictions present?

Holder Distribution:

- Wide distribution = healthier
- High whale concentration = manipulation risk
- Same-wallet trading patterns = wash trading

Risk Assessment Matrix



Score each category 1-10: Low (¡4), Medium (4-7), High (¿7).

Risk Categories

Five Key Risk Types:

1. **Liquidity Risk:** Can you sell when needed?
2. **Smart Contract Risk:** Bugs, exploits, centralization
3. **Market Risk:** Volatility, bear markets
4. **Rug Pull Risk:** Team abandonment, exit scam
5. **Platform Risk:** Marketplace dependency

Risk Scoring:

- Rate each 1-10, calculate weighted average
- Low (¡4), Medium (4-7), High (¿7)

Identifying Wash Trading

Indicators of Wash Trading:

- High volume with few unique owners
- Repeated trades between same wallets
- All trades at similar sizes
- Concentrated trading during specific hours

Organic Trading Signs:

- Diverse trade sizes and timing
- Wide distribution of traders
- Natural price discovery patterns

Key Takeaways

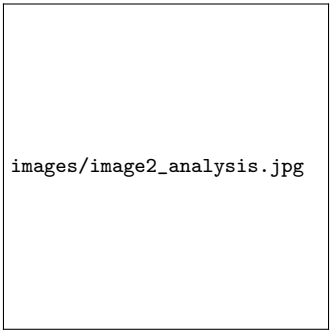
1. **DYOR:** Always research before investing – most NFT projects fail
2. **Team:** Anonymous = higher risk; doxxed with track record = safer
3. **On-Chain:** Verify contract, analyze holder distribution
4. **Red Flags:** Guaranteed profits, fake partnerships, copied art
5. **Risk Score:** Rate liquidity, contract, market, rug pull, platform risks

Final Action: Produce Buy/Hold/Avoid recommendation with evidence.

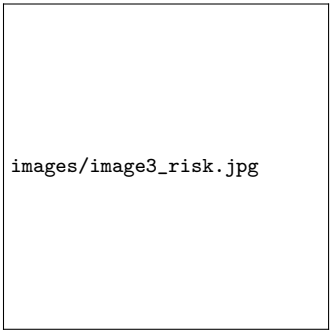
(c) Joerg Osterrieder 2025

NFT Evaluation in Practice

Project Research



On-Chain Analysis



Risk Assessment

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What does DYOR stand for?
A) Develop Your Own Revenue B) Do Your Own Research
C) Determine Your Own Risks D) Deploy Your Own Records

Quiz (1/2)

Q1. What does DYOR stand for?
A) Develop Your Own Revenue B) Do Your Own Research
C) Determine Your Own Risks D) Deploy Your Own Records
Answer: B – Fundamental before any NFT investment.

Q2. Which is a major red flag for an NFT project team?
A) Active LinkedIn B) Delivered milestones
C) Anonymous with no track record D) Verified partnerships

Quiz (1/2)

Q1. What does DYOR stand for?
A) Develop Your Own Revenue B) Do Your Own Research
C) Determine Your Own Risks D) Deploy Your Own Records
Answer: B – Fundamental before any NFT investment.

Q2. Which is a major red flag for an NFT project team?
A) Active LinkedIn B) Delivered milestones
C) Anonymous with no track record D) Verified partnerships
Answer: C – Anonymous teams pose high rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address verification
C) Transaction count D) Block number

Quiz (1/2)

Q1. What does DYOR stand for?
A) Develop Your Own Revenue B) Do Your Own Research
C) Determine Your Own Risks D) Deploy Your Own Records
Answer: B – Fundamental before any NFT investment.

Q2. Which is a major red flag for an NFT project team?
A) Active LinkedIn B) Delivered milestones
C) Anonymous with no track record D) Verified partnerships
Answer: C – Anonymous teams pose high rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address verification
C) Transaction count D) Block number
Answer: B – Contract verification ensures code transparency.

Q4. What indicates unhealthy holder distribution?
A) Wide distribution B) High whale concentration
C) Organic patterns D) Many unique owners

Quiz (1/2)

Q1. What does DYOR stand for?
A) Develop Your Own Revenue B) Do Your Own Research
C) Determine Your Own Risks D) Deploy Your Own Records
Answer: B – Fundamental before any NFT investment.

Q2. Which is a major red flag for an NFT project team?
A) Active LinkedIn B) Delivered milestones
C) Anonymous with no track record D) Verified partnerships
Answer: C – Anonymous teams pose high rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address verification
C) Transaction count D) Block number
Answer: B – Contract verification ensures code transparency.

Q4. What indicates unhealthy holder distribution?
A) Wide distribution B) High whale concentration
C) Organic patterns D) Many unique owners
Answer: B – High concentration creates manipulation risk.

Q5. Which risk score range indicates HIGH risk?
A) Less than 4 B) 4 to 7 C) Greater than 7 D) Exactly 5

Quiz (1/2)

Q1. What does DYOR stand for?
A) Develop Your Own Revenue B) Do Your Own Research
C) Determine Your Own Risks D) Deploy Your Own Records
Answer: B – Fundamental before any NFT investment.

Q2. Which is a major red flag for an NFT project team?
A) Active LinkedIn B) Delivered milestones
C) Anonymous with no track record D) Verified partnerships
Answer: C – Anonymous teams pose high rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address verification
C) Transaction count D) Block number
Answer: B – Contract verification ensures code transparency.

Q4. What indicates unhealthy holder distribution?
A) Wide distribution B) High whale concentration
C) Organic patterns D) Many unique owners
Answer: B – High concentration creates manipulation risk.

Q5. Which risk score range indicates HIGH risk?
A) Less than 4 B) 4 to 7 C) Greater than 7 D) Exactly 5
Answer: C – Above 7 warrants caution or avoidance.

Quiz (2/2)

Q6. What indicates wash trading?
A) Diverse trade sizes B) Trades between same wallets
C) Many unique buyers D) Random timing

Quiz (2/2)

Q6. What indicates wash trading?
A) Diverse trade sizes B) Trades between same wallets
C) Many unique buyers D) Random timing
Answer: B – Same-wallet trading creates artificial volume.

Q7. What does liquidity risk refer to?
A) Water damage B) Ability to sell when needed
C) Contract bugs D) Team reputation

Quiz (2/2)

Q6. What indicates wash trading?
A) Diverse trade sizes B) Trades between same wallets
C) Many unique buyers D) Random timing
Answer: B – Same-wallet trading creates artificial volume.

Q7. What does liquidity risk refer to?
A) Water damage B) Ability to sell when needed
C) Contract bugs D) Team reputation
Answer: B – Whether you can exit your position.

Q8. What should be enforced in the mint function?
A) Minimum price B) Maximum supply cap
C) Transaction speed D) Gas limit

Quiz (2/2)

Q6. What indicates wash trading?
A) Diverse trade sizes B) Trades between same wallets
C) Many unique buyers D) Random timing
Answer: B – Same-wallet trading creates artificial volume.

Q7. What does liquidity risk refer to?
A) Water damage B) Ability to sell when needed
C) Contract bugs D) Team reputation
Answer: B – Whether you can exit your position.

Q8. What should be enforced in the mint function?
A) Minimum price B) Maximum supply cap
C) Transaction speed D) Gas limit
Answer: B – Max supply prevents value dilution.

Q9. What does doxxed team mean?
A) Uses pseudonyms B) Real identities publicly known
C) No social media D) Anonymous

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. What indicates wash trading?
A) Diverse trade sizes B) Trades between same wallets
C) Many unique buyers D) Random timing
Answer: B – Same-wallet trading creates artificial volume.

Q7. What does liquidity risk refer to?
A) Water damage B) Ability to sell when needed
C) Contract bugs D) Team reputation
Answer: B – Whether you can exit your position.

Q8. What should be enforced in the mint function?
A) Minimum price B) Maximum supply cap
C) Transaction speed D) Gas limit
Answer: B – Max supply prevents value dilution.

Q9. What does doxxed team mean?
A) Uses pseudonyms B) Real identities publicly known
C) No social media D) Anonymous
Answer: B – Identities disclosed and verifiable.

Q10. What is the final recommendation format?
A) Maybe/Perhaps B) Buy/Hold/Avoid
C) Good/Bad D) Yes/No

Quiz (2/2)

Q6. What indicates wash trading?
A) Diverse trade sizes B) Trades between same wallets
C) Many unique buyers D) Random timing
Answer: B – Same-wallet trading creates artificial volume.

Q7. What does liquidity risk refer to?
A) Water damage B) Ability to sell when needed
C) Contract bugs D) Team reputation
Answer: B – Whether you can exit your position.

Q8. What should be enforced in the mint function?
A) Minimum price B) Maximum supply cap
C) Transaction speed D) Gas limit
Answer: B – Max supply prevents value dilution.

Q9. What does doxxed team mean?
A) Uses pseudonyms B) Real identities publicly known
C) No social media D) Anonymous
Answer: B – Identities disclosed and verifiable.

Q10. What is the final recommendation format?
A) Maybe/Perhaps B) Buy/Hold/Avoid
C) Good/Bad D) Yes/No
Answer: B – Clear actionable recommendation.

Thank you

Questions?

Next: L29 – Tokenomics Fundamentals

Quiz: Lab NFT Evaluation

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Risks D) Deploy Records

Quiz (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Risks D) Deploy Records
Answer: B – Fundamental principle before any NFT investment.

Q2. Which is the biggest red flag for an NFT project?
A) Active LinkedIn B) Delivered milestones C) Anonymous team, no track record D) Verified partners

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Risks D) Deploy Records
Answer: B – Fundamental principle before any NFT investment.

Q2. Which is the biggest red flag for an NFT project?
A) Active LinkedIn B) Delivered milestones C) Anonymous team, no track record D) Verified partners
Answer: C – Anonymous teams have highest rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address and source verification C) Transaction count D) Block number

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Risks D) Deploy Records
Answer: B – Fundamental principle before any NFT investment.

Q2. Which is the biggest red flag for an NFT project?
A) Active LinkedIn B) Delivered milestones C) Anonymous team, no track record D) Verified partners
Answer: C – Anonymous teams have highest rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address and source verification C) Transaction count D) Block number
Answer: B – Verified source enables security review.

Q4. What indicates unhealthy holder distribution?
A) Wide distribution B) High whale concentration C) Organic trading D) Many holders

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Risks D) Deploy Records
Answer: B – Fundamental principle before any NFT investment.

Q2. Which is the biggest red flag for an NFT project?
A) Active LinkedIn B) Delivered milestones C) Anonymous team, no track record D) Verified partners
Answer: C – Anonymous teams have highest rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address and source verification C) Transaction count D) Block number
Answer: B – Verified source enables security review.

Q4. What indicates unhealthy holder distribution?
A) Wide distribution B) High whale concentration C) Organic trading D) Many holders
Answer: B – Few wallets holding most supply = manipulation risk.

Q5. Which risk score range indicates HIGH risk?
A) Less than 4 B) 4 to 7 C) Greater than 7 D) Exactly 5

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What does DYOR stand for in NFT evaluation?
A) Develop Your Own Revenue B) Do Your Own Research C) Determine Risks D) Deploy Records
Answer: B – Fundamental principle before any NFT investment.

Q2. Which is the biggest red flag for an NFT project?
A) Active LinkedIn B) Delivered milestones C) Anonymous team, no track record D) Verified partners
Answer: C – Anonymous teams have highest rug pull risk.

Q3. What should you verify first on Etherscan?
A) Gas price B) Contract address and source verification C) Transaction count D) Block number
Answer: B – Verified source enables security review.

Q4. What indicates unhealthy holder distribution?
A) Wide distribution B) High whale concentration C) Organic trading D) Many holders
Answer: B – Few wallets holding most supply = manipulation risk.

Q5. Which risk score range indicates HIGH risk?
A) Less than 4 B) 4 to 7 C) Greater than 7 D) Exactly 5
Answer: C – Scores above 7 warrant caution or avoidance.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which indicates wash trading?
A) Diverse sizes B) Same wallets trading repeatedly C) Varied timing D) Many participants

Quiz (6–10)

Q6. Which indicates wash trading?
A) Diverse sizes B) Same wallets trading repeatedly C) Varied timing D) Many participants
Answer: B – Repeated trades between related addresses = artificial volume.

Q7. What is liquidity risk in NFT evaluation?
A) Water damage B) Ability to sell when needed C) Smart contract bugs D) Team reputation

Quiz (6–10)

Q6. Which indicates wash trading?
A) Diverse sizes B) Same wallets trading repeatedly C) Varied timing D) Many participants
Answer: B – Repeated trades between related addresses = artificial volume.

Q7. What is liquidity risk in NFT evaluation?
A) Water damage B) Ability to sell when needed C) Smart contract bugs D) Team reputation
Answer: B – Can you exit your position when desired?

Q8. What should the mint function enforce?
A) Minimum price B) Maximum supply cap C) Transaction speed D) Gas limit

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which indicates wash trading?
A) Diverse sizes B) Same wallets trading repeatedly C) Varied timing D) Many participants
Answer: B – Repeated trades between related addresses = artificial volume.

Q7. What is liquidity risk in NFT evaluation?
A) Water damage B) Ability to sell when needed C) Smart contract bugs D) Team reputation
Answer: B – Can you exit your position when desired?

Q8. What should the mint function enforce?
A) Minimum price B) Maximum supply cap C) Transaction speed D) Gas limit
Answer: B – Max supply enforcement prevents dilution.

Q9. What does a doxxed team mean?
A) Uses pseudonyms B) Identities publicly known and verified C) No social media D) Anonymous

Quiz (6–10)

Q6. Which indicates wash trading?
A) Diverse sizes B) Same wallets trading repeatedly C) Varied timing D) Many participants
Answer: B – Repeated trades between related addresses = artificial volume.

Q7. What is liquidity risk in NFT evaluation?
A) Water damage B) Ability to sell when needed C) Smart contract bugs D) Team reputation
Answer: B – Can you exit your position when desired?

Q8. What should the mint function enforce?
A) Minimum price B) Maximum supply cap C) Transaction speed D) Gas limit
Answer: B – Max supply enforcement prevents dilution.

Q9. What does a doxxed team mean?
A) Uses pseudonyms B) Identities publicly known and verified C) No social media D) Anonymous
Answer: B – Real identities disclosed and verifiable.

Q10. What is the final recommendation format?
A) Maybe/Perhaps B) Buy/Hold/Avoid C) Good/Bad D) Yes/No

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Which indicates wash trading?
A) Diverse sizes B) Same wallets trading repeatedly C) Varied timing D) Many participants
Answer: B – Repeated trades between related addresses = artificial volume.

Q7. What is liquidity risk in NFT evaluation?
A) Water damage B) Ability to sell when needed C) Smart contract bugs D) Team reputation
Answer: B – Can you exit your position when desired?

Q8. What should the mint function enforce?
A) Minimum price B) Maximum supply cap C) Transaction speed D) Gas limit
Answer: B – Max supply enforcement prevents dilution.

Q9. What does a doxxed team mean?
A) Uses pseudonyms B) Identities publicly known and verified C) No social media D) Anonymous
Answer: B – Real identities disclosed and verifiable.

Q10. What is the final recommendation format?
A) Maybe/Perhaps B) Buy/Hold/Avoid C) Good/Bad D) Yes/No
Answer: B – Clear actionable recommendations for investment decisions.

(c) Joerg Osterrieder 2025

L29: Token Economics Fundamentals

Mini-Lecture — Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand different token types and their purposes
- Analyze value accrual mechanisms in token economies
- Evaluate token supply models and their implications

Why Tokenomics Matters:
Tokenomics determines the long-term sustainability and success of crypto projects.

What is Tokenomics?

Definition: The study of the economic systems governing the creation, distribution, and management of tokens in blockchain ecosystems.

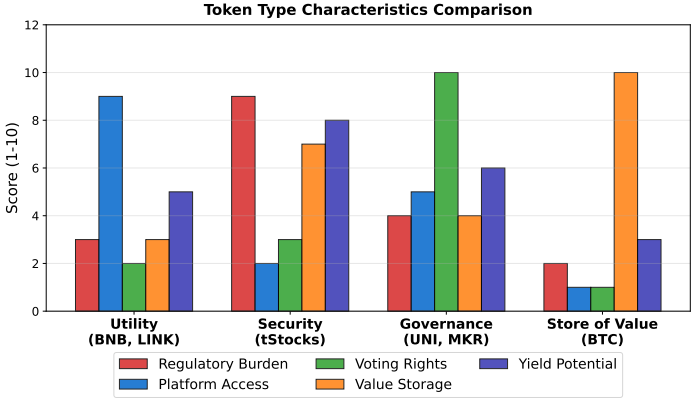
Key Components:

- Token design and purpose
- Supply and distribution mechanics
- Incentive structures and value capture

Think of tokenomics as the "monetary policy" for a crypto project.

(c) Joerg Osterrieder 2025

Token Types Overview



Security tokens have highest regulatory burden; governance tokens offer strongest voting rights.

Value Accrual Mechanisms

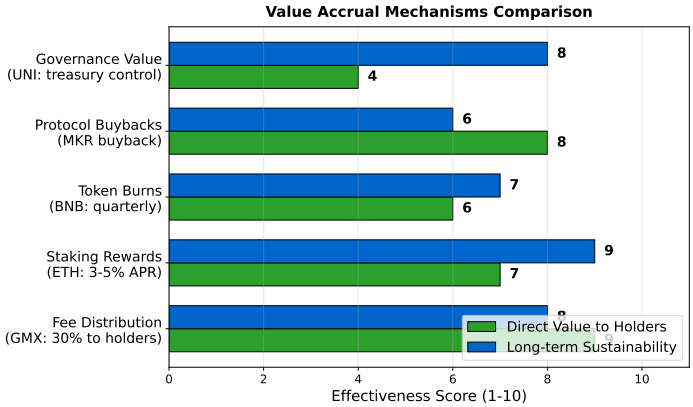
How do tokens capture value from protocol success?

1. **Fee Distribution** – Protocol fees shared with holders (e.g., GMX: 30%)
2. **Staking Rewards** – Lock tokens to earn yield (e.g., ETH validators)
3. **Token Burns** – Reduce circulating supply (e.g., BNB, ETH EIP-1559)

Strong value accrual connects token price to actual protocol success.

(c) Joerg Osterrieder 2025

Value Accrual Comparison



Fee distribution provides direct value; staking rewards offer best sustainability.

Supply Models: Fixed vs. Inflationary

Fixed Supply (Bitcoin Model):

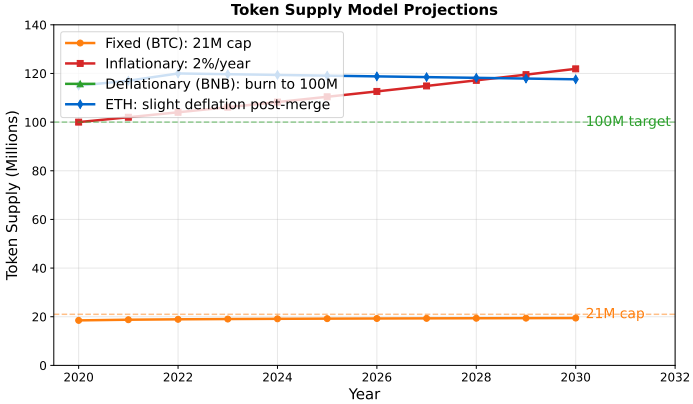
- Maximum 21 million BTC – no new tokens after cap
- Halving every 4 years creates scarcity

Inflationary/Deflationary:

- BNB: Burns toward 100M target (from 200M initial)
- ETH: Slightly deflationary post-Merge (0.5% issuance)

Supply model determines long-term price dynamics and holder incentives.

Supply Model Projections



BTC approaches 21M cap; BNB burns toward 100M; ETH slightly deflationary.

Token Velocity Problem

Problem: High token velocity (frequent buying/selling) suppresses price.

Equation of Exchange: $MV = PQ$

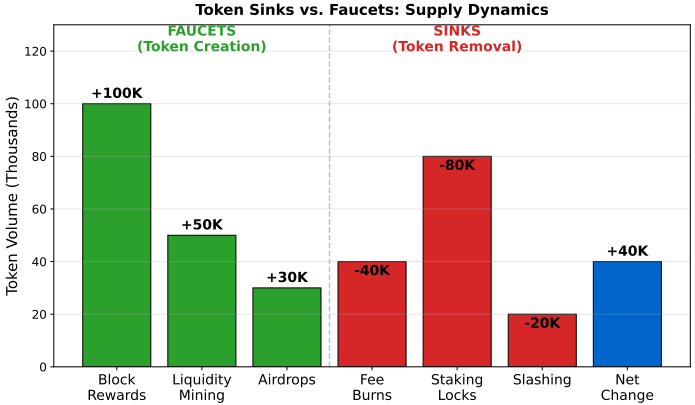
- M = Token supply, V = Velocity, P = Price, Q = Quantity
- High V means lower P for same economic activity

Solutions:

- Staking mechanisms (reduce velocity)
- Governance rights that require holding

(c) Joerg Osterrieder 2025

Token Sinks vs. Faucets



Healthy tokenomics balances faucets (creation) with sinks (removal).

Good vs. Bad Tokenomics

Good Tokenomics:

- Clear value accrual
- Long vesting periods
- Low team allocation (¡20%)

Red Flags:

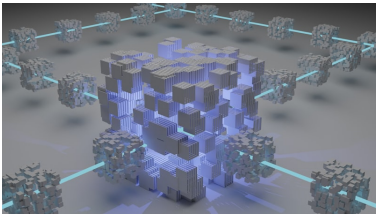
- No clear value capture
- Short/no vesting
- ¿30% insider allocation

Key Metrics: Circulating vs. total supply, inflation rate, unlock schedule.

(c) Joerg Osterrieder 2025

Token Economics in Practice

Economic Design
Token incentives shape behavior



Digital Assets
Tokens represent value

Supply Dynamics
Scarcity drives value

Images: Unsplash (CC0). Tokenomics combines economics, game theory, and cryptography.

Quiz Questions (1–5)

Q1. What best defines tokenomics?
A) Crypto price B) Economic systems governing tokens C) Mining difficulty D) Exchange volume
Answer: B

Q2. Primary characteristic of utility tokens?
A) Ownership B) Platform access C) Voting only D) Digital gold
Answer: B

Q3. Bitcoin's maximum supply?
A) 18.5M B) 21M C) 100M D) Unlimited
Answer: B

Q4. What does EIP-1559 do?
A) Increase blocks B) Burn base fees C) Eliminate fees D) Double rewards
Answer: B

Q5. High token velocity (V) typically:
A) Increases price B) Suppresses price C) No effect D) Doubles supply
Answer: B

Quiz Questions (6–10)

Q6. BNB's target supply after burns?
A) 50M B) 100M C) 144M D) 200M
Answer: B

Q7. Which is a "token sink"?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops
Answer: C

Q8. ETH issuance after The Merge?
A) +90% B) Same C) -90% D) Stopped
Answer: C

Q9. Major tokenomics red flag?
A) Long vesting B) Transparency C) ¿30% team allocation D) Fee sharing
Answer: C

Q10. Large gap between circulating and total supply indicates:
A) Strong tokenomics B) Dilution risk C) Deflation D) High demand
Answer: B

(c) Joerg Osterrieder 2025

L29: Token Economics Fundamentals

Mini-Lecture Version

Blockchain & Cryptocurrency

Module D: Tokenomics

December 2025

Learning Objectives: Understand token types — Analyze value accrual mechanisms — Evaluate supply models — Apply tokenomics principles

What is Tokenomics?

Formal Definition

The study of economic systems governing the creation, distribution, and management of tokens in blockchain ecosystems.

Key Components:

- Token design and purpose (e.g., utility, governance, security)
- Supply mechanics (fixed: BTC 21M, inflationary: ETH pre-merge)
- Value accrual mechanisms (fees, burns, staking)

(c) Joerg Osterrieder 2025

Token Types Overview

Utility Tokens

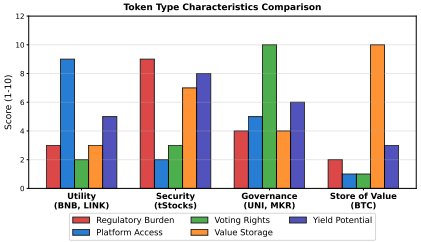
Access platform services
Payment for fees

Examples: BNB, LINK, FIL

Governance Tokens

Voting on protocol changes
DAO participation

Examples: UNI, AAVE, MKR



Security Tokens

Ownership/dividends
SEC-regulated

Examples: tokenized stocks

Store of Value

Digital gold analogy
Limited supply

Example: BTC

Security tokens have highest regulatory burden; governance tokens offer strongest voting rights

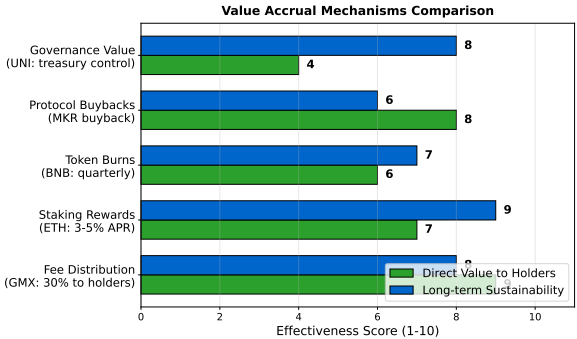
Value Accrual Mechanisms

How do tokens capture protocol value?

- **Fee Distribution** (GMX: 30% to holders)
- **Staking Rewards** (ETH: 3-5% APR)
- **Token Burns** (BNB quarterly, ETH EIP-1559)

Impact on Token Value:

- Fee sharing: direct income
- Burns: reduce supply, increase scarcity
- Staking: reduce velocity



Fee distribution provides direct value; staking rewards offer best sustainability

Supply Models: Fixed vs. Inflationary vs. Deflationary

Fixed Supply:

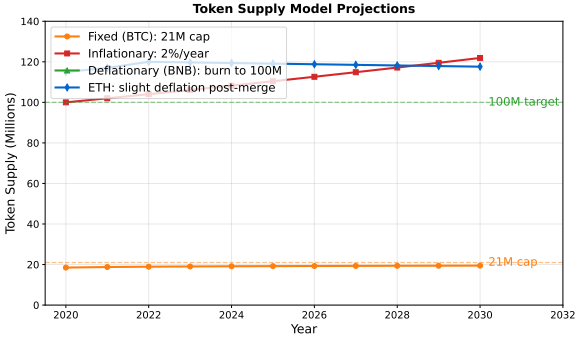
- BTC: 21M cap, 19.5M circulating
- Halving every 210K blocks
- Final coin: year 2140

Inflationary:

- New tokens continuously created
- Incentivizes participation

Deflationary:

- BNB: 200M initial, target 100M
- ETH: net deflationary post-merge



BTC approaches 21M cap; BNB burns toward 100M; ETH slightly deflationary post-merge

Token Velocity and Supply Dynamics

Token Velocity Problem
High velocity suppresses price: $MV = PQ$

Token Sinks (Removal):

- Transaction fee burns
- Staking locks
- Governance participation

Token Faucets (Creation):

- Block rewards
- Liquidity mining
- Airdrops, grants

Solutions to High Velocity:

- Staking with lock-ups
- Vesting periods
- Utility requiring holding

Healthy tokenomics balances faucets (creation) with sinks (removal)

(c) Joerg Osterrieder 2025

Case Study: ETH Tokenomics Evolution

Pre-EIP-1559 (Before Aug 2021):

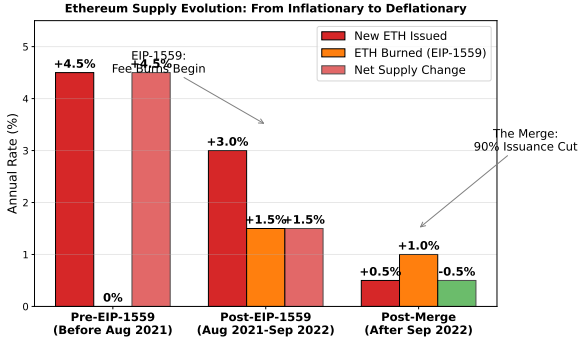
- 4.5% annual issuance
- All fees to miners

Post-EIP-1559:

- Base fee burned
- Priority tips to miners

Post-Merge (Sept 2022):

- Issuance cut 90%
- Net deflationary during high activity
- Staking yields: 3-5% APR



EIP-1559 introduced burns; The Merge cut issuance 90%, achieving net deflation

Key Takeaways

1. Token type determines purpose and regulatory treatment (utility vs. security)
2. Value accrual mechanisms connect token price to protocol success (GMX 30% fees)
3. Supply models have trade-offs: fixed (BTC), inflationary, or deflationary (ETH)
4. Token velocity must be managed via staking locks and vesting periods

Bottom Line: Good tokenomics aligns incentives across all stakeholders with transparent distribution, sustainable emission, and real utility beyond speculation.

(c) Joerg Osterrieder 2025

Concrete Examples: Making It Real

Supply Metrics (Dec 2025)

- BTC: 19.5M / 21M circulating
- ETH: 120M supply, net deflationary
- BNB: 144M / 100M target

Value Accrual Examples

- GMX: 30% trading fees distributed
- ETH staking: 3-5% APR
- EIP-1559: ¿4M ETH burned since launch

Token Governance

- UNI: 1 token = 1 vote
- MKR: governs $8B DAI system
- AAVE: protocol parameter votes

Red Flags to Avoid

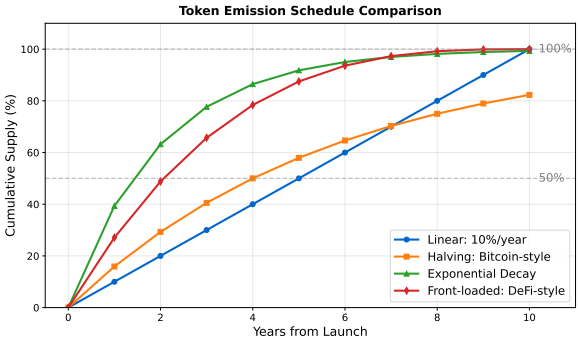
- Team allocation ¿30%
- Short/no vesting periods
- Unsustainable yields (¿100% APY)
- No clear value accrual

All data verified Dec 2025 — Sources: CoinGecko, DefiLlama, ultrasound.money

(c) Joerg Osterrieder 2025

Emission Schedule Models

1. **Linear Emission**
   - Constant rate of new tokens
   - Predictable but perpetual inflation
2. **Halving (Bitcoin model)**
   - Every 210K blocks (4 years)
   - Gradually reducing inflation
3. **Algorithmic Adjustment**
   - Based on network metrics
   - Ethereum's variable issuance



DeFi protocols often use front-loaded emission; Bitcoin uses halving model

Quiz Questions (1–5)

Q1. Which best defines tokenomics?
A) Cryptocurrency price B) Economic systems governing token creation/management
C) Mining algorithms D) Exchange trading volumes

Quiz Questions (1–5)

Q1. Which best defines tokenomics?
A) Cryptocurrency price B) Economic systems governing token creation/management
C) Mining algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents company ownership B) Grants access to platform services
C) Voting rights only D) Functions as digital gold

Quiz Questions (1–5)

Q1. Which best defines tokenomics?
A) Cryptocurrency price B) Economic systems governing token creation/management
C) Mining algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents company ownership B) Grants access to platform services
C) Voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited

Quiz Questions (1–5)

Q1. Which best defines tokenomics?
A) Cryptocurrency price B) Economic systems governing token creation/management
C) Mining algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents company ownership B) Grants access to platform services
C) Voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q4. What is EIP-1559's main tokenomics effect?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate fees D) Double staking rewards

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. Which best defines tokenomics?
A) Cryptocurrency price B) Economic systems governing token creation/management
C) Mining algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents company ownership B) Grants access to platform services
C) Voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q4. What is EIP-1559's main tokenomics effect?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q5. Which is a "token sink" that removes tokens from circulation?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. Which best defines tokenomics?
A) Cryptocurrency price B) Economic systems governing token creation/management
C) Mining algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents company ownership B) Grants access to platform services
C) Voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q4. What is EIP-1559's main tokenomics effect?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q5. Which is a "token sink" that removes tokens from circulation?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops
Answer: C – Staking locks reduce circulating supply.

Quiz Questions (6–10)

Q6. Which token provides governance functionality?
A) BTC B) USDT C) UNI D) WBTC

Quiz Questions (6–10)

Q6. Which token provides governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Q7. In MV = PQ, high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect D) Doubles money supply

Quiz Questions (6–10)

Q6. Which token provides governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Q7. In MV = PQ, high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect D) Doubles money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q8. What is BNB's target supply after all burns?
A) 50 million B) 100 million C) 144 million D) 200 million

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. Which token provides governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Q7. In MV = PQ, high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect D) Doubles money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q8. What is BNB's target supply after all burns?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q9. What happened to ETH issuance after The Merge (Sept 2022)?
A) Increased 90% B) Stayed same C) Reduced 90% D) Stopped completely

(c) Joerg Osterrieder 2025

Quiz Questions (6–10)

Q6. Which token provides governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Q7. In MV = PQ, high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect D) Doubles money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q8. What is BNB's target supply after all burns?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q9. What happened to ETH issuance after The Merge (Sept 2022)?
A) Increased 90% B) Stayed same C) Reduced 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q10. What is a major tokenomics red flag?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation ¿30% D) Fee sharing mechanism

Quiz Questions (6–10)

Q6. Which token provides governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Q7. In MV = PQ, high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect D) Doubles money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q8. What is BNB's target supply after all burns?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q9. What happened to ETH issuance after The Merge (Sept 2022)?
A) Increased 90% B) Stayed same C) Reduced 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q10. What is a major tokenomics red flag?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation ¿30% D) Fee sharing mechanism
Answer: C – Excessive insider allocation risks dumping and misaligned incentives.

L29: Token Economics Fundamentals

Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Describe different token types (utility, governance, security) and their purposes
- Analyze value accrual mechanisms in token economies
- Evaluate token supply models and their implications
- Apply tokenomics principles to real-world projects

The Problem: How do we create sustainable token economies?

The Challenge
Designing a token that aligns incentives across users, developers, investors, and validators without collapsing into a speculative bubble or death spiral. Most token economies fail because they prioritize short-term hype over long-term sustainability.

Why It Matters

- Over 95% of ICO-era tokens failed due to poor economic design
- Terra/Luna collapsed ($40B) from flawed algorithmic stablecoin tokenomics
- Inflationary token spirals destroy user trust and protocol viability

What We Need

- Economic alignment of actors
- Sound monetary policy (supply schedules, emission rates)
- Real utility beyond speculation (value capture mechanisms)

The Cryptoeconomics Question
How do we design incentives so participants act in the protocol's best interest while pursuing their own gains?

Today's lesson: How Token Economics addresses this challenge

What is Tokenomics?

Definition: The study of the economic systems governing the creation, distribution, and management of tokens in blockchain ecosystems.

Key Components:

- Token design and purpose
- Supply and distribution mechanics
- Incentive structures
- Value capture mechanisms
- Governance and utility

Why It Matters: Tokenomics determines the long-term sustainability and success of crypto projects.

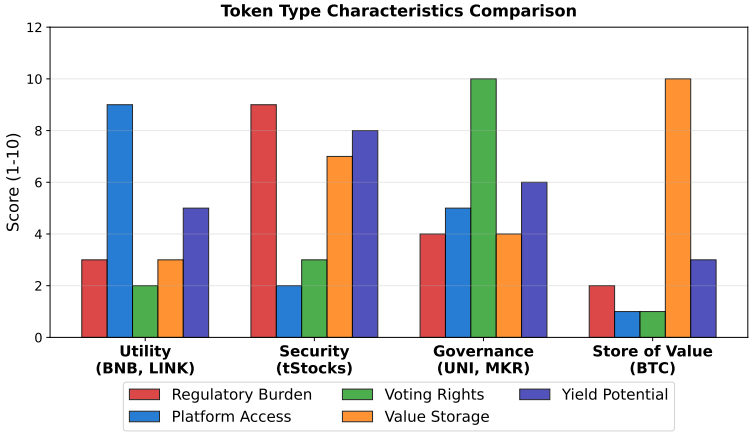
(c) Joerg Osterrieder 2025

Token Types: Overview

1. **Utility Tokens**
   - Access to platform services
   - Payment for network fees
   - Examples: BNB, LINK, FIL
2. **Security Tokens**
   - Represent ownership/dividends
   - Subject to securities laws
   - Examples: tokenized stocks, bonds
3. **Governance Tokens**
   - Voting rights on protocol changes
   - DAO participation
   - Examples: UNI, AAVE, MKR
4. **Store of Value Tokens**
   - Digital gold analogy
   - Limited supply
   - Example: BTC

(c) Joerg Osterrieder 2025

Token Types Characteristics



Security tokens have highest regulatory burden; governance tokens offer strongest voting rights

Utility Tokens: Deep Dive

Purpose: Access to products/services
Characteristics:

- Not designed as investments
- Required for platform interaction
- Value linked to usage
- May offer fee discounts

Example: Binance Coin (BNB)

- Trading fee discounts on exchange
- Gas fees on BNB Chain
- Token sale participation (Launchpad)
- Quarterly burns based on volume

Security Tokens

Definition: Investment contracts subject to securities regulations

Howey Test Criteria:

1. Investment of money
2. In a common enterprise
3. Expectation of profits
4. From efforts of others

Implications:

- Must comply with SEC (US)
- Require registration/exemption
- Investor protections apply
- Often limited to accredited investors

Examples: Tokenized stocks, bonds, real estate

Governance Tokens

Purpose: Decentralized decision-making
Voting Rights:

- Protocol parameter changes
- Treasury allocation
- Fee structure modifications
- Smart contract upgrades

Example: Uniswap (UNI)

- Protocol fee governance
- Treasury management ($B+ assets)
- Grant program decisions
- 1 UNI = 1 vote (delegatable)

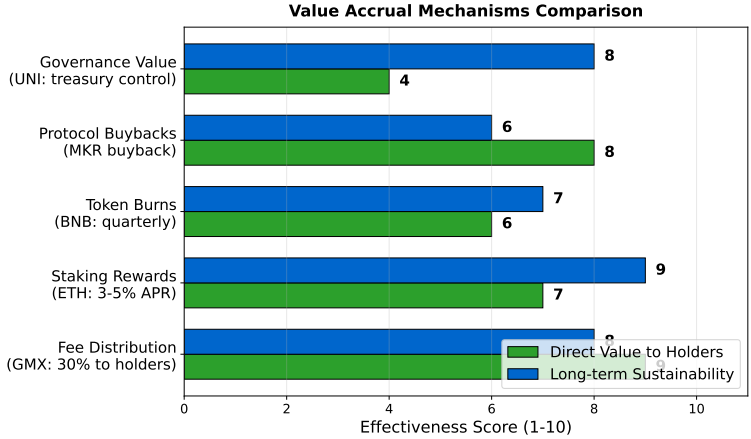
(c) Joerg Osterrieder 2025

Value Accrual Mechanisms

How do tokens capture value from protocol success?

1. **Fee Distribution**
   - Protocol fees shared with token holders
   - Example: GMX distributes 30% of trading fees
2. **Staking Rewards**
   - Lock tokens to earn yield
   - Example: Ethereum validators earn ETH rewards
3. **Token Burns**
   - Reduce circulating supply
   - Example: BNB quarterly burns, ETH EIP-1559

Value Accrual Mechanisms Comparison



Fee distribution provides direct value; staking rewards offer best sustainability

Supply Models: Fixed Supply

Characteristics:

- Predetermined max supply
- No new tokens after cap
- Deflationary if burned

Advantages:

- Scarcity drives value
- Predictable monetary policy
- Inflation protection

Bitcoin Example:

- Max: 21 million BTC
- Current: 19.5M (2024)
- Halving every 4 years
- Final BTC: year 2140

Supply Models: Inflationary vs. Deflationary

Inflationary:

- New tokens continuously created
- Rate may be fixed or decreasing
- Incentivizes participation

Deflationary:

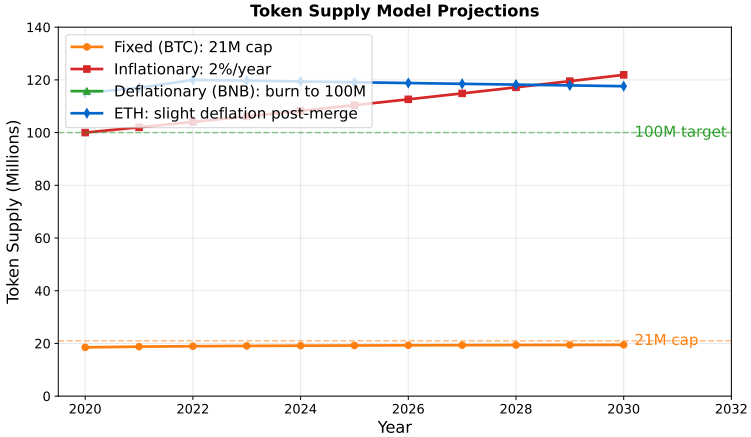
- Supply decreases over time
- Tokens removed via burns
- Creates scarcity pressure

BNB Burn Mechanism:

- Auto-Burn: based on gas fees
- Target: 100M (from 200M)
- Current: 144M (Dec 2024)

(c) Joerg Osterrieder 2025

Supply Model Projections



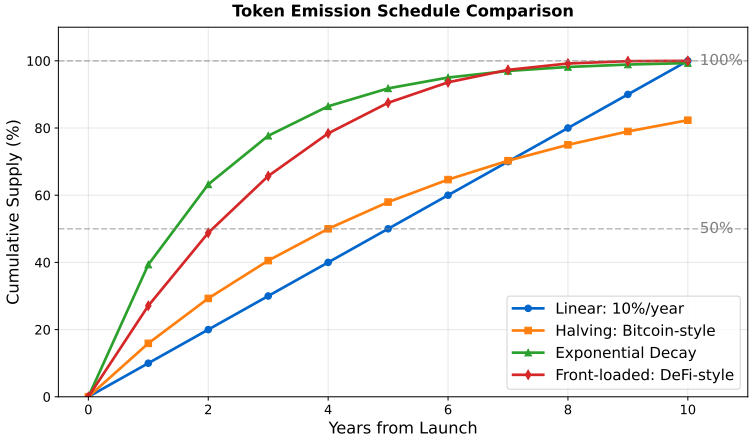
BTC approaches 21M cap; BNB burns toward 100M; ETH slightly deflationary post-merge

Emission Schedules

How tokens enter circulation over time:

1. **Linear Emission**
   - Constant rate of new tokens
   - Predictable but perpetual inflation
2. **Decreasing Emission**
   - Halving events (Bitcoin model)
   - Gradually reducing inflation
3. **Exponential Decay**
   - Rapid initial distribution
   - Asymptotically approaches max supply
4. **Algorithmic Adjustment**
   - Based on network metrics
   - Example: Ethereum's variable issuance

Emission Schedule Comparison



DeFi protocols often use front-loaded emission; Bitcoin uses halving model

Token Velocity Problem

Problem: High token velocity (frequent buying/selling) can suppress token price.

Equation of Exchange:

$$MV = PQ$$

where:

- M = Money supply (token supply)
- V = Velocity (transaction frequency)
- P = Price level
- Q = Quantity of goods/services

Solutions:

- Staking mechanisms (reduce velocity)
- Vesting periods
- Utility that requires holding (governance, fee discounts)

Token Sinks vs. Faucets

Token Sinks (Removal)

- Transaction fee burns
- Protocol penalties (slashing)
- Staking locks
- Governance participation locks

Effect: Reduce circulating supply, increase scarcity.

Token Faucets (Creation)

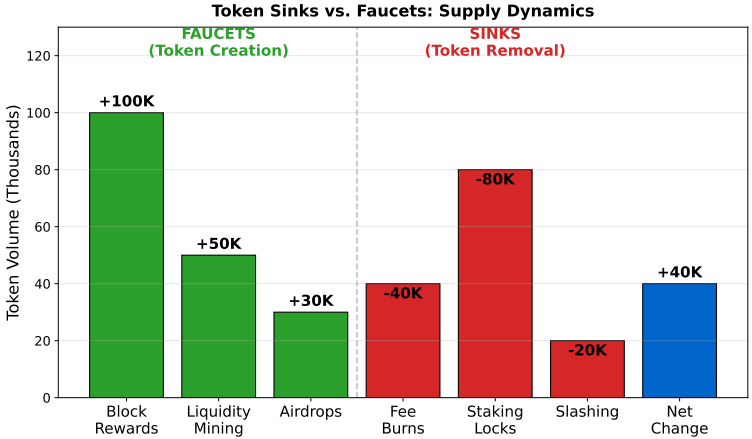
- Block rewards
- Liquidity mining rewards
- Airdrops
- Developer grants

Effect: Increase supply, incentivize participation.

Balance: Healthy tokenomics requires equilibrium between sinks and faucets.

(c) Joerg Osterrieder 2025

Token Supply Dynamics



Healthy tokenomics balances faucets (creation) with sinks (removal)

Case Study: ETH Tokenomics Evolution

Pre-EIP-1559:
(Before Aug 2021)

- 4.5% inflation
- All fees to miners
- Unpredictable fees

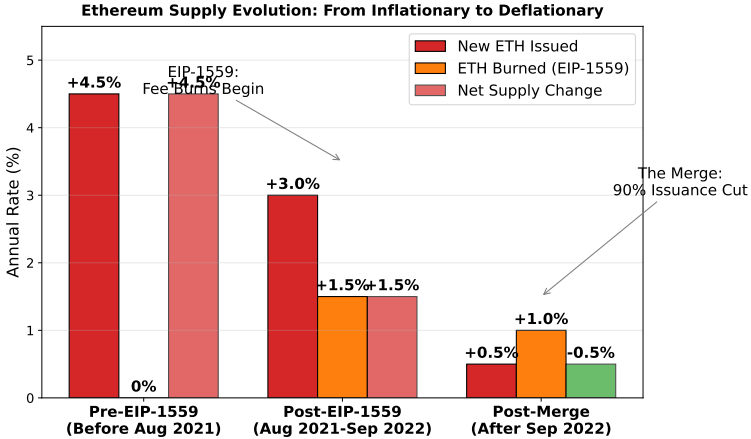
Post-EIP-1559:

- Base fee burned
- Tips to miners
- Predictable fees

Post-Merge:
(Sept 2022)

- Issuance -90%
- Net deflationary
- 3-5% staking APR

ETH Supply Evolution



EIP-1559 introduced burns; The Merge cut issuance 90%, achieving net deflation

Good vs. Bad Tokenomics

Good Tokenomics

- Clear value accrual
- Sustainable incentives
- Low initial team/VC allocation
- Long vesting periods
- Transparent distribution
- Real utility beyond speculation

Bad Tokenomics

- No clear value capture
- Ponzi-like dynamics
- High team/insider allocation
- Short/no vesting
- Opaque distribution
- Pure speculation

Red Flags:

- Excessive token supply to insiders (¿30%)
- Unsustainable yield promises (¿100% APY)

Key Metrics to Evaluate

1. **Circulating vs Total Supply**
   Large gap = future dilution
2. **Token Distribution**
   Top holder concentration, team %
3. **Inflation Rate**
   Current and projected annual
4. **Value Accrual**
   Fee sharing, burns, staking
5. **Unlock Schedule**
   When do vested tokens circulate?

Key: Evaluate all metrics together for complete picture

(c) Joerg Osterrieder 2025

Problem Solved? Token Economics

The Original Problem

How do we create sustainable token economies that don't collapse?

How Token Economics Solves It

- **Supply schedules**: Fixed (BTC), inflationary (ETH pre-merge), or deflationary (BNB burns) – predictable monetary policy
- **Value accrual**: Fee distribution, staking rewards, token burns create organic demand
- **Velocity control**: Staking locks and governance utility reduce sell pressure

Remaining Limitations

- **Speculation dominates utility**: Even well-designed tokens suffer from price volatility unrelated to fundamentals
- **Behavioral unpredictability**: Token velocity, holder psychology, and market cycles are hard to model

Open Questions

- What makes a token economy sustainable long-term? (No token has survived multiple market cycles with stable demand)
- Risk: Incentive misalignment if team allocations are excessive or vesting too short

Token Economics provides frameworks but no guarantees – success depends on execution and market conditions

Summary

Key Takeaways:

- Token type determines purpose and regulatory treatment
- Value accrual mechanisms connect token price to protocol success
- Supply models (fixed, inflationary, deflationary) have trade-offs
- Good tokenomics aligns incentives across all stakeholders
- Token velocity must be managed to maintain value
- Transparent distribution and vesting are crucial

Next Lecture: Distribution and Vesting - How tokens are allocated and released over time.

Questions for Reflection

1. How does Bitcoin's fixed supply model compare to Ethereum's flexible issuance?
2. What are the trade-offs between utility tokens and governance tokens?
3. How can a protocol reduce token velocity without harming liquidity?
4. Why might high team/VC allocations be problematic?
5. What role do token burns play in value accrual?

Quiz Questions (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. According to the Howey Test, which criterion does NOT determine if a token is a security?
A) Investment of money B) Common enterprise
C) Token name includes "coin" D) Expectation of profits from others' efforts
Answer: C – The Howey Test has 4 criteria; token naming is not one of them.

Q4. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q5. Which token provides an example of governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Quiz Questions (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops
Answer: B – Fee distribution shares protocol fees with token holders (e.g., GMX).

Q8. In the equation of exchange ($MV = PQ$), high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect on price D) Doubles the money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q9. What is BNB's target supply after all burns are complete?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q10. Which of these is a "token sink" (removes tokens from circulation)?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops
Answer: C – Token sinks reduce circulating supply; staking locks achieve this.

Quiz Questions (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment
Answer: C – Bitcoin halves block rewards every 210,000 blocks (4 years).

Q13. What is a major red flag in tokenomics design?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation exceeding 30% D) Fee sharing mechanism
Answer: C – Excessive insider allocation risks dumping and misaligned incentives.

Q14. Which strategy can reduce token velocity?
A) Encouraging frequent trading B) Staking mechanisms with lock-up periods
C) Removing governance rights D) Increasing transaction fees to 50%
Answer: B – Staking locks tokens, reducing velocity and sell pressure.

Q15. What does a large difference between circulating supply and total supply indicate?
A) Strong tokenomics B) Future dilution risk
C) Deflationary pressure D) High demand
Answer: B – Unvested tokens entering circulation can dilute existing holders.

Quiz Questions (16–20)

Q16. Which token is an example of a "store of value" token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers
Answer: B – Governance tokens allow holders to vote on protocol decisions.

Q18. In a deflationary token model, what happens to circulating supply over time?
A) Increases steadily B) Remains constant
C) Decreases through burns D) Doubles every 4 years
Answer: C – Deflationary models reduce supply via token burns.

Q19. What percentage of trading fees does GMX distribute to token holders?
A) 10% B) 20% C) 30% D) 50%
Answer: C – GMX distributes 30% of trading fees as value accrual.

Q20. Which year is Bitcoin's final BTC estimated to be mined?
A) 2040 B) 2100 C) 2140 D) 2200
Answer: C – Bitcoin's final coin is projected to be mined around 2140.

L29: Token Economics Fundamentals

Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Describe different token types (utility, governance, security) and their purposes
- Analyze value accrual mechanisms in token economies
- Evaluate token supply models and their implications
- Apply tokenomics principles to real-world projects

Building on L28: Lab: NFT Evaluation

The Token Economy Challenge

[COMIC: Supply and demand basics]

A visual narrative showing the fundamental tension in token economics

Visual framing: The balance between token creation and value preservation

What This Illustrates

- Token supply must match demand to maintain value
- Emission schedules affect long-term price dynamics
- Scarcity vs. accessibility trade-offs

The Question

How do we design token economies that don't collapse under their own weight?

(c) Joerg Osterrieder 2025

The Problem: How do we create sustainable token economies?

The Challenge
Designing a token that aligns incentives across users, developers, investors, and validators without collapsing into a speculative bubble or death spiral. Most token economies fail because they prioritize short-term hype over long-term sustainability.

Why It Matters

- Over 95% of ICO-era tokens failed due to poor economic design
- Terra/Luna collapsed ($40B) from flawed algorithmic stablecoin tokenomics
- Inflationary token spirals destroy user trust and protocol viability

What We Need

- Economic alignment of actors
- Sound monetary policy (supply schedules, emission rates)
- Real utility beyond speculation (value capture mechanisms)

The Cryptoeconomics Question
How do we design incentives so participants act in the protocol's best interest while pursuing their own gains?

Today's lesson: How Token Economics addresses this challenge

What is Tokenomics?

Definition: The study of the economic systems governing the creation, distribution, and management of tokens in blockchain ecosystems.

Key Components:

- Token design and purpose
- Supply and distribution mechanics
- Incentive structures
- Value capture mechanisms
- Governance and utility

Why It Matters: Tokenomics determines the long-term sustainability and success of crypto projects.

Problem: Why do most tokens fail economically? — Tokenomics provides frameworks to design sustainable supply, demand, and incentive structures

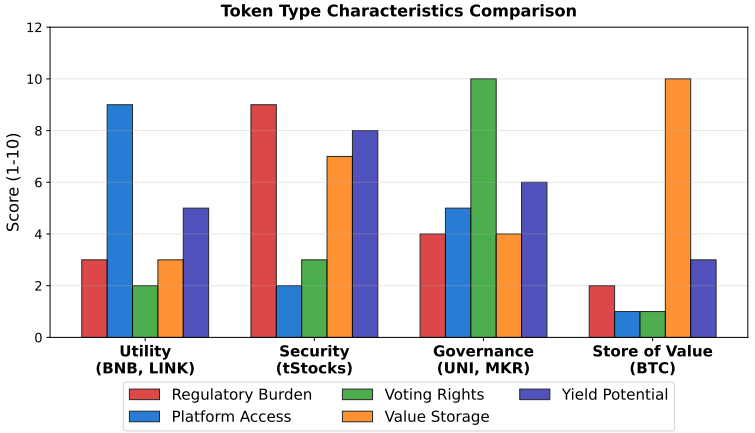
(c) Joerg Osterrieder 2025

What Are the Main Types of Tokens?

1. **Utility Tokens**
   - Access to platform services
   - Payment for network fees
   - Examples: BNB, LINK, FIL
2. **Security Tokens**
   - Represent ownership/dividends
   - Subject to securities laws
   - Examples: tokenized stocks, bonds
3. **Governance Tokens**
   - Voting rights on protocol changes
   - DAO participation
   - Examples: UNI, AAVE, MKR
4. **Store of Value Tokens**
   - Digital gold analogy
   - Limited supply
   - Example: BTC

(c) Joerg Osterrieder 2025

Token Types Characteristics



Security tokens have highest regulatory burden; governance tokens offer strongest voting rights

How Do Utility Tokens Work?

Purpose: Access to products/services
Characteristics:

- Not designed as investments
- Required for platform interaction
- Value linked to usage
- May offer fee discounts

Example: Binance Coin (BNB)

- Trading fee discounts on exchange
- Gas fees on BNB Chain
- Token sale participation (Launchpad)
- Quarterly burns based on volume

(c) Joerg Osterrieder 2025

What Makes a Token a Security?

Definition: Investment contracts subject to securities regulations

Howey Test Criteria:

1. Investment of money
2. In a common enterprise
3. Expectation of profits
4. From efforts of others

Implications:

- Must comply with SEC (US)
- Require registration/exemption
- Investor protections apply
- Often limited to accredited investors

Examples: Tokenized stocks, bonds, real estate

How Do Governance Tokens Create Alignment?

Purpose: Decentralized decision-making
Voting Rights:

- Protocol parameter changes
- Treasury allocation
- Fee structure modifications
- Smart contract upgrades

Example: Uniswap (UNI)

- Protocol fee governance
- Treasury management ($B+ assets)
- Grant program decisions
- 1 UNI = 1 vote (delegatable)

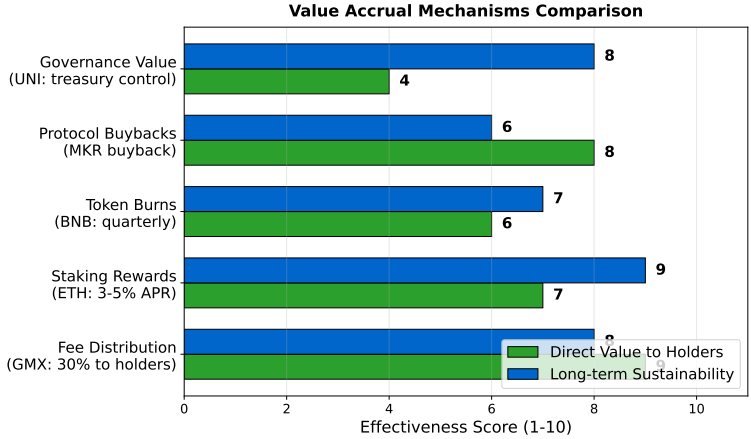
Problem: How do we align token holder interests with protocol success? — Governance tokens create economic skin-in-the-game by tying voting power to token ownership

How Do Tokens Capture Value from Protocol Success?

1. **Fee Distribution**
   - Protocol fees shared with token holders
   - Example: GMX distributes 30% of trading fees
2. **Staking Rewards**
   - Lock tokens to earn yield
   - Example: Ethereum validators earn ETH rewards
3. **Token Burns**
   - Reduce circulating supply
   - Example: BNB quarterly burns, ETH EIP-1559

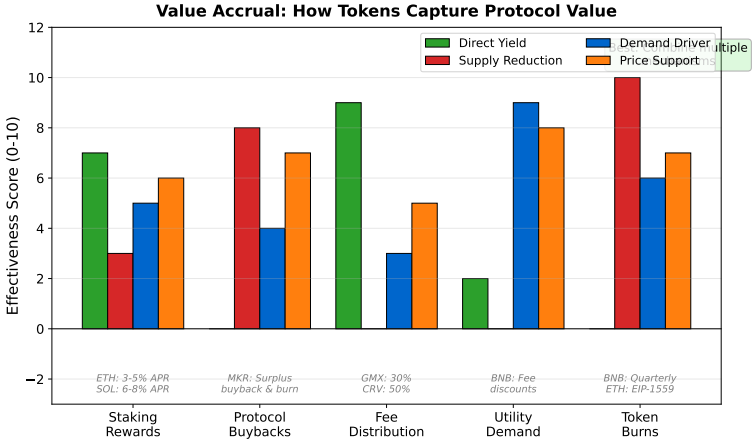
(c) Joerg Osterrieder 2025

Value Accrual Mechanisms Comparison



Fee distribution provides direct value; staking rewards offer best sustainability

Value Accrual: Capturing Protocol Value



Best tokenomics combine multiple mechanisms: staking for yield, burns for supply reduction, utility for organic demand

Why Choose Fixed Supply Models?

Characteristics:

- Predetermined max supply
- No new tokens after cap
- Deflationary if burned

Advantages:

- Scarcity drives value
- Predictable monetary policy
- Inflation protection

Bitcoin Example:

- Max: 21 million BTC
- Current: 19.5M (2024)
- Halving every 4 years
- Final BTC: year 2140

What's the Difference Between Inflationary and Deflationary Models?

Inflationary:

- New tokens continuously created
- Rate may be fixed or decreasing
- Incentivizes participation

Deflationary:

- Supply decreases over time
- Tokens removed via burns
- Creates scarcity pressure

BNB Burn Mechanism:

- Auto-Burn: based on gas fees
- Target: 100M (from 200M)
- Current: 144M (Dec 2024)

Problem Check-In: Token Economics

Recall Our Problem

How do we create sustainable token economies?

What We've Learned So Far

- Token types (utility, governance, security) serve different economic purposes and face different regulations
- Value accrual mechanisms (fee distribution, staking, burns) connect token price to protocol success
- Understanding token purpose and value capture is the foundation of sustainable token design

Still to Address

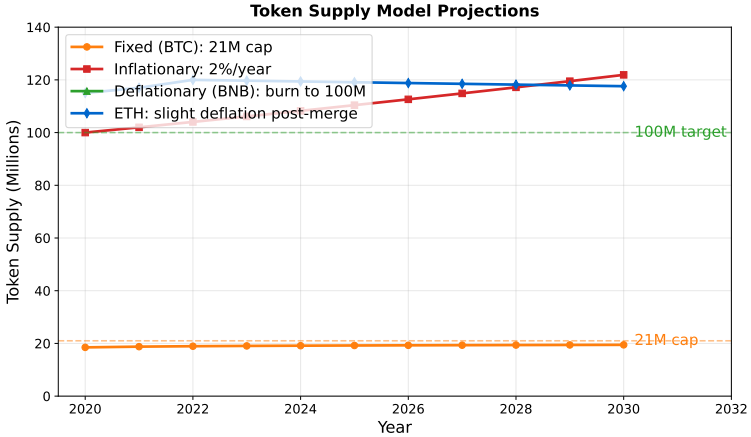
- Supply models, emission schedules, and velocity control mechanisms
- How do we balance token creation incentives with long-term scarcity?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we create sustainable token..."?

Supply Model Projections

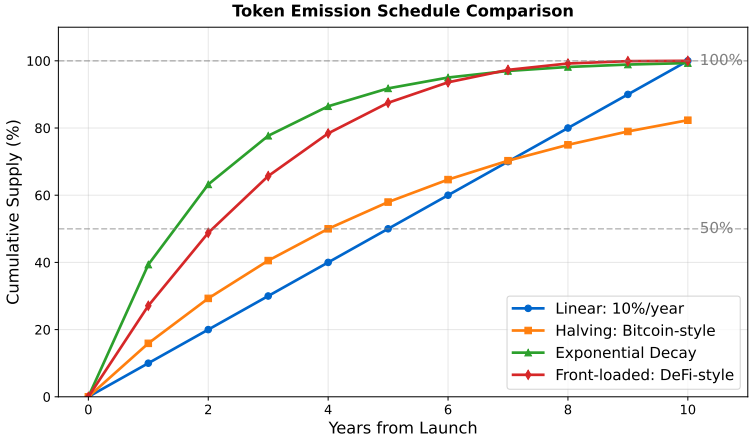


BTC approaches 21M cap; BNB burns toward 100M; ETH slightly deflationary post-merge — Supply schedules create predictable scarcity, a key sustainability factor

How Do Tokens Enter Circulation Over Time?

1. **Linear Emission**
   - Constant rate of new tokens
   - Predictable but perpetual inflation
2. **Decreasing Emission**
   - Halving events (Bitcoin model)
   - Gradually reducing inflation
3. **Exponential Decay**
   - Rapid initial distribution
   - Asymptotically approaches max supply
4. **Algorithmic Adjustment**
   - Based on network metrics
   - Example: Ethereum's variable issuance

Emission Schedule Comparison



DeFi protocols often use front-loaded emission; Bitcoin uses halving model

Why Does High Velocity Suppress Token Price?

High token velocity (frequent buying/selling) can suppress token price.

Equation of Exchange:

$$MV = PQ$$

where:

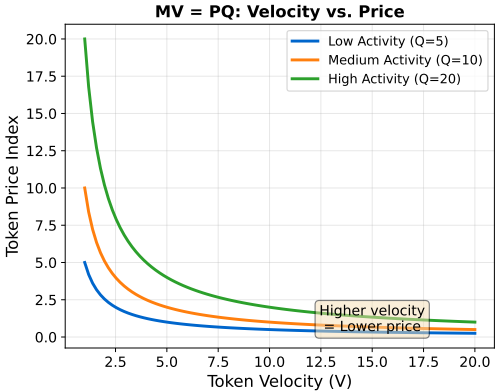
- M = Money supply (token supply)
- V = Velocity (transaction frequency)
- P = Price level
- Q = Quantity of goods/services

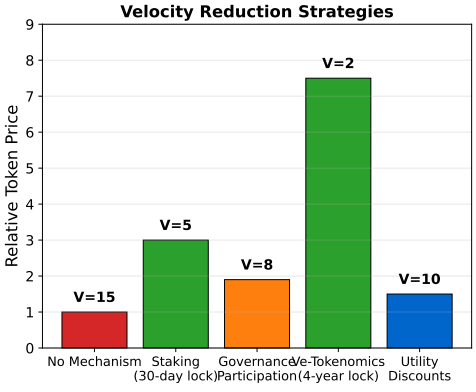
Solutions:

- Staking mechanisms (reduce velocity)
- Vesting periods
- Utility that requires holding (governance, fee discounts)

(c) Joerg Osterrieder 2025

Token Velocity and Price Dynamics





Higher velocity suppresses price; ve-tokenomics (4-year locks) most effective at reducing velocity

Pseudocode: Token Vesting Schedule

Linear Vesting with Cliff

```
function claimable_tokens(beneficiary):
  if current_time < cliff_end:
    return 0 // Nothing before cliff
  elapsed = current_time - vesting_start
  total_vesting_period = 4 years
  vested = total_allocation * (elapsed / total_vesting_period)
  vested = min(vested, total_allocation) // Cap at 100%
  claimable = vested - already_claimed
  return claimable
```

Key Insight: Vesting reduces velocity by preventing immediate selling. A 1-year cliff + 4-year linear vesting is the industry standard. Without vesting, insiders could dump tokens at launch, crashing prices.

Vesting is a velocity control mechanism: tokens locked today cannot be sold, reducing sell pressure

What Creates Balance: Token Sinks vs. Faucets?

Token Sinks (Removal)

- Transaction fee burns
- Protocol penalties (slashing—automatic destruction of staked tokens as punishment for misbehavior)
- Staking locks
- Governance participation locks

Effect: Reduce circulating supply, increase scarcity.

Token Faucets (Creation)

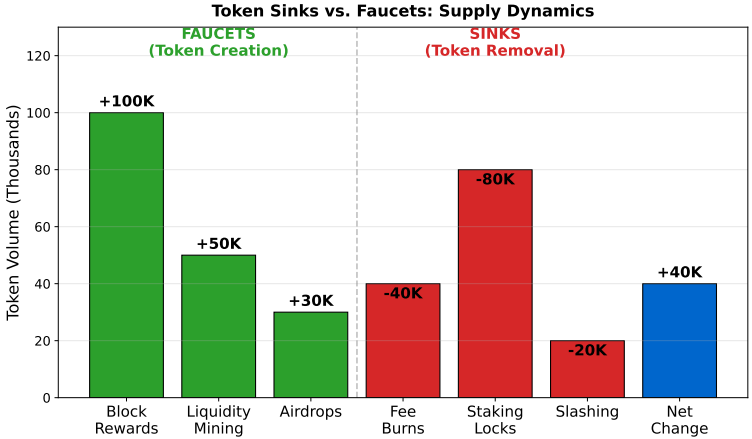
- Block rewards
- Liquidity mining rewards
- Airdrops
- Developer grants

Effect: Increase supply, incentivize participation.

Balance: Healthy tokenomics requires equilibrium between sinks and faucets.

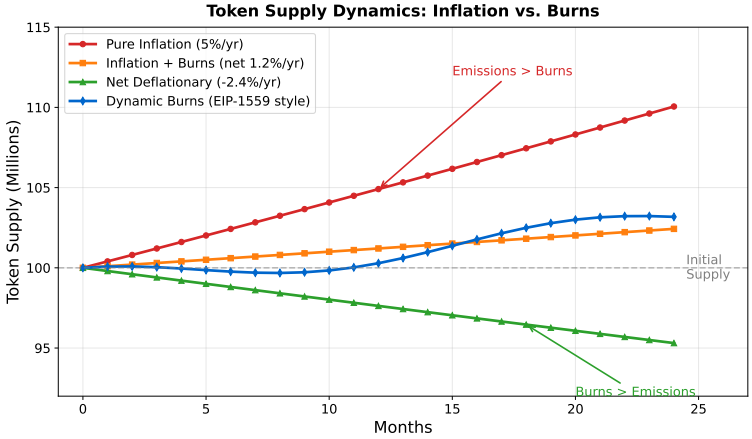
(c) Joerg Osterrieder 2025

Token Supply Dynamics



Healthy tokenomics balances faucets (creation) with sinks (removal) — Equilibrium between token creation and removal prevents hyperinflation or deflationary spirals

Supply Dynamics: Inflation vs. Burns



Pure inflation expands supply; burns can offset or exceed emissions; dynamic burns (EIP-1559) respond to network activity

How Did Ethereum's Tokenomics Evolve?

Pre-EIP-1559:
(Before Aug 2021)

- 4.5% inflation
- All fees to miners
- Unpredictable fees

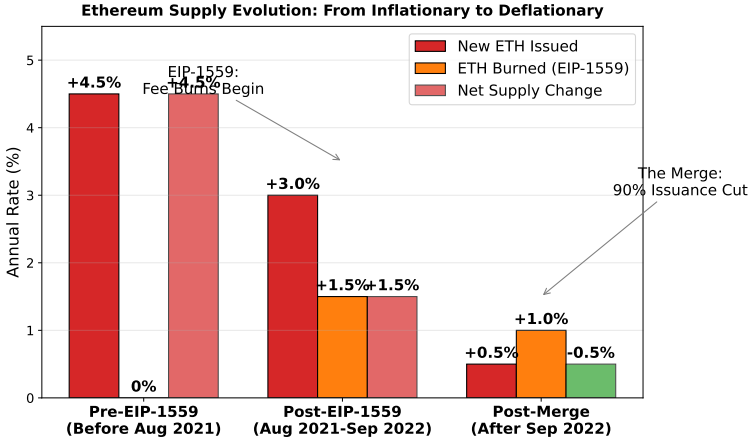
Post-EIP-1559:

- Base fee burned
- Tips to miners
- Predictable fees

Post-Merge:
(Sept 2022)

- Issuance -90%
- Net deflationary
- 3-5% staking APR (Annual Percentage Rate—simple yearly interest without compounding)

ETH Supply Evolution



EIP-1559 introduced burns; The Merge cut issuance 90%, achieving net deflation

How Do You Spot Bad Tokenomics?

Good Tokenomics

- Clear value accrual
- Sustainable incentives
- Low initial team/VC allocation
- Long vesting periods
- Transparent distribution
- Real utility beyond speculation

Red Flags:

- Excessive token supply to insiders (¿30%)
- Unsustainable yield promises (¿100% APY)

Bad Tokenomics

- No clear value capture
- Ponzi-like dynamics
- High team/insider allocation
- Short/no vesting
- Opaque distribution
- Pure speculation

What Metrics Should You Check First?

1. **Circulating vs Total Supply**
   Large gap = future dilution
2. **Token Distribution**
   Top holder concentration, team %
3. **Inflation Rate**
   Current and projected annual
4. **Value Accrual**
   Fee sharing, burns, staking
5. **Unlock Schedule**
   When do vested tokens circulate?

Key: Evaluate all metrics together for complete picture

Problem Solved? Token Economics

The Original Problem

How do we create sustainable token economies that don't collapse?

How Token Economics Solves It

- **Supply schedules**: Fixed (BTC), inflationary (ETH pre-merge), or deflationary (BNB burns) – predictable monetary policy
- **Value accrual**: Fee distribution, staking rewards, token burns create organic demand
- **Velocity control**: Staking locks and governance utility reduce sell pressure

Remaining Limitations

- **Speculation dominates utility**: Even well-designed tokens suffer from price volatility unrelated to fundamentals
- **Behavioral unpredictability**: Token velocity, holder psychology, and market cycles are hard to model

Open Questions

- What makes a token economy sustainable long-term? (No token has survived multiple market cycles with stable demand)
- Risk: Incentive misalignment if team allocations are excessive or vesting too short

Token Economics provides frameworks but no guarantees – success depends on execution and market conditions

The Economics of Token Economics

Incentive Structure

- **Core Problem:** Aligning individual and collective interests
- **Why act honestly?** Rewards for honest behavior, penalties for cheating
- **Value Flow:** Protocol gains security, participants earn rewards

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium (a game theory state where no player benefits from changing strategy unilaterally)

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Protocol gains security, participants earn rewards

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Token Economics

Alternatives Considered

1. **Chosen Design:** Reward curves, slashing conditions
2. **Alternative:** Alternative reward mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Token Economics

Critical Failure Mode

- **What breaks:** Incentive misalignment, free-rider problems
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

The Inflation-Deflation Tug of War

[COMIC: Inflation vs deflation tension]

A visual narrative showing the perpetual struggle between inflationary emission and deflationary burns

What We Learned

- Token supply schedules create predictable scarcity
- Burns (EIP-1559, BNB) counteract inflation
- No perfect balance exists—all choices are trade-offs

The Takeaway

Sustainable tokenomics requires careful equilibrium between token creation incentives and value preservation.

Visual synthesis: The ongoing battle that defines every token economy

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- Token type determines purpose and regulatory treatment
- Value accrual mechanisms connect token price to protocol success
- Supply models (fixed, inflationary, deflationary) have trade-offs
- Good tokenomics aligns incentives across all stakeholders
- Token velocity must be managed to maintain value
- Transparent distribution and vesting are crucial

Next Lecture: Distribution and Vesting - How tokens are allocated and released over time.

Next Lesson: L30 – Distribution and Vesting

Questions for Reflection

1. How does Bitcoin's fixed supply model compare to Ethereum's flexible issuance?
2. What are the trade-offs between utility tokens and governance tokens?
3. How can a protocol reduce token velocity without harming liquidity?
4. Why might high team/VC allocations be problematic?
5. What role do token burns play in value accrual?

Quiz Questions (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. According to the Howey Test, which criterion does NOT determine if a token is a security?
A) Investment of money B) Common enterprise
C) Token name includes "coin" D) Expectation of profits from others' efforts
Answer: C – The Howey Test has 4 criteria; token naming is not one of them.

Q4. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q5. Which token provides an example of governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

Quiz Questions (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops
Answer: B – Fee distribution shares protocol fees with token holders (e.g., GMX).

Q8. In the equation of exchange ($MV = PQ$), high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect on price D) Doubles the money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q9. What is BNB's target supply after all burns are complete?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q10. Which of these is a "token sink" (removes tokens from circulation)?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops
Answer: C – Token sinks reduce circulating supply; staking locks achieve this.

Quiz Questions (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment
Answer: C – Bitcoin halves block rewards every 210,000 blocks (4 years).

Q13. What is a major red flag in tokenomics design?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation exceeding 30% D) Fee sharing mechanism
Answer: C – Excessive insider allocation risks dumping and misaligned incentives.

Q14. Which strategy can reduce token velocity?
A) Encouraging frequent trading B) Staking mechanisms with lock-up periods
C) Removing governance rights D) Increasing transaction fees to 50%
Answer: B – Staking locks tokens, reducing velocity and sell pressure.

Q15. What does a large difference between circulating supply and total supply indicate?
A) Strong tokenomics B) Future dilution risk
C) Deflationary pressure D) High demand
Answer: B – Unvested tokens entering circulation can dilute existing holders.

Quiz Questions (16–20)

Q16. Which token is an example of a "store of value" token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers
Answer: B – Governance tokens allow holders to vote on protocol decisions.

Q18. In a deflationary token model, what happens to circulating supply over time?
A) Increases steadily B) Remains constant
C) Decreases through burns D) Doubles every 4 years
Answer: C – Deflationary models reduce supply via token burns.

Q19. What percentage of trading fees does GMX distribute to token holders?
A) 10% B) 20% C) 30% D) 50%
Answer: C – GMX distributes 30% of trading fees as value accrual.

Q20. Which year is Bitcoin's final BTC estimated to be mined?
A) 2040 B) 2100 C) 2140 D) 2200
Answer: C – Bitcoin's final coin is projected to be mined around 2140.

Quiz: Token Economics

Instructions: Multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes

Quiz (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold

Quiz (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. According to the Howey Test, which criterion does NOT determine if a token is a security?
A) Investment of money B) Common enterprise
C) Token name includes "coin" D) Expectation of profits from others' efforts

Quiz (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. According to the Howey Test, which criterion does NOT determine if a token is a security?
A) Investment of money B) Common enterprise
C) Token name includes "coin" D) Expectation of profits from others' efforts
Answer: C – The Howey Test has 4 criteria; token naming is not one of them.

Q4. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited

Quiz (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. According to the Howey Test, which criterion does NOT determine if a token is a security?
A) Investment of money B) Common enterprise
C) Token name includes "coin" D) Expectation of profits from others' efforts
Answer: C – The Howey Test has 4 criteria; token naming is not one of them.

Q4. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q5. Which token provides an example of governance functionality?
A) BTC B) USDT C) UNI D) WBTC

Quiz (1–5)

Q1. Which of the following best defines tokenomics?
A) The price of a cryptocurrency B) The study of economic systems governing token creation and management
C) Mining difficulty algorithms D) Exchange trading volumes
Answer: B – Tokenomics encompasses token design, distribution, incentives, and value capture.

Q2. What is the primary characteristic of a utility token?
A) Represents ownership in a company B) Grants access to platform services
C) Provides voting rights only D) Functions as digital gold
Answer: B – Utility tokens are required for platform interaction and service access.

Q3. According to the Howey Test, which criterion does NOT determine if a token is a security?
A) Investment of money B) Common enterprise
C) Token name includes "coin" D) Expectation of profits from others' efforts
Answer: C – The Howey Test has 4 criteria; token naming is not one of them.

Q4. What is the maximum supply of Bitcoin?
A) 18.5 million B) 21 million C) 100 million D) Unlimited
Answer: B – Bitcoin has a predetermined cap of 21 million BTC.

Q5. Which token provides an example of governance functionality?
A) BTC B) USDT C) UNI D) WBTC
Answer: C – Uniswap (UNI) allows holders to vote on protocol changes.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards

Quiz (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops

Quiz (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops
Answer: B – Fee distribution shares protocol fees with token holders (e.g., GMX).

Q8. In the equation of exchange ($MV = PQ$), high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect on price D) Doubles the money supply

Quiz (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops
Answer: B – Fee distribution shares protocol fees with token holders (e.g., GMX).

Q8. In the equation of exchange ($MV = PQ$), high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect on price D) Doubles the money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q9. What is BNB's target supply after all burns are complete?
A) 50 million B) 100 million C) 144 million D) 200 million

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops
Answer: B – Fee distribution shares protocol fees with token holders (e.g., GMX).

Q8. In the equation of exchange ($MV = PQ$), high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect on price D) Doubles the money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q9. What is BNB's target supply after all burns are complete?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q10. Which of these is a "token sink" (removes tokens from circulation)?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the purpose of EIP-1559 in Ethereum's tokenomics?
A) Increase block size B) Burn base fees to reduce supply
C) Eliminate all transaction fees D) Double staking rewards
Answer: B – EIP-1559 burns the base fee, creating a deflationary mechanism.

Q7. Which value accrual mechanism directly distributes protocol revenue to token holders?
A) Token burns B) Fee distribution
C) Halving events D) Airdrops
Answer: B – Fee distribution shares protocol fees with token holders (e.g., GMX).

Q8. In the equation of exchange ($MV = PQ$), high token velocity (V) typically:
A) Increases token price B) Suppresses token price
C) Has no effect on price D) Doubles the money supply
Answer: B – High velocity means tokens change hands quickly, suppressing price.

Q9. What is BNB's target supply after all burns are complete?
A) 50 million B) 100 million C) 144 million D) 200 million
Answer: B – BNB aims to burn from 200M initial supply down to 100M.

Q10. Which of these is a "token sink" (removes tokens from circulation)?
A) Block rewards B) Liquidity mining C) Staking locks D) Airdrops
Answer: C – Token sinks reduce circulating supply; staking locks achieve this.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely

Quiz (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment

Quiz (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment
Answer: C – Bitcoin halves block rewards every 210,000 blocks (4 years).

Q13. What is a major red flag in tokenomics design?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation exceeding 30% D) Fee sharing mechanism

Quiz (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment
Answer: C – Bitcoin halves block rewards every 210,000 blocks (4 years).

Q13. What is a major red flag in tokenomics design?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation exceeding 30% D) Fee sharing mechanism
Answer: C – Excessive insider allocation risks dumping and misaligned incentives.

Q14. Which strategy can reduce token velocity?
A) Encouraging frequent trading B) Staking mechanisms with lock-up periods
C) Removing governance rights D) Increasing transaction fees to 50%

Quiz (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment
Answer: C – Bitcoin halves block rewards every 210,000 blocks (4 years).

Q13. What is a major red flag in tokenomics design?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation exceeding 30% D) Fee sharing mechanism
Answer: C – Excessive insider allocation risks dumping and misaligned incentives.

Q14. Which strategy can reduce token velocity?
A) Encouraging frequent trading B) Staking mechanisms with lock-up periods
C) Removing governance rights D) Increasing transaction fees to 50%
Answer: B – Staking locks tokens, reducing velocity and sell pressure.

Q15. What does a large difference between circulating supply and total supply indicate?
A) Strong tokenomics B) Future dilution risk
C) Deflationary pressure D) High demand

Quiz (11–15)

Q11. What happened to ETH issuance after The Merge in September 2022?
A) Increased by 90% B) Stayed the same
C) Reduced by 90% D) Stopped completely
Answer: C – The Merge cut issuance from 4.5% to 0.5% annually.

Q12. Which emission schedule model does Bitcoin use?
A) Linear emission B) Exponential decay
C) Halving events (decreasing emission) D) Algorithmic adjustment
Answer: C – Bitcoin halves block rewards every 210,000 blocks (4 years).

Q13. What is a major red flag in tokenomics design?
A) Long vesting periods B) Transparent distribution
C) Team/insider allocation exceeding 30% D) Fee sharing mechanism
Answer: C – Excessive insider allocation risks dumping and misaligned incentives.

Q14. Which strategy can reduce token velocity?
A) Encouraging frequent trading B) Staking mechanisms with lock-up periods
C) Removing governance rights D) Increasing transaction fees to 50%
Answer: B – Staking locks tokens, reducing velocity and sell pressure.

Q15. What does a large difference between circulating supply and total supply indicate?
A) Strong tokenomics B) Future dilution risk
C) Deflationary pressure D) High demand
Answer: B – Unvested tokens entering circulation can dilute existing holders.

Quiz (16–20)

Q16. Which token is an example of a “store of value” token?
A) LINK B) UNI C) BTC D) BNB

Quiz (16–20)

Q16. Which token is an example of a “store of value” token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers

Quiz (16–20)

Q16. Which token is an example of a "store of value" token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers
Answer: B – Governance tokens allow holders to vote on protocol decisions.

Q18. In a deflationary token model, what happens to circulating supply over time?
A) Increases steadily B) Remains constant
C) Decreases through burns D) Doubles every 4 years

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. Which token is an example of a "store of value" token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers
Answer: B – Governance tokens allow holders to vote on protocol decisions.

Q18. In a deflationary token model, what happens to circulating supply over time?
A) Increases steadily B) Remains constant
C) Decreases through burns D) Doubles every 4 years
Answer: C – Deflationary models reduce supply via token burns.

Q19. What percentage of trading fees does GMX distribute to token holders?
A) 10% B) 20% C) 30% D) 50%

Quiz (16–20)

Q16. Which token is an example of a "store of value" token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers
Answer: B – Governance tokens allow holders to vote on protocol decisions.

Q18. In a deflationary token model, what happens to circulating supply over time?
A) Increases steadily B) Remains constant
C) Decreases through burns D) Doubles every 4 years
Answer: C – Deflationary models reduce supply via token burns.

Q19. What percentage of trading fees does GMX distribute to token holders?
A) 10% B) 20% C) 30% D) 50%
Answer: C – GMX distributes 30% of trading fees as value accrual.

Q20. Which year is Bitcoin's final BTC estimated to be mined?
A) 2040 B) 2100 C) 2140 D) 2200

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. Which token is an example of a "store of value" token?
A) LINK B) UNI C) BTC D) BNB
Answer: C – Bitcoin is designed as digital gold with limited supply.

Q17. What is the primary function of governance tokens?
A) Pay network fees B) Enable decentralized voting on protocol changes
C) Generate passive income D) Facilitate cross-chain transfers
Answer: B – Governance tokens allow holders to vote on protocol decisions.

Q18. In a deflationary token model, what happens to circulating supply over time?
A) Increases steadily B) Remains constant
C) Decreases through burns D) Doubles every 4 years
Answer: C – Deflationary models reduce supply via token burns.

Q19. What percentage of trading fees does GMX distribute to token holders?
A) 10% B) 20% C) 30% D) 50%
Answer: C – GMX distributes 30% of trading fees as value accrual.

Q20. Which year is Bitcoin's final BTC estimated to be mined?
A) 2040 B) 2100 C) 2140 D) 2200
Answer: C – Bitcoin's final coin is projected to be mined around 2140.

(c) Joerg Osterrieder 2025

L30: Distribution and Vesting

Mini-Lecture – Module D: Tokenomics

Blockchain & Cryptocurrency Course

January 2026

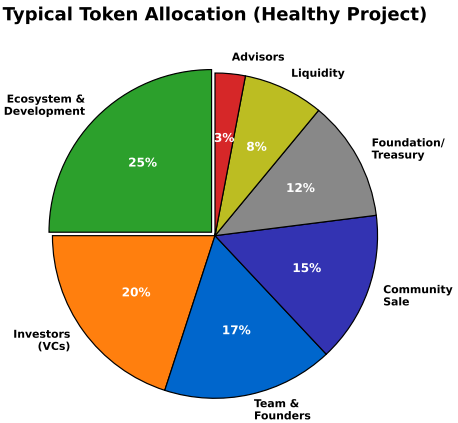
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Describe token allocation categories and their purposes
- Analyze vesting schedules and cliff periods
- Evaluate impact of unlock events on token price
- Identify red flags in token distribution

Typical Token Allocation Breakdown



Insiders (Team+VCs+Advisors): ~40% | Community: ~60%

Red Flag: Team + Investors $> 50\%$ indicates high centralization risk.

Token Allocation Categories

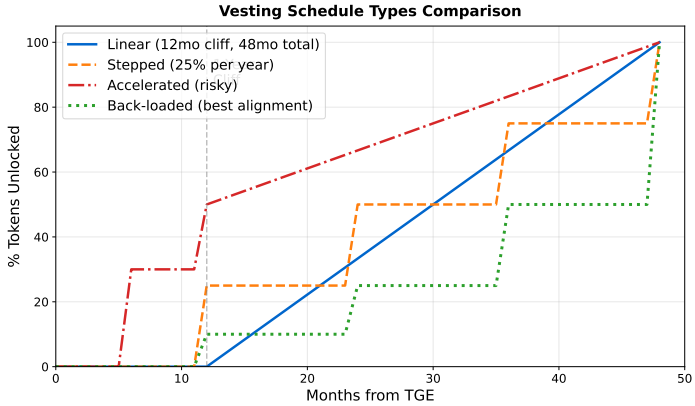
Common Categories:

- **Team/Founders:** 15-20%, 4-year vesting, 1-year cliff
- **Investors (Seed/A/B):** 15-30%, 2-3 year vesting
- **Community Sale:** 10-15% (ICO/IEO/IDO)
- **Ecosystem/Treasury:** 15-25%
- **Airdrops:** 5-15%

Best Practice:

- Team + VCs $< 40\%$
- Long vesting (3-4 years) for insiders
- Transparent allocation documentation

Vesting Schedule Types



Back-loaded: Strongest long-term alignment — **Front-loaded:** Highest dump risk

Vesting Key Concepts

Key Terms:

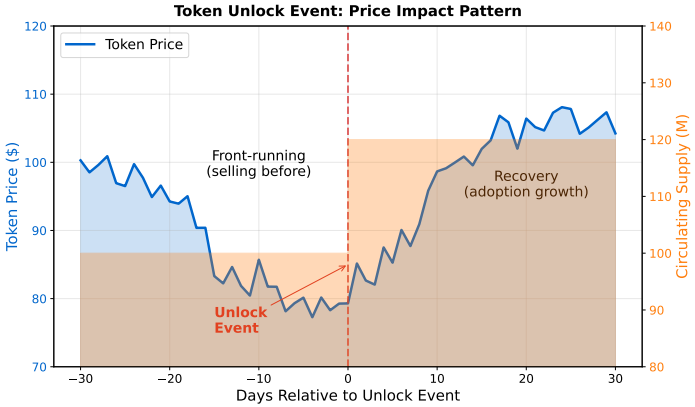
- **Cliff Period:** Initial wait before any tokens unlock (usually 12 months)
- **Vesting Period:** Total duration until all tokens unlocked
- **Linear Vesting:** Equal amounts at regular intervals
- **TGE:** Token Generation Event (initial launch)

Example:

- 1,000,000 tokens, 12-month cliff, 48-month total vesting
- Month 1-12: 0 tokens unlock (cliff)
- Month 13-48: 27,778 tokens/month (linear)

(c) Joerg Osterrieder 2025

Unlock Event Price Impact



Market front-runs unlocks: Price typically drops 15-20% around major events.

Case Study: Solana Unlocks

SOL Token Unlocks:

- Total supply: 500M (inflating to 700M by 2030)
- Jan 2023: 13.8M SOL unlocked (seed investors)
- Mar 2023: 17.8M SOL unlocked (early investors)
- Ongoing: Monthly validator/foundation unlocks

Price Impact: SOL dropped 15-20% around major unlocks

Mitigation Strategy: Solana staking 7% APY incentivizes holding.

2024 Trend: Points Programs

What are Points?

- Off-chain loyalty system tracking user activity
- Converted to tokens at future TGE
- Replaced traditional airdrops in 2024

Examples:

- **EigenLayer:** Points for restaking
- **Blast:** Points + Gold for L2 deposits
- **Ethena:** Points for USDe staking

Criticism: Opaque, favors whales, mercenary capital

Key Takeaways

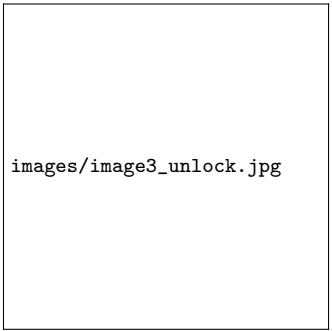
1. **Allocation:** Team + VCs $< 40\%$, long vesting (3-4 years)
2. **Cliff:** 12-month cliff for team prevents immediate dumping
3. **Unlock Impact:** Markets front-run, 15-20% drops typical
4. **Red Flags:** Insiders $> 50\%$, short vesting, opaque allocation
5. **2024 Trend:** Points programs replacing traditional airdrops

Tools: Token Unlocks, Messari, CoinGecko for monitoring schedules.

Distribution and Vesting in Practice

Token Distribution

Vesting Schedule



Unlock Events

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is a cliff period in token vesting?
A) Maximum tokens B) Initial wait before any unlock
C) Price floor D) Trading restriction

Quiz (1/2)

Q1. What is a cliff period in token vesting?
A) Maximum tokens B) Initial wait before any unlock
C) Price floor D) Trading restriction
Answer: B – Cliff ensures minimum commitment before tokens unlock.

Q2. What is considered a red flag for team/VC allocation?
A) 10% team B) 20% VCs C) Team + VCs $>$ 50%
D) 4-year vesting

Quiz (1/2)

Q1. What is a cliff period in token vesting?
A) Maximum tokens B) Initial wait before any unlock
C) Price floor D) Trading restriction
Answer: B – Cliff ensures minimum commitment before tokens unlock.

Q2. What is considered a red flag for team/VC allocation?
A) 10% team B) 20% VCs C) Team + VCs $>$ 50%
D) 4-year vesting
Answer: C – Insiders $>$ 50% indicates high centralization risk.

Q3. Which investment round has the longest vesting?
A) Public Sale B) Series B C) Series A D) Seed

Quiz (1/2)

Q1. What is a cliff period in token vesting?
A) Maximum tokens B) Initial wait before any unlock
C) Price floor D) Trading restriction
Answer: B – Cliff ensures minimum commitment before tokens unlock.

Q2. What is considered a red flag for team/VC allocation?
A) 10% team B) 20% VCs C) Team + VCs $>$ 50%
D) 4-year vesting
Answer: C – Insiders $>$ 50% indicates high centralization risk.

Q3. Which investment round has the longest vesting?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting (earliest, highest risk).

Q4. What is linear vesting?
A) All at once B) Equal amounts at regular intervals
C) Random amounts D) Exponential increase

Quiz (1/2)

Q1. What is a cliff period in token vesting?
A) Maximum tokens B) Initial wait before any unlock
C) Price floor D) Trading restriction
Answer: B – Cliff ensures minimum commitment before tokens unlock.

Q2. What is considered a red flag for team/VC allocation?
A) 10% team B) 20% VCs C) Team + VCs $>$ 50%
D) 4-year vesting
Answer: C – Insiders $>$ 50% indicates high centralization risk.

Q3. Which investment round has the longest vesting?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting (earliest, highest risk).

Q4. What is linear vesting?
A) All at once B) Equal amounts at regular intervals
C) Random amounts D) Exponential increase
Answer: B – Linear releases equal tokens monthly/daily after cliff.

Q5. Typical price impact of major unlock events?
A) 5% B) 15-20% drop C) 50% drop D) No impact

Quiz (1/2)

Q1. What is a cliff period in token vesting?
A) Maximum tokens B) Initial wait before any unlock
C) Price floor D) Trading restriction
Answer: B – Cliff ensures minimum commitment before tokens unlock.

Q2. What is considered a red flag for team/VC allocation?
A) 10% team B) 20% VCs C) Team + VCs $>$ 50%
D) 4-year vesting
Answer: C – Insiders $>$ 50% indicates high centralization risk.

Q3. Which investment round has the longest vesting?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting (earliest, highest risk).

Q4. What is linear vesting?
A) All at once B) Equal amounts at regular intervals
C) Random amounts D) Exponential increase
Answer: B – Linear releases equal tokens monthly/daily after cliff.

Q5. Typical price impact of major unlock events?
A) 5% B) 15-20% drop C) 50% drop D) No impact
Answer: B – Markets front-run, 15-20% drops typical.

Quiz (2/2)

Q6. Recommended minimum team vesting period?
A) 6 months B) 1 year C) 2 years D) 4 years

Quiz (2/2)

Q6. Recommended minimum team vesting period?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years for team tokens.

Q7. What replaced traditional airdrops in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining

Quiz (2/2)

Q6. Recommended minimum team vesting period?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years for team tokens.

Q7. What replaced traditional airdrops in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – EigenLayer, Blast, Ethena use points systems.

Q8. How many tokens unlock during a 12-month cliff?
A) 50% B) 25% C) 10% D) 0 tokens

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. Recommended minimum team vesting period?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years for team tokens.

Q7. What replaced traditional airdrops in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – EigenLayer, Blast, Ethena use points systems.

Q8. How many tokens unlock during a 12-month cliff?
A) 50% B) 25% C) 10% D) 0 tokens
Answer: D – Zero tokens unlock during cliff period.

Q9. What was Uniswap's airdrop per eligible address?
A) 100 UNI B) 400 UNI C) 1000 UNI D) 10000 UNI

Quiz (2/2)

Q6. Recommended minimum team vesting period?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years for team tokens.

Q7. What replaced traditional airdrops in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – EigenLayer, Blast, Ethena use points systems.

Q8. How many tokens unlock during a 12-month cliff?
A) 50% B) 25% C) 10% D) 0 tokens
Answer: D – Zero tokens unlock during cliff period.

Q9. What was Uniswap's airdrop per eligible address?
A) 100 UNI B) 400 UNI C) 1000 UNI D) 10000 UNI
Answer: B – 400 UNI per address ($1,200 at claim time).

Q10. Which is an example of a fair launch?
A) Ethereum B) Solana C) YFI D) Cardano

Quiz (2/2)

Q6. Recommended minimum team vesting period?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years for team tokens.

Q7. What replaced traditional airdrops in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – EigenLayer, Blast, Ethena use points systems.

Q8. How many tokens unlock during a 12-month cliff?
A) 50% B) 25% C) 10% D) 0 tokens
Answer: D – Zero tokens unlock during cliff period.

Q9. What was Uniswap's airdrop per eligible address?
A) 100 UNI B) 400 UNI C) 1000 UNI D) 10000 UNI
Answer: B – 400 UNI per address ($1,200 at claim time).

Q10. Which is an example of a fair launch?
A) Ethereum B) Solana C) YFI D) Cardano
Answer: C – YFI had no pre-sale, everyone bought at same price.

Thank you

Questions?

Next: L31 – Token Classification and Valuation

L30: Distribution and Vesting

Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Describe token allocation categories (team, investors, community) and their purposes
- Analyze vesting schedules and cliff periods
- Evaluate the impact of unlock events on token price
- Apply distribution analysis to real projects
- Case Study: Solana token unlocks

The Problem: How do we fairly distribute tokens over time?

The Challenge
How do we fairly distribute tokens over time without enabling insider dumps? Early contributors deserve rewards, but instant liquidity creates misaligned incentives and pump-and-dump schemes.

Why It Matters

- Unfair distributions lead to insider selling and community distrust
- Historical example: ICO-era instant unlocks caused 90% crashes; FTX/Alameda token manipulation (2022)

What We Need

- Economic alignment of actors
- Alignment between team and community incentives over multi-year horizons

The Cryptoeconomics Question
Aligning individual and collective interests

Today's lesson: How Distribution & Vesting addresses this challenge

(c) Joerg Osterrieder 2025

Token Distribution Overview

Definition: The initial allocation of tokens among different stakeholder groups.

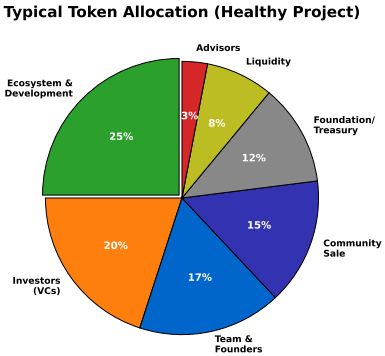
Common Allocation Categories:

- Team and Founders / Early Investors (Seed, Series A/B/C)
- Advisors / Community Sale (ICO/IEO/IDO)
- Ecosystem Development / Liquidity Provision
- Foundation/Treasury / Airdrops

Goal: Balance early supporter rewards with long-term community alignment.

(c) Joerg Osterrieder 2025

Typical Allocation Breakdown



Insiders (Team+VCs+Advisors): ~40% | Community: ~60%

Red Flag: Team + Investors ¿ 50% indicates high centralization risk

Team and Founder Allocation

Best Practices:

- 15-20% of total supply
- 4 years minimum vesting
- 1-year cliff period
- Linear unlock after cliff

Why Long Vesting?

- Prevents insider dumps
- Demonstrates commitment
- Aligns long-term incentives
- Builds community trust

Example: 20M tokens, 1-year cliff, then 416,667 tokens/month for 48 months

(c) Joerg Osterrieder 2025

Investor Allocation Rounds

Typical Investment Rounds:

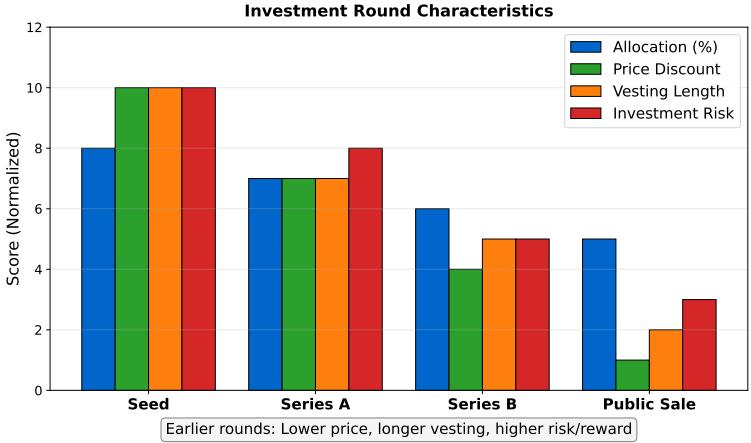
Round	Allocation	Price	Vesting
Seed	5-10%	Lowest	2-3 years
Series A	5-10%	Low	18-24 months
Series B	5-10%	Medium	12-18 months
Public Sale	10-15%	Highest	0-6 months

Key Considerations:

- Earlier investors = longer vesting
- Discount compensates for higher risk
- Too many investors = fragmented governance

(c) Joerg Osterrieder 2025

Investment Round Characteristics



Earlier rounds get bigger discounts but longer lock-ups and higher risk

Community Sale Methods

ICO (2017 Era):

- Direct sale to public
- Minimal regulation

IEO:

- On centralized exchange
- Exchange vets project

IDO:

- Launch on DEX
- Immediate liquidity

Fair Launch:

- No pre-sale/VC rounds
- Same price for all (e.g., YFI)

(c) Joerg Osterrieder 2025

What is Vesting?

Definition: Schedule controlling when allocated tokens become accessible.

Key Terms:

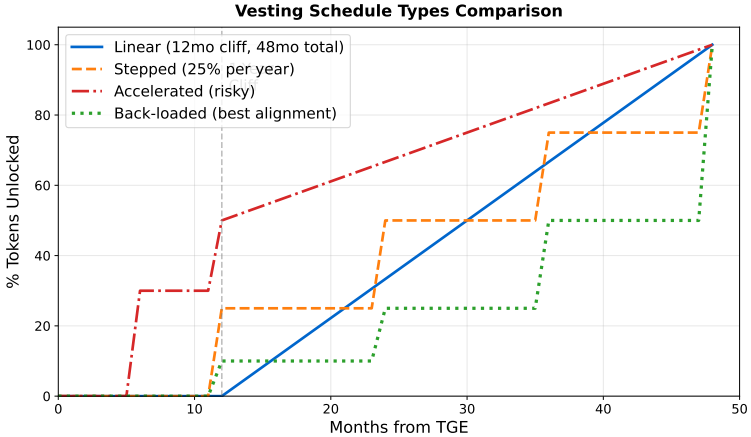
- **Cliff:** Initial wait period
- **Vesting:** Total unlock duration
- **Linear:** Equal regular unlocks
- **Unlock Event:** Transfer date

Example (1M tokens):

- Cliff: 12 months (0 unlock)
- Vesting: 48 months total
- Post-cliff: 27,778/month
- Full vest: month 48

(c) Joerg Osterrieder 2025

Vesting Schedule Types



Back-loaded vesting provides strongest long-term alignment; accelerated is risky

Cliff Periods

Typical Durations:

- Team: 12 months
- Investors: 6-12 months
- Advisors: 6 months
- Community: often 0

Why Use Cliffs?

- Prevents immediate dumps
- Tests commitment
- Project maturation time
- Reduces initial supply

Investor Perspective: Cliffs protect against early team departures

(c) Joerg Osterrieder 2025

Token Unlock Events

Market Impact:

- Increases circulating supply
- Creates selling pressure
- Price drops before/during
- Market front-runs unlocks

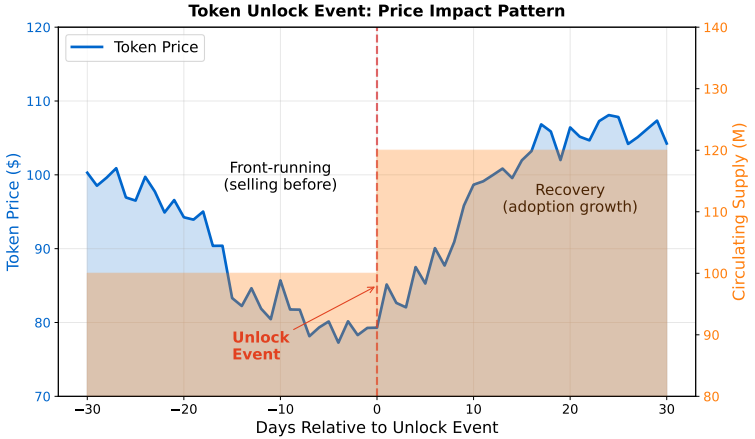
Types of Unlocks:

- **Cliff:** Large one-time release
- **Linear:** Monthly/daily streams
- **TGE:** Initial launch unlocks

Tools:
Token Unlocks, Messari, CoinGecko

(c) Joerg Osterrieder 2025

Unlock Event Price Impact



Market front-runs unlocks; price typically drops 15-20% around major events

Case Study: Solana (SOL) Unlocks

Background:

- 500M SOL (to 700M by 2030)
- Major unlocks 2021-2025
- VC: a16z, Multicoin, etc.

Key Events:

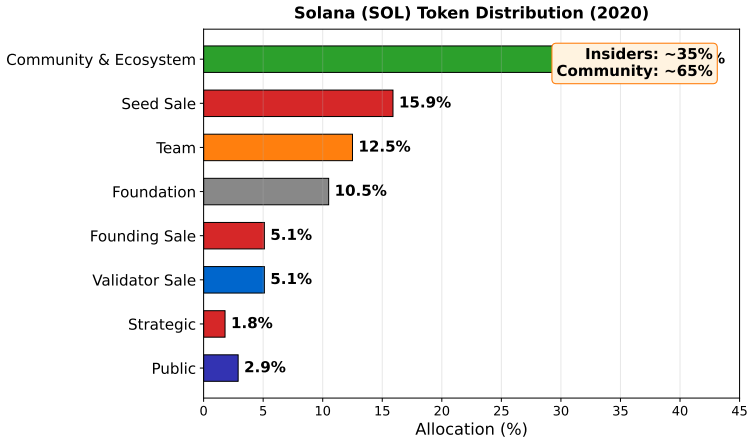
- Jan 2023: 13.8M (seed)
- Mar 2023: 17.8M (early)
- Ongoing: validator unlocks

Price Impact:

- 15-20% drops at unlocks
- Long-term recovery
- Market front-runs events

Lesson:
Strong fundamentals absorb unlock pressure over time

Solana Distribution Breakdown



Insiders 35% with long vesting helped manage dilution over time

Managing Unlock Pressure

Staking Incentives:

- High yields lock tokens
- Ex: SOL 7% APY

Gradual Unlocks:

- Daily/monthly releases
- Smooths supply shock

Lockup Extensions:

- Voluntary extra vesting
- Bonus for extended locks

Strong Fundamentals:

- Demand ¿ supply growth
- Adoption absorbs pressure

(c) Joerg Osterrieder 2025

Airdrops as Distribution

Airdrop Types:

- **Retroactive:** Past users (UNI)
- **Holder:** Existing holders
- **Task-based:** Actions
- **Governance:** DAO participation

Benefits:

- Bootstrap community
- Decentralize ownership
- Reward early adopters

Risks:
Hunters, immediate selling pressure

Famous Airdrop: Uniswap (UNI)

September 2020:

- 400 UNI per address
- 250,000 addresses eligible
- 150M UNI (15% supply)
- $1,200 value at claim

Impact:

- Instant decentralization
- Massive publicity
- Long-term holding
- DeFi airdrop standard

Key Insight: Retroactive airdrops reward genuine users, not speculators

Red Flags in Distribution

Excessive Insiders:

- Team + VCs ¿ 50%

Short/No Vesting:

- Team vesting ¡ 2 years
- No cliff period

Opaque Distribution:

- No published allocations
- Unknown wallet holders

Centralized Control:

- Foundation ¿ 30% forever

Multiple red flags = high risk of insider dumping

2024 Trend: Points Programs

What are Points?

- Off-chain loyalty tracking
- Converts to tokens at TGE
- Replaces traditional airdrops

How They Work:

- Track actions (deposits, trades)
- Accumulate proportionally
- Convert at TGE

2024 Examples:

- EigenLayer: restaking
- Blast: L2 deposits
- Ethena: USDe staking

Criticism:
Opaque, favors whales, mercenary capital

(c) Joerg Osterrieder 2025

Problem Solved? Distribution & Vesting

The Original Problem

How do we fairly distribute tokens over time?

How Distribution & Vesting Solves It

- Vesting schedules with cliffs create time-locked incentive alignment
- Community airdrops with anti-sybil measures reward genuine users
- Gradual unlock schedules smooth supply shocks (daily/monthly releases)

Remaining Limitations

- Vesting can be circumvented via derivatives (token loans, synthetic positions)
- Airdrops are often farmed by professional hunters, not real users

Open Questions

- What distribution model best aligns long-term interests without creating insider advantages?
- Risk: Incentive misalignment, free-rider problems

Distribution & Vesting partially solves "we fairly distribute tokens over time" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Summary

Distribution:

- Determines ownership concentration
- Healthy: Team+VCs ¡ 40%
- 3-4 year vesting standard
- Cliffs prevent immediate dumps

Next: Token Classification and Valuation

Market Dynamics:

- Unlocks = predictable pressure
- Points replacing airdrops (2024)
- Transparency builds trust
- Check Token Unlocks first

Questions for Reflection

1. Why do early investors typically have longer vesting than public sale participants?
2. How did Solana's unlock events impact its price trajectory?
3. What are the pros and cons of retroactive airdrops vs. task-based airdrops?
4. How can a project mitigate selling pressure during major unlocks?
5. What vesting schedule would you design for a new token launch?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit for minimum duration.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%
Answer: C – Team + VCs ¿ 50% indicates high centralization risk.

Q3. Which investment round typically has the longest vesting period?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting (longest) due to earliest entry and highest risk.

Q4. What is linear vesting?
A) Tokens unlock all at once B) Equal amounts unlock at regular intervals C) Exponential unlock schedule D) Random unlock dates
Answer: B – Linear vesting releases equal token amounts monthly/daily after the cliff period.

Q5. What was the typical price impact of Solana's major unlock events?
A) 5-8% drop B) 15-20% drop C) 30-40% drop D) No impact
Answer: B – SOL dropped 15-20% around major unlocks as market front-ran selling pressure.

Quiz Questions (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance
Answer: C – Retroactive airdrops reward genuine past users (e.g., Uniswap's 400 UNI per address).

Q8. What was the value of Uniswap's airdrop per eligible address in September 2020?
A) $400 B) $800 C) $1,200 D) $2,000
Answer: C – 400 UNI per address was worth approximately $1,200 at claim time.

Q9. Which sale method involves launching directly on a decentralized exchange?
A) ICO B) IEO C) IDO D) IPO
Answer: C – IDO (Initial DEX Offering) provides immediate liquidity on decentralized exchanges.

Q10. What is a typical team allocation percentage of total token supply?
A) 5-10% B) 15-20% C) 30-40% D) 50-60%
Answer: B – Best practice is 15-20% for team allocation to balance incentives and decentralization.

Quiz Questions (11–15)

Q11. What is the primary risk of airdrops to protocols?
A) Too expensive B) Airdrop hunters and immediate selling pressure C) Legal issues D) Technical complexity
Answer: B – Airdrop hunters farm rewards without genuine interest, creating immediate sell pressure.

Q12. How many tokens unlock during a 12-month cliff period?
A) 50% of allocation B) 25% of allocation C) 10% of allocation D) 0 tokens
Answer: D – Cliff means zero tokens unlock during that period; all unlocking starts after cliff ends.

Q13. Which vesting type provides the strongest long-term alignment?
A) Linear B) Front-loaded C) Back-loaded D) Accelerated
Answer: C – Back-loaded vesting releases more tokens later, keeping incentives aligned longer.

Q14. What is TGE in token distribution?
A) Token Growth Event B) Token Generation Event C) Total Gas Estimation D) Treasury Governance Entity
Answer: B – TGE (Token Generation Event) is the initial launch with first token unlocks.

Q15. What strategy can mitigate unlock selling pressure?
A) Delete tokens B) Staking incentives with high yields C) Burn all unlocked tokens D) Ban selling
Answer: B – High staking yields incentivize holders to lock tokens instead of selling (e.g., Solana 7% APY).

Quiz Questions (16–20)

Q16. What replaced traditional airdrops as the primary distribution mechanism in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – Points programs track off-chain activity and convert to tokens at TGE (e.g., EigenLayer, Blast).

Q17. Which project is an example of a Fair Launch with no pre-sale?
A) Ethereum B) Solana C) YFI (Yearn Finance) D) Cardano
Answer: C – YFI had a fair launch where everyone bought at the same price with no VC rounds.

Q18. What percentage of Uniswap's total supply was airdropped in September 2020?
A) 5% B) 10% C) 15% D) 25%
Answer: C – Approximately 150M UNI (15% of supply) was airdropped to 250,000 addresses.

Q19. What is the recommended maximum for Foundation/Treasury holdings?
A) ¡10% B) ¡20% C) ¡30% D) ¡50%
Answer: C – Foundation holding ¿30% indefinitely is a centralization red flag.

Q20. Why do earlier investors receive longer vesting periods?
A) Regulatory requirement B) Compensates for higher risk and bigger discounts C) Technical limitation D) Random assignment
Answer: B – Early investors take highest risk, get biggest discounts, so longer vesting aligns long-term incentives.

L30: Distribution and Vesting

Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Describe token allocation categories (team, investors, community) and their purposes
- Analyze vesting schedules and cliff periods
- Evaluate the impact of unlock events on token price
- Apply distribution analysis to real projects
- Case Study: Solana token unlocks

Building on L29: Token Economics

The Distribution Dilemma

[COMIC: Insider vs retail allocation]

A visual narrative showing the tension between early investors and public participants

What This Illustrates

- Early investors want rewards for risk
- Retail investors want fair access
- Teams must balance both without enabling dumps

The Question

How do we reward early contributors without enabling insider exploitation?

Visual framing: The allocation tension between insiders and community

The Problem: How do we fairly distribute tokens over time?

The Challenge
How do we fairly distribute tokens over time without enabling insider dumps? Early contributors deserve rewards, but instant liquidity creates misaligned incentives and pump-and-dump schemes.

Why It Matters

- Unfair distributions lead to insider selling and community distrust
- Historical example: ICO-era instant unlocks caused 90% crashes; FTX/Alameda token manipulation (2022)

What We Need

- Economic alignment of actors
- Alignment between team and community incentives over multi-year horizons

The Cryptoeconomics Question
Aligning individual and collective interests

Today's lesson: How Distribution & Vesting addresses this challenge

(c) Joerg Osterrieder 2025

What is Token Distribution?

Definition: The initial allocation of tokens among different stakeholder groups.

Common Allocation Categories:

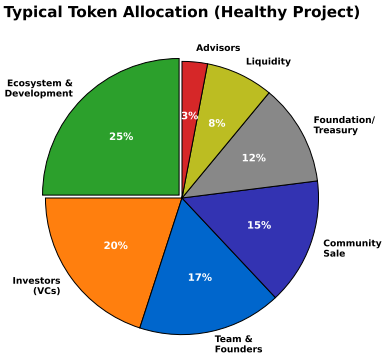
- Team and Founders / Early Investors (Seed, Series A/B/C)
- Advisors / Community Sale (ICO/IEO/IDO)
- Ecosystem Development / Liquidity Provision
- Foundation/Treasury / Airdrops

Goal: Balance early supporter rewards with long-term community alignment.

Problem: How do we reward early contributors without enabling pump-and-dump schemes? — Distribution categories balance insider rewards with community fairness

(c) Joerg Osterrieder 2025

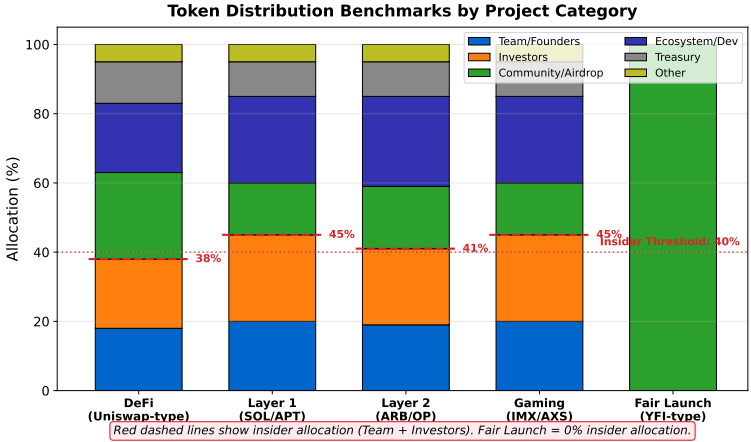
Typical Allocation Breakdown



Insiders (Team+VCs+Advisors): ~40% | Community: ~60%

Red Flag: Team + Investors ¿ 50% indicates high centralization risk

Distribution Benchmarks by Category



DeFi/L1/L2 projects allocate 38-45% to insiders; Fair Launch projects allocate 0%

Why Do Teams Lock Their Tokens for Years?

Best Practices:

- 15-20% of total supply
- 4 years minimum vesting
- 1-year cliff period
- Linear unlock after cliff

Why Long Vesting?

- Prevents insider dumps
- Demonstrates commitment
- Aligns long-term incentives
- Builds community trust

Example: 20M tokens, 1-year cliff, then 416,667 tokens/month for 48 months

(c) Joerg Osterrieder 2025

How Do Investment Rounds Differ?

Typical Investment Rounds:

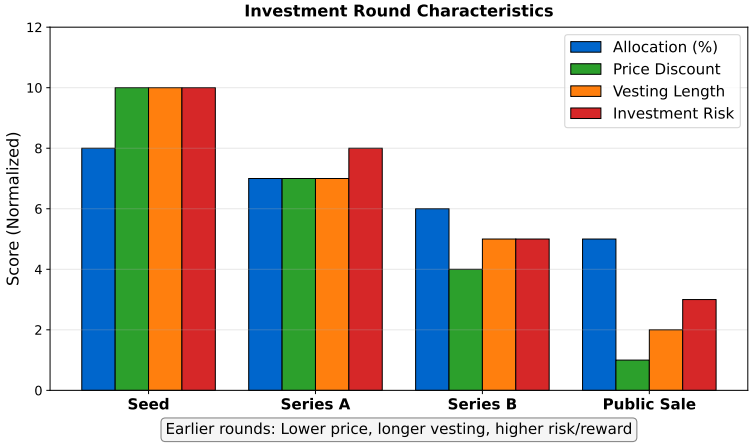
Round	Allocation	Price	Vesting
Seed	5-10%	Lowest	2-3 years
Series A	5-10%	Low	18-24 months
Series B	5-10%	Medium	12-18 months
Public Sale	10-15%	Highest	0-6 months

Key Considerations:

- Earlier investors = longer vesting
- Discount compensates for higher risk
- Too many investors = fragmented governance

(c) Joerg Osterrieder 2025

Investment Round Characteristics



Earlier rounds get bigger discounts but longer lock-ups and higher risk — Tiered vesting compensates early risk-takers while preventing immediate dumping

What Are the Different Community Sale Methods?

ICO (Initial Coin Offering, 2017 Era):

- Direct sale to public
- Minimal regulation

IEO (Initial Exchange Offering):

- On centralized exchange
- Exchange vets project

IDO (Initial DEX Offering):

- Launch on DEX (Decentralized Exchange)
- Immediate liquidity

Fair Launch:

- No pre-sale/VC rounds
- Same price for all (e.g., YFI)

How Does Vesting Work?

Definition: Schedule controlling when allocated tokens become accessible.

Key Terms:

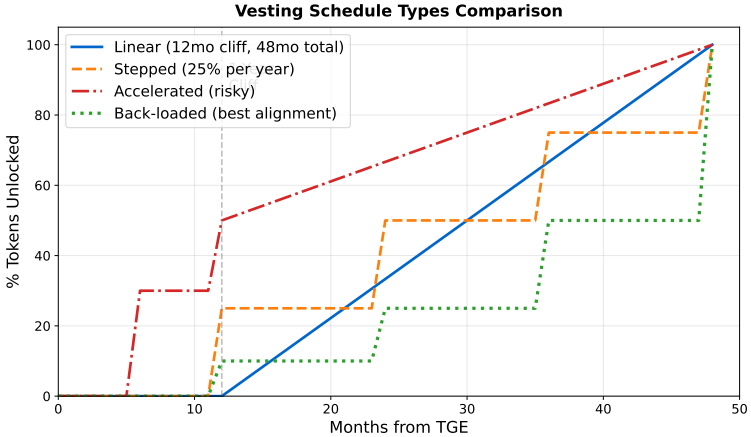
- **Cliff:** Initial wait period
- **Vesting:** Total unlock duration
- **Linear:** Equal regular unlocks
- **Unlock Event:** Transfer date

Example (1M tokens):

- Cliff: 12 months (0 unlock)
- Vesting: 48 months total
- Post-cliff: 27,778/month
- Full vest: month 48

(c) Joerg Osterrieder 2025

Vesting Schedule Types



Back-loaded vesting provides strongest long-term alignment; accelerated is risky

What's the Purpose of Cliff Periods?

Typical Durations:

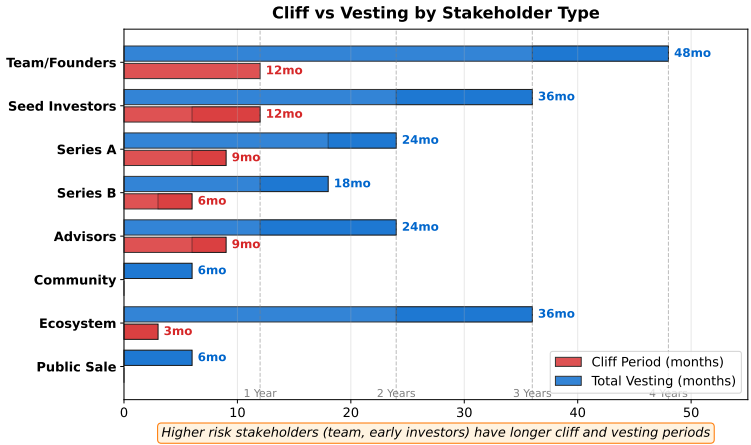
- Team: 12 months
- Investors: 6-12 months
- Advisors: 6 months
- Community: often 0

Why Use Cliffs?

- Prevents immediate dumps
- Tests commitment
- Project maturation time
- Reduces initial supply

Investor Perspective: Cliffs protect against early team departures

Cliff vs Vesting by Stakeholder



Team/founders have longest cliff (12mo) and vesting (48mo); community often has none

How Do Unlock Events Impact Price?

Market Impact:

- Increases circulating supply
- Creates selling pressure
- Price drops before/during
- Market front-runs unlocks

Types of Unlocks:

- **Cliff:** Large one-time release
- **Linear:** Monthly/daily streams
- **TGE (Token Generation Event):** Initial launch when tokens first become transferable

Tools:
Token Unlocks, Messari, CoinGecko

Problem: How do unlocks affect token price? — Predictable unlock schedules allow markets to price in selling pressure, reducing volatility

(c) Joerg Osterrieder 2025

Problem Check-In: Distribution & Vesting

Recall Our Problem

How do we fairly distribute tokens over time?

What We've Learned So Far

- Token allocation categories (team, investors, community) determine ownership concentration
- Vesting schedules with cliff periods prevent immediate insider dumps
- Structured distribution aligns incentives between early contributors and long-term community

Still to Address

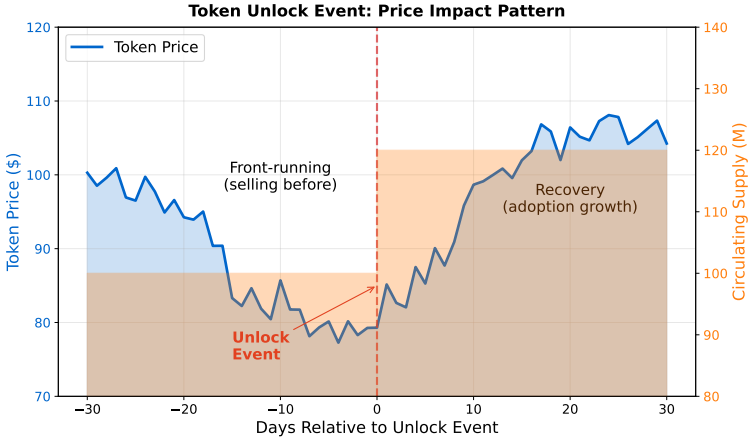
- How markets react to unlock events and strategies to manage selling pressure
- Can vesting schedules prevent all forms of insider manipulation?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

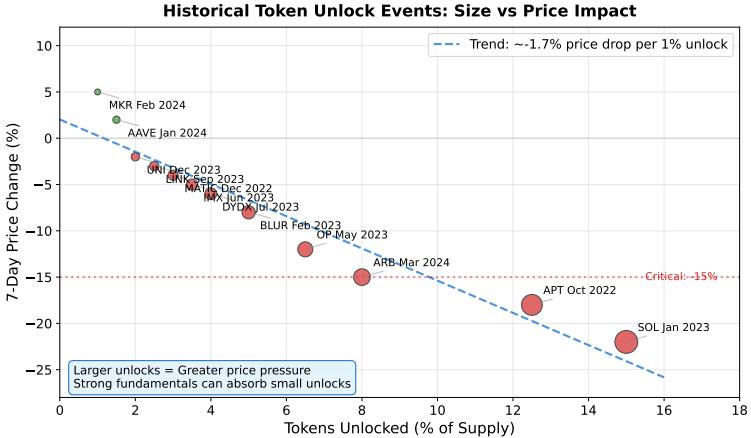
Pause and reflect: How does what we've learned so far address "How do we fairly distribute tokens over..."?

Unlock Event Price Impact



Market front-runs unlocks; price typically drops 15-20% around major events

Historical Unlock Events: Size vs Impact



Larger unlocks correlate with deeper price drops; strong projects can absorb small unlocks

What Can We Learn from Solana's Unlock Events?

Background:

- 500M SOL (to 700M by 2030)
- Major unlocks 2021-2025
- VC: a16z, Multicoin, etc.

Key Events:

- Jan 2023: 13.8M (seed)
- Mar 2023: 17.8M (early)
- Ongoing: validator unlocks

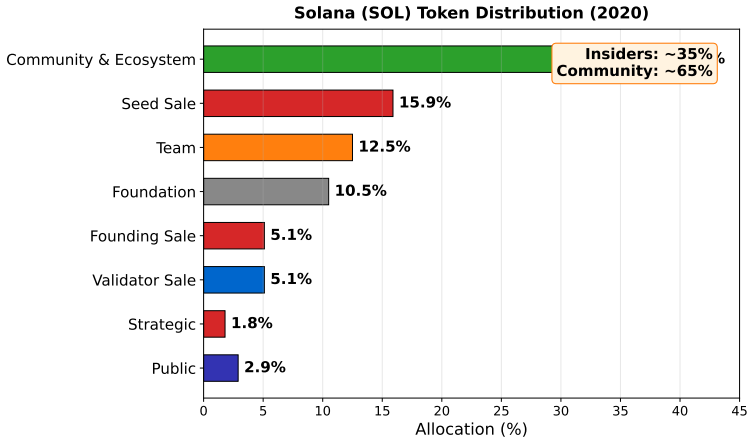
Price Impact:

- 15-20% drops at unlocks
- Long-term recovery
- Market front-runs events

Lesson:
Strong fundamentals absorb unlock pressure over time

(c) Joerg Osterrieder 2025

Solana Distribution Breakdown



Insiders 35% with long vesting helped manage dilution over time

How Can Projects Manage Unlock Pressure?

Staking Incentives:

- High yields lock tokens
- Ex: SOL 7% APY (Annual Percentage Yield—yearly return including compounding)

Gradual Unlocks:

- Daily/monthly releases
- Smooths supply shock

Lockup Extensions:

- Voluntary extra vesting
- Bonus for extended locks

Strong Fundamentals:

- Demand ¿ supply growth
- Adoption absorbs pressure

Problem: Can we mitigate unlock selling pressure? — Staking incentives, gradual releases, and strong fundamentals absorb supply shocks over time

(c) Joerg Osterrieder 2025

Why Use Airdrops for Distribution?

Airdrop Types:

- **Retroactive:** Past users (UNI)
- **Holder:** Existing holders
- **Task-based:** Actions
- **Governance:** DAO participation

Benefits:

- Bootstrap community
- Decentralize ownership
- Reward early adopters

Risks:
Hunters, immediate selling pressure

What Made Uniswap's Airdrop So Successful?

September 2020:

- 400 UNI per address
- 250,000 addresses eligible
- 150M UNI (15% supply)
- $1,200 value at claim

Impact:

- Instant decentralization
- Massive publicity
- Long-term holding
- DeFi airdrop standard

Key Insight: Retroactive airdrops reward genuine users, not speculators

What Are the Red Flags in Token Distribution?

Excessive Insiders:

- Team + VCs ¿ 50%

Short/No Vesting:

- Team vesting ¡ 2 years
- No cliff period

Opaque Distribution:

- No published allocations
- Unknown wallet holders

Centralized Control:

- Foundation ¿ 30% forever

Multiple red flags = high risk of insider dumping

What Are Points Programs and Why Are They Popular?

What are Points?

- Off-chain loyalty tracking
- Converts to tokens at TGE (Token Generation Event—the initial token launch)
- Replaces traditional airdrops

How They Work:

- Track actions (deposits, trades)
- Accumulate proportionally
- Convert at TGE

2024 Examples:

- EigenLayer: restaking
- Blast: L2 deposits
- Ethena: USDe staking

Criticism:
Opaque, favors whales, mercenary capital

(c) Joerg Osterrieder 2025

Problem Solved? Distribution & Vesting

The Original Problem

How do we fairly distribute tokens over time?

How Distribution & Vesting Solves It

- Vesting schedules with cliffs create time-locked incentive alignment
- Community airdrops with anti-sybil measures reward genuine users
- Gradual unlock schedules smooth supply shocks (daily/monthly releases)

Remaining Limitations

- Vesting can be circumvented via derivatives (token loans, synthetic positions)
- Airdrops are often farmed by professional hunters, not real users

Open Questions

- What distribution model best aligns long-term interests without creating insider advantages?
- Risk: Incentive misalignment, free-rider problems

Distribution & Vesting partially solves "we fairly distribute tokens over time" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Distribution & Vesting

Incentive Structure

- **Core Problem:** Aligning individual and collective interests
- **Why act honestly?** Rewards for honest behavior, penalties for cheating
- **Value Flow:** Protocol gains security, participants earn rewards

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium (game theory: no player benefits from unilaterally changing strategy)

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Protocol gains security, participants earn rewards

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Distribution & Vesting

Alternatives Considered

1. **Chosen Design:** Reward curves, slashing conditions
2. **Alternative:** Alternative reward mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Distribution & Vesting

Critical Failure Mode

- **What breaks:** Incentive misalignment, free-rider problems
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

The Unlock Event Panic

[COMIC: Cliff and vesting unlock panic]

A visual narrative showing the market chaos when large token unlocks approach and insiders prepare to sell

What We Learned

- Vesting with cliffs prevents immediate dumps
- Markets front-run predictable unlock events
- Staking incentives can absorb selling pressure

The Takeaway

Well-designed distribution creates alignment, but unlock events remain inevitable stress tests.

Visual synthesis: The recurring drama of token unlock calendars

(c) Joerg Osterrieder 2025

Summary

Distribution:

- Determines ownership concentration
- Healthy: Team+VCs ¡ 40%
- 3-4 year vesting standard
- Cliffs prevent immediate dumps

Next: Token Classification and Valuation

Next Lesson: L31 – Token Classification

Market Dynamics:

- Unlocks = predictable pressure
- Points replacing airdrops (2024)
- Transparency builds trust
- Check Token Unlocks first

Questions for Reflection

1. Why do early investors typically have longer vesting than public sale participants?
2. How did Solana's unlock events impact its price trajectory?
3. What are the pros and cons of retroactive airdrops vs. task-based airdrops?
4. How can a project mitigate selling pressure during major unlocks?
5. What vesting schedule would you design for a new token launch?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit for minimum duration.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%
Answer: C – Team + VCs ¿ 50% indicates high centralization risk.

Q3. Which investment round typically has the longest vesting period?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting (longest) due to earliest entry and highest risk.

Q4. What is linear vesting?
A) Tokens unlock all at once B) Equal amounts unlock at regular intervals C) Exponential unlock schedule D) Random unlock dates
Answer: B – Linear vesting releases equal token amounts monthly/daily after the cliff period.

Q5. What was the typical price impact of Solana's major unlock events?
A) 5-8% drop B) 15-20% drop C) 30-40% drop D) No impact
Answer: B – SOL dropped 15-20% around major unlocks as market front-ran selling pressure.

Quiz Questions (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance
Answer: C – Retroactive airdrops reward genuine past users (e.g., Uniswap's 400 UNI per address).

Q8. What was the value of Uniswap's airdrop per eligible address in September 2020?
A) $400 B) $800 C) $1,200 D) $2,000
Answer: C – 400 UNI per address was worth approximately $1,200 at claim time.

Q9. Which sale method involves launching directly on a decentralized exchange?
A) ICO B) IEO C) IDO D) IPO
Answer: C – IDO (Initial DEX Offering) provides immediate liquidity on decentralized exchanges.

Q10. What is a typical team allocation percentage of total token supply?
A) 5-10% B) 15-20% C) 30-40% D) 50-60%
Answer: B – Best practice is 15-20% for team allocation to balance incentives and decentralization.

Quiz Questions (11–15)

Q11. What is the primary risk of airdrops to protocols?
A) Too expensive B) Airdrop hunters and immediate selling pressure C) Legal issues D) Technical complexity
Answer: B – Airdrop hunters farm rewards without genuine interest, creating immediate sell pressure.

Q12. How many tokens unlock during a 12-month cliff period?
A) 50% of allocation B) 25% of allocation C) 10% of allocation D) 0 tokens
Answer: D – Cliff means zero tokens unlock during that period; all unlocking starts after cliff ends.

Q13. Which vesting type provides the strongest long-term alignment?
A) Linear B) Front-loaded C) Back-loaded D) Accelerated
Answer: C – Back-loaded vesting releases more tokens later, keeping incentives aligned longer.

Q14. What is TGE in token distribution?
A) Token Growth Event B) Token Generation Event C) Total Gas Estimation D) Treasury Governance Entity
Answer: B – TGE (Token Generation Event) is the initial launch with first token unlocks.

Q15. What strategy can mitigate unlock selling pressure?
A) Delete tokens B) Staking incentives with high yields C) Burn all unlocked tokens D) Ban selling
Answer: B – High staking yields incentivize holders to lock tokens instead of selling (e.g., Solana 7% APY).

Quiz Questions (16–20)

Q16. What replaced traditional airdrops as the primary distribution mechanism in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – Points programs track off-chain activity and convert to tokens at TGE (e.g., EigenLayer, Blast).

Q17. Which project is an example of a Fair Launch with no pre-sale?
A) Ethereum B) Solana C) YFI (Yearn Finance) D) Cardano
Answer: C – YFI had a fair launch where everyone bought at the same price with no VC rounds.

Q18. What percentage of Uniswap's total supply was airdropped in September 2020?
A) 5% B) 10% C) 15% D) 25%
Answer: C – Approximately 150M UNI (15% of supply) was airdropped to 250,000 addresses.

Q19. What is the recommended maximum for Foundation/Treasury holdings?
A) ¡10% B) ¡20% C) ¡30% D) ¡50%
Answer: C – Foundation holding ¿30% indefinitely is a centralization red flag.

Q20. Why do earlier investors receive longer vesting periods?
A) Regulatory requirement B) Compensates for higher risk and bigger discounts C) Technical limitation D) Random assignment
Answer: B – Early investors take highest risk, get biggest discounts, so longer vesting aligns long-term incentives.

Quiz: Distribution Vesting

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance

Quiz (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%
Answer: C – Team + VCs ¿ 50% indicates high centralization risk.

Q3. Which investment round typically has the longest vesting period?
A) Public Sale B) Series B C) Series A D) Seed

Quiz (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%
Answer: C – Team + VCs ¿ 50% indicates high centralization risk.

Q3. Which investment round typically has the longest vesting period?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting due to earliest entry and highest risk.

Q4. What was the typical price impact of Solana's major unlock events?
A) 5-8% drop B) 15-20% drop C) 30-40% drop D) No impact

Quiz (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%
Answer: C – Team + VCs ¿ 50% indicates high centralization risk.

Q3. Which investment round typically has the longest vesting period?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting due to earliest entry and highest risk.

Q4. What was the typical price impact of Solana's major unlock events?
A) 5-8% drop B) 15-20% drop C) 30-40% drop D) No impact
Answer: B – SOL dropped 15-20% around major unlocks as market front-ran selling.

Q5. What is TGE in token distribution?
A) Token Growth Event B) Token Generation Event C) Total Gas Estimation D) Treasury Governance

Quiz (1–5)

Q1. What is the primary purpose of a cliff period in token vesting?
A) Increase token price B) Ensure minimum commitment before unlocks C) Reduce gas fees D) Enable governance
Answer: B – Cliff periods prevent immediate dumping and ensure team/advisors commit.

Q2. What is considered a red flag for team and investor allocation?
A) Team 10%, VCs 20% B) Team 15%, VCs 25% C) Team 30%, VCs 25% D) Team 5%, VCs 10%
Answer: C – Team + VCs ¿ 50% indicates high centralization risk.

Q3. Which investment round typically has the longest vesting period?
A) Public Sale B) Series B C) Series A D) Seed
Answer: D – Seed investors get 2-3 years vesting due to earliest entry and highest risk.

Q4. What was the typical price impact of Solana's major unlock events?
A) 5-8% drop B) 15-20% drop C) 30-40% drop D) No impact
Answer: B – SOL dropped 15-20% around major unlocks as market front-ran selling.

Q5. What is TGE in token distribution?
A) Token Growth Event B) Token Generation Event C) Total Gas Estimation D) Treasury Governance
Answer: B – TGE (Token Generation Event) is the initial launch with first unlocks.

Quiz (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years

Quiz (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance
Answer: C – Retroactive airdrops reward genuine past users (e.g., Uniswap's 400 UNI).

Q8. What replaced traditional airdrops as primary distribution in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining

Quiz (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance
Answer: C – Retroactive airdrops reward genuine past users (e.g., Uniswap's 400 UNI).

Q8. What replaced traditional airdrops as primary distribution in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – Points programs track off-chain activity and convert to tokens at TGE.

Q9. What is linear vesting?
A) All tokens unlock at once B) Equal amounts at regular intervals C) Exponential unlock D) Random dates

Quiz (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance
Answer: C – Retroactive airdrops reward genuine past users (e.g., Uniswap's 400 UNI).

Q8. What replaced traditional airdrops as primary distribution in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – Points programs track off-chain activity and convert to tokens at TGE.

Q9. What is linear vesting?
A) All tokens unlock at once B) Equal amounts at regular intervals C) Exponential unlock D) Random dates
Answer: B – Linear vesting releases equal token amounts monthly/daily after the cliff.

Q10. What strategy can mitigate unlock selling pressure?
A) Delete tokens B) Staking incentives with high yields C) Burn unlocked tokens D) Ban selling

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the recommended minimum vesting period for team tokens?
A) 6 months B) 1 year C) 2 years D) 4 years
Answer: D – Best practice is 4 years minimum for team tokens to ensure long-term alignment.

Q7. Which airdrop type rewards past users who already used the protocol?
A) Task-based B) Holder airdrop C) Retroactive D) Governance
Answer: C – Retroactive airdrops reward genuine past users (e.g., Uniswap's 400 UNI).

Q8. What replaced traditional airdrops as primary distribution in 2024?
A) ICOs B) Points programs C) NFT drops D) Mining
Answer: B – Points programs track off-chain activity and convert to tokens at TGE.

Q9. What is linear vesting?
A) All tokens unlock at once B) Equal amounts at regular intervals C) Exponential unlock D) Random dates
Answer: B – Linear vesting releases equal token amounts monthly/daily after the cliff.

Q10. What strategy can mitigate unlock selling pressure?
A) Delete tokens B) Staking incentives with high yields C) Burn unlocked tokens D) Ban selling
Answer: B – High staking yields incentivize holders to lock instead of selling.

(c) Joerg Osterrieder 2025

L31: Token Classification and Valuation

Mini-Lecture – Module D: Tokenomics

Blockchain & Cryptocurrency Course

January 2026

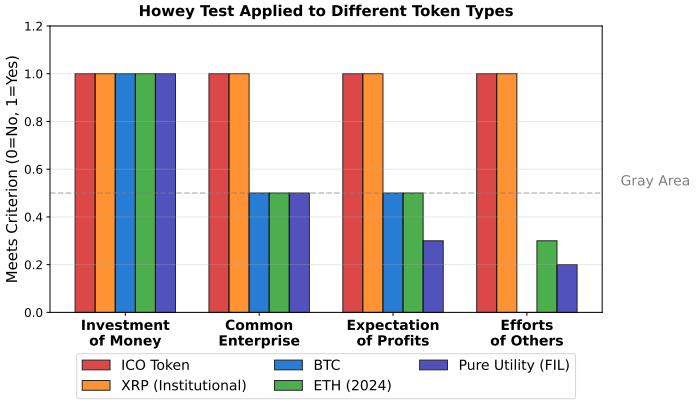
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Apply the Howey Test to classify tokens as securities
- Distinguish between utility and security tokens
- Apply valuation frameworks (NVT, Metcalfe, DCF)
- Analyze SEC vs. Ripple case precedent

Howey Test Applied to Tokens



All four criteria must be met for classification as a security.

The Howey Test (1946)

An investment is a security if it involves:

1. **Investment of Money** – Investors provide capital
2. **Common Enterprise** – Pooled funds or shared outcome
3. **Expectation of Profits** – Investors seek financial return
4. **Efforts of Others** – Profits depend on promoter/third party

Utility vs Security:

- **Utility Token:** Access to product/service, fails "efforts of others" (BNB, FIL)
- **Security Token:** Investment contract, meets all four criteria

BTC/ETH: Sufficiently decentralized to avoid "efforts of others."

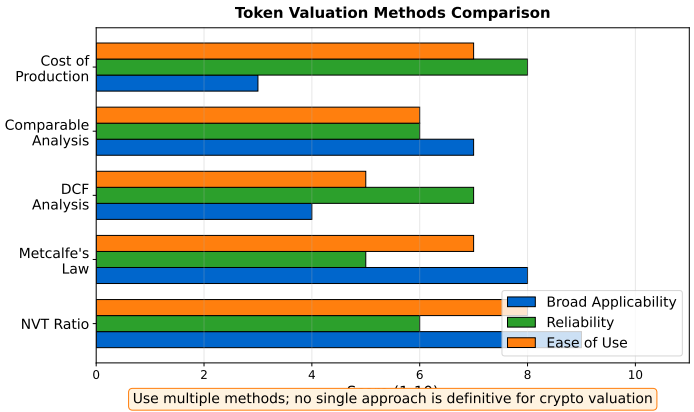
Case Study: SEC vs. Ripple (July 2023)

Key Ruling (Judge Torres):

1. **Institutional Sales = Securities**
   - XRP sold to VCs/hedge funds = securities
   - Buyers expected profits from Ripple's efforts
2. **Programmatic Sales (Exchanges) = NOT Securities**
   - XRP on public exchanges = not securities
   - Buyers didn't know they bought from Ripple

Precedent: Context of sale matters – first major ruling distinguishing sale types.

Token Valuation Methods



NVT: Most widely applicable — **DCF:** Only for yield-generating tokens

Network Value to Transactions (NVT)

Formula:

$$\text{NVT Ratio} = \frac{\text{Market Cap}}{\text{Daily Transaction Volume}}$$

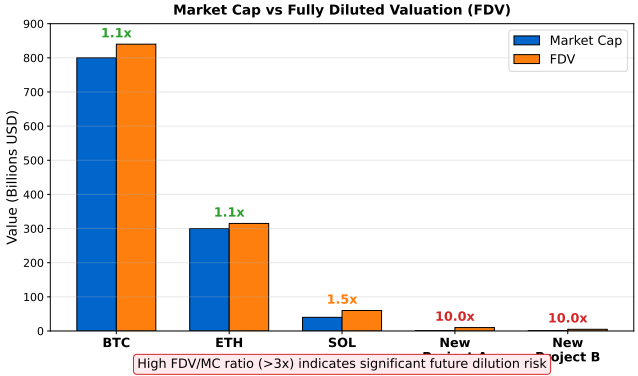
Interpretation (similar to P/E ratio):

- High NVT = Overvalued relative to usage
- Low NVT = Undervalued or high utility

Typical Ranges:

- BTC: 50-100 (store of value, not payment)
- ETH: 20-40 (more transactional)
- Payment tokens: <20 (high tx volume)

Market Cap vs Fully Diluted Valuation



Large FDV/MC ratio (10x+): Massive future dilution risk from unlocks.

Key Valuation Formulas

Market Cap:

$$\text{Market Cap} = \text{Price} \times \text{Circulating Supply}$$

Fully Diluted Valuation (FDV):

$$\text{FDV} = \text{Price} \times \text{Total Supply (Max)}$$

Metcalfe's Law:

$$V \propto n^2 \quad \text{(Network value grows with users squared)}$$

DCF (for staking tokens):

$$\text{Value} = \frac{\text{Annual Staking Reward}}{\text{Discount Rate}}$$

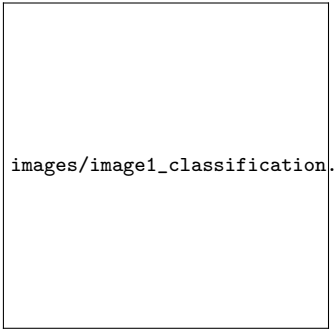
Example: \$100 reward / 10% = \$1,000 value

Key Takeaways

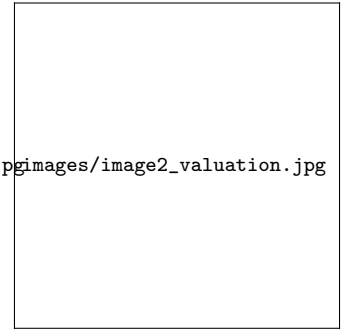
1. **Howey Test:** 4 criteria determine security classification
2. **Ripple Precedent:** Context of sale matters (institutional vs exchange)
3. **NVT Ratio:** High = overvalued, Low = high utility
4. **FDV Warning:** FDV/MC ratio >2 indicates high dilution risk
5. **Multiple Methods:** Crypto valuation is imprecise, use several approaches

BTC/ETH: Sufficiently decentralized – avoid "efforts of others" criterion.

Token Classification in Practice



Classification



Valuation

Metrics

Images: Unsplash (CC0)

Quiz (1/2)

Q1. How many Howey Test criteria must be met for a security?
A) Two B) Three C) Four D) Five

Quiz (1/2)

Q1. How many Howey Test criteria must be met for a security?
A) Two B) Three C) Four D) Five
Answer: C – All four must be met.

Q2. Which Howey criterion do BTC and ETH largely avoid?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others

Quiz (1/2)

Q1. How many Howey Test criteria must be met for a security?
A) Two B) Three C) Four D) Five
Answer: C – All four must be met.

Q2. Which Howey criterion do BTC and ETH largely avoid?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others
Answer: D – Sufficiently decentralized.

Q3. In SEC vs Ripple, which sales were ruled securities?
A) All sales B) Institutional sales to VCs
C) Exchange sales D) Employee compensation

Quiz (1/2)

Q1. How many Howey Test criteria must be met for a security?
A) Two B) Three C) Four D) Five
Answer: C – All four must be met.

Q2. Which Howey criterion do BTC and ETH largely avoid?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others
Answer: D – Sufficiently decentralized.

Q3. In SEC vs Ripple, which sales were ruled securities?
A) All sales B) Institutional sales to VCs
C) Exchange sales D) Employee compensation
Answer: B – Institutional sales met Howey criteria.

Q4. What is the typical NVT ratio for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200

Quiz (1/2)

Q1. How many Howey Test criteria must be met for a security?
A) Two B) Three C) Four D) Five
Answer: C – All four must be met.

Q2. Which Howey criterion do BTC and ETH largely avoid?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others
Answer: D – Sufficiently decentralized.

Q3. In SEC vs Ripple, which sales were ruled securities?
A) All sales B) Institutional sales to VCs
C) Exchange sales D) Employee compensation
Answer: B – Institutional sales met Howey criteria.

Q4. What is the typical NVT ratio for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – Store of value, not payment.

Q5. What does a high NVT ratio indicate?
A) Undervalued B) Overvalued relative to usage
C) High transaction volume D) Low market cap

Quiz (1/2)

Q1. How many Howey Test criteria must be met for a security?
A) Two B) Three C) Four D) Five
Answer: C – All four must be met.

Q2. Which Howey criterion do BTC and ETH largely avoid?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others
Answer: D – Sufficiently decentralized.

Q3. In SEC vs Ripple, which sales were ruled securities?
A) All sales B) Institutional sales to VCs
C) Exchange sales D) Employee compensation
Answer: B – Institutional sales met Howey criteria.

Q4. What is the typical NVT ratio for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – Store of value, not payment.

Q5. What does a high NVT ratio indicate?
A) Undervalued B) Overvalued relative to usage
C) High transaction volume D) Low market cap
Answer: B – Similar to high P/E ratio.

Quiz (2/2)

Q6. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value

Quiz (2/2)

Q6. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – Price $\times$ Total Supply (Max).

Q7. FDV/MC ratio $>$2 indicates:
A) Undervaluation B) High circulation
C) Future dilution risk D) Low token price

Quiz (2/2)

Q6. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – Price $\times$ Total Supply (Max).

Q7. FDV/MC ratio >2 indicates:
A) Undervaluation B) High circulation
C) Future dilution risk D) Low token price
Answer: C – Significant unlocks ahead.

Q8. According to Metcalfe's Law, network value grows with:
A) Linearly (n) B) Logarithmically C) Squared (n^2) D) Exponentially

Quiz (2/2)

Q6. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – Price $\times$ Total Supply (Max).

Q7. FDV/MC ratio $>$2 indicates:
A) Undervaluation B) High circulation
C) Future dilution risk D) Low token price
Answer: C – Significant unlocks ahead.

Q8. According to Metcalfe's Law, network value grows with:
A) Linearly (n) B) Logarithmically C) Squared (n^2) D) Exponentially
Answer: C – $V \propto n^2$.

Q9. What percentage of XRP does Ripple hold?
A) 10% B) 25% C) 50% D) 75%

Quiz (2/2)

Q6. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – Price $\times$ Total Supply (Max).

Q7. FDV/MC ratio >2 indicates:
A) Undervaluation B) High circulation
C) Future dilution risk D) Low token price
Answer: C – Significant unlocks ahead.

Q8. According to Metcalfe's Law, network value grows with:
A) Linearly (n) B) Logarithmically C) Squared (n^2) D) Exponentially
Answer: C – $V \propto n^2$.

Q9. What percentage of XRP does Ripple hold?
A) 10% B) 25% C) 50% D) 75%
Answer: C – Key factor in SEC case.

Q10. DCF (perpetuity): $100 annual reward, 10% discount rate = ?
A) $100 B) $500 C) $1,000 D) $10,000

Quiz (2/2)

Q6. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – Price $\times$ Total Supply (Max).

Q7. FDV/MC ratio >2 indicates:
A) Undervaluation B) High circulation
C) Future dilution risk D) Low token price
Answer: C – Significant unlocks ahead.

Q8. According to Metcalfe's Law, network value grows with:
A) Linearly (n) B) Logarithmically C) Squared (n^2) D) Exponentially
Answer: C – $V \propto n^2$.

Q9. What percentage of XRP does Ripple hold?
A) 10% B) 25% C) 50% D) 75%
Answer: C – Key factor in SEC case.

Q10. DCF (perpetuity): $100 annual reward, 10% discount rate = ?
A) $100 B) $500 C) $1,000 D) $10,000
Answer: C – $100 / 0.10 = $1,000.

Thank you

Questions?

Next: L32 Lab – Tokenomics Analysis

L31: Token Classification and Valuation

Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Apply the Howey Test to classify tokens as securities
- Distinguish between utility and security tokens
- Apply valuation frameworks to crypto assets
- Analyze network value metrics (NVT, Metcalfe)
- Case Study: SEC vs. Ripple

The Problem: When is a token a security?

The Challenge
Token creators and investors face legal uncertainty: launching a token could trigger securities regulations with severe penalties, but the classification rules are ambiguous. The same token might be a security in one jurisdiction but not another, or treated differently based on how it's sold.

Why It Matters

- Misclassification leads to SEC enforcement, delisting, and $1B+ penalties (e.g., Ripple case)
- ICO boom (2017-2018) resulted in 80% of projects facing regulatory scrutiny

What We Need

- Risk management and mitigation
- Clear legal framework distinguishing securities from utility tokens

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Token Classification addresses this challenge

Why Classification Matters

Regulatory Implications:

- Securities require registration with SEC (in US)
- Investor protections apply
- Trading restrictions (accredited investors only)
- Disclosure requirements

Market Implications:

- Exchange listings (securities can't list on most exchanges)
- Global accessibility
- Tax treatment

Bottom Line: Misclassification can lead to enforcement actions, delisting, and legal penalties.

The Howey Test (1946)

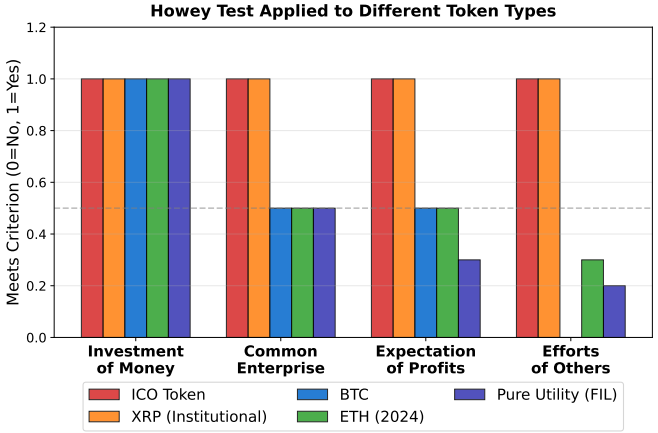
Origin: SEC v. W.J. Howey Co. (Supreme Court case)

An investment is a security if it involves:

1. **Investment of Money** - Investors provide capital
2. **In a Common Enterprise** - Pooled funds or shared outcome
3. **With Expectation of Profits** - Investors seek financial return
4. **Derived from Efforts of Others** - Profits depend on promoter/third party work

All four criteria must be met for classification as a security.

Howey Test Applied to Tokens



BTC and ETH largely avoid "efforts of others" due to decentralization

Utility vs. Security Tokens

Utility Token

- Access to product/service
- Not marketed as investment
- Value from usage, not speculation
- Examples: BNB, FIL

Howey Test:

- Fails “efforts of others” if decentralized

Security Token

- Investment contract
- Promise of profits
- Centralized management
- Examples: Tokenized stocks

Howey Test:

- Meets all four criteria

Reality: Most tokens exist on a spectrum, not binary classification.

Case Study: SEC vs. Ripple

Background:

- Ripple Labs created XRP (2012)
- Used for cross-border payments
- Ripple holds 50% of XRP supply
- $1.3B raised from XRP sales (2013-2020)

SEC Complaint (Dec 2020):

- XRP is an unregistered security
- Ripple raised funds through illegal securities offering

Ripple's Defense:

- XRP is a currency, not a security
- Network is decentralized (1,000+ validators)

Ripple Case: Ruling (July 2023)

Judge Torres Decision - Partial Victory for Ripple:

1. **Institutional Sales = Securities**
   - XRP sold to VCs/hedge funds = securities
   - Buyers had expectation of profits from Ripple's efforts
2. **Programmatic Sales (Exchanges) = NOT Securities**
   - XRP sold on public exchanges = not securities
   - Buyers didn't know they were buying from Ripple
3. **Employee Compensation = NOT Securities**

Impact: First major ruling that distinguished sale context matters.

Token Valuation Challenges

Why Traditional Valuation is Hard:

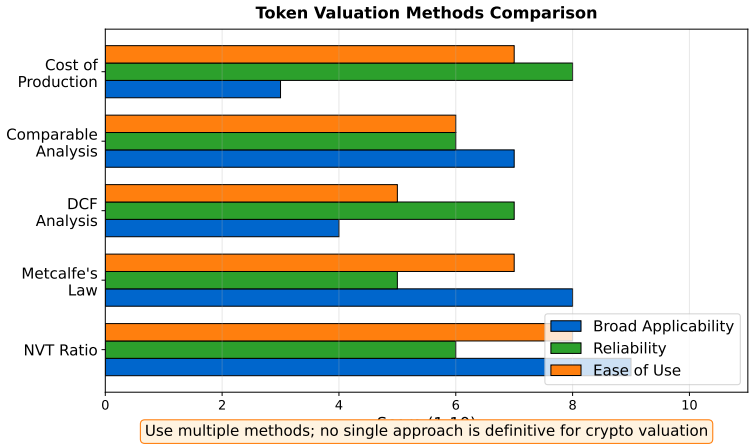
- No cash flows (most tokens)
- No earnings or revenue
- No tangible assets
- Highly speculative markets
- Network effects hard to quantify

Approaches:

1. Network Value to Transactions (NVT)
2. Metcalfe's Law
3. Discounted Cash Flow (DCF) - for productive assets
4. Comparable Analysis
5. Cost of Production (mining)

(c) Joerg Osterrieder 2025

Valuation Methods Comparison



NVT is most widely applicable; DCF only works for yield-generating tokens

Network Value to Transactions (NVT)

Formula:

$$\text{NVT Ratio} = \frac{\text{Market Cap}}{\text{Daily Transaction Volume}}$$

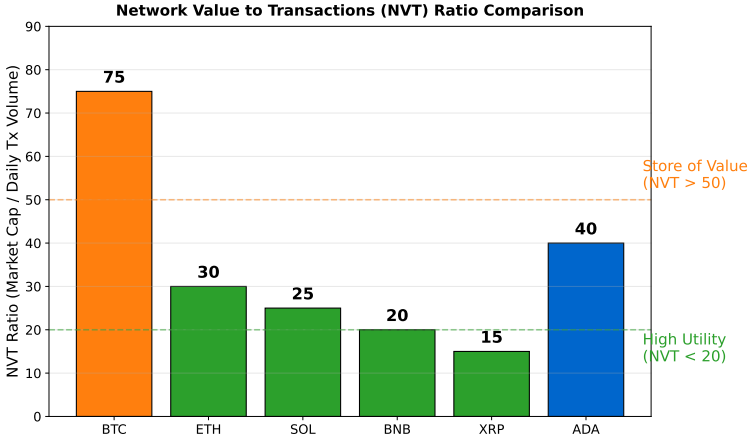
Interpretation:

- Similar to P/E ratio in stocks
- High NVT = overvalued relative to usage
- Low NVT = undervalued or high utility

Typical Ranges:

- BTC: 50-100 (higher = store of value, not payment)
- ETH: 20-40 (more transactional)
- Payment tokens: ¡20 (high transaction volume)

NVT Ratio Comparison



BTC's high NVT reflects store-of-value use; lower NVT indicates payment utility

Metcalfe's Law

Concept: Network value grows with the square of the number of users.

Formula:

$$V \propto n^2$$

where V = network value, n = number of users.

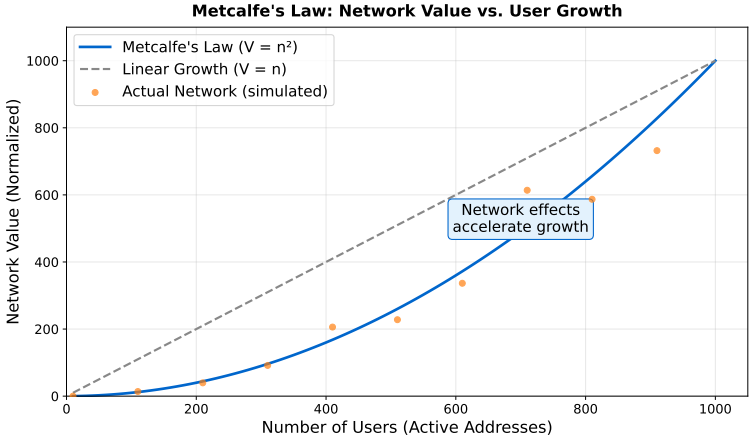
Application to Crypto:

- More users = exponentially more connections
- Active addresses proxy for n
- Studies show BTC/ETH follow Metcalfe's Law loosely

Limitations:

- Not all users create equal value
- Doesn't account for quality of usage

Metcalfe's Law Visualization



Network effects create exponential value growth as user count increases

Discounted Cash Flow (DCF)

When to Use: Tokens with cash flow generation (staking rewards, fee sharing).

Formula:

$$\text{Value} = \sum_{t=1}^{n} \frac{\text{CF}_t}{(1+r)^t}$$

where CF_t = cash flow in year t, r = discount rate.

Example: Staking Token

- Expected annual staking reward: \$100
- Discount rate: 10%
- Perpetual reward assumption

$$\text{Value} = \frac{100}{0.10} = \$1,000$$

Market Cap vs. Fully Diluted Valuation

Market Cap:

$$\text{Market Cap} = \text{Price} \times \text{Circulating Supply}$$

Fully Diluted Valuation (FDV):

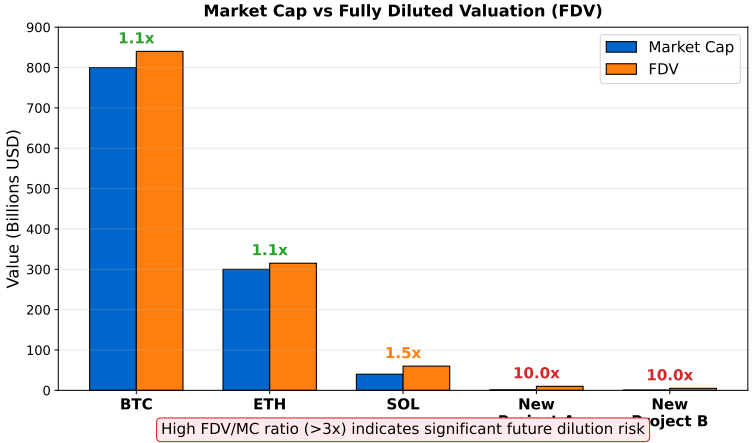
$$\text{FDV} = \text{Price} \times \text{Total Supply (Max)}$$

Example:

- Token price: \$10, Circulating: 100M, Total: 1B
- Market Cap: \$1B
- FDV: \$10B

Warning: Large FDV/MC ratio indicates future dilution risk.

Market Cap vs FDV Comparison



New projects often have 10x+ FDV/MC ratio indicating massive dilution ahead

Token Valuation Checklist

Step-by-Step Analysis:

1. Determine token type and purpose (utility, governance, etc.)
2. Check regulatory status (security vs. non-security)
3. Calculate NVT ratio (compare to peers)
4. Analyze on-chain metrics (addresses, transactions, TVL)
5. Review tokenomics (supply, inflation, unlock schedule)
6. Compare market cap to fundamentals (revenue, usage)
7. Assess FDV vs. Market Cap (dilution risk)

Output: Informed estimate of fair value range (not precise number).

(c) Joerg Osterrieder 2025

Problem Solved? Token Classification

The Original Problem

When is a token a security?

How Token Classification Solves It

- Howey Test provides four-criteria framework: investment of money, common enterprise, expectation of profits, efforts of others
- FINMA taxonomy distinguishes payment, utility, and asset tokens based on economic function
- Context matters: Ripple ruling showed same token can be security (institutional sales) or not (exchange sales)

Remaining Limitations

- Regulatory uncertainty persists: no global standard, jurisdiction shopping common (Switzerland, Singapore)
- Gray area tokens (hybrid utility/governance) still lack clear classification

Open Questions

- Will MiCA (EU) and international coordination lead to regulatory harmonization by 2030?
- Risk: Black swan events (e.g., major exchange listing security unknowingly), cascading enforcement actions

Token Classification partially solves "When is a token a security" but introduces new trade-offs

Summary

Key Takeaways:

- Howey Test determines security classification (4 criteria)
- Context of sale matters (Ripple case precedent)
- NVT ratio helps assess value relative to transaction volume
- Metcalfe's Law suggests network value grows with users squared
- DCF applicable only to tokens with cash flows
- Comparable analysis useful for relative valuation
- Always compare Market Cap to FDV (dilution risk)
- Crypto valuation is imprecise - use multiple methods

Questions for Reflection

1. Apply the Howey Test to a token you're familiar with. Is it a security?
2. Why did the Ripple ruling distinguish between institutional and exchange sales?
3. Calculate the NVT ratio for Bitcoin and Ethereum. What does it tell you?
4. What are the limitations of using Metcalfe's Law for token valuation?
5. How would you value a governance token with no direct cash flows?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. How many criteria must be met under the Howey Test for an asset to be classified as a security?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria (investment of money, common enterprise, expectation of profits, efforts of others) must be met.

Q2. Which of the following is NOT one of the four Howey Test criteria?
A) Investment of money B) Common enterprise C) Government approval D) Efforts of others
Answer: C – Government approval is not part of the Howey Test. The four criteria are: investment of money, common enterprise, expectation of profits, and efforts of others.

Q3. What was the key distinction in the SEC vs. Ripple ruling (July 2023)?
A) All XRP sales were securities B) No XRP sales were securities
C) Context of sale matters (institutional vs. exchange) D) Ripple was completely acquitted
Answer: C – Judge Torres ruled that institutional sales were securities, but programmatic exchange sales were not, establishing that sale context matters.

Q4. What percentage of XRP supply does Ripple Labs hold?
A) 10% B) 25% C) 50% D) 75%
Answer: C – Ripple holds approximately 50% of the XRP supply, which was a key factor in the SEC's case.

Q5. According to the lesson, which tokens are examples of utility tokens?
A) BTC and ETH B) BNB and FIL C) XRP and ADA D) Tokenized stocks
Answer: B – BNB (Binance Coin) and FIL (Filecoin) are cited as examples of utility tokens providing access to products/services.

Quiz Questions (6–10)

Q6. What does NVT stand for in token valuation?
A) Network Value Total B) Network Value to Transactions
C) Net Value Transfer D) New Value Token
Answer: B – NVT stands for Network Value to Transactions, calculated as Market Cap divided by Daily Transaction Volume.

Q7. What is the typical NVT ratio range for Bitcoin according to the lesson?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – BTC typically has an NVT ratio of 50-100, reflecting its primary use as a store of value rather than for payments.

Q8. According to Metcalfe's Law, how does network value grow with the number of users?
A) Linearly (n) B) Logarithmically ($\log n$) C) Squared (n^2) D) Exponentially (e^n)
Answer: C – Metcalfe's Law states that network value is proportional to the square of the number of users ($V \propto n^2$).

Q9. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage
C) High transaction volume D) Low market capitalization
Answer: B – A high NVT ratio suggests the token is overvalued relative to its transaction volume (similar to a high P/E ratio in stocks).

Q10. Which valuation method is most appropriate for tokens with staking rewards?
A) NVT Ratio B) Metcalfe's Law C) Discounted Cash Flow (DCF) D) Cost of Production
Answer: C – DCF is suitable for tokens with cash flow generation, such as staking rewards or fee sharing.

Quiz Questions (11–15)

Q11. What is the formula for Market Cap?
A) Price $\times$ Total Supply B) Price $\times$ Circulating Supply
C) Price $\div$ Circulating Supply D) Total Supply $\times$ FDV
Answer: B – Market Cap = Price $\times$ Circulating Supply (only tokens currently in circulation).

Q12. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – FDV stands for Fully Diluted Valuation, calculated as Price $\times$ Total Supply (maximum).

Q13. A large FDV/Market Cap ratio indicates:
A) Undervaluation B) High current circulation C) Future dilution risk D) Low token price
Answer: C – A high FDV/MC ratio (e.g., 10x+) indicates significant future dilution risk as locked tokens are released.

Q14. Which Howey Test criterion do Bitcoin and Ethereum largely avoid due to decentralization?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others
Answer: D – BTC and ETH are sufficiently decentralized that profits do not primarily depend on the "efforts of others".

Q15. What is a key limitation of using Metcalfe's Law for crypto valuation?
A) It requires cash flow data B) Not all users create equal value
C) It only applies to Bitcoin D) It ignores market capitalization
Answer: B – Metcalfe's Law doesn't account for the quality of usage or the fact that not all users create equal value in the network.

Quiz Questions (16–20)

Q16. In the Ripple case, which type of XRP sales were ruled as securities?
A) All sales B) Institutional sales to VCs and hedge funds
C) Programmatic sales on exchanges D) Employee compensation
Answer: B – Institutional sales to VCs/hedge funds were ruled as securities because buyers had expectation of profits from Ripple's efforts.

Q17. What regulatory requirement applies if a token is classified as a security in the US?
A) Mining permit B) Registration with SEC C) Blockchain audit D) Federal tax exemption
Answer: B – Securities require registration with the SEC, along with investor protections and disclosure requirements.

Q18. If a staking token provides $100 annual rewards with a 10% discount rate (perpetual), what is its DCF value?
A) $100 B) $500 C) $1,000 D) $10,000
Answer: C – Using the perpetuity formula: Value = $100 / 0.10 = $1,000.

Q19. What is the typical NVT ratio range for payment-focused tokens?
A) <20 B) 20-40 C) 50-100 D) >100
Answer: A – Payment tokens typically have NVT < 20 due to high transaction volume relative to market cap.

Q20. Which statement best describes token valuation in crypto?
A) Always use DCF exclusively B) NVT ratio provides precise fair value
C) Use multiple methods; valuation is imprecise D) Market cap alone determines value
Answer: C – Crypto valuation is imprecise and requires using multiple methods (NVT, Metcalfe, DCF, comparables) to estimate a fair value range.

L31: Token Classification and Valuation

Module D: Tokenomics

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Apply the Howey Test to classify tokens as securities
- Distinguish between utility and security tokens
- Apply valuation frameworks to crypto assets
- Analyze network value metrics (NVT, Metcalfe)
- Case Study: SEC vs. Ripple

Building on L30: Distribution and Vesting

The Classification Anxiety

[COMIC: Is it a security? anxiety]

A visual narrative showing founders nervously wondering if regulators will classify their token as a security

What This Illustrates

- Token classification determines legal fate
- Securities face strict regulations and penalties
- The line between utility and security is blurry

The Question

How do we know when a token crosses the line into securities territory?

Visual framing: The regulatory uncertainty haunting token creators

The Problem: When is a token a security?

The Challenge
Token creators and investors face legal uncertainty: launching a token could trigger securities regulations with severe penalties, but the classification rules are ambiguous. The same token might be a security in one jurisdiction but not another, or treated differently based on how it's sold.

Why It Matters

- Misclassification leads to SEC enforcement, delisting, and $1B+ penalties (e.g., Ripple case)
- ICO boom (2017-2018) resulted in 80% of projects facing regulatory scrutiny

What We Need

- Risk management and mitigation
- Clear legal framework distinguishing securities from utility tokens

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Token Classification addresses this challenge

Why Does Token Classification Matter?

Regulatory Implications:

- Securities require registration with SEC (in US)
- Investor protections apply
- Trading restrictions (accredited investors only)
- Disclosure requirements

Market Implications:

- Exchange listings (securities can't list on most exchanges)
- Global accessibility
- Tax treatment

Bottom Line: Misclassification can lead to enforcement actions, delisting, and legal penalties.

Problem: What happens if you misclassify a token? — Securities violations trigger SEC enforcement, exchange delisting, and multi-billion dollar penalties

What Is the Howey Test?

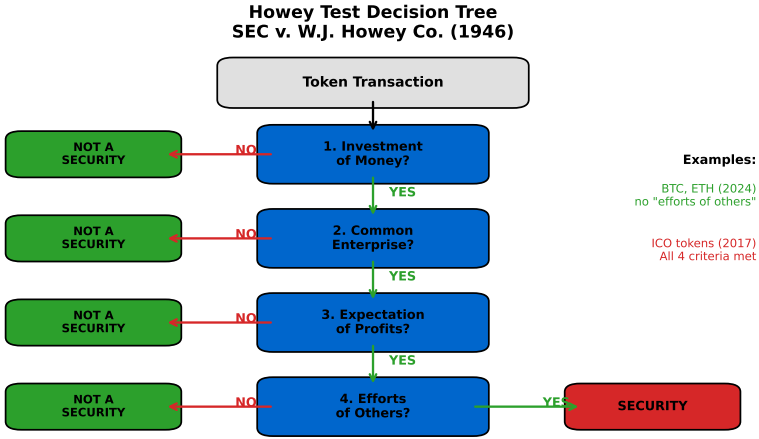
Origin: SEC v. W.J. Howey Co. (Supreme Court case)

An investment is a security if it involves:

1. **Investment of Money** - Investors provide capital
2. **In a Common Enterprise** - Pooled funds with shared economic outcome (investors' fortunes tied together)
3. **With Expectation of Profits** - Investors seek financial return
4. **Derived from Efforts of Others** - Profits depend on promoter/third party work

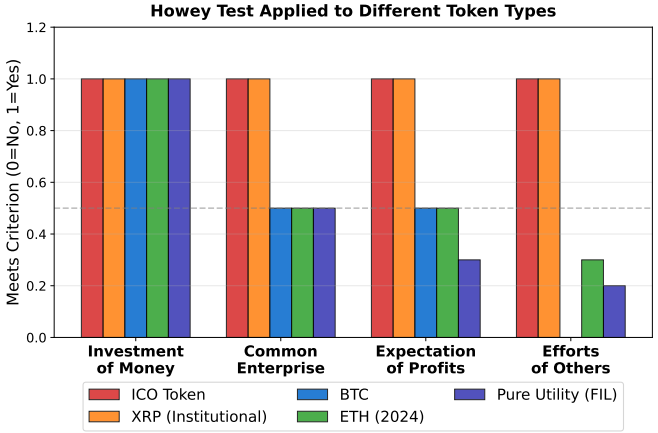
All four criteria must be met for classification as a security.

Howey Test Decision Tree



If ANY criterion fails, the token is NOT a security. All four must be met.

Howey Test Applied to Tokens



BTC and ETH largely avoid "efforts of others" due to decentralization

How Do Utility Tokens Differ from Security Tokens?

Utility Token

- Access to product/service
- Not marketed as investment
- Value from usage, not speculation
- Examples: BNB, FIL

Howey Test:

- Fails "efforts of others" if decentralized

Security Token

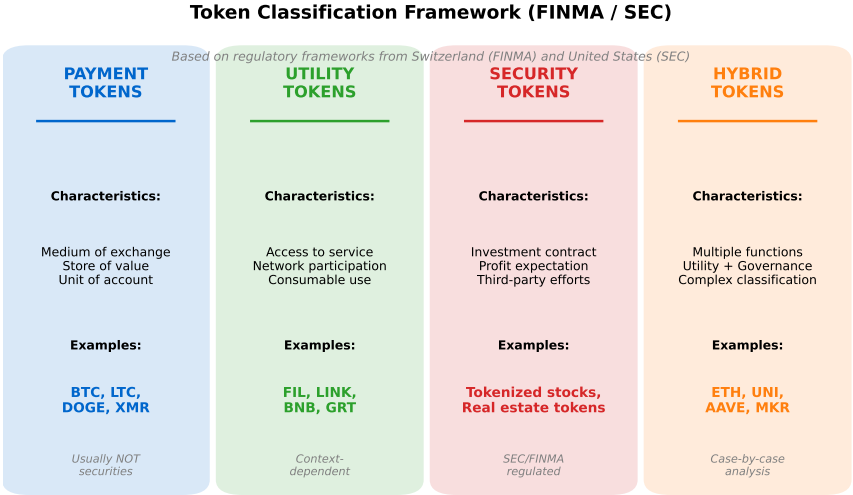
- Investment contract
- Promise of profits
- Centralized management
- Examples: Tokenized stocks

Howey Test:

- Meets all four criteria

Reality: Most tokens exist on a spectrum, not binary classification.

Token Classification Framework



FINMA/SEC taxonomy: Payment, Utility, Security, and Hybrid tokens have distinct regulatory treatment

What Did the Ripple Case Reveal About Classification?

Background:

- Ripple Labs created XRP (2012)
- Used for cross-border payments
- Ripple holds 50% of XRP supply
- $1.3B raised from XRP sales (2013-2020)

SEC Complaint (Dec 2020):

- XRP is an unregistered security
- Ripple raised funds through illegal securities offering

Ripple's Defense:

- XRP is a currency, not a security
- Network is decentralized (1,000+ validators)

Problem: Can the same token be both a security and not a security? — The Ripple case shows context of sale determines classification, not the token itself

What Was the Ripple Verdict?

Judge Torres Decision - Partial Victory for Ripple:

1. **Institutional Sales = Securities**
   - XRP sold to VCs/hedge funds = securities
   - Buyers had expectation of profits from Ripple's efforts
2. **Programmatic Sales (Exchanges) = NOT Securities**
   - XRP sold on public exchanges = not securities
   - Buyers didn't know they were buying from Ripple
3. **Employee Compensation = NOT Securities**

Impact: First major ruling that distinguished sale context matters.

Why Is Token Valuation So Difficult?

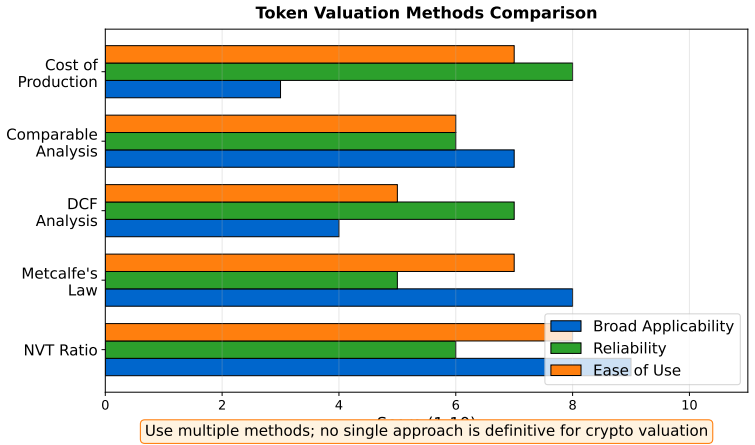
Why Traditional Valuation is Hard:

- No cash flows (most tokens)
- No earnings or revenue
- No tangible assets
- Highly speculative markets
- Network effects hard to quantify

Approaches:

1. Network Value to Transactions (NVT)
2. Metcalfe's Law
3. Discounted Cash Flow (DCF) - for productive assets
4. Comparable Analysis
5. Cost of Production (mining)

Valuation Methods Comparison



NVT is most widely applicable; DCF only works for yield-generating tokens

Problem Check-In: Token Classification

Recall Our Problem

When is a token a security?

What We've Learned So Far

- The Howey Test uses four criteria to determine if an asset is a security
- Utility tokens avoid "efforts of others" criterion through sufficient decentralization
- Classification determines regulatory requirements, exchange access, and legal risk

Still to Address

- Valuation frameworks (NVT, Metcalfe's Law, DCF) for pricing tokens
- How do we value tokens with no cash flows and no comparable assets?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "When is a token a security?"?

How Does NVT Ratio Work?

Formula:

$$\text{NVT Ratio} = \frac{\text{Market Cap}}{\text{Daily Transaction Volume}}$$

Interpretation:

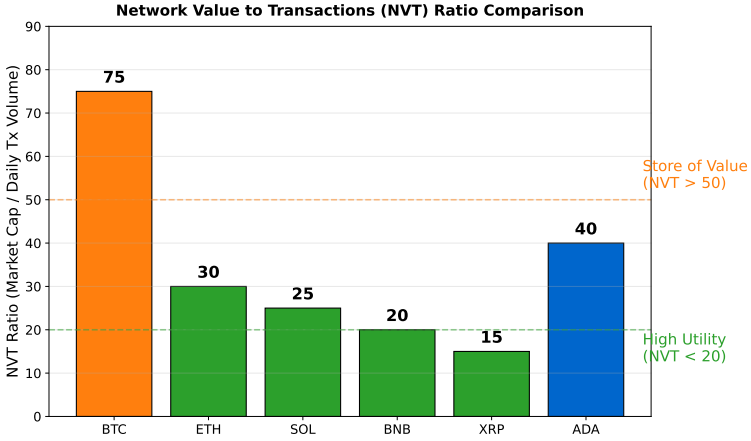
- Similar to P/E ratio in stocks
- High NVT = overvalued relative to usage
- Low NVT = undervalued or high utility

Typical Ranges:

- BTC: 50-100 (higher = store of value, not payment)
- ETH: 20-40 (more transactional)
- Payment tokens: ¡20 (high transaction volume)

Problem: How do we value tokens that generate no cash flows? — NVT ratio compares market cap to usage, providing relative valuation like P/E ratios for stocks

NVT Ratio Comparison



BTC's high NVT reflects store-of-value use; lower NVT indicates payment utility

What Does Metcalfe's Law Tell Us About Network Value?

Concept: Network value grows with the square of the number of users.

Formula:

$$V \propto n^2$$

where V = network value, n = number of users.

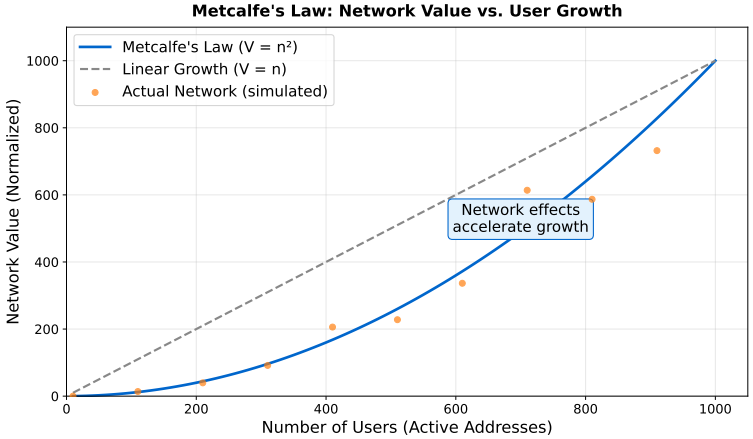
Application to Crypto:

- More users = exponentially more connections
- Active addresses proxy for n
- Studies show BTC/ETH follow Metcalfe's Law loosely

Limitations:

- Not all users create equal value
- Doesn't account for quality of usage

Metcalfe's Law Visualization



Network effects create exponential value growth as user count increases

When Can We Use DCF for Token Valuation?

When to Use: Tokens with cash flow generation (staking rewards, fee sharing).

Note: If you've taken corporate finance, DCF is familiar. If not, think of it as calculating "what is a future stream of payments worth today, accounting for the time value of money?"

Formula:

$$\text{Value} = \sum_{t=1}^{n} \frac{\text{CF}_t}{(1+r)^t}$$

where CF_t = cash flow in year t, r = discount rate.

Example: Staking Token

- Expected annual staking reward: \$100
- Discount rate: 10%
- Perpetual reward assumption

$$\text{Value} = \frac{100}{0.10} = \$1,000$$

Problem: When can we use traditional finance valuation? — DCF applies only to tokens with predictable cash flows (staking rewards, fee sharing)

What's the Difference Between Market Cap and FDV?

Market Cap:

$$\text{Market Cap} = \text{Price} \times \text{Circulating Supply}$$

Fully Diluted Valuation (FDV):

$$\text{FDV} = \text{Price} \times \text{Total Supply (Max)}$$

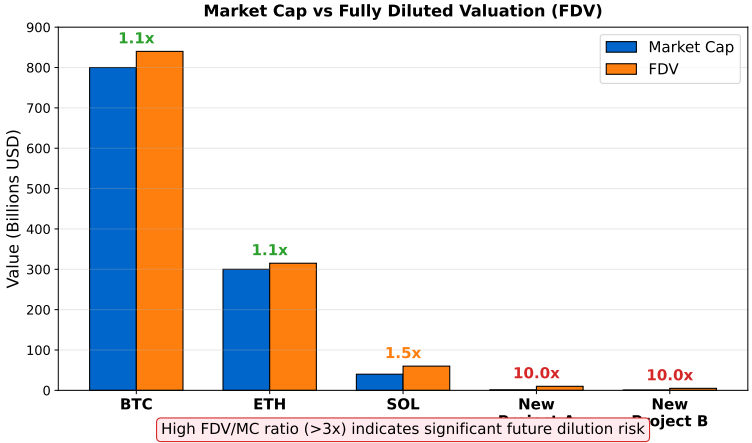
Example:

- Token price: \$10, Circulating: 100M, Total: 1B
- Market Cap: \$1B
- FDV: \$10B

Warning: Large FDV/MC ratio indicates future dilution risk (your ownership percentage shrinks as locked tokens enter circulation).

(c) Joerg Osterrieder 2025

Market Cap vs FDV Comparison



New projects often have 10x+ FDV/MC ratio indicating massive dilution ahead

How Should You Approach Token Valuation?

Step-by-Step Analysis:

1. Determine token type and purpose (utility, governance, etc.)
2. Check regulatory status (security vs. non-security)
3. Calculate NVT ratio (compare to peers)
4. Analyze on-chain metrics (addresses, transactions, TVL)
5. Review tokenomics (supply, inflation, unlock schedule)
6. Compare market cap to fundamentals (revenue, usage)
7. Assess FDV vs. Market Cap (dilution risk)

Output: Informed estimate of fair value range (not precise number).

Problem Solved? Token Classification

The Original Problem

When is a token a security?

How Token Classification Solves It

- Howey Test provides four-criteria framework: investment of money, common enterprise, expectation of profits, efforts of others
- FINMA taxonomy distinguishes payment, utility, and asset tokens based on economic function
- Context matters: Ripple ruling showed same token can be security (institutional sales) or not (exchange sales)

Remaining Limitations

- Regulatory uncertainty persists: no global standard, jurisdiction shopping common (Switzerland, Singapore)
- Gray area tokens (hybrid utility/governance) still lack clear classification

Open Questions

- Will MiCA (EU) and international coordination lead to regulatory harmonization by 2030?
- Risk: Black swan events (e.g., major exchange listing security unknowingly), cascading enforcement actions

Token Classification partially solves "When is a token a security" but introduces new trade-offs

The Economics of Token Classification

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium (game theory: no player gains by unilaterally changing strategy)

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Token Classification

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Token Classification

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

(c) Joerg Osterrieder 2025

The Utility Token Defense

[COMIC: Utility token excuse]

A visual narrative showing a project claiming "it's just a utility token!" while regulators remain skeptical

What We Learned

- Howey Test determines security classification
- Context of sale matters (Ripple precedent)
- "Utility" label doesn't guarantee non-security status

The Takeaway

Classification depends on economic reality, not marketing labels—regulators look at substance over form.

Visual synthesis: The gap between token marketing and regulatory reality

Summary

Key Takeaways:

- Howey Test determines security classification (4 criteria)
- Context of sale matters (Ripple case precedent)
- NVT ratio helps assess value relative to transaction volume
- Metcalfe's Law suggests network value grows with users squared
- DCF applicable only to tokens with cash flows
- Comparable analysis useful for relative valuation
- Always compare Market Cap to FDV (dilution risk)
- Crypto valuation is imprecise - use multiple methods

Next Lesson: L32 – Lab: Tokenomics Analysis

Questions for Reflection

1. Apply the Howey Test to a token you're familiar with. Is it a security?
2. Why did the Ripple ruling distinguish between institutional and exchange sales?
3. Calculate the NVT ratio for Bitcoin and Ethereum. What does it tell you?
4. What are the limitations of using Metcalfe's Law for token valuation?
5. How would you value a governance token with no direct cash flows?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. How many criteria must be met under the Howey Test for an asset to be classified as a security?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria (investment of money, common enterprise, expectation of profits, efforts of others) must be met.

Q2. Which of the following is NOT one of the four Howey Test criteria?
A) Investment of money B) Common enterprise C) Government approval D) Efforts of others
Answer: C – Government approval is not part of the Howey Test. The four criteria are: investment of money, common enterprise, expectation of profits, and efforts of others.

Q3. What was the key distinction in the SEC vs. Ripple ruling (July 2023)?
A) All XRP sales were securities B) No XRP sales were securities
C) Context of sale matters (institutional vs. exchange) D) Ripple was completely acquitted
Answer: C – Judge Torres ruled that institutional sales were securities, but programmatic exchange sales were not, establishing that sale context matters.

Q4. What percentage of XRP supply does Ripple Labs hold?
A) 10% B) 25% C) 50% D) 75%
Answer: C – Ripple holds approximately 50% of the XRP supply, which was a key factor in the SEC's case.

Q5. According to the lesson, which tokens are examples of utility tokens?
A) BTC and ETH B) BNB and FIL C) XRP and ADA D) Tokenized stocks
Answer: B – BNB (Binance Coin) and FIL (Filecoin) are cited as examples of utility tokens providing access to products/services.

Quiz Questions (6–10)

Q6. What does NVT stand for in token valuation?
A) Network Value Total B) Network Value to Transactions
C) Net Value Transfer D) New Value Token
Answer: B – NVT stands for Network Value to Transactions, calculated as Market Cap divided by Daily Transaction Volume.

Q7. What is the typical NVT ratio range for Bitcoin according to the lesson?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – BTC typically has an NVT ratio of 50-100, reflecting its primary use as a store of value rather than for payments.

Q8. According to Metcalfe's Law, how does network value grow with the number of users?
A) Linearly (n) B) Logarithmically ($\log n$) C) Squared (n^2) D) Exponentially (e^n)
Answer: C – Metcalfe's Law states that network value is proportional to the square of the number of users ($V \propto n^2$).

Q9. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage
C) High transaction volume D) Low market capitalization
Answer: B – A high NVT ratio suggests the token is overvalued relative to its transaction volume (similar to a high P/E ratio in stocks).

Q10. Which valuation method is most appropriate for tokens with staking rewards?
A) NVT Ratio B) Metcalfe's Law C) Discounted Cash Flow (DCF) D) Cost of Production
Answer: C – DCF is suitable for tokens with cash flow generation, such as staking rewards or fee sharing.

Quiz Questions (11–15)

Q11. What is the formula for Market Cap?
A) Price $\times$ Total Supply B) Price $\times$ Circulating Supply
C) Price $\div$ Circulating Supply D) Total Supply $\times$ FDV
Answer: B – Market Cap = Price $\times$ Circulating Supply (only tokens currently in circulation).

Q12. What does FDV stand for?
A) Final Distribution Value B) Fully Diluted Valuation
C) Future Development Value D) Fixed Derivative Value
Answer: B – FDV stands for Fully Diluted Valuation, calculated as Price $\times$ Total Supply (maximum).

Q13. A large FDV/Market Cap ratio indicates:
A) Undervaluation B) High current circulation C) Future dilution risk D) Low token price
Answer: C – A high FDV/MC ratio (e.g., 10x+) indicates significant future dilution risk as locked tokens are released.

Q14. Which Howey Test criterion do Bitcoin and Ethereum largely avoid due to decentralization?
A) Investment of money B) Common enterprise
C) Expectation of profits D) Efforts of others
Answer: D – BTC and ETH are sufficiently decentralized that profits do not primarily depend on the "efforts of others".

Q15. What is a key limitation of using Metcalfe's Law for crypto valuation?
A) It requires cash flow data B) Not all users create equal value
C) It only applies to Bitcoin D) It ignores market capitalization
Answer: B – Metcalfe's Law doesn't account for the quality of usage or the fact that not all users create equal value in the network.

Quiz Questions (16–20)

Q16. In the Ripple case, which type of XRP sales were ruled as securities?
A) All sales B) Institutional sales to VCs and hedge funds
C) Programmatic sales on exchanges D) Employee compensation
Answer: B – Institutional sales to VCs/hedge funds were ruled as securities because buyers had expectation of profits from Ripple's efforts.

Q17. What regulatory requirement applies if a token is classified as a security in the US?
A) Mining permit B) Registration with SEC C) Blockchain audit D) Federal tax exemption
Answer: B – Securities require registration with the SEC, along with investor protections and disclosure requirements.

Q18. If a staking token provides $100 annual rewards with a 10% discount rate (perpetual), what is its DCF value?
A) $100 B) $500 C) $1,000 D) $10,000
Answer: C – Using the perpetuity formula: Value = $100 / 0.10 = $1,000.

Q19. What is the typical NVT ratio range for payment-focused tokens?
A) <20 B) 20-40 C) 50-100 D) >100
Answer: A – Payment tokens typically have NVT < 20 due to high transaction volume relative to market cap.

Q20. Which statement best describes token valuation in crypto?
A) Always use DCF exclusively B) NVT ratio provides precise fair value
C) Use multiple methods; valuation is imprecise D) Market cap alone determines value
Answer: C – Crypto valuation is imprecise and requires using multiple methods (NVT, Metcalfe, DCF, comparables) to estimate a fair value range.

Quiz: Token Classification

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. How many Howey Test criteria must be met for security classification?
A) Two B) Three C) Four D) Five

Quiz (1–5)

Q1. How many Howey Test criteria must be met for security classification?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria must be met.

Q2. Which Howey criterion do BTC/ETH avoid due to decentralization?
A) Investment of money B) Common enterprise C) Expectation of profits D) Efforts of others

Quiz (1–5)

Q1. How many Howey Test criteria must be met for security classification?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria must be met.

Q2. Which Howey criterion do BTC/ETH avoid due to decentralization?
A) Investment of money B) Common enterprise C) Expectation of profits D) Efforts of others
Answer: D – Profits don't depend on a central promoter's efforts.

Q3. In SEC vs. Ripple, which sales were ruled as securities?
A) All sales B) Institutional sales C) Exchange sales D) None

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. How many Howey Test criteria must be met for security classification?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria must be met.

Q2. Which Howey criterion do BTC/ETH avoid due to decentralization?
A) Investment of money B) Common enterprise C) Expectation of profits D) Efforts of others
Answer: D – Profits don't depend on a central promoter's efforts.

Q3. In SEC vs. Ripple, which sales were ruled as securities?
A) All sales B) Institutional sales C) Exchange sales D) None
Answer: B – Institutional buyers knew they were buying from Ripple.

Q4. What is the NVT formula?
A) Price / Earnings B) Market Cap / Daily Tx Volume C) Users^2 D) FDV / MC

Quiz (1–5)

Q1. How many Howey Test criteria must be met for security classification?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria must be met.

Q2. Which Howey criterion do BTC/ETH avoid due to decentralization?
A) Investment of money B) Common enterprise C) Expectation of profits D) Efforts of others
Answer: D – Profits don't depend on a central promoter's efforts.

Q3. In SEC vs. Ripple, which sales were ruled as securities?
A) All sales B) Institutional sales C) Exchange sales D) None
Answer: B – Institutional buyers knew they were buying from Ripple.

Q4. What is the NVT formula?
A) Price / Earnings B) Market Cap / Daily Tx Volume C) Users^2 D) FDV / MC
Answer: B – NVT = Market Cap / Daily Transaction Volume.

Q5. According to Metcalfe's Law, network value grows how with users?
A) Linearly (n) B) Logarithmically C) Squared (n^2) D) Cubed (n^3)

Quiz (1–5)

Q1. How many Howey Test criteria must be met for security classification?
A) Two B) Three C) Four D) Five
Answer: C – All four criteria must be met.

Q2. Which Howey criterion do BTC/ETH avoid due to decentralization?
A) Investment of money B) Common enterprise C) Expectation of profits D) Efforts of others
Answer: D – Profits don't depend on a central promoter's efforts.

Q3. In SEC vs. Ripple, which sales were ruled as securities?
A) All sales B) Institutional sales C) Exchange sales D) None
Answer: B – Institutional buyers knew they were buying from Ripple.

Q4. What is the NVT formula?
A) Price / Earnings B) Market Cap / Daily Tx Volume C) Users^2 D) FDV / MC
Answer: B – NVT = Market Cap / Daily Transaction Volume.

Q5. According to Metcalfe's Law, network value grows how with users?
A) Linearly (n) B) Logarithmically C) Squared (n^2) D) Cubed (n^3)
Answer: C – Network value is proportional to n^2.

Quiz (6–10)

Q6. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage C) High transaction volume D) Low price

Quiz (6–10)

Q6. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage C) High transaction volume D) Low price
Answer: B – High NVT means overvalued relative to transaction volume.

Q7. What is the typical NVT range for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200

Quiz (6–10)

Q6. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage C) High transaction volume D) Low price
Answer: B – High NVT means overvalued relative to transaction volume.

Q7. What is the typical NVT range for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – BTC's high NVT reflects store-of-value use, not payments.

Q8. Which valuation method is best for tokens with staking rewards?
A) NVT Ratio B) Metcalfe's Law C) DCF D) Comparable Analysis

Quiz (6–10)

Q6. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage C) High transaction volume D) Low price
Answer: B – High NVT means overvalued relative to transaction volume.

Q7. What is the typical NVT range for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – BTC's high NVT reflects store-of-value use, not payments.

Q8. Which valuation method is best for tokens with staking rewards?
A) NVT Ratio B) Metcalfe's Law C) DCF D) Comparable Analysis
Answer: C – DCF works for tokens with cash flow (staking, fees).

Q9. A large FDV/Market Cap ratio indicates:
A) Undervaluation B) High circulation C) Future dilution risk D) Low volatility

Quiz (6–10)

Q6. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage C) High transaction volume D) Low price
Answer: B – High NVT means overvalued relative to transaction volume.

Q7. What is the typical NVT range for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – BTC's high NVT reflects store-of-value use, not payments.

Q8. Which valuation method is best for tokens with staking rewards?
A) NVT Ratio B) Metcalfe's Law C) DCF D) Comparable Analysis
Answer: C – DCF works for tokens with cash flow (staking, fees).

Q9. A large FDV/Market Cap ratio indicates:
A) Undervaluation B) High circulation C) Future dilution risk D) Low volatility
Answer: C – Large FDV/MC means many tokens still locked = dilution ahead.

Q10. Which is an example of a utility token?
A) Tokenized Apple stock B) BNB (Binance) C) SEC-registered token D) XRP institutional sale

Quiz (6–10)

Q6. What does a high NVT ratio indicate?
A) Undervalued token B) Overvalued relative to usage C) High transaction volume D) Low price
Answer: B – High NVT means overvalued relative to transaction volume.

Q7. What is the typical NVT range for Bitcoin?
A) 5-10 B) 20-40 C) 50-100 D) 150-200
Answer: C – BTC's high NVT reflects store-of-value use, not payments.

Q8. Which valuation method is best for tokens with staking rewards?
A) NVT Ratio B) Metcalfe's Law C) DCF D) Comparable Analysis
Answer: C – DCF works for tokens with cash flow (staking, fees).

Q9. A large FDV/Market Cap ratio indicates:
A) Undervaluation B) High circulation C) Future dilution risk D) Low volatility
Answer: C – Large FDV/MC means many tokens still locked = dilution ahead.

Q10. Which is an example of a utility token?
A) Tokenized Apple stock B) BNB (Binance) C) SEC-registered token D) XRP institutional sale
Answer: B – BNB provides utility (fee discounts) on Binance platform.

L32: Lab – Tokenomics Analysis

Mini-Lecture – Module D: Tokenomics

Blockchain & Cryptocurrency Course

January 2026

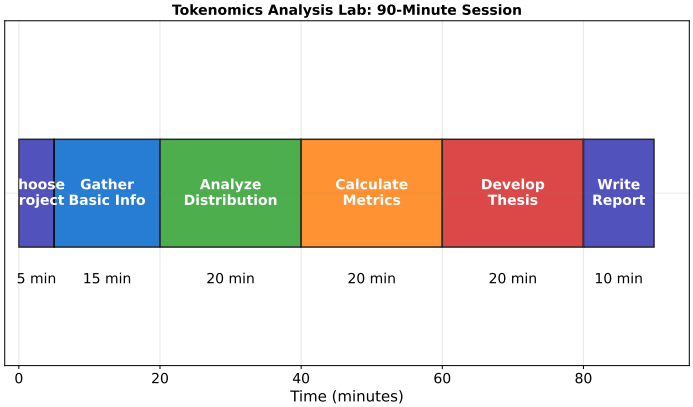
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Calculate key valuation metrics (NVT, FDV, dilution ratio)
- Analyze token distribution and vesting schedules
- Apply Howey Test classification framework
- Develop a structured investment thesis

Tokenomics Analysis Workflow



Complete analysis: Quantitative metrics + qualitative assessment.

Step 1: Choose and Research Project

Suggested Categories:

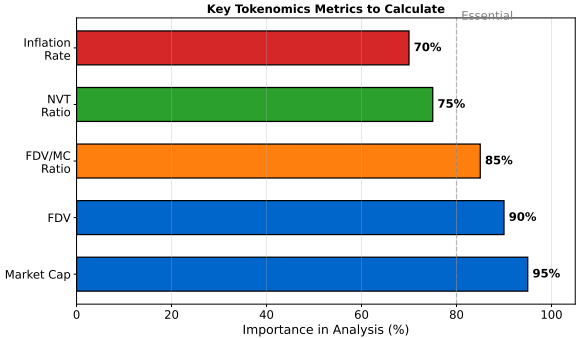
- **DeFi:** UNI, AAVE, CRV, MKR
- **Layer 1:** SOL, AVAX, DOT
- **Infrastructure:** LINK, GRT, FIL

Gather Basic Info:

- Problem solved and core technology
- Current price, market cap, circulating vs total supply
- 24h volume and volatility

Sources: CoinGecko, CoinMarketCap, project website

Key Metrics to Calculate



Market Cap and FDV are essential for understanding dilution.

Valuation Formulas

Fully Diluted Valuation:

$$\text{FDV} = \text{Price} \times \text{Max Total Supply}$$

Dilution Risk Ratio:

$$\text{Dilution Risk} = \frac{\text{FDV}}{\text{Market Cap}}$$

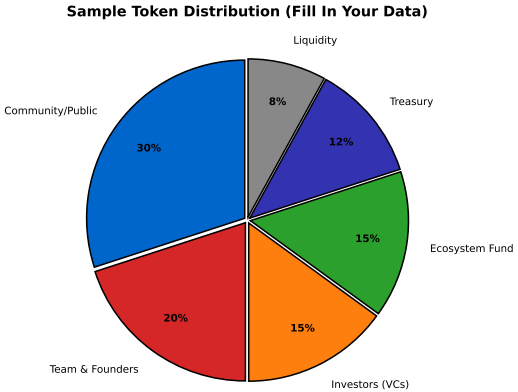
- Ratio > 2: High dilution risk
- Ratio 1-2: Moderate
- Ratio ≈ 1: Low dilution

NVT Ratio:

$$\text{NVT} = \frac{\text{Market Cap}}{\text{Daily Tx Volume (USD)}}$$

(c) Joerg Osterrieder 2025

Distribution Analysis



Critical Questions: What % do insiders hold? Vesting transparent? Upcoming unlocks?

Apply Howey Test

Four Prongs:

1. **Investment of Money?** Did investors pay?
2. **Common Enterprise?** Pooled returns?
3. **Expectation of Profits?** Marketed as investment?
4. **Efforts of Others?** Team drives value?

Classification:

- All four = Likely Security
- Fails "efforts of others" = Likely Utility Token

Develop Investment Thesis

Structure Your Analysis:

1. **Summary:** 2-3 sentences on token purpose
2. **Strengths:** Bullish tokenomics factors
3. **Weaknesses:** Red flags and risks
4. **Verdict:** Buy / Hold / Avoid with justification

Deliverables:

- 2-3 page report with calculated metrics
- Comparison to 2-3 peer projects
- Supporting screenshots and calculations

Note: Educational analysis, not financial advice.

Key Takeaways

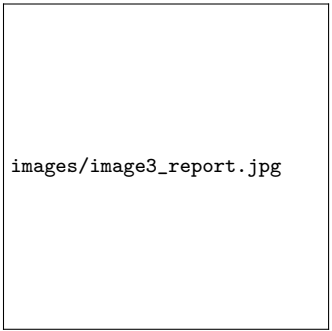
1. **FDV/MC Ratio:** >2 indicates high future dilution
2. **NVT:** Lower = higher network utility relative to valuation
3. **Distribution:** Insider $> 70\%$ is red flag
4. **Howey Test:** Four prongs determine security classification
5. **Compare Peers:** Context for whether metrics are typical

Verdict: Buy / Hold / Avoid – always justify with evidence.

Tokenomics Analysis in Practice

Analysis Tools

Metrics Dashboard



Report Writing

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What does FDV represent?
A) Current market cap B) Price $\times$ circulating supply
C) Price $\times$ max total supply D) Trading volume

Quiz (1/2)

Q1. What does FDV represent?
A) Current market cap B) Price $\times$ circulating supply
C) Price $\times$ max total supply D) Trading volume
Answer: C – Maximum potential market cap.

Q2. FDV $1B, Market Cap $200M. Dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1

Quiz (1/2)

Q1. What does FDV represent?
A) Current market cap B) Price $\times$ circulating supply
C) Price $\times$ max total supply D) Trading volume
Answer: C – Maximum potential market cap.

Q2. FDV $1B, Market Cap $200M. Dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – \$1B/\$200M = 5 (very high risk).

Q3. Which ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1

Quiz (1/2)

Q1. What does FDV represent?
A) Current market cap B) Price $\times$ circulating supply
C) Price $\times$ max total supply D) Trading volume
Answer: C – Maximum potential market cap.

Q2. FDV $1B, Market Cap $200M. Dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – \$1B/\$200M $= 5$ (very high risk).

Q3. Which ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio ≈ 1 is low dilution.

Q4. What does NVT ratio measure?
A) Token velocity B) Market cap vs tx volume
C) Vesting schedule D) Holder concentration

(c) Joerg Osterrieder 2025

Quiz (1/2)

Q1. What does FDV represent?
A) Current market cap B) Price $\times$ circulating supply
C) Price $\times$ max total supply D) Trading volume
Answer: C – Maximum potential market cap.

Q2. FDV $1B, Market Cap $200M. Dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – \$1B/\$200M = 5 (very high risk).

Q3. Which ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio ≈ 1 is low dilution.

Q4. What does NVT ratio measure?
A) Token velocity B) Market cap vs tx volume
C) Vesting schedule D) Holder concentration
Answer: B – Lower = higher network utility.

Q5. First prong of Howey Test?
A) Expectation of profits B) Common enterprise
C) Investment of money D) Efforts of others

Quiz (1/2)

Q1. What does FDV represent?
A) Current market cap B) Price $\times$ circulating supply
C) Price $\times$ max total supply D) Trading volume
Answer: C – Maximum potential market cap.

Q2. FDV $1B, Market Cap $200M. Dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – \$1B/\$200M = 5 (very high risk).

Q3. Which ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio $\approx$ 1 is low dilution.

Q4. What does NVT ratio measure?
A) Token velocity B) Market cap vs tx volume
C) Vesting schedule D) Holder concentration
Answer: B – Lower = higher network utility.

Q5. First prong of Howey Test?
A) Expectation of profits B) Common enterprise
C) Investment of money D) Efforts of others
Answer: C – Investment of money is first.

Quiz (2/2)

Q6. Token passes all four Howey prongs. Classification?
A) Utility token B) Security C) Commodity D) Currency

Quiz (2/2)

Q6. Token passes all four Howey prongs. Classification?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four = likely security.

Q7. What percentage insider holdings is a red flag?
A) 10% B) 25% C) 50% D) 70%+

Quiz (2/2)

Q6. Token passes all four Howey prongs. Classification?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four = likely security.

Q7. What percentage insider holdings is a red flag?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high concentration = risk.

Q8. Market Cap $500M, Daily Tx $50M. NVT ratio?
A) 0.1 B) 1 C) 10 D) 100

Quiz (2/2)

Q6. Token passes all four Howey prongs. Classification?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four = likely security.

Q7. What percentage insider holdings is a red flag?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high concentration = risk.

Q8. Market Cap $500M, Daily Tx $50M. NVT ratio?
A) 0.1 B) 1 C) 10 D) 100
Answer: C – $500M/$50M = 10.

Q9. What does a vesting cliff mean?
A) No tokens for initial period B) Immediate full unlock
C) Daily unlocks D) Random schedule

Quiz (2/2)

Q6. Token passes all four Howey prongs. Classification?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four = likely security.

Q7. What percentage insider holdings is a red flag?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high concentration = risk.

Q8. Market Cap $500M, Daily Tx $50M. NVT ratio?
A) 0.1 B) 1 C) 10 D) 100
Answer: C – $500M/$50M = 10.

Q9. What does a vesting cliff mean?
A) No tokens for initial period B) Immediate full unlock
C) Daily unlocks D) Random schedule
Answer: A – Cliff delays any token release.

Q10. Why compare token to 2-3 peers?
A) Copy their price B) Context for typical metrics
C) Find arbitrage D) Regulatory requirement

Quiz (2/2)

Q6. Token passes all four Howey prongs. Classification?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four = likely security.

Q7. What percentage insider holdings is a red flag?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high concentration = risk.

Q8. Market Cap $500M, Daily Tx $50M. NVT ratio?
A) 0.1 B) 1 C) 10 D) 100
Answer: C – $500M/$50M = 10.

Q9. What does a vesting cliff mean?
A) No tokens for initial period B) Immediate full unlock
C) Daily unlocks D) Random schedule
Answer: A – Cliff delays any token release.

Q10. Why compare token to 2-3 peers?
A) Copy their price B) Context for typical metrics
C) Find arbitrage D) Regulatory requirement
Answer: B – Provides benchmark context.

Thank you

Questions?

Next: L33 – DEX Mechanics and AMMs

Lab Session: Tokenomics Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module D: Tokenomics

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Select and research a real cryptocurrency project
- Calculate key valuation metrics (NVT, FDV, ratios)
- Analyze token distribution and vesting schedules
- Assess token classification (utility vs. security)
- Develop a structured investment thesis

The Problem: Can You Trust the Token?

The Challenge
Most crypto projects publish impressive whitepapers with bold claims, but tokenomics structures often hide risks. Without systematic analysis, investors face: hidden vesting schedules that dump on retail, inflated valuations (FDV 10x market cap), and team allocations that dominate governance.

Why It Matters

- 2021 "VC unlock summer" crashed dozens of tokens 80%+
- Projects with 70%+ insider holdings = centralization risk

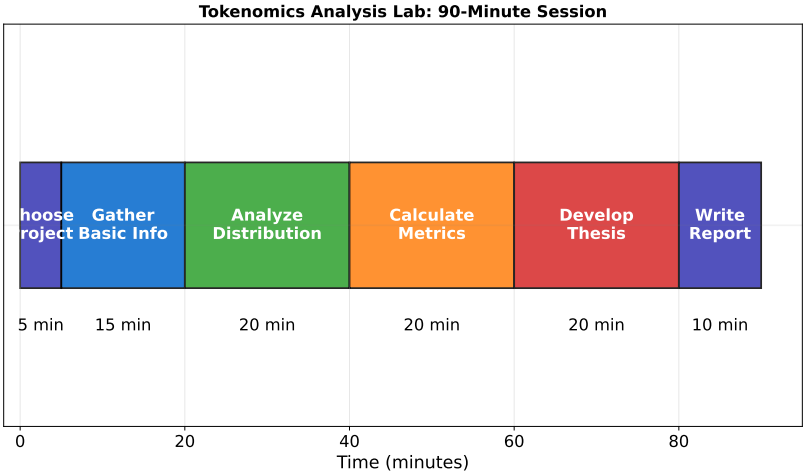
What You'll Explore

- Supply analysis (circulating vs. max supply)
- Vesting schedules and unlock calendars
- Holder distribution (Gini coefficient)
- Emission curves and inflation rates

The Cryptoeconomics Question
How do token economics reveal long-term sustainability and alignment between teams and communities?

Today's lab: Hands-on analysis of real tokenomics to identify red flags and opportunities

Lab Session Structure



Complete analysis requires both quantitative and qualitative assessment

Step 1: Choose a Project

Suggested Categories:

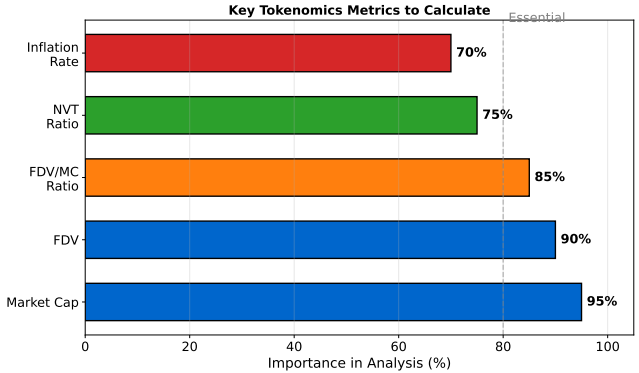
- **DeFi:** UNI, AAVE, CRV, MKR
- **Layer 1:** SOL, AVAX, DOT
- **Infrastructure:** LINK, GRT, FIL

Selection Criteria:

- Publicly available tokenomics documentation
- Active trading on major exchanges
- Sufficient on-chain data available

(c) Joerg Osterrieder 2025

Key Metrics to Calculate



Market cap and FDV are essential; all metrics provide context

Step 2: Gather Basic Information

Project Overview:

- Problem solved and core technology
- Launch date and development status
- Token ticker and blockchain network

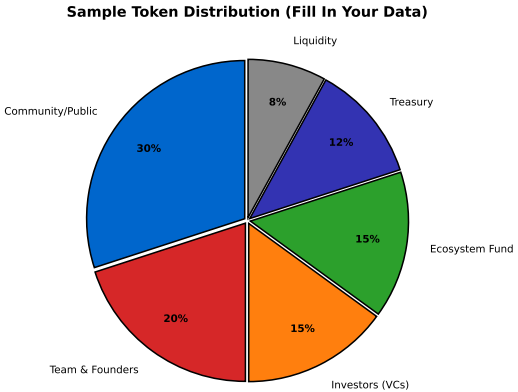
Current Market Data:

- Current price and market cap
- Circulating supply vs. total supply
- 24h volume and volatility

Sources: CoinGecko, CoinMarketCap, project website

(c) Joerg Osterrieder 2025

Distribution Analysis Template



Step 3: Analyze Distribution

Key Categories to Research:

- Team and Founders allocation
- Investor (VC) allocation
- Community and public sale
- Ecosystem and treasury funds

Critical Questions:

- What % do insiders hold?
- Are vesting schedules transparent?
- Upcoming unlock events?

(c) Joerg Osterrieder 2025

Step 4: Calculate Metrics

Fully Diluted Valuation (FDV):

$$\text{FDV} = \text{Current Price} \times \text{Max Total Supply}$$

Dilution Risk Ratio:

$$\text{Dilution Risk} = \frac{\text{FDV}}{\text{Market Cap}}$$

- Ratio ¿ 2: High dilution risk
- Ratio 1-2: Moderate dilution
- Ratio $\approx$ 1: Low dilution

NVT Ratio:

$$\text{NVT} = \frac{\text{Market Cap}}{\text{Daily Tx Volume (USD)}}$$

(c) Joerg Osterrieder 2025

Step 5: Apply Howey Test

Four Prongs:

1. **Investment of Money?** Did investors pay?
2. **Common Enterprise?** Pooled returns?
3. **Expectation of Profits?** Marketed as investment?
4. **Efforts of Others?** Team drives value?

Classification:

- All four = Likely Security
- Fails "efforts of others" = Likely Utility Token

Step 6: Develop Investment Thesis

Structure Your Analysis:

1. **Summary:** 2-3 sentences on token purpose
2. **Strengths:** Bullish tokenomics factors
3. **Weaknesses:** Red flags and risks
4. **Verdict:** Buy / Hold / Avoid with justification

Note: Educational analysis, not financial advice

(c) Joerg Osterrieder 2025

Lab Deliverables

Submit:

1. **Tokenomics Report (2-3 pages):**
   - Project overview and market data
   - Distribution and vesting analysis
   - Valuation metrics calculated
   - Investment thesis with verdict
2. **Supporting Data:**
   - Screenshots of data sources
   - Metric calculations shown
   - Comparison to 2-3 peers

Problem Solved? Systematic Tokenomics Analysis

The Original Problem

Can you trust the token? How do you identify red flags and sustainable tokenomics?

How Analysis Solves It

- **FDV/MC Ratio**: Quantifies dilution risk (ratio ¿ 2 = danger)
- **Vesting Transparency**: Unlock calendars reveal insider sell pressure
- **Distribution Charts**: Expose centralized control (Gini coefficient)
- **NVT Ratio**: Market cap relative to network activity usage

Remaining Limitations

- **Hidden Wallets**: Teams may use undisclosed addresses
- **Governance Capture**: Token holders $\neq$ active voters
- **Emission Changes**: DAOs can vote to alter tokenomics

Open Questions

- How to detect wash trading in volume metrics?
- Can we predict unlock impact on price programmatically?
- Risk: Insiders dump during unlock events; retail left holding bags

Systematic tokenomics analysis reveals risks, but requires ongoing monitoring and cross-referencing on-chain data

(c) Joerg Osterrieder 2025

Key Takeaways

- Tokenomics analysis combines quantitative metrics and qualitative assessment
- Distribution and vesting reveal insider alignment and dilution risk
- FDV/MC ratio is critical for understanding future dilution
- Howey Test helps classify utility vs. security tokens
- Always compare to similar projects for context

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – Dilution Risk = FDV/Market Cap = $1B/$200M = 5 (very high dilution risk).

Q3. Which dilution risk ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio $\approx$ 1 indicates low dilution; ratio ¿ 2 is high risk.

Q4. What does the NVT (Network Value to Transactions) ratio measure?
A) Token velocity B) Market cap relative to transaction volume C) Vesting schedule D) Holder concentration
Answer: B – NVT = Market Cap / Daily Tx Volume (USD); lower values suggest higher utility.

Q5. Which token allocation category typically has vesting schedules?
A) Public sale B) Airdrops C) Team and founders D) Staking rewards
Answer: C – Team/founder allocations usually vest over 2-4 years to align long-term incentives.

Quiz Questions (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four prongs = Likely Security; failing "efforts of others" suggests utility token.

Q8. Which source is recommended for gathering current market data?
A) Twitter polls B) CoinGecko/CoinMarketCap C) Reddit forums D) Telegram groups
Answer: B – CoinGecko, CoinMarketCap, and project websites provide reliable market data.

Q9. What percentage of insider holdings typically raises red flags?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high insider concentration (70%+) creates centralization and dump risk.

Q10. Which metric helps identify if a token is overvalued relative to network activity?
A) Market cap B) Trading volume C) NVT ratio D) Circulating supply
Answer: C – High NVT ratio suggests price may be high relative to actual network usage.

Quiz Questions (11–15)

Q11. What does "unlock event" refer to in tokenomics?
A) New token minting B) Vesting tokens becoming tradable C) Staking rewards distribution D) Token burn
Answer: B – Unlock events occur when vested tokens become liquid, potentially increasing sell pressure.

Q12. Which project category was NOT suggested for lab analysis?
A) DeFi protocols B) Layer 1 blockchains C) Memecoins D) Infrastructure projects
Answer: C – Suggested categories: DeFi, Layer 1, Infrastructure; memecoins have poor tokenomics documentation.

Q13. What is the key difference between circulating supply and total supply?
A) No difference B) Circulating is currently tradable; total includes locked/unvested C) Total is always smaller D) Circulating includes burned tokens
Answer: B – Circulating supply excludes locked/vested tokens not yet in circulation.

Q14. In a tokenomics investment thesis, what does "Buy/Hold/Avoid" represent?
A) Trading advice B) Educational verdict with justification C) Financial advice D) Price prediction
Answer: B – The verdict is an educational analysis, explicitly not financial advice.

Q15. Which allocation typically signals strong community alignment?
A) 60% team, 40% investors B) 50% public sale, 30% community, 20% team C) 80% VC investors D) 100% pre-mine to founders
Answer: B – Larger public/community allocations with modest team/VC shares show better decentralization.

Quiz Questions (16–20)

Q16. What does a vesting "cliff" mean?
A) No tokens released for initial period B) Immediate full unlock C) Linear daily unlocks D) Random unlock schedule
Answer: A – A cliff (e.g., 12 months) delays any token release until the cliff period ends.

Q17. Why should you compare a token to 2-3 peers?
A) To copy their price B) For context on typical metrics/valuations C) To find arbitrage D) Regulatory requirement
Answer: B – Peer comparison provides context for whether metrics are typical, high, or low.

Q18. Which factor is NOT part of the Howey Test?
A) Investment of money B) Common enterprise C) Token burn mechanism D) Expectation of profits
Answer: C – Howey Test prongs: investment of money, common enterprise, expectation of profits, efforts of others.

Q19. What is the primary purpose of an ecosystem/treasury allocation?
A) Founder bonuses B) Fund development, grants, and growth C) VC returns D) Immediate trading
Answer: B – Ecosystem/treasury funds support ongoing development, partnerships, and community initiatives.

Q20. A token has Market Cap $500M and Daily Tx Volume $50M. What is the NVT ratio?
A) 0.1 B) 1 C) 10 D) 100
Answer: C – NVT = \$500M / \$50M = 10; lower NVT suggests more network activity per dollar of valuation.

Lab Session: Tokenomics Analysis

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module D: Tokenomics

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Select and research a real cryptocurrency project
- Calculate key valuation metrics (NVT, FDV, ratios)
- Analyze token distribution and vesting schedules
- Assess token classification (utility vs. security)
- Develop a structured investment thesis

Building on L31: Token Classification

The Tokenomics Investigation

[COMIC: Token distribution pie chart]

A visual narrative showing an investor examining a suspicious token distribution chart with magnifying glass

What This Illustrates

- Not all token distributions are created equal
- Hidden allocations can signal trouble
- Due diligence requires systematic analysis

The Question

Can you spot the red flags hiding in a project's tokenomics?

Visual framing: The detective work of tokenomics analysis

(c) Joerg Osterrieder 2025

The Problem: Can You Trust the Token?

The Challenge
Most crypto projects publish impressive whitepapers with bold claims, but tokenomics structures often hide risks. Without systematic analysis, investors face: hidden vesting schedules that dump on retail, inflated valuations (FDV 10x market cap), and team allocations that dominate governance.

Why It Matters

- 2021 "VC unlock summer" crashed dozens of tokens 80%+
- Projects with 70%+ insider holdings = centralization risk

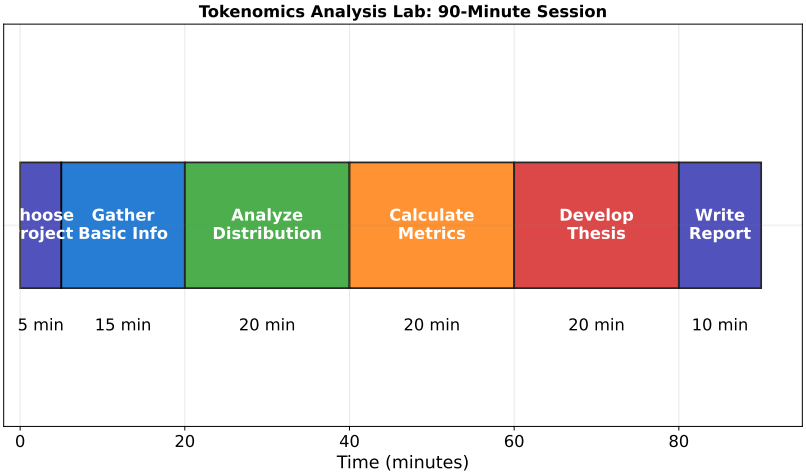
What You'll Explore

- Supply analysis (circulating vs. max supply)
- Vesting schedules and unlock calendars
- Holder distribution (Gini coefficient)
- Emission curves and inflation rates

The Cryptoeconomics Question
How do token economics reveal long-term sustainability and alignment between teams and communities?

Today's lab: Hands-on analysis of real tokenomics to identify red flags and opportunities

Lab Session Structure



Complete analysis requires both quantitative and qualitative assessment

How Do You Choose a Project to Analyze?

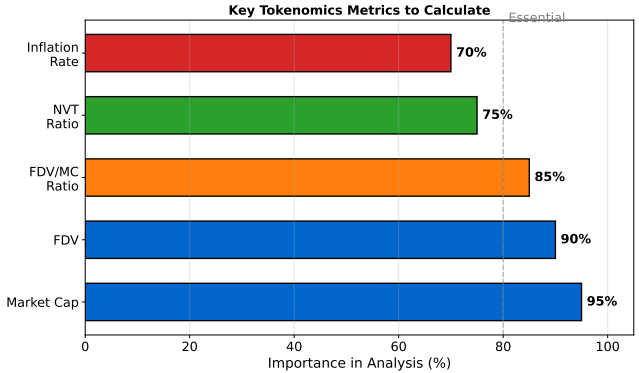
Suggested Categories:

- **DeFi:** UNI, AAVE, CRV, MKR
- **Layer 1:** SOL, AVAX, DOT
- **Infrastructure:** LINK, GRT, FIL

Selection Criteria:

- Publicly available tokenomics documentation
- Active trading on major exchanges
- Sufficient on-chain data available

Key Metrics to Calculate



Market cap and FDV are essential; all metrics provide context

What Basic Information Should You Gather?

Project Overview:

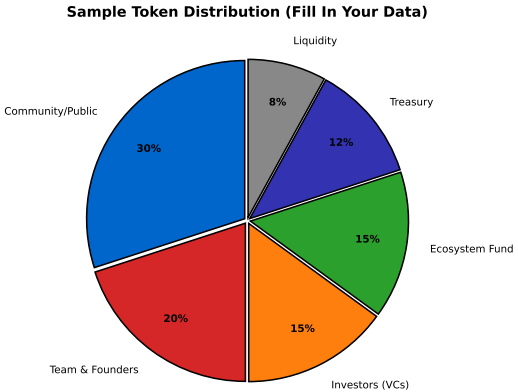
- Problem solved and core technology
- Launch date and development status
- Token ticker and blockchain network

Current Market Data:

- Current price and market cap
- Circulating supply vs. total supply
- 24h volume and volatility

Sources: CoinGecko, CoinMarketCap, project website

Distribution Analysis Template



How Do You Analyze Token Distribution?

Key Categories to Research:

- Team and Founders allocation
- Investor (VC) allocation
- Community and public sale
- Ecosystem and treasury funds

Critical Questions:

- What % do insiders hold?
- Are vesting schedules transparent?
- Upcoming unlock events?

(c) Joerg Osterrieder 2025

Which Metrics Should You Calculate?

Fully Diluted Valuation (FDV):

$$\text{FDV} = \text{Current Price} \times \text{Max Total Supply}$$

Dilution Risk Ratio:

$$\text{Dilution Risk} = \frac{\text{FDV}}{\text{Market Cap}}$$

- Ratio ¿ 2: High dilution risk
- Ratio 1-2: Moderate dilution
- Ratio $\approx$ 1: Low dilution

NVT Ratio:

$$\text{NVT} = \frac{\text{Market Cap}}{\text{Daily Tx Volume (USD)}}$$

(c) Joerg Osterrieder 2025

How Do You Apply the Howey Test?

Four Prongs:

1. **Investment of Money?** Did investors pay?
2. **Common Enterprise?** Pooled returns?
3. **Expectation of Profits?** Marketed as investment?
4. **Efforts of Others?** Team drives value?

Classification:

- All four = Likely Security
- Fails "efforts of others" = Likely Utility Token

How Do You Build an Investment Thesis?

Structure Your Analysis:

1. **Summary:** 2-3 sentences on token purpose
2. **Strengths:** Bullish tokenomics factors
3. **Weaknesses:** Red flags and risks
4. **Verdict:** Buy / Hold / Avoid with justification

Note: Educational analysis, not financial advice

(c) Joerg Osterrieder 2025

What Should You Submit for This Lab?

Submit:

1. **Tokenomics Report (2-3 pages):**
   - Project overview and market data
   - Distribution and vesting analysis
   - Valuation metrics calculated
   - Investment thesis with verdict
2. **Supporting Data:**
   - Screenshots of data sources
   - Metric calculations shown
   - Comparison to 2-3 peers

Problem Solved? Systematic Tokenomics Analysis

The Original Problem

Can you trust the token? How do you identify red flags and sustainable tokenomics?

How Analysis Solves It

- **FDV/MC Ratio**: Quantifies dilution risk (ratio ¿ 2 = danger)
- **Vesting Transparency**: Unlock calendars reveal insider sell pressure
- **Distribution Charts**: Expose centralized control (Gini coefficient)
- **NVT Ratio**: Market cap relative to network activity usage

Remaining Limitations

- **Hidden Wallets**: Teams may use undisclosed addresses
- **Governance Capture**: Token holders $\neq$ active voters
- **Emission Changes**: DAOs can vote to alter tokenomics

Open Questions

- How to detect wash trading in volume metrics?
- Can we predict unlock impact on price programmatically?
- Risk: Insiders dump during unlock events; retail left holding bags

Systematic tokenomics analysis reveals risks, but requires ongoing monitoring and cross-referencing on-chain data

(c) Joerg Osterrieder 2025

The Economics of Tokenomics Analysis

Incentive Structure

- **Core Problem:** Aligning individual and collective interests
- **Why act honestly?** Rewards for honest behavior, penalties for cheating
- **Value Flow:** Protocol gains security, participants earn rewards

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Protocol gains security, participants earn rewards

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Tokenomics Analysis

Alternatives Considered

1. **Chosen Design:** Reward curves, slashing conditions
2. **Alternative:** Alternative reward mechanisms

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Tokenomics Analysis

Critical Failure Mode

- **What breaks:** Incentive misalignment, free-rider problems
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

The Due Diligence Payoff

[COMIC: Red flag detection]

A visual narrative showing an analyst spotting warning signs in tokenomics that casual investors miss

What We Learned

- FDV/MC ratio reveals dilution risk
- Distribution charts expose centralization
- NVT ratio compares price to actual usage

The Takeaway

Systematic tokenomics analysis separates informed investors from those who become exit liquidity.

Visual synthesis: The reward of rigorous tokenomics due diligence

(c) Joerg Osterrieder 2025

Key Takeaways

- Tokenomics analysis combines quantitative metrics and qualitative assessment
- Distribution and vesting reveal insider alignment and dilution risk
- FDV/MC ratio is critical for understanding future dilution
- Howey Test helps classify utility vs. security tokens
- Always compare to similar projects for context

Next Lesson: L33 – Introduction to DeFi

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – Dilution Risk = FDV/Market Cap = $1B/$200M = 5 (very high dilution risk).

Q3. Which dilution risk ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio $\approx$ 1 indicates low dilution; ratio ¿ 2 is high risk.

Q4. What does the NVT (Network Value to Transactions) ratio measure?
A) Token velocity B) Market cap relative to transaction volume C) Vesting schedule D) Holder concentration
Answer: B – NVT = Market Cap / Daily Tx Volume (USD); lower values suggest higher utility.

Q5. Which token allocation category typically has vesting schedules?
A) Public sale B) Airdrops C) Team and founders D) Staking rewards
Answer: C – Team/founder allocations usually vest over 2-4 years to align long-term incentives.

Quiz Questions (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four prongs = Likely Security; failing "efforts of others" suggests utility token.

Q8. Which source is recommended for gathering current market data?
A) Twitter polls B) CoinGecko/CoinMarketCap C) Reddit forums D) Telegram groups
Answer: B – CoinGecko, CoinMarketCap, and project websites provide reliable market data.

Q9. What percentage of insider holdings typically raises red flags?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high insider concentration (70%+) creates centralization and dump risk.

Q10. Which metric helps identify if a token is overvalued relative to network activity?
A) Market cap B) Trading volume C) NVT ratio D) Circulating supply
Answer: C – High NVT ratio suggests price may be high relative to actual network usage.

Quiz Questions (11–15)

Q11. What does "unlock event" refer to in tokenomics?
A) New token minting B) Vesting tokens becoming tradable C) Staking rewards distribution D) Token burn
Answer: B – Unlock events occur when vested tokens become liquid, potentially increasing sell pressure.

Q12. Which project category was NOT suggested for lab analysis?
A) DeFi protocols B) Layer 1 blockchains C) Memecoins D) Infrastructure projects
Answer: C – Suggested categories: DeFi, Layer 1, Infrastructure; memecoins have poor tokenomics documentation.

Q13. What is the key difference between circulating supply and total supply?
A) No difference B) Circulating is currently tradable; total includes locked/unvested C) Total is always smaller D) Circulating includes burned tokens
Answer: B – Circulating supply excludes locked/vested tokens not yet in circulation.

Q14. In a tokenomics investment thesis, what does "Buy/Hold/Avoid" represent?
A) Trading advice B) Educational verdict with justification C) Financial advice D) Price prediction
Answer: B – The verdict is an educational analysis, explicitly not financial advice.

Q15. Which allocation typically signals strong community alignment?
A) 60% team, 40% investors B) 50% public sale, 30% community, 20% team C) 80% VC investors D) 100% pre-mine to founders
Answer: B – Larger public/community allocations with modest team/VC shares show better decentralization.

Quiz Questions (16–20)

Q16. What does a vesting "cliff" mean?
A) No tokens released for initial period B) Immediate full unlock C) Linear daily unlocks D) Random unlock schedule
Answer: A – A cliff (e.g., 12 months) delays any token release until the cliff period ends.

Q17. Why should you compare a token to 2-3 peers?
A) To copy their price B) For context on typical metrics/valuations C) To find arbitrage D) Regulatory requirement
Answer: B – Peer comparison provides context for whether metrics are typical, high, or low.

Q18. Which factor is NOT part of the Howey Test?
A) Investment of money B) Common enterprise C) Token burn mechanism D) Expectation of profits
Answer: C – Howey Test prongs: investment of money, common enterprise, expectation of profits, efforts of others.

Q19. What is the primary purpose of an ecosystem/treasury allocation?
A) Founder bonuses B) Fund development, grants, and growth C) VC returns D) Immediate trading
Answer: B – Ecosystem/treasury funds support ongoing development, partnerships, and community initiatives.

Q20. A token has Market Cap $500M and Daily Tx Volume $50M. What is the NVT ratio?
A) 0.1 B) 1 C) 10 D) 100
Answer: C – NVT = \$500M / \$50M = 10; lower NVT suggests more network activity per dollar of valuation.

Quiz: Lab Tokenomics Analysis

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume

Quiz (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1

Quiz (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – Dilution Risk = FDV/Market Cap = $1B/$200M = 5 (very high dilution risk).

Q3. Which dilution risk ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1

Quiz (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – Dilution Risk = FDV/Market Cap = $1B/$200M = 5 (very high dilution risk).

Q3. Which dilution risk ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio ≈ 1 indicates low dilution; ratio ¿ 2 is high risk.

Q4. What does the NVT (Network Value to Transactions) ratio measure?
A) Token velocity B) Market cap relative to transaction volume C) Vesting schedule D) Holder concentration

Quiz (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – Dilution Risk = FDV/Market Cap = $1B/$200M = 5 (very high dilution risk).

Q3. Which dilution risk ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio ≈ 1 indicates low dilution; ratio ¿ 2 is high risk.

Q4. What does the NVT (Network Value to Transactions) ratio measure?
A) Token velocity B) Market cap relative to transaction volume C) Vesting schedule D) Holder concentration
Answer: B – NVT = Market Cap / Daily Tx Volume (USD); lower values suggest higher utility.

Q5. Which token allocation category typically has vesting schedules?
A) Public sale B) Airdrops C) Team and founders D) Staking rewards

Quiz (1–5)

Q1. What does FDV (Fully Diluted Valuation) represent?
A) Current market cap only B) Price times circulating supply C) Price times max total supply D) Total trading volume
Answer: C – FDV = Current Price × Max Total Supply, showing maximum potential market cap.

Q2. A project has FDV of $1B and Market Cap of $200M. What is the dilution risk ratio?
A) 0.2 B) 2 C) 5 D) 1
Answer: C – Dilution Risk = FDV/Market Cap = $1B/$200M = 5 (very high dilution risk).

Q3. Which dilution risk ratio indicates LOW dilution risk?
A) 5.0 B) 3.5 C) 2.5 D) 1.1
Answer: D – Ratio ≈ 1 indicates low dilution; ratio ¿ 2 is high risk.

Q4. What does the NVT (Network Value to Transactions) ratio measure?
A) Token velocity B) Market cap relative to transaction volume C) Vesting schedule D) Holder concentration
Answer: B – NVT = Market Cap / Daily Tx Volume (USD); lower values suggest higher utility.

Q5. Which token allocation category typically has vesting schedules?
A) Public sale B) Airdrops C) Team and founders D) Staking rewards
Answer: C – Team/founder allocations usually vest over 2-4 years to align long-term incentives.

Quiz (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others

Quiz (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency

Quiz (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four prongs = Likely Security; failing "efforts of others" suggests utility token.

Q8. Which source is recommended for gathering current market data?
A) Twitter polls B) CoinGecko/CoinMarketCap C) Reddit forums D) Telegram groups

Quiz (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four prongs = Likely Security; failing "efforts of others" suggests utility token.

Q8. Which source is recommended for gathering current market data?
A) Twitter polls B) CoinGecko/CoinMarketCap C) Reddit forums D) Telegram groups
Answer: B – CoinGecko, CoinMarketCap, and project websites provide reliable market data.

Q9. What percentage of insider holdings typically raises red flags?
A) 10% B) 25% C) 50% D) 70%+

Quiz (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four prongs = Likely Security; failing "efforts of others" suggests utility token.

Q8. Which source is recommended for gathering current market data?
A) Twitter polls B) CoinGecko/CoinMarketCap C) Reddit forums D) Telegram groups
Answer: B – CoinGecko, CoinMarketCap, and project websites provide reliable market data.

Q9. What percentage of insider holdings typically raises red flags?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high insider concentration (70%+) creates centralization and dump risk.

Q10. Which metric helps identify if a token is overvalued relative to network activity?
A) Market cap B) Trading volume C) NVT ratio D) Circulating supply

Quiz (6–10)

Q6. What is the first prong of the Howey Test?
A) Expectation of profits B) Common enterprise C) Investment of money D) Efforts of others
Answer: C – The four prongs are: (1) Investment of money, (2) Common enterprise, (3) Expectation of profits, (4) Efforts of others.

Q7. A token passes all four prongs of the Howey Test. What is it likely classified as?
A) Utility token B) Security C) Commodity D) Currency
Answer: B – All four prongs = Likely Security; failing "efforts of others" suggests utility token.

Q8. Which source is recommended for gathering current market data?
A) Twitter polls B) CoinGecko/CoinMarketCap C) Reddit forums D) Telegram groups
Answer: B – CoinGecko, CoinMarketCap, and project websites provide reliable market data.

Q9. What percentage of insider holdings typically raises red flags?
A) 10% B) 25% C) 50% D) 70%+
Answer: D – Very high insider concentration (70%+) creates centralization and dump risk.

Q10. Which metric helps identify if a token is overvalued relative to network activity?
A) Market cap B) Trading volume C) NVT ratio D) Circulating supply
Answer: C – High NVT ratio suggests price may be high relative to actual network usage.

L33: Introduction to DeFi

Condensed Mini-Lecture — Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Define Decentralized Finance (DeFi) and its core principles
- Understand Total Value Locked (TVL) as a key metric
- Explore DeFi primitives: DEXs, lending, stablecoins
- Compare DeFi vs. Traditional Finance trade-offs

This condensed lecture covers the essential DeFi concepts in 10 minutes.

What is DeFi?

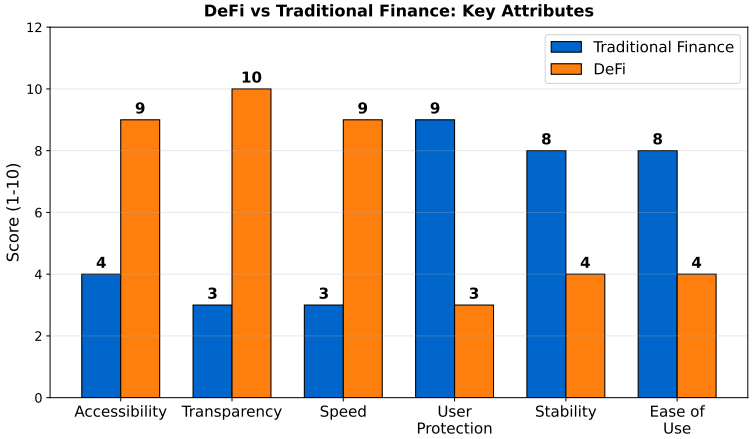
Definition: Financial services on blockchain without traditional intermediaries.

Five Core Principles:

- **Permissionless:** No approval needed – anyone with internet can access
- **Transparent:** All transactions visible on public blockchain
- **Non-custodial:** Users control their own private keys
- **Composable:** Protocols integrate like "money legos"
- **Programmable:** Smart contracts automate execution

Vision: Recreate finance with greater accessibility and transparency.

DeFi vs. Traditional Finance



DeFi excels in accessibility and transparency; TradFi offers stability and user protection.

Total Value Locked (TVL)

Definition: Total USD value of assets deposited in DeFi protocols.

What TVL Measures:

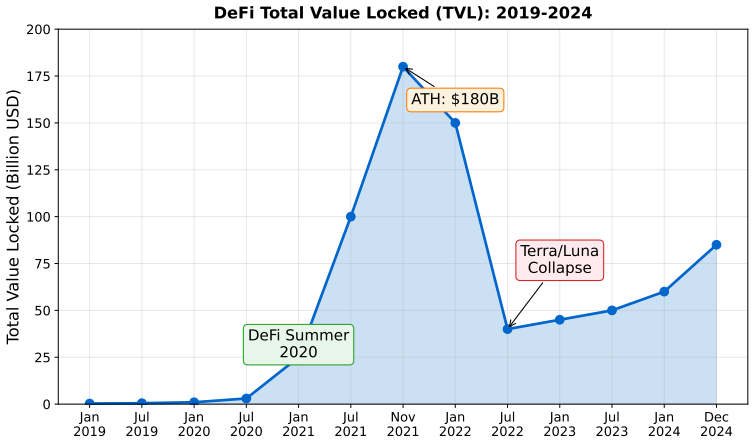
- Capital across lending, DEXs, staking, derivatives
- Proxy for DeFi adoption and liquidity depth

Current State (December 2025):

- Total DeFi TVL: approximately $130 billion
- Ethereum: approximately 55% of TVL
- Top protocols: Aave ($31B), Lido ($26B), EigenLayer ($12.6B)

TVL fluctuates with crypto prices; double-counting can inflate numbers.

The Rise of DeFi: TVL History



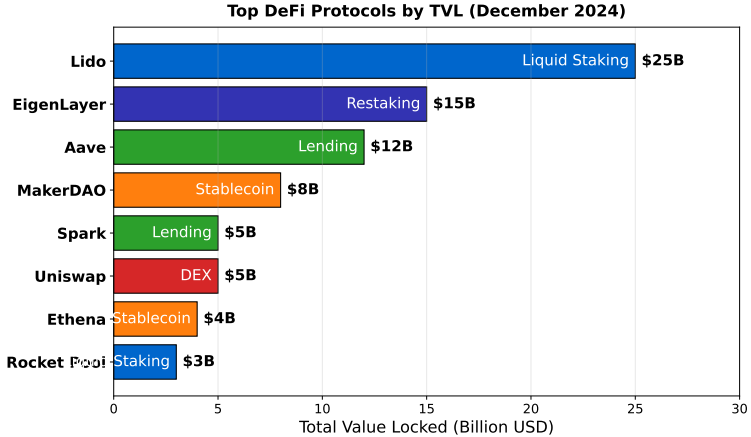
DeFi Summer 2020 marked explosive growth; 2022 bear market saw major correction.

Core DeFi Primitives

1. **Decentralized Exchanges (DEXs):** Token swapping without intermediaries (Uniswap, Curve)
2. **Lending & Borrowing:** Earn interest, borrow against collateral (Aave, Compound)
3. **Stablecoins:** Price-stable cryptocurrencies (USDC, DAI)
4. **Derivatives:** Futures, options, synthetics (dYdX, GMX)
5. **Yield Aggregators:** Automated yield optimization (Yearn Finance)

These primitives combine via composability to create complex financial products.

Top DeFi Protocols by TVL



Liquid staking (Lido) and lending (Aave) dominate; restaking (EigenLayer) is emerging.

Smart Contract Risk and Oracles

Smart Contract Vulnerabilities:

- Reentrancy attacks (DAO hack 2016)
- Oracle manipulation and front-running

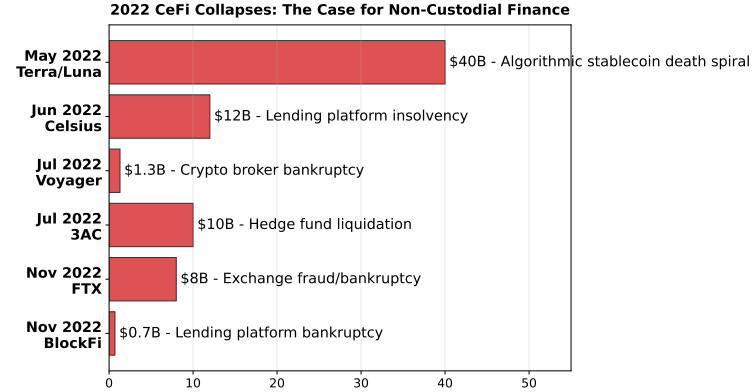
The Oracle Problem:

- Smart contracts cannot access off-chain data natively
- Solution: Oracles like Chainlink feed external prices on-chain

Mitigation: Professional audits, bug bounties, time-locks, multi-sig governance.

Security is paramount – always verify protocol audits before depositing.

2022 CeFi Collapses: The Case for DeFi



Celsius, FTX, BlockFi collapsed – DeFi protocols like Aave operated normally.

Future of DeFi

Emerging Trends:

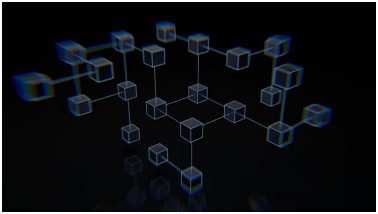
- **Real-World Assets (RWA):** Tokenizing bonds, real estate on-chain
- **Restaking (EigenLayer):** Reusing staked ETH to secure additional services
- **Cross-Chain DeFi:** Seamless interaction across blockchains
- **Institutional Adoption:** Banks exploring DeFi infrastructure

Long-Term Vision: DeFi as backend for traditional finance – 24/7 global settlement.

MiCA regulation in EU provides clearer framework for institutional adoption.

DeFi in Practice

Financial Markets



Decentralized Networks

24/7 Global Trading

Key Insight: DeFi combines the efficiency of traditional markets with blockchain's transparency and accessibility.

Images: Unsplash (CC0 License)

Quiz Questions (1–5)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries.

Q2. What does TVL (Total Value Locked) measure?
A) Users B) Transaction volume C) Assets in protocols D) Token prices
Answer: C – TVL is total USD value of assets deposited in DeFi.

Q3. Which blockchain dominates DeFi TVL (December 2025)?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds approximately 55% of DeFi TVL.

Q4. What problem do oracles solve?
A) High gas fees B) Slow transactions C) Off-chain data access D) Bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts.

Q5. What does "non-custodial" mean in DeFi?
A) No fees B) Users hold their keys C) No contracts D) Central control
Answer: B – Users control assets; no third party holds private keys.

Quiz Questions (6–10)

Q6. What does "composability" mean in DeFi?
A) Code reuse B) Protocols interact seamlessly C) Token swaps D) Wallet sync
Answer: B – Composability allows protocols to work together like "money legos."

Q7. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with approximately $31B TVL.

Q8. What is a reentrancy attack?
A) Oracle exploit B) Recursive function calls before completion C) Front-running D) Pool drain
Answer: B – Reentrancy exploits recursive calls (DAO hack 2016).

Q9. What happened during 2022 CeFi collapses?
A) DeFi failed B) Ethereum stopped C) CeFi froze assets D) Gas spiked
Answer: C – Celsius, FTX collapsed; DeFi protocols operated normally.

Q10. What is a major emerging DeFi trend?
A) Removing contracts B) Real-World Asset tokenization C) No oracles D) Centralized governance
Answer: B – RWA tokenization (bonds, real estate) is growing rapidly.

L33: Introduction to DeFi

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Define Decentralized Finance (DeFi) and its core principles
- Interpret Total Value Locked (TVL) as a key DeFi metric
- Describe the DeFi technology stack and core primitives
- Explain composability (money legos) and its risks

What is DeFi?

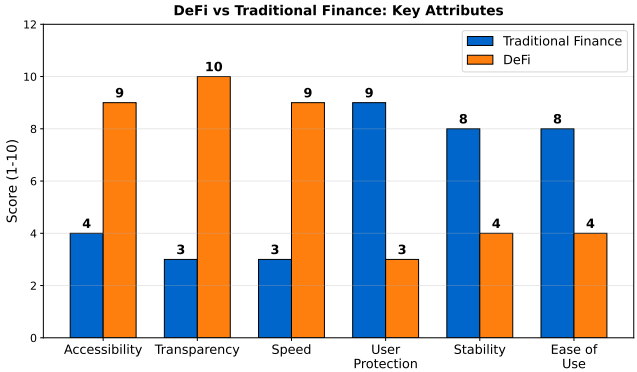
Definition: Financial services built on blockchain, operating without traditional intermediaries.

Core Principles:

- **Permissionless:** Anyone can access without approval
- **Transparent:** All transactions visible on blockchain
- **Non-custodial:** Users control their own assets
- **Composable:** Protocols integrate seamlessly (money legos)
- **Programmable:** Smart contracts automate execution

Vision: Recreate TradFi with greater accessibility, transparency, and efficiency.

DeFi vs Traditional Finance



Trade-off: DeFi offers accessibility and transparency but carries smart contract and regulatory risks.

Total Value Locked (TVL)

Definition: Total USD value of assets deposited in DeFi protocols.

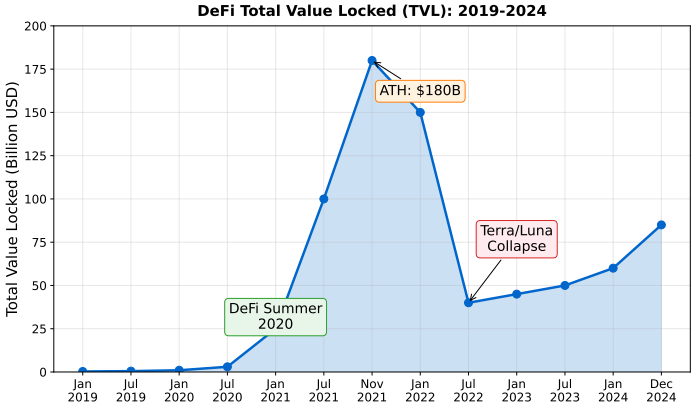
What TVL Measures:

- Capital deployed across lending, DEXs, staking, derivatives
- Proxy for DeFi adoption and trust
- Indicator of liquidity depth

Current State (January 2026):

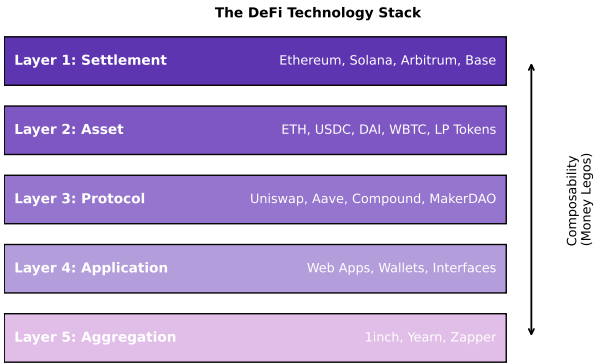
- Total DeFi TVL: $120 billion
- Ethereum: 61% of TVL ($72B)
- Top protocols: Aave ($34B), Lido ($26B), EigenLayer ($13B)

The Rise of DeFi: TVL History



DeFi Summer 2020: Explosive growth; 2022 bear market saw major correction.

The DeFi Technology Stack



Composability: Protocols build on each other like "money legos."

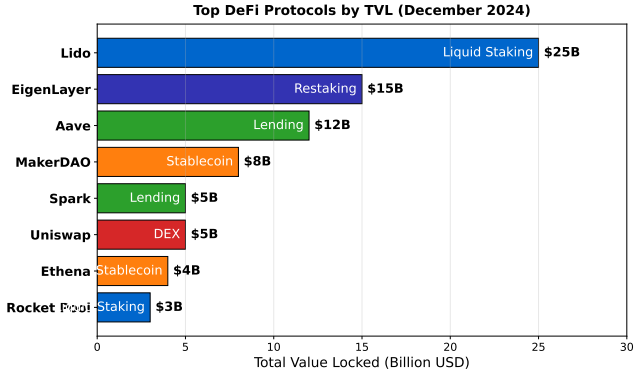
Core DeFi Primitives

1. **Decentralized Exchanges (DEXs):** Token swapping (Uniswap, Curve)
2. **Lending & Borrowing:** Earn interest, borrow against collateral (Aave)
3. **Stablecoins:** Price-stable cryptocurrencies (USDC, DAI)
4. **Derivatives:** Futures, options, synthetics (dYdX, GMX)
5. **Yield Aggregators:** Automated yield optimization (Yearn Finance)

2024 Innovation: Restaking (EigenLayer) – reusing staked ETH to secure additional services.

(c) Joerg Osterrieder 2025

Top DeFi Protocols by TVL



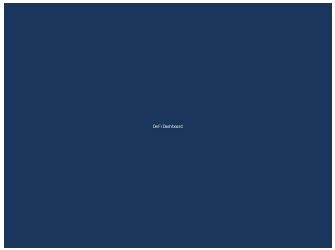
Liquid staking (Lido) and restaking (EigenLayer) dominate; lending and DEXs follow.

Key Takeaways

1. **DeFi:** Financial services on blockchain – permissionless, transparent, non-custodial
2. **TVL:** Key metric measuring capital deployed ($120B in January 2026)
3. **Core Primitives:** DEXs, lending, stablecoins, derivatives, yield aggregators
4. **Composability:** Money legos enable innovation but increase complexity/risk
5. **Ethereum Dominance:** 61% of TVL; L2s growing (Base leads with 43%)

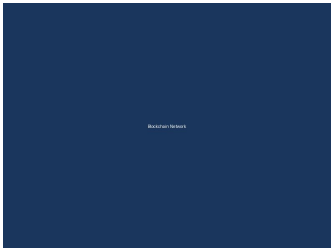
Next: L34 – AMM Mechanics (How automated market makers work)

DeFi in Practice



DeFi Dashboard

Trading Interface



Blockchain Network

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees

Quiz (1/2)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of banks.

Q2. Which is NOT a core DeFi principle?
A) Permissionless B) Transparent C) Custodial D) Composable

Quiz (1/2)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of banks.

Q2. Which is NOT a core DeFi principle?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their assets.

Q3. What does TVL measure?
A) Number of users B) Transaction volume C) Assets in protocols D) Token prices

Quiz (1/2)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of banks.

Q2. Which is NOT a core DeFi principle?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their assets.

Q3. What does TVL measure?
A) Number of users B) Transaction volume C) Assets in protocols D) Token prices
Answer: C – Total USD value of assets deposited.

Q4. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano

Quiz (1/2)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of banks.

Q2. Which is NOT a core DeFi principle?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their assets.

Q3. What does TVL measure?
A) Number of users B) Transaction volume C) Assets in protocols D) Token prices
Answer: C – Total USD value of assets deposited.

Q4. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds 61% of total DeFi TVL.

Q5. What does "composability" mean in DeFi?
A) Code reuse B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility

Quiz (1/2)

Q1. What distinguishes DeFi from Traditional Finance?
A) Higher rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of banks.

Q2. Which is NOT a core DeFi principle?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their assets.

Q3. What does TVL measure?
A) Number of users B) Transaction volume C) Assets in protocols D) Token prices
Answer: C – Total USD value of assets deposited.

Q4. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds 61% of total DeFi TVL.

Q5. What does "composability" mean in DeFi?
A) Code reuse B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Protocols work together like "money legos."

Quiz (2/2)

Q6. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound

Quiz (2/2)

Q6. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $34B TVL.

Q7. What is the main risk of composability?
A) Slower transactions B) Higher fees C) Cascading failures D) Reduced liquidity

Quiz (2/2)

Q6. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $34B TVL.

Q7. What is the main risk of composability?
A) Slower transactions B) Higher fees C) Cascading failures D) Reduced liquidity
Answer: C – One failure can cascade across connected protocols.

Q8. What problem do oracles solve?
A) High gas fees B) Slow transactions C) Off-chain data access D) Contract bugs

Quiz (2/2)

Q6. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $34B TVL.

Q7. What is the main risk of composability?
A) Slower transactions B) Higher fees C) Cascading failures D) Reduced liquidity
Answer: C – One failure can cascade across connected protocols.

Q8. What problem do oracles solve?
A) High gas fees B) Slow transactions C) Off-chain data access D) Contract bugs
Answer: C – Oracles feed external data (prices) to smart contracts.

Q9. What is restaking (EigenLayer)?
A) Unstaking ETH B) Reusing staked ETH for other services C) Staking multiple tokens D) Converting tokens

Quiz (2/2)

Q6. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $34B TVL.

Q7. What is the main risk of composability?
A) Slower transactions B) Higher fees C) Cascading failures D) Reduced liquidity
Answer: C – One failure can cascade across connected protocols.

Q8. What problem do oracles solve?
A) High gas fees B) Slow transactions C) Off-chain data access D) Contract bugs
Answer: C – Oracles feed external data (prices) to smart contracts.

Q9. What is restaking (EigenLayer)?
A) Unstaking ETH B) Reusing staked ETH for other services C) Staking multiple tokens D) Converting tokens
Answer: B – Reusing staked ETH to secure additional networks.

Q10. What does "non-custodial" mean?
A) No fees B) Users hold their own keys C) No contracts D) Centralized control

Quiz (2/2)

Q6. Which protocol had highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $34B TVL.

Q7. What is the main risk of composability?
A) Slower transactions B) Higher fees C) Cascading failures D) Reduced liquidity
Answer: C – One failure can cascade across connected protocols.

Q8. What problem do oracles solve?
A) High gas fees B) Slow transactions C) Off-chain data access D) Contract bugs
Answer: C – Oracles feed external data (prices) to smart contracts.

Q9. What is restaking (EigenLayer)?
A) Unstaking ETH B) Reusing staked ETH for other services C) Staking multiple tokens D) Converting tokens
Answer: B – Reusing staked ETH to secure additional networks.

Q10. What does "non-custodial" mean?
A) No fees B) Users hold their own keys C) No contracts D) Centralized control
Answer: B – Users control assets; no third party holds keys.

Thank you

Questions?

Next: L34 – AMM Mechanics

L33: Introduction to DeFi

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Define Decentralized Finance (DeFi) and its core principles
- Interpret Total Value Locked (TVL) as a key DeFi metric
- Explore the DeFi technology stack
- Analyze composability and its implications
- Compare DeFi to Traditional Finance (TradFi)

The Problem: What is decentralized finance?

The Challenge
Traditional financial systems exclude 1.4 billion unbanked adults worldwide, charge high fees for basic services, and require trust in intermediaries. Can we create financial services that are accessible to anyone with internet access, operate 24/7 without banks, and execute automatically without human intervention?

Why It Matters

- Traditional finance excludes billions due to KYC/AML requirements and geographic restrictions
- Centralized intermediaries charge high fees and introduce counterparty risk (FTX, Celsius collapses 2022)
- MakerDAO (2017) pioneered decentralized stablecoins; Compound (2018) introduced money markets; DeFi Summer (2020) saw explosive growth to $15B TVL

What We Need

- Trustless verification mechanism
- Financial services operating without intermediaries
- Programmable money that executes automatically
- Protocols that can compose like building blocks

The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How DeFi addresses financial inclusion through blockchain-based protocols

What is DeFi?

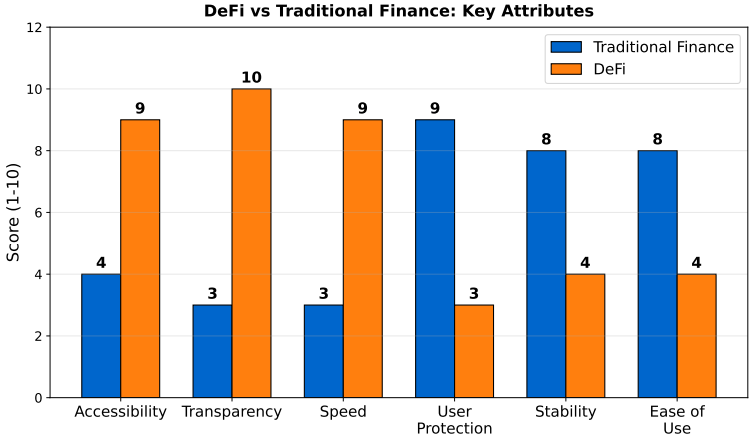
Definition: Decentralized Finance (DeFi) refers to financial services built on blockchain networks, operating without traditional intermediaries.

Core Principles:

- **Permissionless:** Anyone can access without approval
- **Transparent:** All transactions visible on blockchain
- **Non-custodial:** Users control their own assets
- **Composable:** Protocols integrate seamlessly (money legos)
- **Programmable:** Smart contracts automate execution

Vision: Recreate traditional financial system with greater accessibility, transparency, and efficiency.

DeFi vs. Traditional Finance



DeFi excels in accessibility and transparency; TradFi offers stability and user protection

DeFi vs. TradFi: Key Differences

Traditional Finance (TradFi)

- Centralized intermediaries (banks)
- KYC/AML requirements
- Business hours, slow settlements
- Geographic restrictions
- High barriers to entry

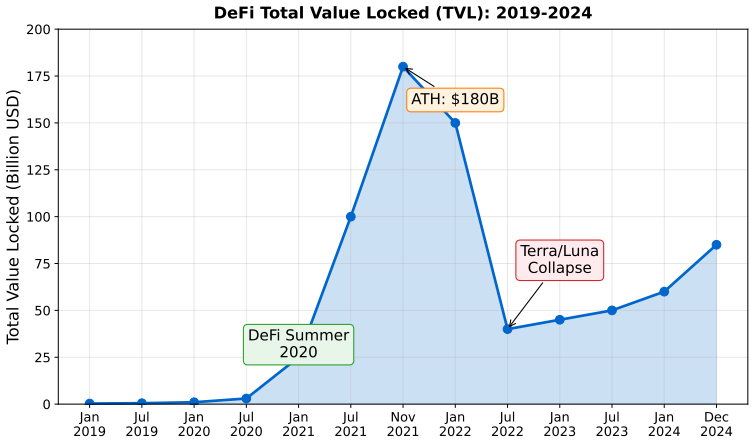
Decentralized Finance (DeFi)

- Smart contracts (no intermediaries)
- Pseudonymous (wallet addresses)
- 24/7 operation, instant settlement
- Global access
- Low barriers (internet + wallet)

Trade-off: DeFi offers accessibility and transparency but carries smart contract risks and regulatory uncertainty.

(c) Joerg Osterrieder 2025

The Rise of DeFi: TVL History



DeFi Summer 2020 marked explosive growth; 2022 bear market saw major correction

Total Value Locked (TVL)

Definition: The total amount of assets deposited in DeFi protocols, measured in USD.

What TVL Measures:

- Capital deployed across lending, DEXs, staking, derivatives
- Proxy for DeFi adoption and trust
- Indicator of liquidity depth

Current State (January 2026):

- Total DeFi TVL: $120 billion (consolidated from December 2024 peak of $140B)
- Ethereum: 61% of TVL ($72B); Base L2 at 43% of L2 market share
- Top protocols: Aave ($34B), Lido ($26B), EigenLayer ($13B)

TVL Calculation Example

Hypothetical Lending Protocol:

Deposits:

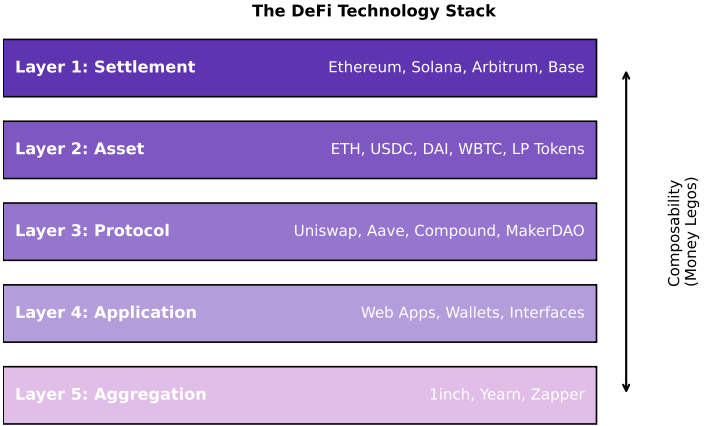
- 1,000 ETH at \$2,000/ETH = \$2,000,000
- 500,000 USDC at \$1/USDC = \$500,000
- 10 BTC at \$40,000/BTC = \$400,000

Total TVL:

$$\text{TVL} = \$2{,}000{,}000 + \$500{,}000 + \$400{,}000 = \$2{,}900{,}000$$

Note: TVL fluctuates with crypto prices; double-counting can inflate numbers.

The DeFi Technology Stack

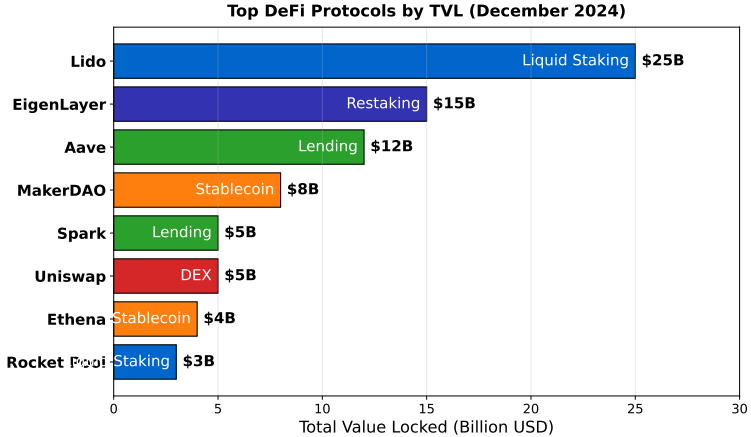


Composability allows protocols to build on each other like "money legos"

Core DeFi Primitives

1. **Decentralized Exchanges (DEXs)**
   - Token swapping without intermediaries (Uniswap, Curve)
2. **Lending & Borrowing**
   - Earn interest on deposits, borrow against collateral (Aave, Compound)
3. **Stablecoins**
   - Price-stable cryptocurrencies (USDC, DAI)
4. **Derivatives**
   - Futures, options, synthetic assets (dYdX, GMX)
5. **Yield Aggregators**
   - Automated yield optimization (Yearn Finance)

Top DeFi Protocols by TVL



Liquid staking (Lido) and restaking (EigenLayer) dominate; lending and DEXs follow

Composability: Money Legos

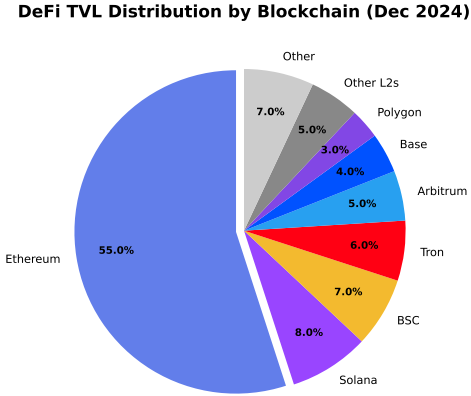
Definition: DeFi protocols can interact seamlessly, allowing complex strategies by combining simple primitives.

Example Workflow:

1. Deposit ETH in Aave, receive aETH (interest-bearing token)
2. Use aETH as collateral to borrow DAI
3. Swap DAI for USDC on Uniswap
4. Deposit USDC in Curve for yield farming

Benefits: Capital efficiency, innovation from combinations
Risks: Complexity increases attack surface, protocol failure can cascade

DeFi TVL by Blockchain



Ethereum maintains dominance; Layer 2s growing share rapidly

Ethereum dominates; L2s growing rapidly

Smart Contract Risk

Definition: Bugs, exploits, or design flaws in smart contract code.

Common Vulnerabilities:

- Reentrancy attacks (famous: DAO hack 2016)
- Oracle manipulation
- Front-running and MEV exploitation
- Access control failures

Mitigation:

- Professional audits (Trail of Bits, OpenZeppelin)
- Bug bounties, formal verification
- Time-locks and multi-sig governance

(c) Joerg Osterrieder 2025

Oracle Problem

Challenge: Smart contracts can't natively access off-chain data (e.g., ETH price).

Solution: Oracles

- Third-party services that feed external data on-chain
- Example: Chainlink (decentralized oracle network)

Oracle Types:

- **Centralized:** Single trusted source (fast but risky)
- **Decentralized:** Multiple providers aggregated (Chainlink)
- **On-chain:** Data derived from blockchain state (Uniswap TWAP)

Risk: Oracle manipulation can drain DeFi protocols (flash loan attacks).

Permissionless and Non-Custodial

Permissionless Access:

- No identity verification, no geographic restrictions
- Only need: internet connection + crypto wallet
- Benefits: Financial inclusion, censorship resistance

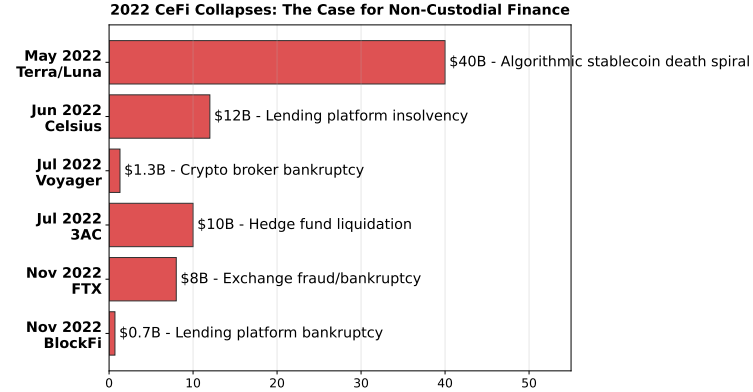
Non-Custodial Finance:

- You hold private keys, smart contract holds funds during interaction
- No third party can freeze or seize
- **Positive:** True ownership, no counterparty risk
- **Negative:** No recovery if you lose keys

Mantra: Not your keys, not your coins.

(c) Joerg Osterrieder 2025

2022 CeFi Collapses: The Case for DeFi



CeFi custodial risk exposed; DeFi protocols like Aave and Uniswap operated normally

DeFi vs. CeFi Comparison

Centralized Crypto Platforms: Coinbase, Binance, BlockFi (collapsed 2022), Celsius (collapsed 2022)

CeFi Advantages

- User-friendly interfaces
- Customer support
- Fiat on/off ramps

CeFi Risks

- Custodial (platform holds assets)
- Counterparty risk (FTX collapse)
- Can freeze accounts

2022 Lesson: Multiple CeFi platforms collapsed (Celsius, FTX), highlighting custodial risk. DeFi protocols survived.

2024 Innovation: Restaking (EigenLayer)

What is Restaking?

- Reusing staked ETH to secure additional networks/services
- Introduced by EigenLayer (major growth 2024)

How It Works:

1. Stake ETH with Ethereum validators (earn 3-4% APY)
2. Opt-in to restaking via EigenLayer
3. Earn extra yield from securing additional services (AVS)

Impact:

- EigenLayer peaked at $19B (June 2024), now $12.6B (December 2025)
- Liquid Restaking Tokens (LRTs): eETH, rsETH, ezETH
- Criticism: Added systemic risk, complexity

Future of DeFi

Emerging Trends:

- **Real-World Assets (RWA):** Tokenizing bonds, real estate
- **Undercollateralized Lending:** Credit scoring on-chain
- **Cross-Chain DeFi:** Seamless interaction across blockchains
- **Institutional Adoption:** Banks exploring DeFi rails
- **Regulation:** Clearer frameworks emerging (MiCA in EU)

Long-Term Vision:

- DeFi as backend infrastructure for TradFi
- 24/7 settlement for global finance
- Financial inclusion for billions

(c) Joerg Osterrieder 2025

Problem Solved? DeFi Introduction

The Original Problem

What is decentralized finance?

How DeFi Solves It

- Smart contracts replace banks and brokers, enabling permissionless access without KYC/AML requirements
- Composability allows protocols to build on each other (Aave $\rightarrow$ Uniswap $\rightarrow$ Curve), creating capital-efficient strategies
- 24/7 operation with instant settlement removes geographic restrictions and business hours

Remaining Limitations

- Smart contract risk: Code bugs and exploits (DAO hack 2016, \$60M loss)
- Oracle dependence: External data manipulation can drain protocols (flash loan attacks)
- Regulatory uncertainty: Unclear legal frameworks for decentralized protocols

Open Questions

- Can DeFi achieve mainstream adoption without sacrificing decentralization?
- How to balance regulatory compliance with permissionless access?

DeFi enables financial services without intermediaries but introduces new technical and regulatory risks

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- DeFi recreates financial services on blockchain: permissionless, transparent, non-custodial
- TVL measures capital deployed ($120B in January 2026, consolidated from December 2024 peak)
- Composability enables innovation but increases complexity
- Smart contract risk and oracle manipulation are key concerns
- Restaking (EigenLayer) emerged as major 2024 innovation (peaked $19B)
- Ethereum dominates (61%); Base L2 leads Layer 2 ecosystem (43% share)

Next Lecture: AMM Mechanics - How automated market makers work.

Questions for Reflection

1. How does TVL differ from traditional finance metrics like AUM?
2. Why is composability both a strength and a risk in DeFi?
3. What are the trade-offs between DeFi and CeFi for retail users?
4. How do oracles solve the external data problem, and what risks remain?
5. What regulatory challenges does DeFi face in the next 5 years?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices
Answer: C – TVL is the total USD value of assets deposited across DeFi protocols.

Q4. As of January 2026, what is the approximate total DeFi TVL?
A) $50 billion B) $80 billion C) $120 billion D) $200 billion
Answer: C – DeFi TVL is $120B as of January 2026, consolidated from 2024 peak.

Q5. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds 61% of total DeFi TVL as of January 2026.

Quiz Questions (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity
Answer: C – Complex protocol interactions increase attack surface; one failure can cascade.

Q9. What is a reentrancy attack?
A) Exploiting oracle data B) Calling a function recursively before it completes C) Front-running trades D) Draining liquidity pools
Answer: B – Reentrancy exploits recursive calls (famous example: DAO hack 2016).

Q10. Which of the following is NOT a DeFi primitive?
A) Decentralized Exchanges B) Lending & Borrowing C) Custodial wallets D) Stablecoins
Answer: C – Custodial wallets are centralized; DeFi uses non-custodial wallets.

Quiz Questions (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings
Answer: B – Anyone can access DeFi without identity verification or approval.

Q14. What happened during the 2022 CeFi collapses?
A) DeFi protocols failed B) Ethereum stopped working C) Centralized platforms froze assets D) Gas fees spiked
Answer: C – Celsius, FTX, and BlockFi collapsed, but DeFi protocols operated normally.

Q15. What is the main advantage of CeFi over DeFi?
A) Decentralization B) User-friendly interfaces C) Lower fees D) Smart contracts
Answer: B – CeFi offers better UX, customer support, and fiat on/off ramps.

Quiz Questions (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads Layer 2 ecosystem with 43% market share as of December 2025.

Q19. What does "non-custodial" mean in DeFi?
A) No transaction fees B) Users hold their own private keys C) No smart contracts D) Centralized control
Answer: B – Non-custodial means users control assets; no third party holds keys.

Q20. What is a major emerging trend in DeFi's future?
A) Removing smart contracts B) Tokenizing Real-World Assets C) Eliminating oracles D) Centralized governance
Answer: B – RWA tokenization (bonds, real estate) is a growing DeFi trend.

L33: Introduction to DeFi

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Banks Hate This Trick

[COMIC: Banks hate this trick]

Placeholder for comic showing traditional bank gatekeeping vs. open DeFi access

The Setup

- Traditional finance: permission required
- Banks as gatekeepers
- Geographic and identity restrictions

The Punchline

- DeFi: permissionless access
- Smart contracts replace bankers
- Anyone with internet can participate

What if finance worked without asking permission?

(c) Joerg Osterrieder 2025

Learning Objectives

- Define Decentralized Finance (DeFi) and its core principles
- Interpret Total Value Locked (TVL) as a key DeFi metric
- Explore the DeFi technology stack
- Analyze composability and its implications
- Compare DeFi to Traditional Finance (TradFi)

Building on L32: Lab: Tokenomics Analysis

The Problem: What is decentralized finance?

The Challenge
Traditional financial systems exclude 1.4 billion unbanked adults worldwide, charge high fees for basic services, and require trust in intermediaries. Can we create financial services that are accessible to anyone with internet access, operate 24/7 without banks, and execute automatically without human intervention?

Why It Matters

- Traditional finance excludes billions due to KYC/AML requirements and geographic restrictions
- Centralized intermediaries charge high fees and introduce counterparty risk (FTX, Celsius collapses 2022)
- MakerDAO (2017) pioneered decentralized stablecoins; Compound (2018) introduced money markets; DeFi Summer (2020) saw explosive growth to $15B TVL

What We Need

- Trustless verification mechanism
- Financial services operating without intermediaries
- Programmable money that executes automatically
- Protocols that can compose like building blocks

The Cryptoeconomics Question
Coordinating without trusted intermediaries

Today's lesson: How DeFi addresses financial inclusion through blockchain-based protocols

What Is DeFi and Why Does It Matter?

Definition: Decentralized Finance (DeFi) refers to financial services built on blockchain networks, operating without traditional intermediaries.

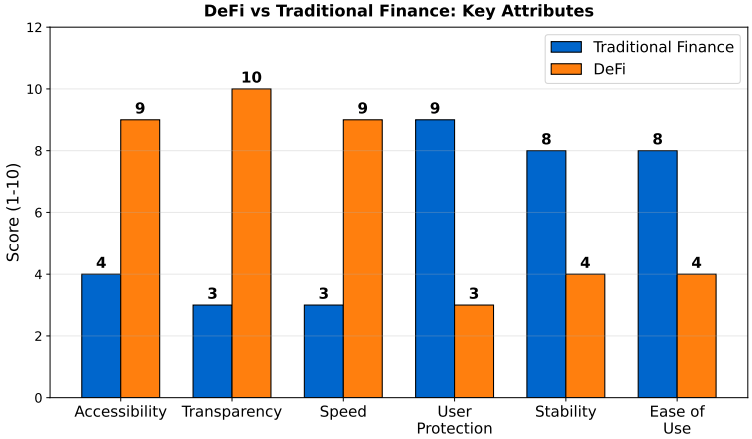
Core Principles:

- **Permissionless:** Anyone can access without approval
- **Transparent:** All transactions visible on blockchain
- **Non-custodial:** Users control their own assets
- **Composable:** Protocols integrate seamlessly (money legos)
- **Programmable:** Smart contracts automate execution

Vision: Recreate traditional financial system with greater accessibility, transparency, and efficiency.

→ *Problem: What is decentralized finance? — What is DeFi? DeFi's core principles directly answer "what is decentralized finance" – finance without banks.*

How Does DeFi Compare to Traditional Finance?



DeFi excels in accessibility and transparency; TradFi offers stability and user protection

What Are the Key Differences Between DeFi and TradFi?

Traditional Finance (TradFi)

- Centralized intermediaries (banks)
- KYC/AML requirements
- Business hours, slow settlements
- Geographic restrictions
- High barriers to entry

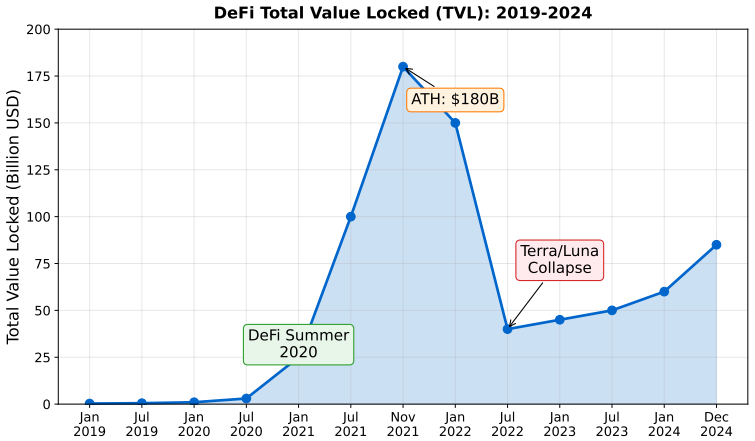
Decentralized Finance (DeFi)

- Smart contracts (no intermediaries)
- Pseudonymous (wallet addresses)
- 24/7 operation, instant settlement
- Global access
- Low barriers (internet + wallet)

Trade-off: DeFi offers accessibility and transparency but carries smart contract risks and regulatory uncertainty.

(c) Joerg Osterrieder 2025

How Has DeFi TVL Evolved Over Time?



DeFi Summer 2020 marked explosive growth; 2022 bear market saw major correction

What Does Total Value Locked (TVL) Measure?

Definition: The total amount of assets deposited in DeFi protocols, measured in USD.

What TVL Measures:

- Capital deployed across lending, DEXs, staking, derivatives
- Proxy for DeFi adoption and trust
- Indicator of liquidity depth

Current State (January 2026):

- Total DeFi TVL: $120 billion (consolidated from December 2024 peak of $140B)
- Ethereum: 61% of TVL ($72B); Base L2 at 43% of L2 market share
- Top protocols: Aave ($34B), Lido ($26B), EigenLayer ($13B)

→ Problem: What is decentralized finance? — Total Value Locked (TVL) TVL measures how much money people trust in DeFi – higher TVL = more confidence that decentralized finance works.

How Is TVL Calculated?

Hypothetical Lending Protocol:

Deposits:

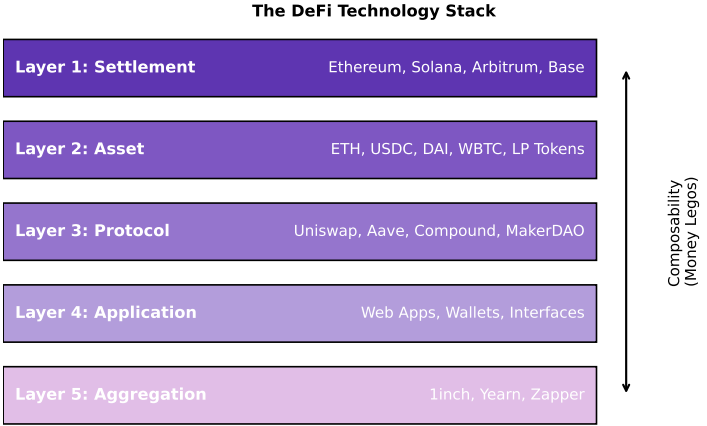
- 1,000 ETH at \$2,000/ETH = \$2,000,000
- 500,000 USDC at \$1/USDC = \$500,000
- 10 BTC at \$40,000/BTC = \$400,000

Total TVL:

$$\text{TVL} = \$2{,}000{,}000 + \$500{,}000 + \$400{,}000 = \$2{,}900{,}000$$

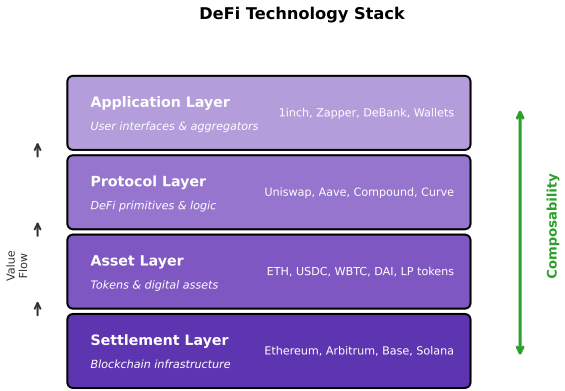
Note: TVL fluctuates with crypto prices; double-counting can inflate numbers.

What Are the Layers of the DeFi Technology Stack?



Composability allows protocols to build on each other like "money legos"

How Do the DeFi Stack Layers Interact?

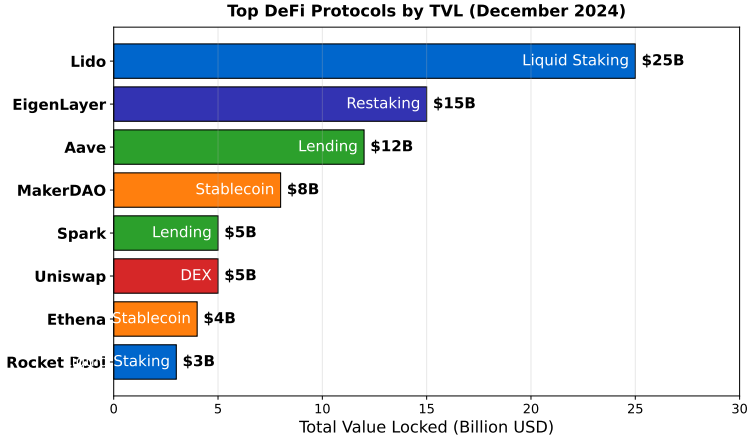


Each layer builds on the one below; value flows up through the stack

What Are the Core DeFi Building Blocks?

1. **Decentralized Exchanges (DEXs)**
   - Token swapping without intermediaries (Uniswap, Curve)
2. **Lending & Borrowing**
   - Earn interest on deposits, borrow against collateral (Aave, Compound)
3. **Stablecoins**
   - Price-stable cryptocurrencies (USDC, DAI)
4. **Derivatives**
   - Futures, options, synthetic assets (dYdX, GMX)
5. **Yield Aggregators**
   - Automated yield optimization (Yearn Finance)

Which Protocols Lead DeFi by TVL?



Liquid staking (Lido) and restaking (EigenLayer) dominate; lending and DEXs follow

Problem Check-In: DeFi Introduction

Recall Our Problem

What is decentralized finance?

What We've Learned So Far

- DeFi replaces banks with smart contracts (self-executing code on blockchain)
- TVL (Total Value Locked) measures trust: $120B deposited in DeFi protocols
- Together they show DeFi is real and growing – billions trusted to code, not banks

Still to Address

- Risks: smart contract bugs, oracle attacks, regulatory uncertainty
- Can DeFi scale to mainstream adoption without sacrificing decentralization?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "What is decentralized finance?"?

How Do DeFi Protocols Build on Each Other?

Definition: DeFi protocols can interact seamlessly, allowing complex strategies by combining simple primitives.

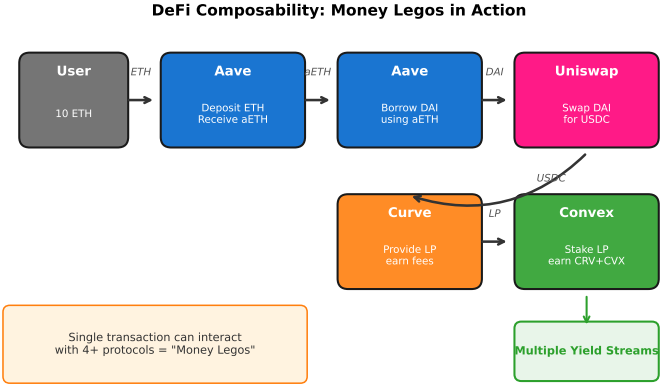
Example Workflow:

1. Deposit ETH in Aave, receive aETH (interest-bearing token)
2. Use aETH as collateral to borrow DAI
3. Swap DAI for USDC on Uniswap
4. Deposit USDC in Curve for yield farming (depositing crypto into DeFi protocols to earn interest or rewards)

Benefits: Capital efficiency, innovation from combinations
Risks: Complexity increases attack surface, protocol failure can cascade

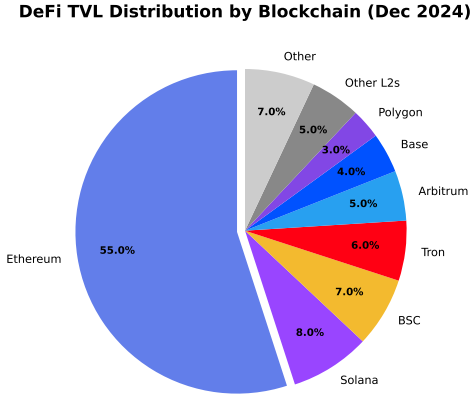
→ Problem: What is decentralized finance? — Composability: Money Legos Composability ("money legos") makes DeFi powerful – protocols stack like building blocks.

How Does Composability Work in Practice?



A single user can chain multiple protocols in one transaction for yield optimization

Which Blockchains Dominate DeFi TVL?



Ethereum maintains dominance; Layer 2s growing share rapidly

Ethereum dominates; L2s growing rapidly

What Can Go Wrong with Smart Contracts?

Definition: Bugs, exploits, or design flaws in smart contract code.

Common Vulnerabilities:

- Reentrancy attacks (famous: DAO hack 2016)
- Oracle (external data feed) manipulation
- Front-running and MEV exploitation
- Access control failures

Mitigation:

- Professional audits (Trail of Bits, OpenZeppelin)
- Bug bounties, formal verification
- Time-locks and multi-sig governance

How Do Smart Contracts Get External Data?

Challenge: Smart contracts can't natively access off-chain data (e.g., ETH price).

Solution: Oracles

- Third-party services that feed external data on-chain
- Example: Chainlink (decentralized oracle network)

Oracle Types:

- **Centralized:** Single trusted source (fast but risky)
- **Decentralized:** Multiple providers aggregated (Chainlink)
- **On-chain:** Data derived from blockchain state (Uniswap TWAP)

Risk: Oracle manipulation can drain DeFi protocols (flash loan attacks).

What Makes DeFi Permissionless?

Permissionless Access:

- No identity verification, no geographic restrictions
- Only need: internet connection + crypto wallet
- Benefits: Financial inclusion, censorship resistance

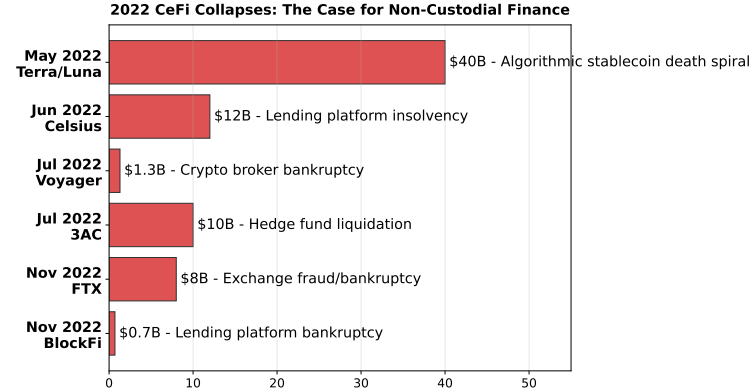
Non-Custodial Finance:

- You hold private keys, smart contract holds funds during interaction
- No third party can freeze or seize
- **Positive:** True ownership, no counterparty risk
- **Negative:** No recovery if you lose keys

Mantra: Not your keys, not your coins.

→ *Problem: What is decentralized finance? — Permissionless and Non-Custodial Permissionless access means anyone with internet can use DeFi – removing gatekeepers entirely.*

What Did the 2022 CeFi Collapses Reveal?



CeFi custodial risk exposed; DeFi protocols like Aave and Uniswap operated normally

How Does DeFi Compare to CeFi Platforms?

Centralized Crypto Platforms: Coinbase, Binance, BlockFi (collapsed 2022), Celsius (collapsed 2022)

CeFi Advantages

- User-friendly interfaces
- Customer support
- Fiat on/off ramps

CeFi Risks

- Custodial (platform holds assets)
- Counterparty risk (FTX collapse)
- Can freeze accounts

2022 Lesson: Multiple CeFi platforms collapsed (Celsius, FTX), highlighting custodial risk. DeFi protocols survived.

What Is Restaking and Why Does It Matter?

What is Restaking?

- Reusing staked ETH to secure additional networks/services
- Introduced by EigenLayer (major growth 2024)

How It Works:

1. Stake ETH with Ethereum validators (earn 3-4% APY)
2. Opt-in to restaking via EigenLayer
3. Earn extra yield from securing additional services (AVS)

Impact:

- EigenLayer peaked at $19B (June 2024), now $12.6B (December 2025)
- Liquid Restaking Tokens (LRTs): eETH, rsETH, ezETH
- Criticism: Added systemic risk, complexity

Where Is DeFi Heading Next?

Emerging Trends:

- **Real-World Assets (RWA):** Tokenizing bonds, real estate
- **Undercollateralized Lending:** Credit scoring on-chain
- **Cross-Chain DeFi:** Seamless interaction across blockchains
- **Institutional Adoption:** Banks exploring DeFi rails
- **Regulation:** Clearer frameworks emerging (MiCA in EU)

Long-Term Vision:

- DeFi as backend infrastructure for TradFi
- 24/7 settlement for global finance
- Financial inclusion for billions

(c) Joerg Osterrieder 2025

Problem Solved? DeFi Introduction

The Original Problem

What is decentralized finance?

How DeFi Solves It

- Smart contracts replace banks and brokers, enabling permissionless access without KYC/AML requirements
- Composability allows protocols to build on each other (Aave $\rightarrow$ Uniswap $\rightarrow$ Curve), creating capital-efficient strategies
- 24/7 operation with instant settlement removes geographic restrictions and business hours

Remaining Limitations

- Smart contract risk: Code bugs and exploits (DAO hack 2016, \$60M loss)
- Oracle dependence: External data manipulation can drain protocols (flash loan attacks)
- Regulatory uncertainty: Unclear legal frameworks for decentralized protocols

Open Questions

- Can DeFi achieve mainstream adoption without sacrificing decentralization?
- How to balance regulatory compliance with permissionless access?

DeFi enables financial services without intermediaries but introduces new technical and regulatory risks

(c) Joerg Osterrieder 2025

The Economics of DeFi Introduction

Incentive Structure

- **Core Problem:** Coordinating without trusted intermediaries
- **Why act honestly?** Participants verify rather than trust
- **Value Flow:** Users gain trustlessness, pay in complexity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users gain trustlessness, pay in complexity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: DeFi Introduction

Alternatives Considered

1. **Chosen Design:** Permissioned vs permissionless
2. **Alternative:** Traditional trusted third parties

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: DeFi Introduction

Critical Failure Mode

- **What breaks:** Sybil attacks, eclipse attacks
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Composability Risk Stack

[COMIC: Composability risk stack]

Placeholder for comic showing "money legos" stacked precariously, with one piece failing and whole tower collapsing

The Reality Check

- Composability = power + risk
- Each protocol layer adds vulnerability
- One failure can cascade through stack

Warning Signs

- Complex yield strategies
- Multiple protocol dependencies
- "Too good to be true" returns

Money legos are powerful – until one piece fails and the whole tower falls

Summary: Key Takeaways

Key Takeaways:

- DeFi recreates financial services on blockchain: permissionless, transparent, non-custodial
- TVL measures capital deployed ($120B in January 2026, consolidated from December 2024 peak)
- Composability enables innovation but increases complexity
- Smart contract risk and oracle manipulation are key concerns
- Restaking (EigenLayer) emerged as major 2024 innovation (peaked $19B)
- Ethereum dominates (61%); Base L2 leads Layer 2 ecosystem (43% share)

Next Lecture: AMM Mechanics - How automated market makers work.

Next Lesson: L34 – AMM Mechanics

Questions for Reflection

1. How does TVL differ from traditional finance metrics like AUM?
2. Why is composability both a strength and a risk in DeFi?
3. What are the trade-offs between DeFi and CeFi for retail users?
4. How do oracles solve the external data problem, and what risks remain?
5. What regulatory challenges does DeFi face in the next 5 years?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices
Answer: C – TVL is the total USD value of assets deposited across DeFi protocols.

Q4. As of January 2026, what is the approximate total DeFi TVL?
A) $50 billion B) $80 billion C) $120 billion D) $200 billion
Answer: C – DeFi TVL is $120B as of January 2026, consolidated from 2024 peak.

Q5. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds 61% of total DeFi TVL as of January 2026.

Quiz Questions (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity
Answer: C – Complex protocol interactions increase attack surface; one failure can cascade.

Q9. What is a reentrancy attack?
A) Exploiting oracle data B) Calling a function recursively before it completes C) Front-running trades D) Draining liquidity pools
Answer: B – Reentrancy exploits recursive calls (famous example: DAO hack 2016).

Q10. Which of the following is NOT a DeFi primitive?
A) Decentralized Exchanges B) Lending & Borrowing C) Custodial wallets D) Stablecoins
Answer: C – Custodial wallets are centralized; DeFi uses non-custodial wallets.

Quiz Questions (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings
Answer: B – Anyone can access DeFi without identity verification or approval.

Q14. What happened during the 2022 CeFi collapses?
A) DeFi protocols failed B) Ethereum stopped working C) Centralized platforms froze assets D) Gas fees spiked
Answer: C – Celsius, FTX, and BlockFi collapsed, but DeFi protocols operated normally.

Q15. What is the main advantage of CeFi over DeFi?
A) Decentralization B) User-friendly interfaces C) Lower fees D) Smart contracts
Answer: B – CeFi offers better UX, customer support, and fiat on/off ramps.

Quiz Questions (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads Layer 2 ecosystem with 43% market share as of December 2025.

Q19. What does "non-custodial" mean in DeFi?
A) No transaction fees B) Users hold their own private keys C) No smart contracts D) Centralized control
Answer: B – Non-custodial means users control assets; no third party holds keys.

Q20. What is a major emerging trend in DeFi's future?
A) Removing smart contracts B) Tokenizing Real-World Assets C) Eliminating oracles D) Centralized governance
Answer: B – RWA tokenization (bonds, real estate) is a growing DeFi trend.

Quiz: Intro DeFi

Instructions: 23 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees

Quiz (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable

Quiz (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices

Quiz (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices
Answer: C – TVL is the total USD value of assets deposited across DeFi protocols.

Q4. As of December 2025, what is the approximate total DeFi TVL?
A) $50 billion B) $88 billion C) $130 billion D) $200 billion

Quiz (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices
Answer: C – TVL is the total USD value of assets deposited across DeFi protocols.

Q4. As of December 2025, what is the approximate total DeFi TVL?
A) $50 billion B) $88 billion C) $130 billion D) $200 billion
Answer: C – DeFi TVL recovered to $130B after dipping to $88B in March 2025.

Q5. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano

Quiz (1–5)

Q1. What is the primary characteristic that distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries like banks.

Q2. Which of the following is NOT a core principle of DeFi?
A) Permissionless B) Transparent C) Custodial D) Composable
Answer: C – DeFi is non-custodial; users control their own assets with private keys.

Q3. What does TVL (Total Value Locked) measure?
A) Number of users B) Transaction volume C) Assets deposited in protocols D) Token prices
Answer: C – TVL is the total USD value of assets deposited across DeFi protocols.

Q4. As of December 2025, what is the approximate total DeFi TVL?
A) \$50 billion B) \$88 billion C) \$130 billion D) \$200 billion
Answer: C – DeFi TVL recovered to \$130B after dipping to \$88B in March 2025.

Q5. Which blockchain dominates DeFi TVL?
A) Bitcoin B) Ethereum C) Solana D) Cardano
Answer: B – Ethereum holds 55% of total DeFi TVL as of December 2025.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What does “composability” mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility

Quiz (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound

Quiz (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity

Quiz (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity
Answer: C – Complex protocol interactions increase attack surface; one failure can cascade.

Q9. What is a reentrancy attack?
A) Exploiting oracle data B) Calling a function recursively before it completes C) Front-running trades D) Draining liquidity pools

Quiz (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity
Answer: C – Complex protocol interactions increase attack surface; one failure can cascade.

Q9. What is a reentrancy attack?
A) Exploiting oracle data B) Calling a function recursively before it completes C) Front-running trades D) Draining liquidity pools
Answer: B – Reentrancy exploits recursive calls (famous example: DAO hack 2016).

Q10. Which of the following is NOT a DeFi primitive?
A) Decentralized Exchanges B) Lending & Borrowing C) Custodial wallets D) Stablecoins

Quiz (6–10)

Q6. What does "composability" mean in the context of DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows DeFi protocols to work together like "money legos."

Q7. Which protocol had the highest TVL in December 2025?
A) Uniswap B) Curve C) Aave D) Compound
Answer: C – Aave leads with $31B TVL, followed by Lido ($26B).

Q8. What is the main risk of composability in DeFi?
A) Slower transactions B) Higher gas fees C) Cascading failures D) Reduced liquidity
Answer: C – Complex protocol interactions increase attack surface; one failure can cascade.

Q9. What is a reentrancy attack?
A) Exploiting oracle data B) Calling a function recursively before it completes C) Front-running trades D) Draining liquidity pools
Answer: B – Reentrancy exploits recursive calls (famous example: DAO hack 2016).

Q10. Which of the following is NOT a DeFi primitive?
A) Decentralized Exchanges B) Lending & Borrowing C) Custodial wallets D) Stablecoins
Answer: C – Custodial wallets are centralized; DeFi uses non-custodial wallets.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs

Quiz (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API

Quiz (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings

Quiz (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings
Answer: B – Anyone can access DeFi without identity verification or approval.

Q14. What happened during the 2022 CeFi collapses?
A) DeFi protocols failed B) Ethereum stopped working C) Centralized platforms froze assets D) Gas fees spiked

Quiz (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings
Answer: B – Anyone can access DeFi without identity verification or approval.

Q14. What happened during the 2022 CeFi collapses?
A) DeFi protocols failed B) Ethereum stopped working C) Centralized platforms froze assets D) Gas fees spiked
Answer: C – Celsius, FTX, and BlockFi collapsed, but DeFi protocols operated normally.

Q15. What is the main advantage of CeFi over DeFi?
A) Decentralization B) User-friendly interfaces C) Lower fees D) Smart contracts

Quiz (11–15)

Q11. What problem do oracles solve in DeFi?
A) High gas fees B) Slow transactions C) Access to off-chain data D) Smart contract bugs
Answer: C – Oracles feed external data (e.g., prices) to smart contracts on-chain.

Q12. Which oracle type is considered most decentralized?
A) Single trusted source B) Chainlink aggregated feeds C) Uniswap TWAP D) Exchange API
Answer: B – Chainlink uses multiple providers with aggregation for decentralization.

Q13. What does "permissionless" mean in DeFi?
A) No fees required B) No KYC/AML verification needed C) No smart contracts D) No token holdings
Answer: B – Anyone can access DeFi without identity verification or approval.

Q14. What happened during the 2022 CeFi collapses?
A) DeFi protocols failed B) Ethereum stopped working C) Centralized platforms froze assets D) Gas fees spiked
Answer: C – Celsius, FTX, and BlockFi collapsed, but DeFi protocols operated normally.

Q15. What is the main advantage of CeFi over DeFi?
A) Decentralization B) User-friendly interfaces C) Lower fees D) Smart contracts
Answer: B – CeFi offers better UX, customer support, and fiat on/off ramps.

Quiz (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens
D) Converting staked tokens

Quiz (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens
D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens
D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync

Quiz (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens
D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads Layer 2 ecosystem with 43% market share as of December 2025.

Q19. What does "non-custodial" mean in DeFi?
A) No transaction fees B) Users hold their own private keys C) No smart contracts D) Centralized control

Quiz (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads Layer 2 ecosystem with 43% market share as of December 2025.

Q19. What does "non-custodial" mean in DeFi?
A) No transaction fees B) Users hold their own private keys C) No smart contracts D) Centralized control
Answer: B – Non-custodial means users control assets; no third party holds keys.

Q20. What is a major emerging trend in DeFi's future?
A) Removing smart contracts B) Tokenizing Real-World Assets C) Eliminating oracles D) Centralized governance

Quiz (16–20)

Q16. What is restaking in the context of EigenLayer?
A) Unstaking and restaking ETH B) Reusing staked ETH to secure other services C) Staking multiple tokens D) Converting staked tokens
Answer: B – Restaking allows staked ETH to secure additional networks for extra yield.

Q17. What was EigenLayer's peak TVL in 2024?
A) $5 billion B) $12.6 billion C) $19 billion D) $31 billion
Answer: C – EigenLayer peaked at $19B in June 2024, now $12.6B (December 2025).

Q18. Which Layer 2 network has the largest share of L2 TVL?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads Layer 2 ecosystem with 43% market share as of December 2025.

Q19. What does "non-custodial" mean in DeFi?
A) No transaction fees B) Users hold their own private keys C) No smart contracts D) Centralized control
Answer: B – Non-custodial means users control assets; no third party holds keys.

Q20. What is a major emerging trend in DeFi's future?
A) Removing smart contracts B) Tokenizing Real-World Assets C) Eliminating oracles D) Centralized governance
Answer: B – RWA tokenization (bonds, real estate) is a growing DeFi trend.

Quiz (21–23)

Q21. What distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees

Quiz (21–23)

Q21. What distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries.

Q22. What does "composability" mean in DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility

Quiz (21–23)

Q21. What distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries.

Q22. What does "composability" mean in DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows protocols to work together like "money legos."

Q23. What is restaking (EigenLayer)?
A) Unstaking and restaking ETH B) Reusing staked ETH for extra yield C) Staking multiple tokens D) Converting tokens

Quiz (21–23)

Q21. What distinguishes DeFi from Traditional Finance?
A) Higher interest rates B) Faster transactions C) No intermediaries D) Lower fees
Answer: C – DeFi uses smart contracts instead of centralized intermediaries.

Q22. What does "composability" mean in DeFi?
A) Code reusability B) Protocols interact seamlessly C) Token swapping D) Wallet compatibility
Answer: B – Composability allows protocols to work together like "money legos."

Q23. What is restaking (EigenLayer)?
A) Unstaking and restaking ETH B) Reusing staked ETH for extra yield C) Staking multiple tokens D) Converting tokens
Answer: B – Restaking reuses staked ETH to secure additional services.

L34: AMM Mechanics

Mini-Lecture — Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand the constant product formula ($x \cdot y = k$)
- Calculate slippage and impermanent loss
- Compare AMMs to traditional order book exchanges

Traditional Order Book vs AMMs

Order Book (CEX)

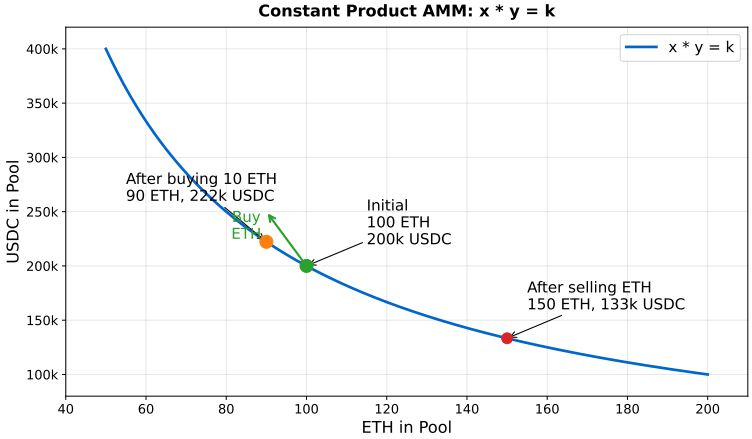
- Buyers place bids, sellers place asks
- Matching engine pairs orders
- Requires active market makers

AMM (DEX)

- Liquidity pools replace order books
- Algorithm sets price from ratio
- 24/7 passive liquidity

Key Insight: AMMs enable permissionless trading without counterparties.

The Constant Product Formula



Trades move along the curve; price is the slope at any point

Constant Product: How It Works

Uniswap V2 Model:

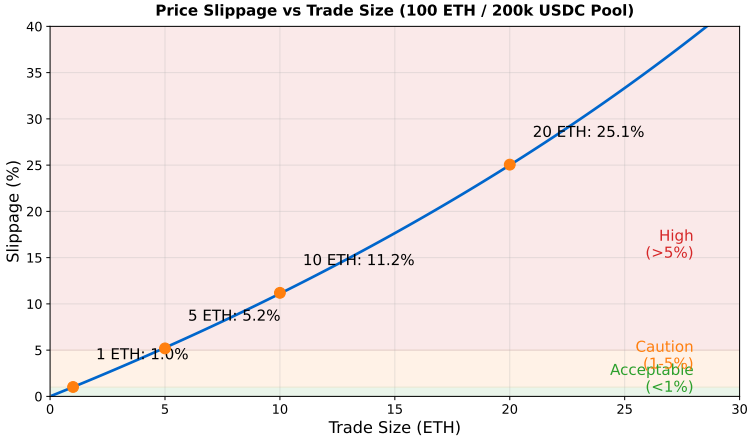
$$x \cdot y = k$$

where x = token A, y = token B, k = constant.

Example: Pool has 100 ETH + 200,000 USDC

- $k = 100 \times 200{,}000 = 20{,}000{,}000$
- Price: $\frac{200{,}000}{100} = 2{,}000$ USDC/ETH
- Buy 10 ETH $\rightarrow$ New ETH: 90, USDC: $\frac{k}{90} = 222{,}222$
- Cost: 22,222 USDC = \$2,222/ETH average

Slippage vs Trade Size



Slippage increases non-linearly; larger pools reduce slippage

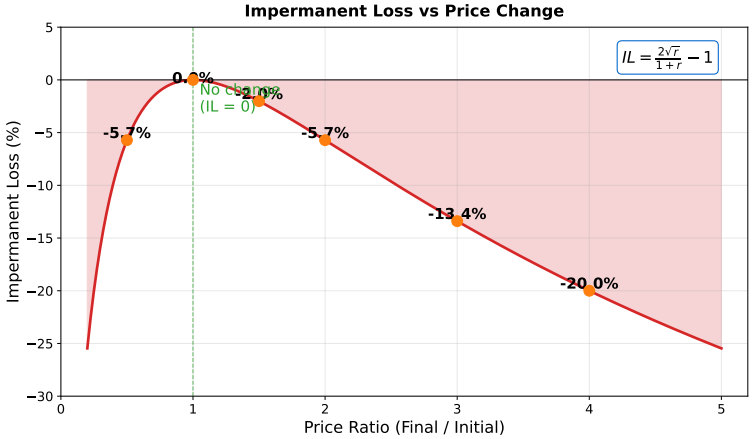
Liquidity Provision

How to Become an LP:

1. Deposit equal value of both tokens
2. Receive LP tokens representing pool share
3. Earn 0.3% fee on every trade (Uniswap V2)

Example: Deposit 10 ETH + 20,000 USDC into pool of 100 ETH + 200,000 USDC
Your share: $\frac{10}{110} = 9.09\%$ of fees and reserves.

Impermanent Loss



IL increases with price divergence; symmetric whether price rises or falls

Impermanent Loss: Key Values

Formula:

$$\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$$

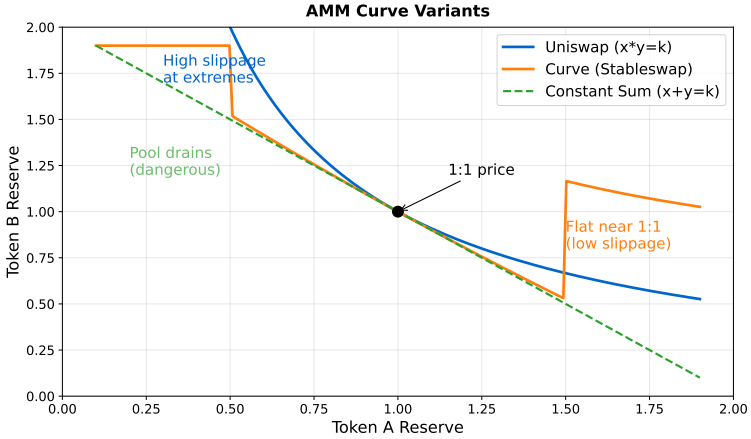
where r = price ratio (final/initial).

Common Scenarios:

- 1.5x price change: -2.0% IL
- 2x price change: -5.7% IL
- 4x price change: -20.0% IL

Why "Impermanent"? Loss only realized on withdrawal.

AMM Curve Variants



Different curves optimize for different use cases

Summary

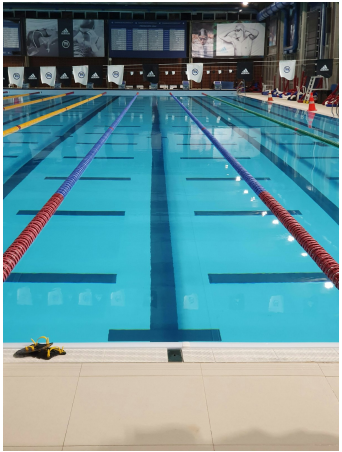
Key Takeaways:

- AMMs use $x \cdot y = k$ to provide algorithmic liquidity
- Slippage increases non-linearly with trade size
- LPs earn fees but face impermanent loss when prices diverge
- Curve optimizes for stables; Balancer for weighted pools

Next Lecture: Uniswap Deep Dive – V1 to V4 evolution.

Image Credits

Liquidity concept
Cesar Couto / Unsplash



Pool metaphor
Unsplash

Trading interface
Anne Nygard / Unsplash

All images: CC0 license via Unsplash

Quiz Questions (1–3)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Quiz Questions (4–6)

Q4. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q5. What do LPs receive when depositing tokens into a pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q6. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

L34: AMM Mechanics

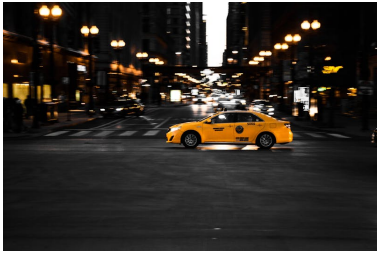
Mini-Lecture Version

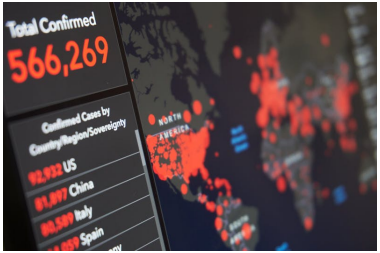
Blockchain & Cryptocurrency

Module E: DeFi Ecosystem

December 2025

Learning Objectives: Constant product formula ($x \cdot y = k$) — Liquidity provision mechanics — Impermanent loss calculation — Slippage and price impact — AMM vs order book comparison




Total Confirmed
566,269
Confirmed Cases by Country/Region/Sovereignty
92,932 US
81,897 China
80,589 Italy
Spain

What is an Automated Market Maker?

Definition

An AMM replaces traditional order books with liquidity pools governed by mathematical formulas, enabling permissionless, algorithmic trading.

Key Components:

- Liquidity pool with token pairs (e.g., ETH/USDC)
- Algorithmic pricing based on reserve ratio
- LP tokens representing pool share (e.g., UNI-V2 LP tokens)

Uniswap pioneered the constant product AMM model in 2018

The Constant Product Formula

Uniswap V2 Model:

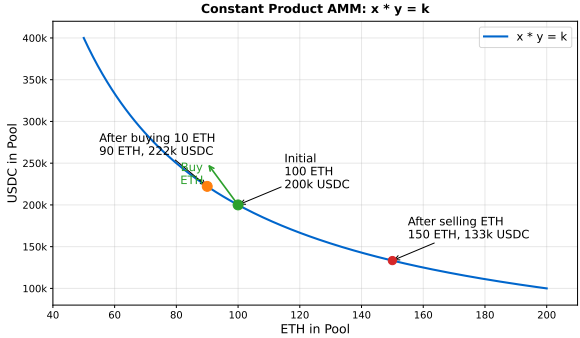
$$x \cdot y = k$$

Example Pool:

- 100 ETH + 200,000 USDC
- $k = 20{,}000{,}000$
- Price: \$2,000/ETH

After buying 10 ETH:

- New: 90 ETH, 222,222 USDC
- Cost: \$2,222/ETH average



Trades move along the curve; price is the slope at any point

Slippage and Price Impact

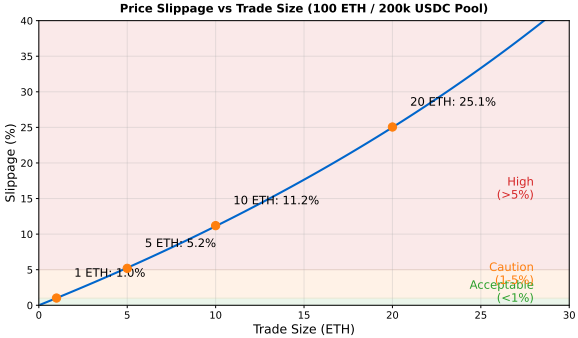
Why Slippage Occurs:

- Formula moves price as reserves change
- Larger trades = larger price impact
- Smaller pools = more slippage

Slippage Formula:

$$\text{Slippage} = \frac{\Delta P}{P_0} \times 100\%$$

Tolerance: Users set max (e.g., 0.5%, 1%); tx reverts if exceeded.



Slippage increases non-linearly; larger pools reduce slippage

Liquidity Provision and Impermanent Loss

Becoming an LP:

1. Deposit equal value of both tokens
2. Receive LP tokens (pool share)
3. Earn 0.3% trading fees (Uniswap V2)
4. Withdraw anytime (burn LP tokens)

IL: ETH doubles to $4,000

- If held: $6,000
- If LP: $5,656
- **IL: 5.7%**

IL by Price Change:

- 1.25x: -0.6% IL
- 1.5x: -2.0% IL
- 2x: -5.7% IL
- 3x: -13.4% IL
- 4x: -20.0% IL

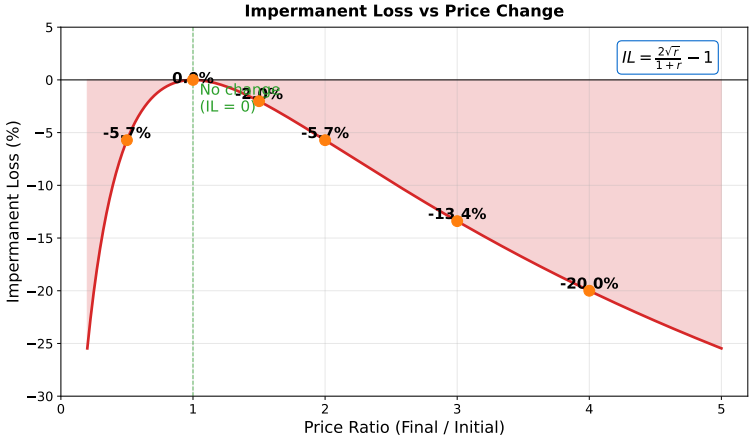
IL Formula:

$$\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$$

"Impermanent" because loss disappears if prices return to original ratio

(c) Joerg Osterrieder 2025

Impermanent Loss Visualization



IL increases with price divergence; symmetric whether price rises or falls

AMM Curve Variants

Uniswap (Constant Product):

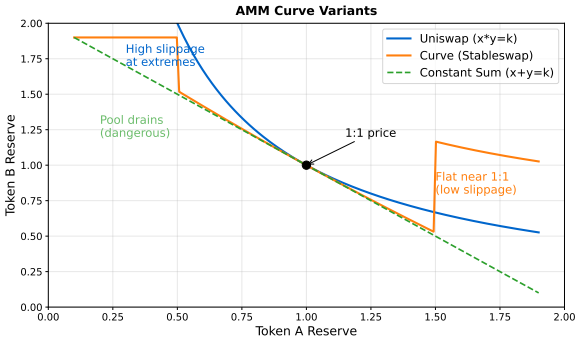
- $x \cdot y = k$
- General purpose, any pair

Curve (StableSwap):

- Hybrid formula
- Low slippage for stables (USDC/DAI)

Balancer (Weighted):

- $\prod x_i^{w_i} = k$
- Custom weights (e.g., 80/20)



Different curves optimize for different use cases

Arbitrage and MEV

Arbitrage Mechanism:

1. External price deviates from AMM
2. Arbitrageur exploits difference
3. Pool rebalances to match market

Example:

- CEX: 1 ETH = \$2,100
- Uniswap: 1 ETH = \$2,000
- Profit: \$100/ETH

MEV Strategies:

- **Front-Running:** Buy before large order
- **Sandwich:** Buy before, sell after victim
- **Arbitrage:** Cross-venue profit

Mitigation:

- Flashbots Protect
- CoW Swap batch auctions

MEV is a hidden cost for AMM traders; private mempools help

(c) Joerg Osterrieder 2025

Key Takeaways

1. AMMs use $x \cdot y = k$ to provide 24/7 algorithmic liquidity without order books
2. Slippage increases non-linearly with trade size; larger pools reduce impact
3. LPs earn fees (0.3% per trade) but face impermanent loss when prices diverge
4. Different AMM curves (Uniswap, Curve, Balancer) optimize for different use cases

Bottom Line: AMMs democratize market making but require understanding trade-offs between fees earned and impermanent loss risk.

(c) Joerg Osterrieder 2025

Concrete Examples: Making It Real

Pool Calculation Example

- Pool: 100 ETH + 200,000 USDC
- $k = 20{,}000{,}000$
- Buy 5 ETH: Cost = $10,526 (vs $10,000 spot)
- Slippage: 5.26%

Real Protocol Data (Dec 2025)

- Uniswap V3 TVL: $4.8B
- Curve TVL: $1.9B
- Balancer TVL: $850M

Fee Comparison

- Uniswap V2: 0.30%
- Uniswap V3: 0.01%, 0.05%, 0.30%, 1%
- Curve: 0.04% (stables)

IL Real Example

- Deposit: 1 ETH ($2,000) + 2,000 USDC
- ETH rises to $4,000
- Hold value: $6,000
- LP value: $5,657
- IL: $343 (5.7%)

Data verified Dec 2025 — Sources: DefiLlama, Uniswap Analytics

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k stays the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k stays the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k stays the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q4. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) SushiSwap

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k stays the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q4. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) SushiSwap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q5. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing liquidity D) Freezing txs

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k stays the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q4. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) SushiSwap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q5. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing liquidity D) Freezing txs
Answer: A – Attacker front-runs victim's buy, then back-runs with a sell.

Quiz Questions (6–10)

Q6. What do LPs receive when depositing tokens into an AMM pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights

Quiz Questions (6–10)

Q6. What do LPs receive when depositing tokens into an AMM pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q7. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) Paid by traders

Quiz Questions (6–10)

Q6. What do LPs receive when depositing tokens into an AMM pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q7. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) Paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q8. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio

Quiz Questions (6–10)

Q6. What do LPs receive when depositing tokens into an AMM pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q7. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) Paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q8. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage mechanics.

Q9. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%

Quiz Questions (6–10)

Q6. What do LPs receive when depositing tokens into an AMM pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q7. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) Paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q8. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage mechanics.

Q9. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q10. Compared to order books, AMMs provide:
A) No liquidity B) Always available liquidity C) Better large trade prices D) No fees

Quiz Questions (6–10)

Q6. What do LPs receive when depositing tokens into an AMM pool?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q7. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) Paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q8. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage mechanics.

Q9. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q10. Compared to order books, AMMs provide:
A) No liquidity B) Always available liquidity C) Better large trade prices D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

L34: AMM Mechanics

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Derive the constant product formula ($x \cdot y = k$) and its implications
- Analyze how liquidity provision works in AMMs
- Calculate impermanent loss and its implications
- Calculate slippage and price impact for trades
- Compare AMMs to traditional order book exchanges

The Problem: How can we trade without order books?

The Challenge
Traditional exchanges require continuous market makers to maintain order books. On blockchain, updating orders is expensive (gas costs) and slow (block times). We need a trading mechanism that works algorithmically without human market makers.

Why It Matters

- Without liquidity, decentralized exchanges can't compete with CEXs
- Order books are vulnerable to manipulation and front-running

What We Need

- System design principles
- Algorithmic pricing that adjusts automatically to supply and demand
- Passive liquidity provision without active management

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How AMM Mechanics addresses this challenge

Traditional Order Book Exchanges

How They Work:

- **Buyers** place bids, **sellers** place asks
- **Matching engine** pairs buy/sell orders
- Trade executes when bid meets ask

Example Order Book:

	Price	Size
Bids (Buy)	$1,999	5 ETH
	$1,998	10 ETH

	Price	Size
Asks (Sell)	$2,000	8 ETH
	$2,001	12 ETH

Challenges on Blockchain: Gas costs for order updates, slow block times, front-running.

Automated Market Makers (AMMs)

Key Idea: Replace order books with liquidity pools governed by mathematical formulas.

How It Works:

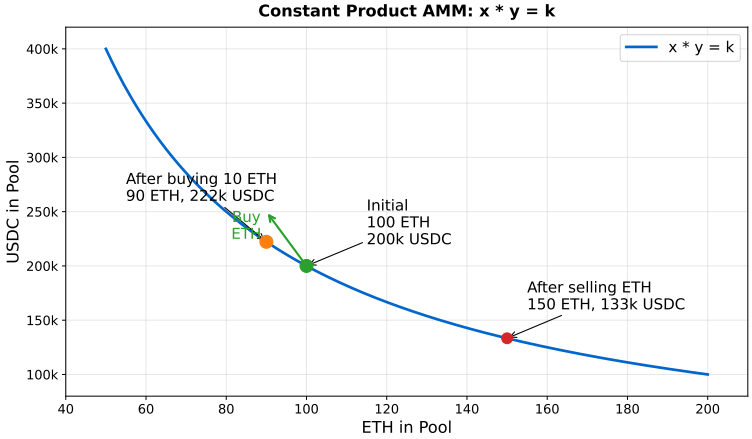
- Liquidity Providers (LPs) deposit token pairs into a pool
- Algorithm sets price based on pool ratio
- Users trade directly against the pool

Advantages:

- Always available liquidity (no need to wait for orders)
- Passive income for LPs (earn trading fees)
- Gas efficient (fewer transactions)

Trade-off: Price determined by formula, not market consensus.

The Constant Product Formula



Trades move along the curve; price is the slope at any point

Constant Product: Mathematics

Uniswap V2 Model:

$$x \cdot y = k$$

where x = token A quantity, y = token B quantity, k = constant.

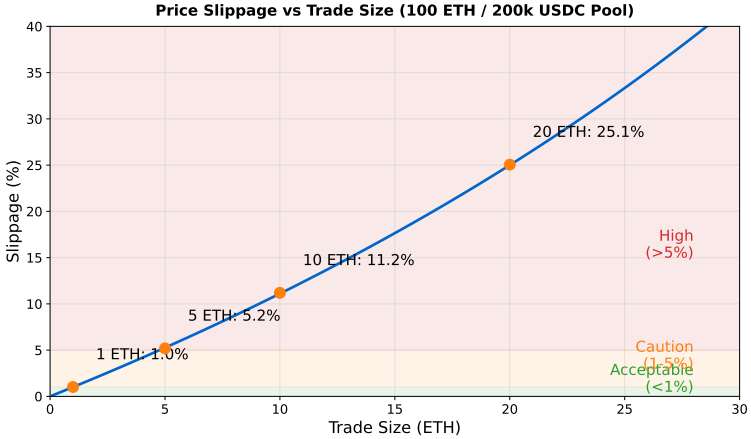
Example Pool:

- 100 ETH and 200,000 USDC
- $k = 100 \times 200{,}000 = 20{,}000{,}000$
- Price: $\frac{y}{x} = \frac{200{,}000}{100} = 2{,}000$ USDC per ETH

After Buying 10 ETH:

- New ETH: 90, New USDC: $\frac{20{,}000{,}000}{90} = 222{,}222$
- Cost: 22,222 USDC for 10 ETH = \$2,222/ETH average

Slippage vs Trade Size



Slippage increases non-linearly; larger pools reduce slippage

Slippage Explained

Definition: The difference between expected price and executed price due to trade size.

Why Slippage Occurs:

- AMM formula moves price as reserves change
- Larger trades = larger price impact
- Smaller pools = more slippage

Slippage Formula:

$$\text{Slippage} = \frac{\text{Executed Price} - \text{Initial Price}}{\text{Initial Price}} \times 100\%$$

Slippage Tolerance: Users set maximum acceptable (e.g., 0.5%, 1%). Transaction reverts if exceeded.

Liquidity Provision

How to Become an LP:

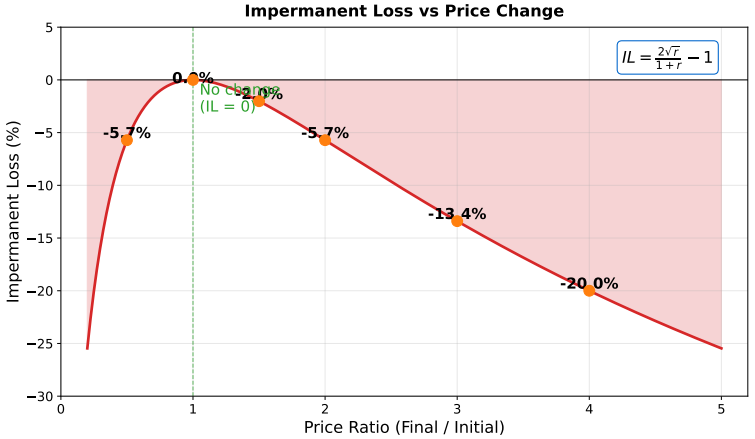
1. Deposit equal value of both tokens (e.g., 1 ETH + 2,000 USDC)
2. Receive LP tokens representing pool share
3. Earn trading fees proportional to share
4. Withdraw anytime (burn LP tokens, receive reserves)

Example:

- Pool has 100 ETH + 200,000 USDC
- You deposit 10 ETH + 20,000 USDC
- Your share: $\frac{10}{110} = 9.09\%$ of pool

Fee Earnings: Uniswap charges 0.3% per trade; fees compound in pool reserves.

Impermanent Loss



IL increases with price divergence; symmetric whether price rises or falls

Impermanent Loss: Concept

Definition: The opportunity cost of providing liquidity vs. simply holding tokens.

Occurs when:

- Token prices diverge from deposit ratio
- Arbitrageurs rebalance pool to match external prices
- LPs end up with more of the depreciated token

Example: ETH doubles to $4,000

- Initial: 1 ETH + 2,000 USDC = $4,000 total
- If held: 1 ETH @ $4,000 + 2,000 USDC = $6,000
- If LP: 0.707 ETH + 2,828 USDC = $5,656
- **IL: $344 (5.7%)**

Impermanent Loss: Key Values

Formula:

$$\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$$

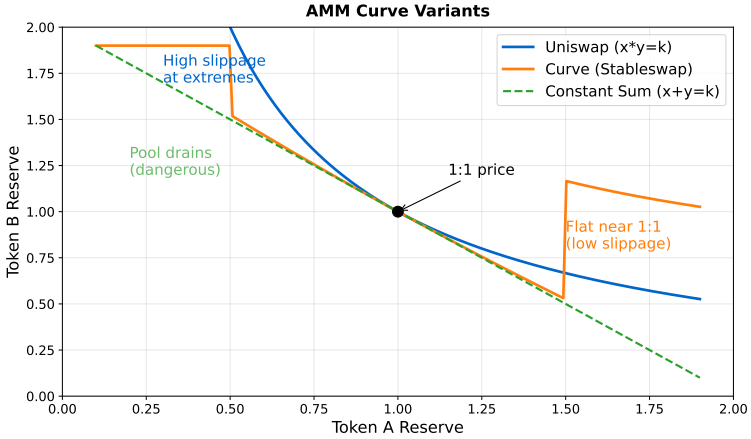
where r is the price ratio (final/initial).

Common Scenarios:

- 1.25x price change: -0.6% IL
- 1.5x price change: -2.0% IL
- 2x price change: -5.7% IL
- 3x price change: -13.4% IL
- 4x price change: -20.0% IL

Why "Impermanent"? Loss only realized on withdrawal; if prices return, loss disappears.

AMM Curve Variants



Different curves optimize for different use cases

AMM Variants Explained

Uniswap (Constant Product): $x \cdot y = k$

- General purpose, works for any pair
- Higher slippage near extremes

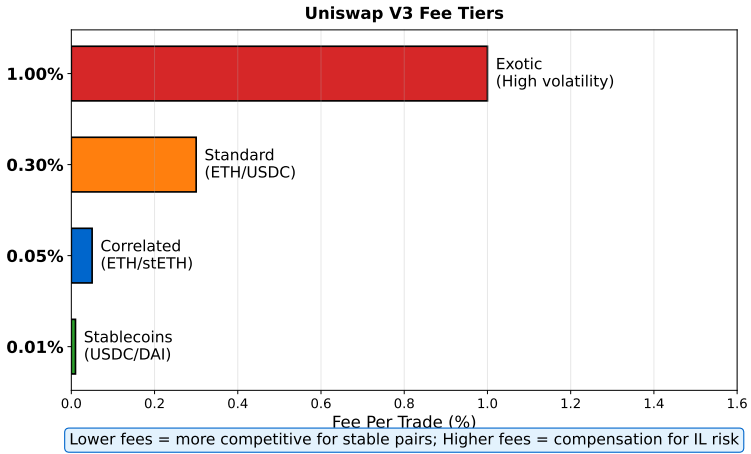
Curve (Stableswap): Hybrid formula

- Flat curve near 1:1 (low slippage for stables)
- Dominates stablecoin swaps (USDC/DAI)

Balancer (Weighted): $\prod x_i^{w_i} = k$

- Custom weights (e.g., 80/20 instead of 50/50)
- Index fund functionality

Fee Tiers in AMMs



Higher fees compensate LPs for impermanent loss risk in volatile pairs

Arbitrage in AMMs

How Arbitrage Works:

1. External market price deviates from AMM price
2. Arbitrageur buys cheaper asset, sells expensive one
3. AMM pool rebalances to match external price

Example:

- CEX: 1 ETH = \$2,100
- Uniswap pool: 1 ETH = \$2,000
- Arbitrageur: Buy on Uniswap, sell on CEX, profit \$100/ETH

Benefit: Keeps AMM prices aligned with global markets.
Cost: LPs experience impermanent loss from adjustments.

MEV and Front-Running

Maximal Extractable Value (MEV):

- Profit from reordering/inserting transactions
- Particularly prevalent in AMM trades

Common MEV Strategies:

1. **Front-Running:** See large buy, buy first, sell after
2. **Sandwich Attacks:** Buy before user, sell after
3. **Arbitrage:** Exploit price differences

Mitigation:

- Private mempools (Flashbots Protect)
- Batch auctions (CoW Swap)

(c) Joerg Osterrieder 2025

Comparison: AMM vs Order Book

AMM (Uniswap)

- Always available liquidity
- Passive LP income
- Slippage on large trades
- Impermanent loss risk

Order Book (Binance)

- Liquidity depends on makers
- Active market making
- Better for large trades
- No impermanent loss

Trend: Hybrid models emerging (e.g., dYdX order book on Cosmos).

(c) Joerg Osterrieder 2025

Problem Solved? AMM Mechanics

The Original Problem

How can we trade without order books?

How AMM Mechanics Solves It

- The constant product formula ($x \cdot y = k$) provides algorithmic pricing without manual order placement
- Liquidity providers deposit token pairs and earn passive trading fees (0.3% per trade)
- Pool always has liquidity available 24/7, no need to wait for matching orders

Remaining Limitations

- Impermanent loss: LPs face opportunity cost when token prices diverge (up to 20%+ for 4x price moves)
- Capital inefficiency: Liquidity spread across entire price curve, not concentrated where trades occur
- MEV extraction: Sandwich attacks and front-running impose hidden costs on traders

Open Questions

- Can AMMs ever achieve the capital efficiency of centralized exchange order books?
- Risk: Are trading fees sufficient to compensate LPs for impermanent loss in volatile pairs?

AMM Mechanics solves the order book problem but introduces new trade-offs between accessibility and efficiency

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- AMMs use $x \cdot y = k$ to provide algorithmic liquidity
- Price determined by reserve ratio; trades move price
- Slippage increases non-linearly with trade size
- LPs earn fees but face impermanent loss when prices diverge
- IL formula: $\frac{2\sqrt{r}}{1+r} - 1$ (up to 20%+ for 4x moves)
- Curve optimizes for stables; Balancer for weighted pools
- MEV is a hidden cost for AMM traders

Next Lecture: Uniswap Deep Dive - V1 to V4 evolution, concentrated liquidity.

Questions for Reflection

1. Calculate the cost to buy 5 ETH from a pool with 100 ETH and 200,000 USDC.
2. Why does slippage increase non-linearly with trade size?
3. How do trading fees help offset impermanent loss for LPs?
4. Why is Curve more suitable for stablecoin trading than Uniswap V2?
5. What are the trade-offs of concentrated liquidity in Uniswap V3?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage from AMM mechanics.

Q4. What is the primary benefit of providing liquidity to an AMM pool?
A) Guaranteed returns B) Earning trading fees C) Price speculation D) Voting rights
Answer: B – LPs earn a share of trading fees (e.g., 0.3% in Uniswap V2).

Q5. If you set a 1% slippage tolerance and actual slippage is 1.5%, what happens?
A) Trade executes normally B) Transaction reverts C) Fees double D) Pool pauses
Answer: B – Transaction reverts to protect user from excessive slippage.

Quiz Questions (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q8. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q9. You deposit 1 ETH + 2,000 USDC into a pool. What do you receive?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q10. In a pool with 0.3% trading fee, who receives the fees?
A) Protocol treasury B) Validators C) Liquidity providers D) Traders
Answer: C – Trading fees accrue to LPs proportional to their pool share.

Quiz Questions (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100
Answer: C – Balancer supports arbitrary weights (e.g., 80/20, 60/40).

Q13. What is the main role of arbitrageurs in AMMs?
A) Provide liquidity B) Pay gas fees C) Align AMM prices with external markets D) Vote on upgrades
Answer: C – Arbitrageurs exploit price differences, keeping AMM prices accurate.

Q14. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing all liquidity D) Freezing transactions
Answer: A – Attacker front-runs victim's buy, then back-runs with a sell.

Q15. What does MEV stand for?
A) Maximum Ethereum Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficient Value
Answer: C – MEV (formerly "Miner") is now "Maximal Extractable Value".

Quiz Questions (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH
Answer: A – Pool loses 10 ETH, leaving 90 ETH (USDC increases to maintain k).

Q18. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q19. Which factor INCREASES impermanent loss?
A) Price stability B) High trading fees C) Large price divergence D) Low slippage
Answer: C – Greater price divergence (e.g., 4x) causes higher IL (up to 20%+).

Q20. To withdraw liquidity from an AMM, you must:
A) Wait 30 days B) Burn LP tokens C) Pay a penalty D) Sell all assets
Answer: B – Burning LP tokens returns your share of pool reserves.

L34: AMM Mechanics

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Liquidity Pool as Swimming Pool

[COMIC: Liquidity pool as swimming pool]

Placeholder for comic showing swimmers (traders) jumping in/out of pool, with pool depth changing and lifeguards (LPs) maintaining water levels

The Setup

- Traditional exchange: find a trading partner
- Order books: wait for someone to match
- Problem: what if no one wants to trade?

The Punchline

- AMM: trade against the pool itself
- Pool always has liquidity
- Price adjusts automatically

Why find a trading partner when you can just jump in the pool?

Learning Objectives

- Derive the constant product formula ($x \cdot y = k$) and its implications
- Analyze how liquidity provision works in AMMs
- Calculate impermanent loss and its implications
- Calculate slippage and price impact for trades
- Compare AMMs to traditional order book exchanges

Building on L33: Introduction to DeFi

The Problem: How can we trade without order books?

The Challenge
Traditional exchanges require continuous market makers to maintain order books. On blockchain, updating orders is expensive (gas costs) and slow (block times). We need a trading mechanism that works algorithmically without human market makers.

Why It Matters

- Without liquidity, decentralized exchanges can't compete with CEXs
- Order books are vulnerable to manipulation and front-running

What We Need

- System design principles
- Algorithmic pricing that adjusts automatically to supply and demand
- Passive liquidity provision without active management

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How AMM Mechanics addresses this challenge

How Do Traditional Order Book Exchanges Work?

The Mechanics:

- **Buyers** place bids, **sellers** place asks
- **Matching engine** pairs buy/sell orders
- Trade executes when bid meets ask

Example Order Book:

	Price	Size
Bids (Buy)	$1,999	5 ETH
	$1,998	10 ETH

	Price	Size
Asks (Sell)	$2,000	8 ETH
	$2,001	12 ETH

Challenges on Blockchain: Gas costs for order updates, slow block times, front-running.

→ *Problem: How can we trade without order books? — Traditional Order Book Exchanges. Order books cost gas per change. AMMs use math formulas instead of order matching.*

How Do Automated Market Makers Work?

Key Idea: Replace order books with liquidity pools governed by mathematical formulas.

How It Works:

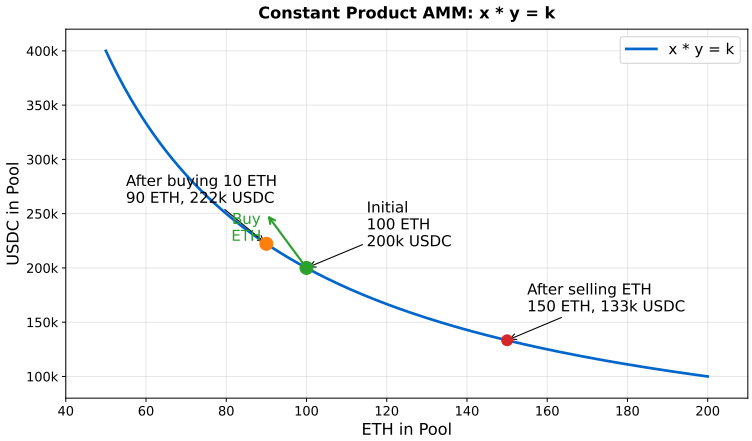
- Liquidity Providers (LPs) deposit token pairs into a pool
- Algorithm sets price based on pool ratio
- Users trade directly against the pool

Advantages:

- Always available liquidity (no need to wait for orders)
- Passive income for LPs (earn trading fees)
- Gas efficient (fewer transactions)

Trade-off: Price determined by formula, not market consensus.

What Is the Constant Product Formula?



Trades move along the curve; price is the slope at any point

How Does the Constant Product Formula Work Mathematically?

Uniswap V2 Model:

$$x \cdot y = k$$

where x = token A quantity, y = token B quantity, k = constant.

Example Pool:

- 100 ETH and 200,000 USDC
- $k = 100 \times 200{,}000 = 20{,}000{,}000$
- Price: $\frac{y}{x} = \frac{200{,}000}{100} = 2{,}000$ USDC per ETH

After Buying 10 ETH:

- New ETH: 90, New USDC: $\frac{20{,}000{,}000}{90} = 222{,}222$
- Cost: 22,222 USDC for 10 ETH = \$2,222/ETH average

Pseudocode: Constant Product Swap

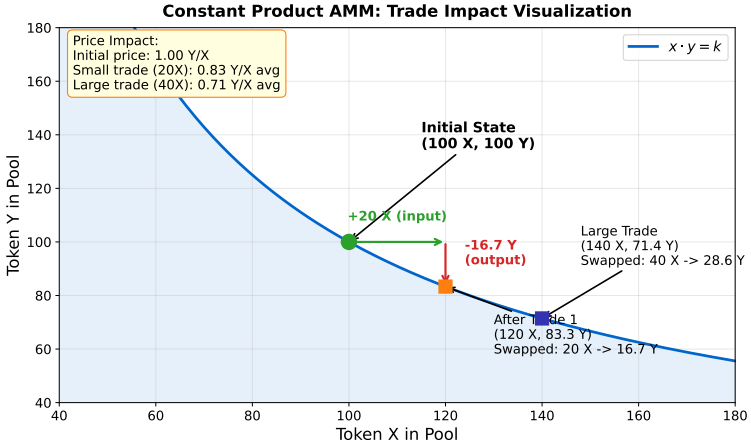
AMM Swap Execution

```
function swap(amount_in, reserve_in, reserve_out):
  fee = amount_in * 0.003
  amount_in_with_fee = amount_in - fee
  // Constant product:  x * y = k
  new_reserve_in = reserve_in + amount_in_with_fee
  new_reserve_out = k / new_reserve_in
  amount_out = reserve_out - new_reserve_out
  // Slippage = (amount_out / amount_in) vs spot price
  assert new_reserve_in * new_reserve_out >= k
  return amount_out
```

Key Insight: The `assert` line enforces the invariant – no trade can reduce k. Fees accumulate in the pool, increasing k over time and benefiting LPs.

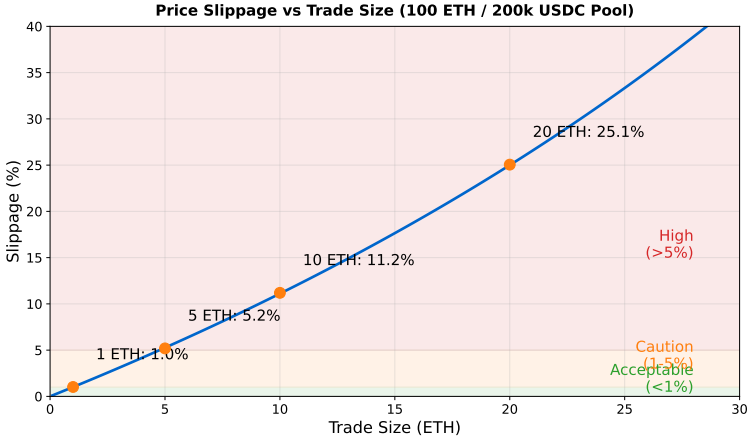
This is the core logic behind every Uniswap V2 swap – 10 lines that move billions daily

How Do Trades Impact the Curve?



Larger trades receive worse average prices; the curve ensures liquidity never runs out

How Does Slippage Vary with Trade Size?



Slippage increases non-linearly; larger pools reduce slippage | → Problem: How can we trade without order books? — Slippage vs Trade Size. Slippage is the cost of orderbook-free trading – larger trades move price more.

Why Does Price Change When You Trade?

Definition: The difference between expected price and executed price due to trade size.

Why Slippage Occurs:

- AMM formula moves price as reserves change
- Larger trades = larger price impact
- Smaller pools = more slippage

Slippage Formula:

$$\text{Slippage} = \frac{\text{Executed Price} - \text{Initial Price}}{\text{Initial Price}} \times 100\%$$

Slippage Tolerance: Users set maximum acceptable (e.g., 0.5%, 1%). Transaction reverts if exceeded.

How Do You Provide Liquidity?

How to Become an LP:

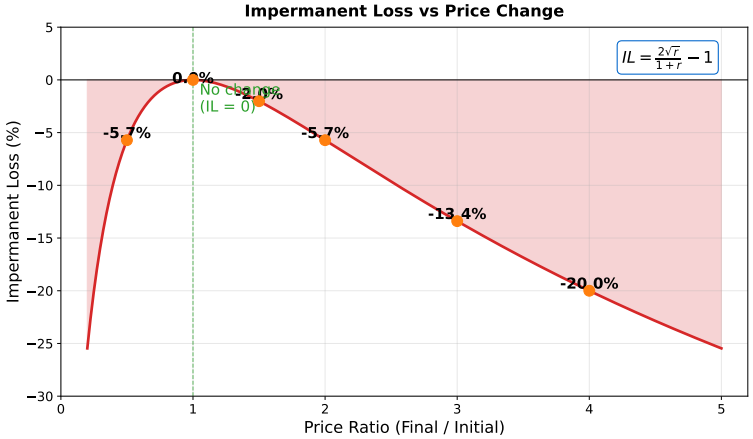
1. Deposit equal value of both tokens (e.g., 1 ETH + 2,000 USDC)
2. Receive LP tokens (receipts proving your share of a liquidity pool) representing pool share
3. Earn trading fees proportional to share
4. Withdraw anytime (burn LP tokens, receive reserves)

Example:

- Pool has 100 ETH + 200,000 USDC
- You deposit 10 ETH + 20,000 USDC
- Your share: $\frac{10}{110} = 9.09\%$ of pool

Fee Earnings: Uniswap charges 0.3% per trade; fees compound in pool reserves.

What Is Impermanent Loss?



IL increases with price divergence; symmetric whether price rises or falls

What Causes Impermanent Loss?

Definition: The opportunity cost of providing liquidity vs. simply holding tokens.

Occurs when:

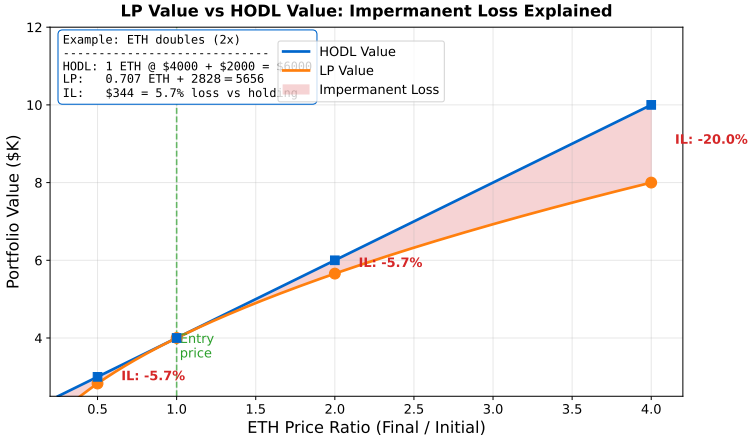
- Token prices diverge from deposit ratio
- Arbitrageurs rebalance pool to match external prices
- LPs end up with more of the depreciated token

Example: ETH doubles to $4,000

- Initial: 1 ETH + 2,000 USDC = $4,000 total
- If held: 1 ETH @ $4,000 + 2,000 USDC = $6,000
- If LP: 0.707 ETH + 2,828 USDC = $5,656
- **IL: $344 (5.7%)**

→ Problem: How can we trade without order books? — Impermanent Loss: Concept. Impermanent loss is what LPs pay for orderbook-free trading – they lose vs. just holding.

How Does LP Value Compare to HODL Value?



LP always underperforms HODL when prices diverge; gap widens with larger moves

Problem Check-In: AMM Mechanics

Recall Our Problem

How can we trade without order books?

What We've Learned So Far

- The formula $x \cdot y = k$ sets prices automatically – no humans needed to match buyers and sellers
- Liquidity providers (LPs) deposit token pairs and earn trading fees (0.3% per trade)
- Math replaces the order book: pools always have liquidity, prices adjust automatically

Still to Address

- Impermanent loss: LPs can lose money if token prices diverge significantly
- Are trading fees enough to compensate LPs for the risk of impermanent loss?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How can we trade without order books?"?

How Much Can You Lose to Impermanent Loss?

Formula:

$$\text{IL} = \frac{2\sqrt{r}}{1+r} - 1$$

where r is the price ratio (final/initial).

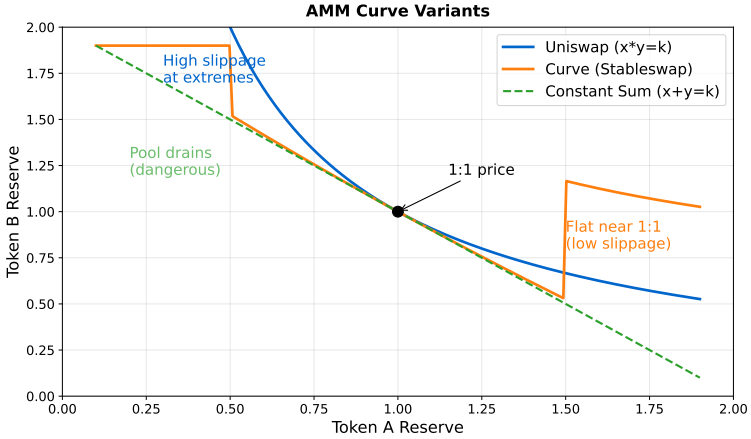
Common Scenarios:

- 1.25x price change: -0.6% IL
- 1.5x price change: -2.0% IL
- 2x price change: -5.7% IL
- 3x price change: -13.4% IL
- 4x price change: -20.0% IL

Why "Impermanent"? Loss only realized on withdrawal; if prices return, loss disappears.

(c) Joerg Osterrieder 2025

What Are the Different AMM Curve Variants?



Different curves optimize for different use cases

How Do Different AMM Variants Work?

Uniswap (Constant Product): $x \cdot y = k$

- General purpose, works for any pair
- Higher slippage near extremes

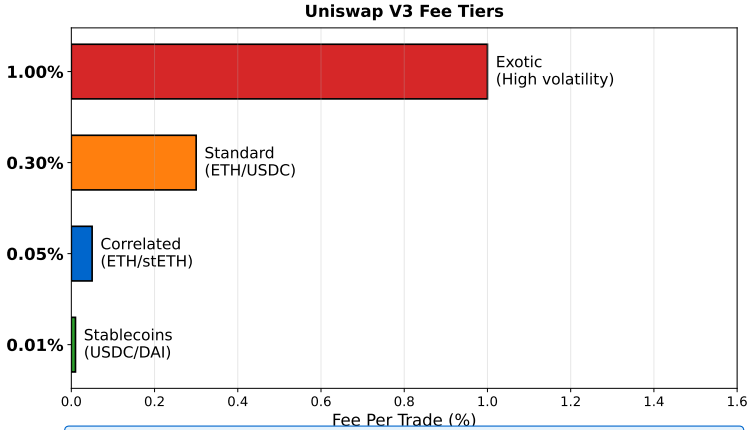
Curve (Stableswap): Hybrid formula

- Flat curve near 1:1 (low slippage for stables)
- Dominates stablecoin swaps (USDC/DAI)

Balancer (Weighted): $\prod x_i^{w_i} = k$

- Custom weights (e.g., 80/20 instead of 50/50)
- Index fund functionality

How Do Fee Tiers Work in AMMs?



Higher fees compensate LPs for impermanent loss risk in volatile pairs | → Problem: How can we trade without order books? — Fee Tiers in AMMs. Fee tiers let markets price liquidity – volatile pairs need higher fees despite IL risk.

How Do AMM Prices Stay Accurate?

How Arbitrage Works:

1. External market price deviates from AMM price
2. Arbitrageur buys cheaper asset, sells expensive one
3. AMM pool rebalances to match external price

Example:

- CEX: 1 ETH = \$2,100
- Uniswap pool: 1 ETH = \$2,000
- Arbitrageur: Buy on Uniswap, sell on CEX, profit \$100/ETH

Benefit: Keeps AMM prices aligned with global markets.
Cost: LPs experience impermanent loss from adjustments.

What Is MEV and How Does It Extract Value?

MEV (Maximal Extractable Value—profit from reordering transactions):

- Profit from reordering/inserting transactions in mempool
- Particularly prevalent in AMM trades

Common MEV Strategies:

1. **Front-Running:** See large buy, buy first, sell after
2. **Sandwich Attacks:** Buy before user, sell after
3. **Arbitrage:** Exploit price differences

Mitigation:

- Private mempools (Flashbots Protect)
- Batch auctions (CoW Swap)

How Do AMMs Compare to Order Books?

AMM (Uniswap)

- Always available liquidity
- Passive LP income
- Slippage on large trades
- Impermanent loss risk

Order Book (Binance)

- Liquidity depends on makers
- Active market making
- Better for large trades
- No impermanent loss

Trend: Hybrid models emerging (e.g., dYdX order book on Cosmos).

(c) Joerg Osterrieder 2025

Problem Solved? AMM Mechanics

The Original Problem

How can we trade without order books?

How AMM Mechanics Solves It

- The constant product formula ($x \cdot y = k$) provides algorithmic pricing without manual order placement
- Liquidity providers deposit token pairs and earn passive trading fees (0.3% per trade)
- Pool always has liquidity available 24/7, no need to wait for matching orders

Remaining Limitations

- Impermanent loss: LPs face opportunity cost when token prices diverge (up to 20%+ for 4x price moves)
- Capital inefficiency: Liquidity spread across entire price curve, not concentrated where trades occur
- MEV extraction: Sandwich attacks and front-running impose hidden costs on traders

Open Questions

- Can AMMs ever achieve the capital efficiency of centralized exchange order books?
- Risk: Are trading fees sufficient to compensate LPs for impermanent loss in volatile pairs?

AMM Mechanics solves the order book problem but introduces new trade-offs between accessibility and efficiency

(c) Joerg Osterrieder 2025

The Economics of AMM Mechanics

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: AMM Mechanics

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: AMM Mechanics

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Impermanent Loss Realization

[COMIC: Impermanent loss realization]

Placeholder for comic showing LP happily providing liquidity, then shocked face when withdrawing with less value than if they had just held

The Hidden Cost

- "Impermanent" sounds temporary
- Reality: loss crystallizes on withdrawal
- Price divergence = guaranteed underperformance vs. HODL

The Math Doesn't Lie

- 2x price change: -5.7% IL
- 4x price change: -20% IL
- Fees must exceed IL to profit

"Impermanent" loss becomes very permanent when you withdraw

What Are the Key Takeaways?

Core Concepts:

- AMMs use $x \cdot y = k$ to provide algorithmic liquidity
- Price determined by reserve ratio; trades move price
- Slippage increases non-linearly with trade size
- LPs earn fees but face impermanent loss when prices diverge
- IL formula: $\frac{2\sqrt{r}}{1+r} - 1$ (up to 20%+ for 4x moves)
- Curve optimizes for stables; Balancer for weighted pools
- MEV is a hidden cost for AMM traders

Next Lecture: Uniswap Deep Dive - V1 to V4 evolution, concentrated liquidity.

Next Lesson: L35 – Uniswap Deep Dive

Questions for Reflection

1. Calculate the cost to buy 5 ETH from a pool with 100 ETH and 200,000 USDC.
2. Why does slippage increase non-linearly with trade size?
3. How do trading fees help offset impermanent loss for LPs?
4. Why is Curve more suitable for stablecoin trading than Uniswap V2?
5. What are the trade-offs of concentrated liquidity in Uniswap V3?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage from AMM mechanics.

Q4. What is the primary benefit of providing liquidity to an AMM pool?
A) Guaranteed returns B) Earning trading fees C) Price speculation D) Voting rights
Answer: B – LPs earn a share of trading fees (e.g., 0.3% in Uniswap V2).

Q5. If you set a 1% slippage tolerance and actual slippage is 1.5%, what happens?
A) Trade executes normally B) Transaction reverts C) Fees double D) Pool pauses
Answer: B – Transaction reverts to protect user from excessive slippage.

Quiz Questions (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q8. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q9. You deposit 1 ETH + 2,000 USDC into a pool. What do you receive?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q10. In a pool with 0.3% trading fee, who receives the fees?
A) Protocol treasury B) Validators C) Liquidity providers D) Traders
Answer: C – Trading fees accrue to LPs proportional to their pool share.

Quiz Questions (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100
Answer: C – Balancer supports arbitrary weights (e.g., 80/20, 60/40).

Q13. What is the main role of arbitrageurs in AMMs?
A) Provide liquidity B) Pay gas fees C) Align AMM prices with external markets D) Vote on upgrades
Answer: C – Arbitrageurs exploit price differences, keeping AMM prices accurate.

Q14. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing all liquidity D) Freezing transactions
Answer: A – Attacker front-runs victim's buy, then back-runs with a sell.

Q15. What does MEV stand for?
A) Maximum Ethereum Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficient Value
Answer: C – MEV (formerly "Miner") is now "Maximal Extractable Value".

Quiz Questions (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH
Answer: A – Pool loses 10 ETH, leaving 90 ETH (USDC increases to maintain k).

Q18. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q19. Which factor INCREASES impermanent loss?
A) Price stability B) High trading fees C) Large price divergence D) Low slippage
Answer: C – Greater price divergence (e.g., 4x) causes higher IL (up to 20%+).

Q20. To withdraw liquidity from an AMM, you must:
A) Wait 30 days B) Burn LP tokens C) Pay a penalty D) Sell all assets
Answer: B – Burning LP tokens returns your share of pool reserves.

Quiz: AMM Mechanics

Instructions: Multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero

Quiz (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000

Quiz (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio

Quiz (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage from AMM mechanics.

Q4. What is the primary benefit of providing liquidity to an AMM pool?
A) Guaranteed returns B) Earning trading fees C) Price speculation D) Voting rights

Quiz (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage from AMM mechanics.

Q4. What is the primary benefit of providing liquidity to an AMM pool?
A) Guaranteed returns B) Earning trading fees C) Price speculation D) Voting rights
Answer: B – LPs earn a share of trading fees (e.g., 0.3% in Uniswap V2).

Q5. If you set a 1% slippage tolerance and actual slippage is 1.5%, what happens?
A) Trade executes normally B) Transaction reverts C) Fees double D) Pool pauses

Quiz (1–5)

Q1. In the constant product formula $x \cdot y = k$, what happens to k when a trade occurs?
A) Increases B) Decreases C) Remains constant D) Becomes zero
Answer: C – The constant k remains the same; only x and y change inversely.

Q2. A pool has 100 ETH and 200,000 USDC. What is the current price per ETH?
A) \$1,000 B) \$2,000 C) \$100 D) \$20,000
Answer: B – Price $= y/x = 200{,}000/100 = 2{,}000$ USDC per ETH.

Q3. Which factor does NOT contribute to slippage in an AMM?
A) Trade size B) Pool depth C) Block time D) Reserve ratio
Answer: C – Block time affects confirmation speed, not price slippage from AMM mechanics.

Q4. What is the primary benefit of providing liquidity to an AMM pool?
A) Guaranteed returns B) Earning trading fees C) Price speculation D) Voting rights
Answer: B – LPs earn a share of trading fees (e.g., 0.3% in Uniswap V2).

Q5. If you set a 1% slippage tolerance and actual slippage is 1.5%, what happens?
A) Trade executes normally B) Transaction reverts C) Fees double D) Pool pauses
Answer: B – Transaction reverts to protect user from excessive slippage.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise

Quiz (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%

Quiz (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q8. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders

Quiz (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q8. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q9. You deposit 1 ETH + 2,000 USDC into a pool. What do you receive?
A) Interest payments B) LP tokens C) More ETH D) Governance rights

Quiz (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q8. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q9. You deposit 1 ETH + 2,000 USDC into a pool. What do you receive?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q10. In a pool with 0.3% trading fee, who receives the fees?
A) Protocol treasury B) Validators C) Liquidity providers D) Traders

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. Impermanent loss occurs when:
A) Fees are too low B) Token prices diverge C) Pool is empty D) Gas costs rise
Answer: B – IL happens when token prices change relative to deposit ratio.

Q7. If ETH price doubles (2x), what is the approximate impermanent loss?
A) 2.0% B) 5.7% C) 13.4% D) 20.0%
Answer: B – 2x price change results in approximately 5.7% IL.

Q8. Why is impermanent loss called "impermanent"?
A) It's always small B) Fees offset it C) Loss disappears if prices return D) It's paid by traders
Answer: C – If token prices return to original ratio, the loss vanishes.

Q9. You deposit 1 ETH + 2,000 USDC into a pool. What do you receive?
A) Interest payments B) LP tokens C) More ETH D) Governance rights
Answer: B – LPs receive LP tokens representing their share of the pool.

Q10. In a pool with 0.3% trading fee, who receives the fees?
A) Protocol treasury B) Validators C) Liquidity providers D) Traders
Answer: C – Trading fees accrue to LPs proportional to their pool share.

Quiz (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap

Quiz (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100

Quiz (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100
Answer: C – Balancer supports arbitrary weights (e.g., 80/20, 60/40).

Q13. What is the main role of arbitrageurs in AMMs?
A) Provide liquidity B) Pay gas fees C) Align AMM prices with external markets D) Vote on upgrades

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100
Answer: C – Balancer supports arbitrary weights (e.g., 80/20, 60/40).

Q13. What is the main role of arbitrageurs in AMMs?
A) Provide liquidity B) Pay gas fees C) Align AMM prices with external markets D) Vote on upgrades
Answer: C – Arbitrageurs exploit price differences, keeping AMM prices accurate.

Q14. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing all liquidity D) Freezing transactions

Quiz (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100
Answer: C – Balancer supports arbitrary weights (e.g., 80/20, 60/40).

Q13. What is the main role of arbitrageurs in AMMs?
A) Provide liquidity B) Pay gas fees C) Align AMM prices with external markets D) Vote on upgrades
Answer: C – Arbitrageurs exploit price differences, keeping AMM prices accurate.

Q14. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing all liquidity D) Freezing transactions
Answer: A – Attacker front-runs victim's buy, then back-runs with a sell.

Q15. What does MEV stand for?
A) Maximum Ethereum Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficient Value

Quiz (11–15)

Q11. Which AMM variant is optimized for stablecoin trading?
A) Uniswap V2 B) Curve C) Balancer D) Sushiswap
Answer: B – Curve's StableSwap formula minimizes slippage near 1:1 ratios.

Q12. Balancer's weighted pools allow custom ratios like:
A) Only 50/50 B) Only 33/33/33 C) 80/20 or any weights D) Must equal 100
Answer: C – Balancer supports arbitrary weights (e.g., 80/20, 60/40).

Q13. What is the main role of arbitrageurs in AMMs?
A) Provide liquidity B) Pay gas fees C) Align AMM prices with external markets D) Vote on upgrades
Answer: C – Arbitrageurs exploit price differences, keeping AMM prices accurate.

Q14. A sandwich attack involves:
A) Buying before and selling after victim's trade B) Hacking the pool C) Withdrawing all liquidity D) Freezing transactions
Answer: A – Attacker front-runs victim's buy, then back-runs with a sell.

Q15. What does MEV stand for?
A) Maximum Ethereum Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficient Value
Answer: C – MEV (formerly "Miner") is now "Maximal Extractable Value".

Quiz (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees

Quiz (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH

Quiz (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH
Answer: A – Pool loses 10 ETH, leaving 90 ETH (USDC increases to maintain k).

Q18. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%

Quiz (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH
Answer: A – Pool loses 10 ETH, leaving 90 ETH (USDC increases to maintain k).

Q18. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q19. Which factor INCREASES impermanent loss?
A) Price stability B) High trading fees C) Large price divergence D) Low slippage

Quiz (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH
Answer: A – Pool loses 10 ETH, leaving 90 ETH (USDC increases to maintain k).

Q18. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q19. Which factor INCREASES impermanent loss?
A) Price stability B) High trading fees C) Large price divergence D) Low slippage
Answer: C – Greater price divergence (e.g., 4x) causes higher IL (up to 20%+).

Q20. To withdraw liquidity from an AMM, you must:
A) Wait 30 days B) Burn LP tokens C) Pay a penalty D) Sell all assets

Quiz (16–20)

Q16. Compared to order books, AMMs have:
A) No liquidity B) Always available liquidity C) Better prices for large trades D) No fees
Answer: B – AMMs provide algorithmic liquidity 24/7 without waiting for makers.

Q17. After buying 10 ETH from a 100 ETH pool with $k = 20{,}000{,}000$, the new ETH reserve is:
A) 90 ETH B) 100 ETH C) 110 ETH D) 80 ETH
Answer: A – Pool loses 10 ETH, leaving 90 ETH (USDC increases to maintain k).

Q18. Uniswap V2's standard fee per trade is:
A) 0.05% B) 0.3% C) 1.0% D) 5.0%
Answer: B – Uniswap V2 charges 0.3% on all trades.

Q19. Which factor INCREASES impermanent loss?
A) Price stability B) High trading fees C) Large price divergence D) Low slippage
Answer: C – Greater price divergence (e.g., 4x) causes higher IL (up to 20%+).

Q20. To withdraw liquidity from an AMM, you must:
A) Wait 30 days B) Burn LP tokens C) Pay a penalty D) Sell all assets
Answer: B – Burning LP tokens returns your share of pool reserves.

L35: Uniswap Deep Dive

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

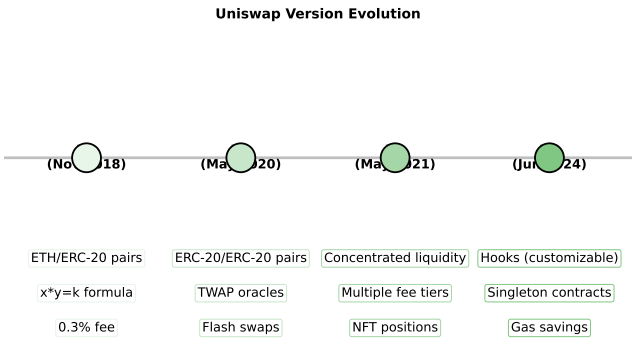
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Trace Uniswap's evolution from V1 to V4
- Explain concentrated liquidity mechanics in V3
- Describe fee tier optimization strategies
- Analyze UNI token governance and fee switch debate

Uniswap Version Evolution



Market Position (Dec 2025): Largest DEX, $4.5B TVL, V4 launched Jan 2025.

Uniswap V1 and V2

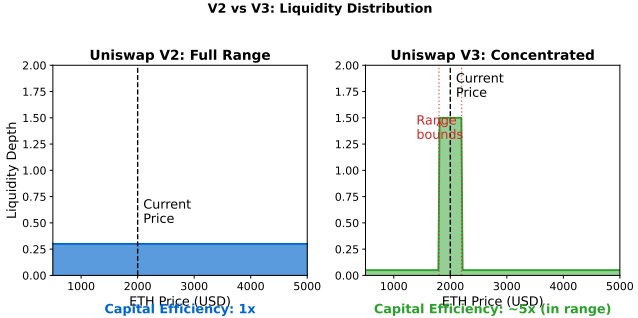
V1 (2018):

- ETH/ERC-20 pairs only, $x \cdot y = k$ formula
- 0.3% fee (100% to LPs)

V2 (2020) Improvements:

- **ERC-20/ERC-20 pairs:** Direct trading without ETH
- **TWAP oracles:** Manipulation-resistant price feeds
- **Flash swaps:** Borrow tokens, repay in same tx
- **Protocol fee switch:** 0.05% potential fee (not activated)

V3: Concentrated Liquidity



Innovation: LPs choose specific price ranges; 10-200x capital efficiency.

Concentrated Liquidity Mechanics

How It Works:

- LP sets price bounds (e.g., \$1,900-\$2,100)
- Earns fees only when price in range
- Position exits range = stops earning

Example:

- Deposit 1 ETH + 2,000 USDC with range \$1,900-\$2,100
- ETH = \$2,000: Position active, earns fees
- ETH = \$2,200: Fully in USDC, no fees

Trade-off: Higher efficiency requires active management.

V3 Fee Tiers

Fee Tier	Use Case	Examples
0.01%	Stablecoins	USDC/USDT, DAI/USDC
0.05%	Correlated assets	ETH/stETH
0.30%	Standard pairs	ETH/USDC
1.00%	Exotic/volatile	Low-liquidity tokens

Rationale: Stablecoins need low fees; volatile pairs need higher fees for IL compensation.

(c) Joerg Osterrieder 2025

Uniswap V4: Hooks (Jan 2025)

Innovation: Customizable pool behavior via hooks.

What are Hooks?

- Smart contracts at specific trade lifecycle points
- Before/after swap, before/after adding liquidity

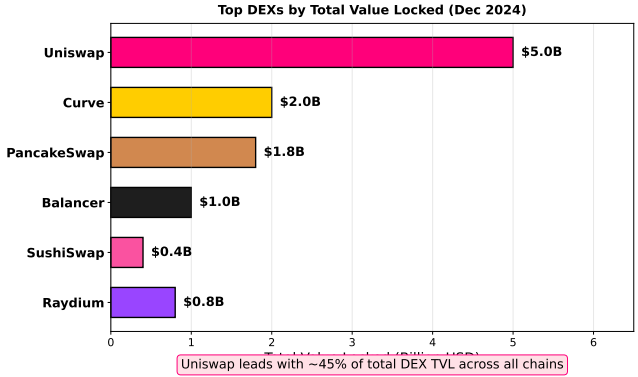
Use Cases:

- Dynamic fees based on volatility
- On-chain limit orders, TWAP execution
- Auto-rebalancing, MEV protection

Singleton Contract: All pools in one contract (gas savings).

(c) Joerg Osterrieder 2025

DEX Market Comparison



Uniswap's Moat: Brand recognition, deepest liquidity, innovation leadership.

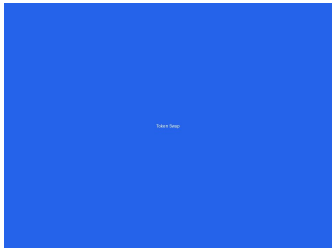
Key Takeaways

1. **Evolution:** V1 (simple AMM) to V4 (customizable hooks)
2. **V3 Concentrated Liquidity:** 10-200x capital efficiency
3. **Fee Tiers:** 0.01% (stables) to 1% (exotic)
4. **V4 Hooks:** Custom pool logic (dynamic fees, limit orders)
5. **UNI Governance:** Controls protocol but no direct revenue (yet)

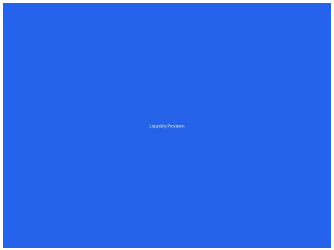
Next: L36 Lab – Testnet Swap (hands-on experience)

(c) Joerg Osterrieder 2025

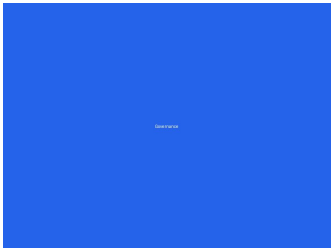
Uniswap in Practice



Token Swap



Liquidity Provision



Governance

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What was the primary innovation in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Fee tiers

Quiz (1/2)

Q1. What was the primary innovation in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading.

Q2. What happens if price moves outside your V3 range?
A) Lose position B) Auto-rebalances C) Stop earning fees D) Fees double

Quiz (1/2)

Q1. What was the primary innovation in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading.

Q2. What happens if price moves outside your V3 range?
A) Lose position B) Auto-rebalances C) Stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within range.

Q3. Which fee tier is best for USDC/USDT?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%

Quiz (1/2)

Q1. What was the primary innovation in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading.

Q2. What happens if price moves outside your V3 range?
A) Lose position B) Auto-rebalances C) Stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within range.

Q3. Which fee tier is best for USDC/USDT?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% due to low volatility.

Q4. What is V3 capital efficiency advantage?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage

Quiz (1/2)

Q1. What was the primary innovation in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading.

Q2. What happens if price moves outside your V3 range?
A) Lose position B) Auto-rebalances C) Stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within range.

Q3. Which fee tier is best for USDC/USDT?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% due to low volatility.

Q4. What is V3 capital efficiency advantage?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage
Answer: B – Concentrated liquidity achieves 10-200x efficiency.

Q5. How many UNI were airdropped per user in 2020?
A) 100 B) 200 C) 400 D) 1000

Quiz (1/2)

Q1. What was the primary innovation in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading.

Q2. What happens if price moves outside your V3 range?
A) Lose position B) Auto-rebalances C) Stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within range.

Q3. Which fee tier is best for USDC/USDT?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% due to low volatility.

Q4. What is V3 capital efficiency advantage?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage
Answer: B – Concentrated liquidity achieves 10-200x efficiency.

Q5. How many UNI were airdropped per user in 2020?
A) 100 B) 200 C) 400 D) 1000
Answer: C – 400 UNI airdropped to each early user.

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX

Quiz (2/2)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks for custom pool logic.

Q7. Why are V3 LP positions NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings

Quiz (2/2)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks for custom pool logic.

Q7. Why are V3 LP positions NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters.

Q8. What is the proposed protocol fee if switch activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%

Quiz (2/2)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks for custom pool logic.

Q7. Why are V3 LP positions NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters.

Q8. What is the proposed protocol fee if switch activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% to UNI holders.

Q9. What is a "singleton contract" in V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain

Quiz (2/2)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks for custom pool logic.

Q7. Why are V3 LP positions NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters.

Q8. What is the proposed protocol fee if switch activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% to UNI holders.

Q9. What is a "singleton contract" in V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain
Answer: B – All pools in single contract for gas optimization.

Q10. What formula does Uniswap V1/V2 use?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$

Quiz (2/2)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks for custom pool logic.

Q7. Why are V3 LP positions NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters.

Q8. What is the proposed protocol fee if switch activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% to UNI holders.

Q9. What is a "singleton contract" in V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain
Answer: B – All pools in single contract for gas optimization.

Q10. What formula does Uniswap V1/V2 use?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – Constant product formula $x \cdot y = k$.

Thank you

Questions?

Next: L36 Lab – Testnet Swap

L35: Uniswap Deep Dive

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Trace Uniswap's evolution from V1 to V4
- Explain concentrated liquidity mechanics in Uniswap V3
- Analyze fee tier optimization
- Explore UNI token governance and the fee switch debate
- Case Study: Fee switch governance controversy

The Problem: How does the largest DEX work?

The Challenge
How does Uniswap process billions in trading volume without a traditional order book, match buyers with sellers across volatile price ranges, and continuously innovate while maintaining backward compatibility?

Why It Matters

- Uniswap processes $110B+ in volume, setting DEX industry standards
- V1 (2018) pioneered AMMs, V2 (2020) added pairs, V3 (2021) brought concentrated liquidity, V4 (2025) introduced hooks

What We Need

- System design principles
- Understanding of DEX architecture evolution and capital efficiency optimization

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How Uniswap Deep Dive addresses this challenge

Uniswap: Origins

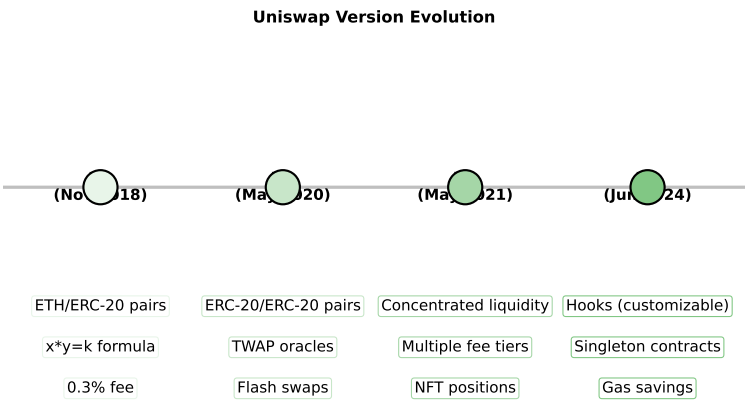
Created by: Hayden Adams (inspired by Vitalik Buterin's post)

Market Position (Dec 2025):

- Largest DEX by volume ($110B+ cumulative v4 volume)
- $4.5B TVL across all chains (v4: $1B+ in 6 months)
- Deployed on 10+ chains including Unichain L2

Impact: Pioneered AMM model, inspired hundreds of forks.

Uniswap Version Evolution



Each version added significant innovation while maintaining core AMM principles

Uniswap V1 and V2

V1 (2018):

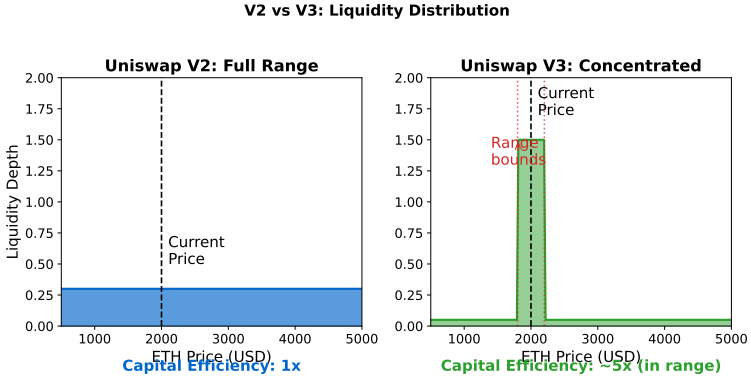
- ETH/ERC-20 pairs only, $x \cdot y = k$ formula
- 0.3% fee (100% to LPs)

V2 (2020) - Major Improvements:

- **ERC-20/ERC-20 pairs:** Direct trading without ETH
- **TWAP oracles:** Manipulation-resistant price feeds
- **Flash swaps:** Borrow tokens, repay in same tx
- **Protocol fee switch:** 0.05% potential fee (not activated)

Flash Swaps: Enable arbitrage without upfront capital.

Uniswap V3: Concentrated Liquidity



V3 concentrates liquidity in active trading ranges for higher efficiency

Concentrated Liquidity Explained

Revolutionary Concept: LPs choose specific price ranges for liquidity.

How It Works:

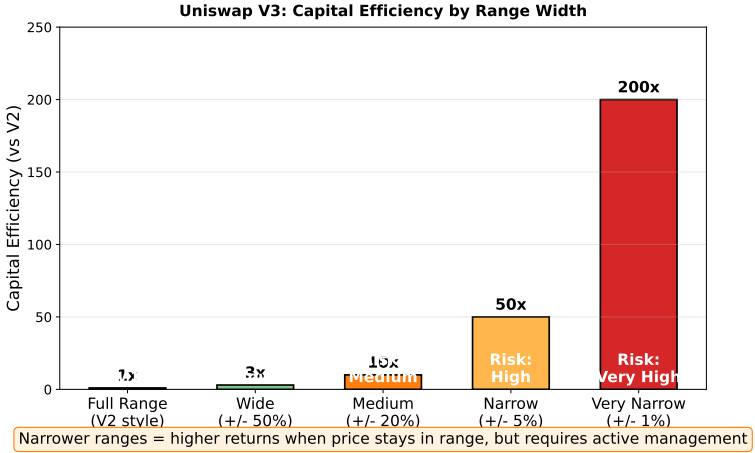
- Instead of infinite range, LP sets bounds (e.g., \$1,900-\$2,100)
- Liquidity only active within range
- Earns fees only when price in range

Example:

- LP deposits 1 ETH + 2,000 USDC with range \$1,900-\$2,100
- ETH = \$2,000: Position active, earns fees
- ETH = \$2,200: Position fully in USDC, no fees
- ETH = \$1,800: Position fully in ETH, no fees

(c) Joerg Osterrieder 2025

Capital Efficiency by Range Width



Trade-off: Higher efficiency requires active management as price moves

Concentrated Liquidity: Management

Challenge: Price may exit your range, requiring rebalancing.

Strategies:

1. **Passive (Wide Range):** Low returns, minimal management
2. **Active (Narrow Range):** High returns if price stable, frequent rebalance
3. **Automated (Vault Services):** Gamma, Arrakis auto-rebalance for 0.1-0.5% fee

V3 LP Positions: Non-fungible (NFTs) - each position has custom range.
Impact: Less composable with other DeFi (wrapper protocols needed).

Uniswap V3: Fee Tiers

Innovation: Multiple fee tiers for same pair.

Fee Tier	Use Case	Examples
0.01%	Stablecoins	USDC/USDT, DAI/USDC
0.05%	Correlated assets	ETH/stETH
0.30%	Standard pairs	ETH/USDC
1.00%	Exotic/volatile	Low-liquidity tokens

Rationale: Stablecoins need low fees to attract volume; volatile pairs need higher fees to compensate IL.

Uniswap V4 (Jan 2025): Hooks

Key Innovation: Customizable pool behavior via hooks.

What are Hooks?

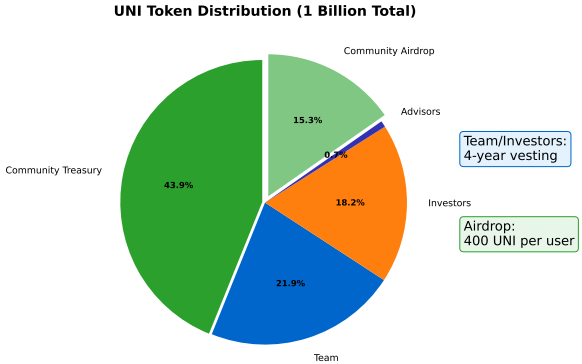
- Smart contracts executing at specific points in trade lifecycle
- Before/after swap, before/after adding liquidity
- Add custom logic without forking Uniswap

Example Use Cases:

- Dynamic fees based on volatility
- On-chain limit orders, TWAP execution
- Auto-rebalancing liquidity, MEV protection

Singleton Contract: All pools in one contract (gas savings).

UNI Token Distribution



Community received 60% (airdrop + treasury); team/investors 40% with 4-year vesting

UNI Token: Governance

Launch: September 2020 (400 UNI airdropped to every user)

Governance Rights:

- Vote on protocol upgrades
- Treasury allocation ($5B+ in assets)
- Fee switch activation (controversial)
- Cross-chain deployment approvals

Voting: 1 UNI = 1 vote (can delegate)
Thresholds: 2.5M UNI to propose, 40M quorum

Current Utility: Governance only - no direct fee revenue (yet).

The Fee Switch Debate

Current State: 0.3% fee goes 100% to LPs
Potential: Protocol can redirect 0.05% to UNI holders

Arguments For:

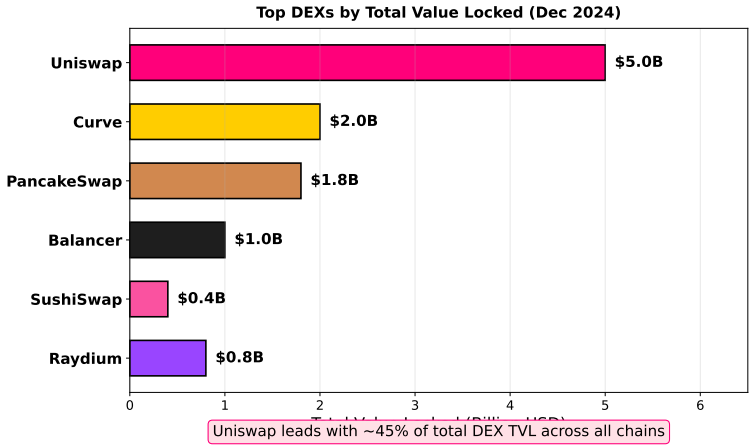
- Value accrual for UNI token
- Sustainable protocol development revenue

Arguments Against:

- Reduces LP returns (may lose liquidity)
- Regulatory risk (UNI could be deemed security)
- Current model working well

Status (Dec 2025): Governance voted to burn 100M tokens; protocol fees under review.

DEX Market Comparison



Uniswap maintains market leadership through innovation and brand recognition

Uniswap's Multi-Chain Strategy

Deployments (Dec 2025):

- 10+ chains: Ethereum, Arbitrum, Base, Optimism, Polygon, BNB, Unichain

Benefits:

- Lower gas fees on L2s (10-100x cheaper)
- Access different user bases
- Maintain dominance across ecosystems

Challenge: Liquidity fragmentation across chains.

Uniswap's Moat: Brand recognition, deepest liquidity, innovation leadership.

Regulatory Challenges

SEC Wells Notice (April 2024):

- Allegations: Operating unregistered securities exchange
- Response: Protocol is decentralized; Labs just builds software

Legal Arguments:

- Protocol vs. Interface distinction
- Smart contracts are speech (First Amendment)
- Users choose tokens, not Uniswap

Potential Outcomes:

- Settlement, lawsuit, or favorable ruling
- Precedent-setting for all DeFi

Status (Dec 2025): SEC closed 4-year investigation; no enforcement action taken.

Problem Solved? Uniswap Deep Dive

The Original Problem

How does the largest DEX work?

How Uniswap Deep Dive Solves It

- V3 concentrated liquidity delivers 10-200x capital efficiency by focusing liquidity in active price ranges
- Fee tiers (0.01%-1.00%) allow market-driven pricing - stablecoins pay less, volatile pairs pay more
- V4 hooks enable customizable pool behavior without forking, unlocking new DeFi primitives

Remaining Limitations

- V3 complexity increases LP management burden - narrow ranges require frequent rebalancing
- Impermanent loss persists in V3 despite efficiency gains, especially in volatile markets
- MEV exposure remains - sandwich attacks can extract value from traders

Open Questions

- Will V4 hooks enable fundamentally new DeFi primitives, or just marginal improvements?
- Risk: Hook vulnerabilities, governance capture, regulatory pressure on fee switch

Uniswap Deep Dive partially solves "How does the largest DEX work" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- Uniswap evolved from V1 (simple AMM) to V4 (customizable hooks)
- V3 concentrated liquidity: 10-200x capital efficiency
- Fee tiers: 0.01% (stables) to 1% (exotic)
- UNI governs protocol but lacks direct cash flow
- Fee switch debate: value vs. LP retention vs. regulation
- Multi-chain expansion maintains market dominance

Next Lecture: Lab - Testnet Swap (hands-on Uniswap experience).

Questions for Reflection

1. How does concentrated liquidity improve capital efficiency?
2. Why might activating the fee switch harm Uniswap's position?
3. What are the trade-offs of NFT-based LP positions in V3?
4. How do hooks in V4 enable new DeFi primitives?
5. Should Uniswap prioritize decentralization or regulatory compliance?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What was the primary innovation introduced in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Multiple fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading without requiring ETH as intermediary.

Q2. In Uniswap V3, what happens if the market price moves outside your liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within the specified range.

Q3. Which fee tier is most appropriate for USDC/USDT trading?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% fee tier due to low volatility and price stability.

Q4. What is the capital efficiency advantage of concentrated liquidity?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage
Answer: B – V3 can achieve 10-200x capital efficiency by concentrating liquidity in active ranges.

Q5. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Quiz Questions (6–10)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks allowing custom logic at swap/liquidity lifecycle points.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters, making them non-fungible.

Q8. What is the proposed protocol fee if the fee switch is activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% from the 0.30% fee to UNI holders.

Q9. How many UNI tokens are required to submit a governance proposal?
A) 100K UNI B) 500K UNI C) 2.5M UNI D) 10M UNI
Answer: C – 2.5 million UNI tokens are required to submit a proposal.

Q10. What was Uniswap's total V4 cumulative volume by Dec 2025?
A) $10B+ B) $50B+ C) $110B+ D) $500B+
Answer: C – V4 reached over $110 billion in cumulative trading volume.

Quiz Questions (11–15)

Q11. Which Uniswap version first introduced TWAP price oracles?
A) V1 B) V2 C) V3 D) V4
Answer: B – V2 introduced manipulation-resistant Time-Weighted Average Price oracles.

Q12. What is the main regulatory risk of activating the fee switch?
A) Higher taxes B) UNI deemed security C) Protocol shutdown D) Lower volume
Answer: B – Fee revenue to token holders could classify UNI as a security under Howey Test.

Q13. Which fee tier is recommended for ETH/stETH pairs?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: B – 0.05% tier is for correlated assets like ETH and its staked derivative.

Q14. What percentage of UNI token supply was allocated to the community?
A) 20% B) 40% C) 60% D) 80%
Answer: C – 60% went to community (airdrop + treasury); 40% to team/investors.

Q15. What is a "singleton contract" in Uniswap V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain deployment
Answer: B – All pools exist in a single contract for gas optimization.

Quiz Questions (16–20)

Q16. What was the outcome of the SEC investigation into Uniswap (Dec 2025)?
A) Lawsuit filed B) Settlement reached C) Closed with no action D) Ongoing
Answer: C – SEC closed its 4-year investigation without taking enforcement action.

Q17. Which strategy requires the most active management in V3?
A) Wide range B) Full range C) Narrow range D) No range
Answer: C – Narrow ranges need frequent rebalancing as price moves outside bounds.

Q18. What is the quorum requirement for Uniswap governance votes?
A) 10M UNI B) 20M UNI C) 40M UNI D) 100M UNI
Answer: C – 40 million UNI tokens must participate for a vote to be valid.

Q19. Which of the following is NOT a potential use case for V4 hooks?
A) Dynamic fees B) On-chain limit orders C) Increased TVL D) MEV protection
Answer: C – Hooks enable custom logic (dynamic fees, orders, MEV protection) not TVL itself.

Q20. What formula does Uniswap V1 and V2 use for constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

L35: Uniswap Deep Dive

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

V2 vs V3 Complexity

[COMIC: V2 vs V3 complexity]

Placeholder for comic showing V2 as simple "set and forget" LP vs. V3 LP frantically adjusting price ranges like a day trader

The Setup

- V2: deposit tokens, earn fees, relax
- Simple 50/50 split across all prices
- Capital inefficient but easy

The Punchline

- V3: choose your price range
- 10-200x capital efficiency... if you manage it
- Miss the range = earn nothing

With great efficiency comes great responsibility (and complexity)

Learning Objectives

- Trace Uniswap's evolution from V1 to V4
- Explain concentrated liquidity mechanics in Uniswap V3
- Analyze fee tier optimization
- Explore UNI token governance and the fee switch debate
- Case Study: Fee switch governance controversy

Building on L34: AMM Mechanics

The Problem: How does the largest DEX work?

The Challenge
How does Uniswap process billions in trading volume without a traditional order book, match buyers with sellers across volatile price ranges, and continuously innovate while maintaining backward compatibility?

Why It Matters

- Uniswap processes $110B+ in volume, setting DEX industry standards
- V1 (2018) pioneered AMMs, V2 (2020) added pairs, V3 (2021) brought concentrated liquidity, V4 (2025) introduced hooks

What We Need

- System design principles
- Understanding of DEX architecture evolution and capital efficiency optimization

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How Uniswap Deep Dive addresses this challenge

How Did Uniswap Originate?

Created by: Hayden Adams (inspired by Vitalik Buterin's post)

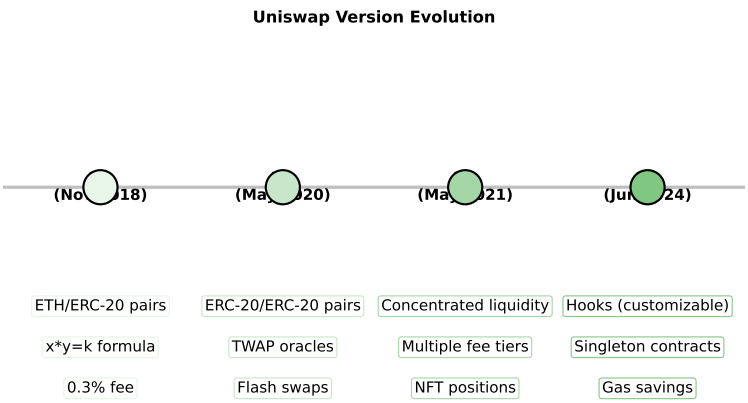
Market Position (Dec 2025):

- Largest DEX by volume ($110B+ cumulative v4 volume)
- $4.5B TVL across all chains (v4: $1B+ in 6 months)
- Deployed on 10+ chains including Unichain L2

Impact: Pioneered AMM model, inspired hundreds of forks.

→ Problem: How does the largest DEX work? — Uniswap: Origins — Uniswap pioneered AMMs in 2018 – explaining how the largest DEX works without order books.

Uniswap Version Evolution



Each version added significant innovation while maintaining core AMM principles

What Were the Key Differences Between V1 and V2?

V1 (2018):

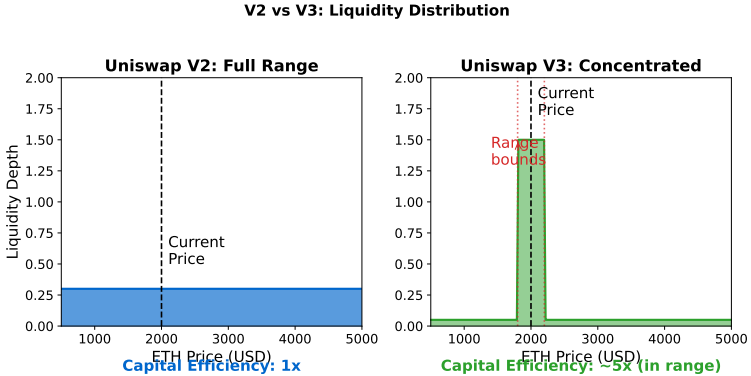
- ETH/ERC-20 pairs only, $x \cdot y = k$ formula
- 0.3% fee (100% to LPs)

V2 (2020) - Major Improvements:

- **ERC-20/ERC-20 pairs:** Direct trading without ETH
- **TWAP (Time-Weighted Average Price—averaged over time to resist manipulation) oracles:** Manipulation-resistant price feeds
- **Flash swaps:** Borrow tokens, repay in same tx (flash loans: borrow any amount, repay in same transaction)
- **Protocol fee switch:** 0.05% potential fee (not activated)

Flash Swaps: Flash loans enable arbitrage without upfront capital.

Uniswap V3: Concentrated Liquidity



V3 concentrates liquidity in active trading ranges for higher efficiency | → Problem: How does the largest DEX work? — Uniswap V3: Concentrated Liquidity — Concentrated liquidity (V3) solved capital efficiency – LPs focus liquidity where trades happen.

How Does Concentrated Liquidity Work?

Revolutionary Concept: LPs choose specific price ranges for liquidity.

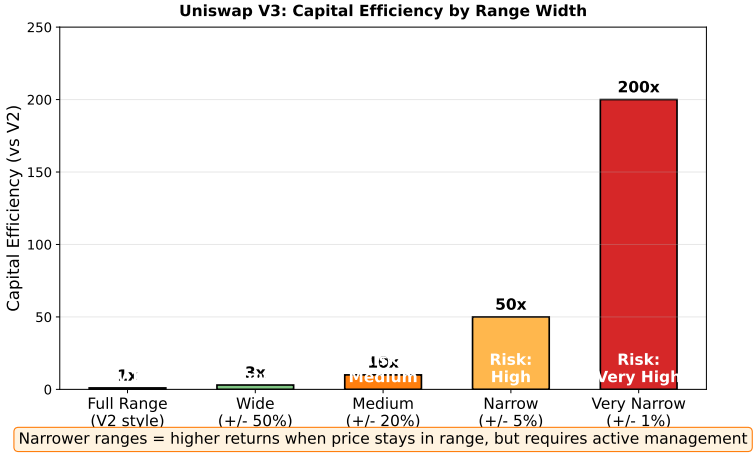
How It Works:

- Instead of infinite range, LP sets bounds (e.g., \$1,900-\$2,100)
- Liquidity only active within range
- Earns fees only when price in range

Example:

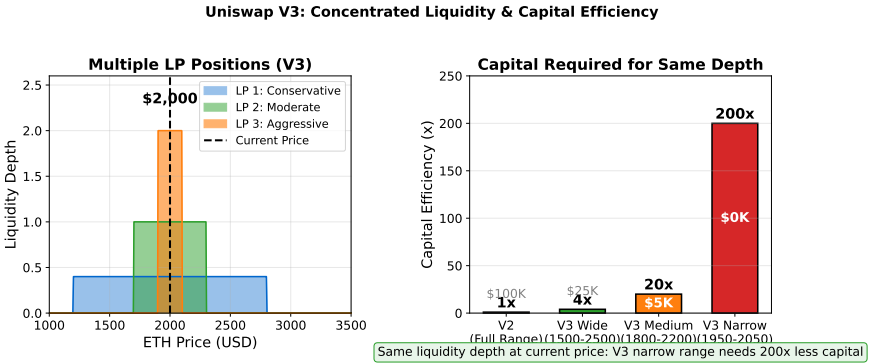
- LP deposits 1 ETH + 2,000 USDC with range \$1,900-\$2,100
- ETH = \$2,000: Position active, earns fees
- ETH = \$2,200: Position fully in USDC, no fees
- ETH = \$1,800: Position fully in ETH, no fees

Capital Efficiency by Range Width



Trade-off: Higher efficiency requires active management as price moves

V3 Concentrated Liquidity: LP Positions & Efficiency



Multiple LPs can overlap ranges; narrower ranges = higher efficiency but more active management

How Do You Manage Concentrated Liquidity?

Challenge: Price may exit your range, requiring rebalancing.

Strategies:

1. **Passive (Wide Range):** Low returns, minimal management
2. **Active (Narrow Range):** High returns if price stable, frequent rebalance
3. **Automated (Vault Services):** Gamma, Arrakis auto-rebalance for 0.1-0.5% fee

V3 LP Positions: Non-fungible (NFTs) - each position has custom range.
Impact: Less composable with other DeFi (wrapper protocols needed).

Why Does Uniswap V3 Have Multiple Fee Tiers?

Innovation: Multiple fee tiers for same pair.

Fee Tier	Use Case	Examples
0.01%	Stablecoins	USDC/USDT, DAI/USDC
0.05%	Correlated assets	ETH/stETH
0.30%	Standard pairs	ETH/USDC
1.00%	Exotic/volatile	Low-liquidity tokens

Rationale: Stablecoins need low fees to attract volume; volatile pairs need higher fees to compensate IL.

→ *Problem: How does the largest DEX work? — Uniswap V3: Fee Tiers — Fee tiers optimize for different pairs – 0.01% for stables, 1% for volatile tokens.*

Problem Check-In: Uniswap Deep Dive

Recall Our Problem

How does the largest DEX work?

What We've Learned So Far

- Uniswap evolved through 4 versions (V2: token pairs, V3: concentrated liquidity, V4: hooks)
- Concentrated liquidity provides 10-200x capital efficiency by focusing on active trading ranges
- Innovation explains dominance: Uniswap leads by continuously improving its AMM design

Still to Address

- Governance: how UNI token holders control protocol decisions and the fee switch debate
- Will V4 hooks unlock new DeFi primitives or just incremental improvements?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How does the largest DEX work?"?

What Are Uniswap V4 Hooks?

Key Innovation: Customizable pool behavior via hooks.

What are Hooks?

- Smart contracts executing at specific points in trade lifecycle
- Before/after swap, before/after adding liquidity
- Add custom logic without forking Uniswap

Example Use Cases:

- Dynamic fees based on volatility
- On-chain limit orders, TWAP execution
- Auto-rebalancing liquidity, MEV protection

Singleton Contract: All pools in one contract (gas savings).

Uniswap Version Evolution: V1 to V4

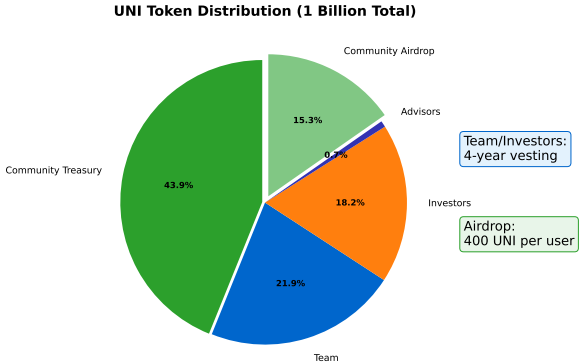
Uniswap Version Evolution: V1 → V2 → V3 → V4

	V1 Nov 2018	V2 May 2020	V3 May 2021	V4 Jan 2025
Trading Pairs	ETH/ERC-20 only	Any ERC-20 pair	Any ERC-20 pair	Any ERC-20 pair
Liquidity Type	Full range	Full range	Concentrated	Concentrated + Hooks
LP Positions	Fungible (ERC-20)	Fungible (ERC-20)	Non-fungible (NFT)	Non-fungible (NFT)
Fee Tiers	0.3% fixed	0.3% fixed	0.01-1% (4 tiers)	Dynamic (via hooks)
Capital Efficiency	1x	1x	10-200x	10-200x+
Key Innovation	x*y=k AMM	TWAP oracles	Concentrated LP	Hooks (custom logic)

Evolution: Simple AMM → Multi-pair → Capital efficient → Customizable

Each version builds on previous innovations: AMM → Multi-pair → Concentrated LP → Hooks

UNI Token Distribution



Community received 60% (airdrop + treasury); team/investors 40% with 4-year vesting

How Does UNI Token Governance Work?

Launch: September 2020 (400 UNI airdropped to every user)

Governance Rights (governance token: grants voting rights on protocol decisions):

- Vote on protocol upgrades
- Treasury allocation ($5B+ in assets)
- Fee switch activation (controversial)
- Cross-chain deployment approvals

Voting: 1 UNI = 1 vote (can delegate)
Thresholds: 2.5M UNI to propose, 40M quorum

Current Utility: Governance only - no direct fee revenue (yet).

Should UNI Holders Capture Value?

Current State: 0.3% fee goes 100% to LPs
Potential: Protocol can redirect 0.05% to UNI holders

Arguments For:

- Value accrual for UNI token
- Sustainable protocol development revenue

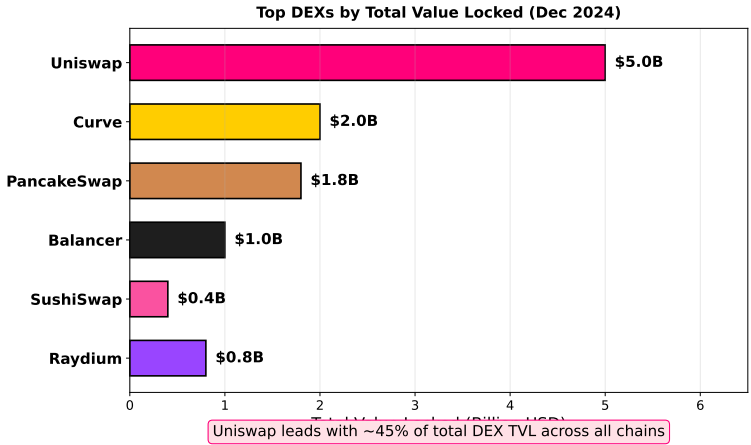
Arguments Against:

- Reduces LP returns (may lose liquidity)
- Regulatory risk (UNI could be deemed security)
- Current model working well

Status (Dec 2025): Governance voted to burn 100M tokens; protocol fees under review.

→ *Problem: How does the largest DEX work? — The Fee Switch Debate — The fee switch debate: should UNI holders capture value, or should LPs keep all fees?*

DEX Market Comparison



Uniswap maintains market leadership through innovation and brand recognition

Why Did Uniswap Deploy on Multiple Chains?

Deployments (Dec 2025):

- 10+ chains: Ethereum, Arbitrum, Base, Optimism, Polygon, BNB, Unichain

Benefits:

- Lower gas fees on L2s (10-100x cheaper)
- Access different user bases
- Maintain dominance across ecosystems

Challenge: Liquidity fragmentation across chains.

Uniswap's Moat: Brand recognition, deepest liquidity, innovation leadership.

What Regulatory Challenges Does Uniswap Face?

SEC Wells Notice (April 2024):

- Allegations: Operating unregistered securities exchange
- Response: Protocol is decentralized; Labs just builds software

Legal Arguments:

- Protocol vs. Interface distinction
- Smart contracts are speech (First Amendment)
- Users choose tokens, not Uniswap

Potential Outcomes:

- Settlement, lawsuit, or favorable ruling
- Precedent-setting for all DeFi

Status (Dec 2025): SEC closed 4-year investigation; no enforcement action taken.

Problem Solved? Uniswap Deep Dive

The Original Problem

How does the largest DEX work?

How Uniswap Deep Dive Solves It

- V3 concentrated liquidity delivers 10-200x capital efficiency by focusing liquidity in active price ranges
- Fee tiers (0.01%-1.00%) allow market-driven pricing - stablecoins pay less, volatile pairs pay more
- V4 hooks enable customizable pool behavior without forking, unlocking new DeFi primitives

Remaining Limitations

- V3 complexity increases LP management burden - narrow ranges require frequent rebalancing
- Impermanent loss persists in V3 despite efficiency gains, especially in volatile markets
- MEV exposure remains - sandwich attacks can extract value from traders

Open Questions

- Will V4 hooks enable fundamentally new DeFi primitives, or just marginal improvements?
- Risk: Hook vulnerabilities, governance capture, regulatory pressure on fee switch

Uniswap Deep Dive partially solves "How does the largest DEX work" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Uniswap Deep Dive

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Uniswap Deep Dive

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Uniswap Deep Dive

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Concentrated Liquidity Management

[COMIC: Concentrated liquidity management]

Placeholder for comic showing LP watching price ticker like a hawk, price moving outside their range, and LP missing all fees while others profit

The Trade-off

- Narrow range = high efficiency
- But price can exit your range
- Out of range = zero fee earnings

Management Required

- Active rebalancing needed
- Gas costs eat into profits
- Or pay 0.5% to vault managers

Concentrated liquidity: be a professional LP or use a vault – no in-between

Summary

Key Takeaways:

- Uniswap evolved from V1 (simple AMM) to V4 (customizable hooks)
- V3 concentrated liquidity: 10-200x capital efficiency
- Fee tiers: 0.01% (stables) to 1% (exotic)
- UNI governs protocol but lacks direct cash flow
- Fee switch debate: value vs. LP retention vs. regulation
- Multi-chain expansion maintains market dominance

Next Lecture: Lab - Testnet Swap (hands-on Uniswap experience).

Next Lesson: L36 – Lab: Testnet Swap

Questions for Reflection

1. How does concentrated liquidity improve capital efficiency?
2. Why might activating the fee switch harm Uniswap's position?
3. What are the trade-offs of NFT-based LP positions in V3?
4. How do hooks in V4 enable new DeFi primitives?
5. Should Uniswap prioritize decentralization or regulatory compliance?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What was the primary innovation introduced in Uniswap V2?
A) Concentrated liquidity B) ERC-20/ERC-20 pairs C) Hooks D) Multiple fee tiers
Answer: B – V2 enabled direct ERC-20/ERC-20 trading without requiring ETH as intermediary.

Q2. In Uniswap V3, what happens if the market price moves outside your liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within the specified range.

Q3. Which fee tier is most appropriate for USDC/USDT trading?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% fee tier due to low volatility and price stability.

Q4. What is the capital efficiency advantage of concentrated liquidity?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage
Answer: B – V3 can achieve 10-200x capital efficiency by concentrating liquidity in active ranges.

Q5. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Quiz Questions (6–10)

Q6. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks allowing custom logic at swap/liquidity lifecycle points.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters, making them non-fungible.

Q8. What is the proposed protocol fee if the fee switch is activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% from the 0.30% fee to UNI holders.

Q9. How many UNI tokens are required to submit a governance proposal?
A) 100K UNI B) 500K UNI C) 2.5M UNI D) 10M UNI
Answer: C – 2.5 million UNI tokens are required to submit a proposal.

Q10. What was Uniswap's total V4 cumulative volume by Dec 2025?
A) $10B+ B) $50B+ C) $110B+ D) $500B+
Answer: C – V4 reached over $110 billion in cumulative trading volume.

Quiz Questions (11–15)

Q11. Which Uniswap version first introduced TWAP price oracles?
A) V1 B) V2 C) V3 D) V4
Answer: B – V2 introduced manipulation-resistant Time-Weighted Average Price oracles.

Q12. What is the main regulatory risk of activating the fee switch?
A) Higher taxes B) UNI deemed security C) Protocol shutdown D) Lower volume
Answer: B – Fee revenue to token holders could classify UNI as a security under Howey Test.

Q13. Which fee tier is recommended for ETH/stETH pairs?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: B – 0.05% tier is for correlated assets like ETH and its staked derivative.

Q14. What percentage of UNI token supply was allocated to the community?
A) 20% B) 40% C) 60% D) 80%
Answer: C – 60% went to community (airdrop + treasury); 40% to team/investors.

Q15. What is a "singleton contract" in Uniswap V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain deployment
Answer: B – All pools exist in a single contract for gas optimization.

Quiz Questions (16–20)

Q16. What was the outcome of the SEC investigation into Uniswap (Dec 2025)?
A) Lawsuit filed B) Settlement reached C) Closed with no action D) Ongoing
Answer: C – SEC closed its 4-year investigation without taking enforcement action.

Q17. Which strategy requires the most active management in V3?
A) Wide range B) Full range C) Narrow range D) No range
Answer: C – Narrow ranges need frequent rebalancing as price moves outside bounds.

Q18. What is the quorum requirement for Uniswap governance votes?
A) 10M UNI B) 20M UNI C) 40M UNI D) 100M UNI
Answer: C – 40 million UNI tokens must participate for a vote to be valid.

Q19. Which of the following is NOT a potential use case for V4 hooks?
A) Dynamic fees B) On-chain limit orders C) Increased TVL D) MEV protection
Answer: C – Hooks enable custom logic (dynamic fees, orders, MEV protection) not TVL itself.

Q20. What formula does Uniswap V1 and V2 use for constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

Quiz: Uniswap Deep Dive

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What formula does Uniswap V1 and V2 use for the constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$

Quiz (1–5)

Q1. What formula does Uniswap V1 and V2 use for the constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

Q2. What happens if the market price moves outside your V3 liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double

Quiz (1–5)

Q1. What formula does Uniswap V1 and V2 use for the constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

Q2. What happens if the market price moves outside your V3 liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within the specified range.

Q3. Which fee tier is most appropriate for USDC/USDT trading?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%

Quiz (1–5)

Q1. What formula does Uniswap V1 and V2 use for the constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

Q2. What happens if the market price moves outside your V3 liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within the specified range.

Q3. Which fee tier is most appropriate for USDC/USDT trading?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% fee tier due to low volatility and price stability.

Q4. What is the capital efficiency advantage of concentrated liquidity?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What formula does Uniswap V1 and V2 use for the constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

Q2. What happens if the market price moves outside your V3 liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within the specified range.

Q3. Which fee tier is most appropriate for USDC/USDT trading?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% fee tier due to low volatility and price stability.

Q4. What is the capital efficiency advantage of concentrated liquidity?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage
Answer: B – V3 can achieve 10-200x capital efficiency by concentrating liquidity in active ranges.

Q5. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What formula does Uniswap V1 and V2 use for the constant product AMM?
A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$
Answer: B – The constant product formula $x \cdot y = k$ ensures balanced liquidity.

Q2. What happens if the market price moves outside your V3 liquidity range?
A) You lose your position B) Position auto-rebalances C) You stop earning fees D) Fees double
Answer: C – Liquidity only earns fees when price is within the specified range.

Q3. Which fee tier is most appropriate for USDC/USDT trading?
A) 0.01% B) 0.05% C) 0.30% D) 1.00%
Answer: A – Stablecoins use 0.01% fee tier due to low volatility and price stability.

Q4. What is the capital efficiency advantage of concentrated liquidity?
A) 2-5x B) 10-200x C) 500-1000x D) No advantage
Answer: B – V3 can achieve 10-200x capital efficiency by concentrating liquidity in active ranges.

Q5. What is the main innovation of Uniswap V4?
A) Lower fees B) Hooks for customization C) Faster swaps D) Better UX
Answer: B – V4 introduced hooks allowing custom logic at swap/liquidity lifecycle points.

Quiz (6–10)

Q6. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI

Quiz (6–10)

Q6. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings

Quiz (6–10)

Q6. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters, making them non-fungible.

Q8. What is the proposed protocol fee if the fee switch is activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters, making them non-fungible.

Q8. What is the proposed protocol fee if the fee switch is activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% from the 0.30% fee to UNI holders.

Q9. Which Uniswap version first introduced ERC-20/ERC-20 pairs?
A) V1 B) V2 C) V3 D) V4

Quiz (6–10)

Q6. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters, making them non-fungible.

Q8. What is the proposed protocol fee if the fee switch is activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% from the 0.30% fee to UNI holders.

Q9. Which Uniswap version first introduced ERC-20/ERC-20 pairs?
A) V1 B) V2 C) V3 D) V4
Answer: B – V2 enabled direct ERC-20/ERC-20 trading without requiring ETH as intermediary.

Q10. What is a "singleton contract" in Uniswap V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain deployment

Quiz (6–10)

Q6. How many UNI tokens were airdropped to each early Uniswap user in 2020?
A) 100 UNI B) 200 UNI C) 400 UNI D) 1000 UNI
Answer: C – 400 UNI were airdropped to every user who had interacted with the protocol.

Q7. Why are Uniswap V3 LP positions represented as NFTs?
A) Better liquidity B) Tax benefits C) Each has custom range D) Gas savings
Answer: C – Each position has unique price range parameters, making them non-fungible.

Q8. What is the proposed protocol fee if the fee switch is activated?
A) 0.01% B) 0.05% C) 0.10% D) 0.30%
Answer: B – Protocol could redirect 0.05% from the 0.30% fee to UNI holders.

Q9. Which Uniswap version first introduced ERC-20/ERC-20 pairs?
A) V1 B) V2 C) V3 D) V4
Answer: B – V2 enabled direct ERC-20/ERC-20 trading without requiring ETH as intermediary.

Q10. What is a "singleton contract" in Uniswap V4?
A) One pool only B) All pools in one contract C) Single fee tier D) One chain deployment
Answer: B – All pools exist in a single contract for gas optimization.

(c) Joerg Osterrieder 2025

L36: Lab – Testnet Swap

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

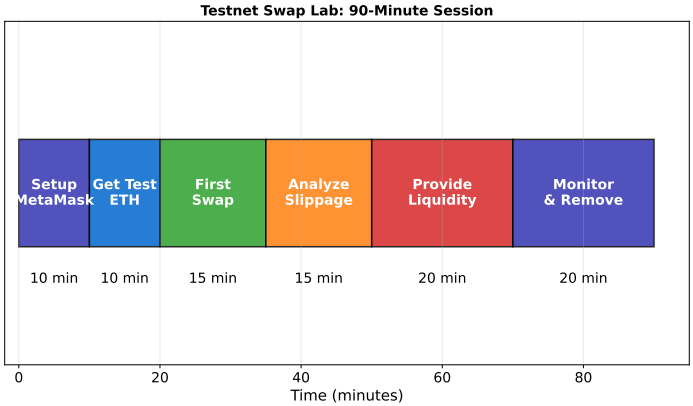
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Set up MetaMask wallet on Sepolia testnet
- Execute token swaps on Uniswap
- Analyze slippage behavior
- Provide and remove liquidity from AMM pools

Lab Session Workflow



Goal: Hands-on DeFi experience with zero financial risk.

Step 1-2: Setup MetaMask and Get Testnet ETH

MetaMask Setup:

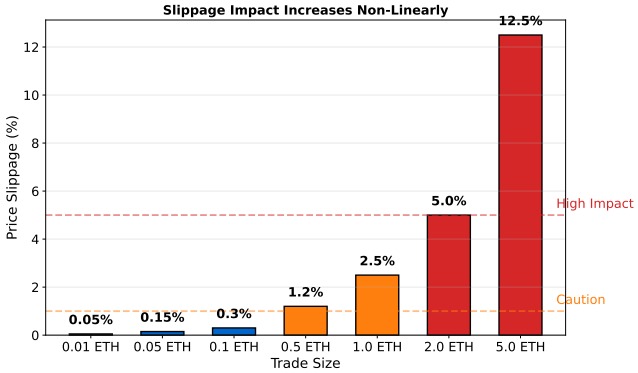
1. Install MetaMask browser extension
2. Create new wallet, save seed phrase securely
3. Enable test networks in settings
4. Switch to Sepolia Test Network

Get Testnet ETH:

- Faucets: sepoliafaucet.com, alchemy.com/faucets
- Request 0.5-1 testnet ETH (no real value)

Safety: Never share seed phrase; don't send real ETH to testnet.

Understanding Slippage



Key Insight: Larger trades face exponentially higher slippage.

Step 3-4: Execute Swap and Analyze Slippage

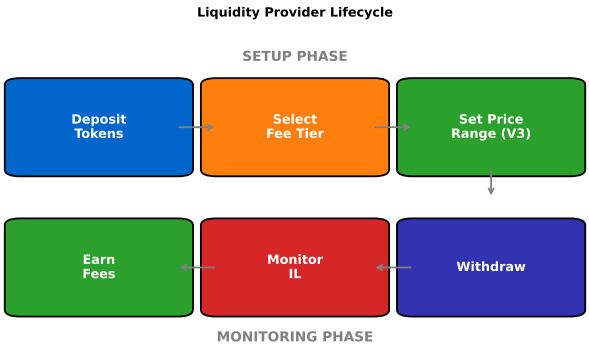
First Swap:

1. Connect wallet at app.uniswap.org
2. Swap 0.1 ETH for USDC
3. Review rate and confirm in MetaMask
4. Record: exchange rate, gas fee, tx hash

Slippage Analysis (quote, don't execute):

- Quote 0.01 ETH, 0.1 ETH, 1 ETH swaps
- Compare rates – how does price change with size?
- Pool liquidity determines slippage impact

LP Lifecycle



LPs earn fees but face impermanent loss risk.

Step 5-6: Provide and Remove Liquidity

Provide Liquidity:

1. Click “Pool” tab on Uniswap
2. Select ETH/USDC pair, 0.3% fee tier
3. Enter equal USD value of both tokens
4. Approve and confirm transaction

Remove Liquidity:

- Check pool share and fees earned
- Click “Remove Liquidity” on your position
- Compare final amounts to initial deposit
- Calculate impermanent loss (if any)

(c) Joerg Osterrieder 2025

Lab Deliverables

Lab Report (3-4 pages):

1. Swap details and exchange rates
2. Slippage analysis observations
3. LP position and impermanent loss calculation
4. Reflection on DeFi user experience

Supporting Evidence:

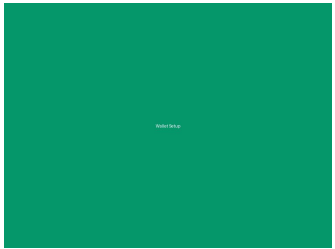
- Transaction hashes (Etherscan links)
- Screenshots of key steps

Key Takeaways

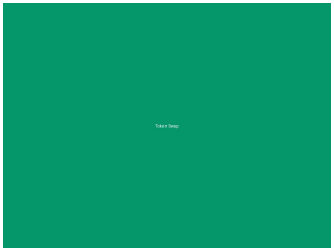
1. **Testnets:** Enable risk-free DeFi experimentation
2. **Slippage:** Increases non-linearly with trade size
3. **LP Returns:** Fees earned but impermanent loss possible
4. **DEX UX:** More complex than CEX (self-custody, gas)
5. **Practice First:** Understand mechanics before real funds

Next: L37 – Lending Protocols (Aave, Compound)

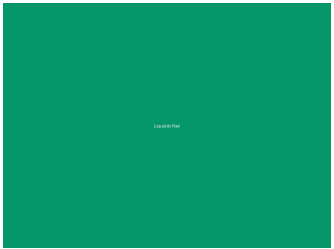
Testnet Swap in Practice



Wallet Setup



Token Swap



Liquidity Pool

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Why use Sepolia testnet for this lab?
A) Earn crypto B) Practice without risk C) Mine ETH D) Bypass gas

Quiz (1/2)

Q1. Why use Sepolia testnet for this lab?
A) Earn crypto B) Practice without risk C) Mine ETH D) Bypass gas
Answer: B – Testnet funds have no real value.

Q2. What should NEVER be shared?
A) Testnet address B) Tx hash C) Seed phrase D) Balance

Quiz (1/2)

Q1. Why use Sepolia testnet for this lab?
A) Earn crypto B) Practice without risk C) Mine ETH D) Bypass gas
Answer: B – Testnet funds have no real value.

Q2. What should NEVER be shared?
A) Testnet address B) Tx hash C) Seed phrase D) Balance
Answer: C – Seed phrase grants full wallet access.

Q3. What does slippage measure?
A) Gas fee B) Expected vs executed price difference C) Network congestion D) LP fee

Quiz (1/2)

Q1. Why use Sepolia testnet for this lab?
A) Earn crypto B) Practice without risk C) Mine ETH D) Bypass gas
Answer: B – Testnet funds have no real value.

Q2. What should NEVER be shared?
A) Testnet address B) Tx hash C) Seed phrase D) Balance
Answer: C – Seed phrase grants full wallet access.

Q3. What does slippage measure?
A) Gas fee B) Expected vs executed price difference C) Network congestion D) LP fee
Answer: B – Price difference due to trade impact.

Q4. How does slippage change with trade size?
A) Constant B) Decreases C) Increases non-linearly D) Becomes negative

Quiz (1/2)

Q1. Why use Sepolia testnet for this lab?
A) Earn crypto B) Practice without risk C) Mine ETH D) Bypass gas
Answer: B – Testnet funds have no real value.

Q2. What should NEVER be shared?
A) Testnet address B) Tx hash C) Seed phrase D) Balance
Answer: C – Seed phrase grants full wallet access.

Q3. What does slippage measure?
A) Gas fee B) Expected vs executed price difference C) Network congestion D) LP fee
Answer: B – Price difference due to trade impact.

Q4. How does slippage change with trade size?
A) Constant B) Decreases C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete reserves faster.

Q5. Which fee tier for ETH/USDC pool?
A) 0.01% B) 0.05% C) 0.3% D) 1%

Quiz (1/2)

Q1. Why use Sepolia testnet for this lab?
A) Earn crypto B) Practice without risk C) Mine ETH D) Bypass gas
Answer: B – Testnet funds have no real value.

Q2. What should NEVER be shared?
A) Testnet address B) Tx hash C) Seed phrase D) Balance
Answer: C – Seed phrase grants full wallet access.

Q3. What does slippage measure?
A) Gas fee B) Expected vs executed price difference C) Network congestion D) LP fee
Answer: B – Price difference due to trade impact.

Q4. How does slippage change with trade size?
A) Constant B) Decreases C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete reserves faster.

Q5. Which fee tier for ETH/USDC pool?
A) 0.01% B) 0.05% C) 0.3% D) 1%
Answer: C – Standard for medium volatility pairs.

Quiz (2/2)

Q6. What do LPs earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens

Quiz (2/2)

Q6. What do LPs earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens
Answer: B – Proportional share of trading fees.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage

Quiz (2/2)

Q6. What do LPs earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens
Answer: B – Proportional share of trading fees.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – Occurs when token prices change vs deposit.

Q8. What must you deposit to provide liquidity?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio

(c) Joerg Osterrieder 2025

Quiz (2/2)

Q6. What do LPs earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens
Answer: B – Proportional share of trading fees.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – Occurs when token prices change vs deposit.

Q8. What must you deposit to provide liquidity?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio
Answer: C – AMMs require balanced deposits.

Q9. What are tx hashes used for in the lab?
A) Verify on-chain activity B) Claim rewards C) Increase grades D) Mine blocks

Quiz (2/2)

Q6. What do LPs earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens
Answer: B – Proportional share of trading fees.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – Occurs when token prices change vs deposit.

Q8. What must you deposit to provide liquidity?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio
Answer: C – AMMs require balanced deposits.

Q9. What are tx hashes used for in the lab?
A) Verify on-chain activity B) Claim rewards C) Increase grades D) Mine blocks
Answer: A – Allow verification via Etherscan.

Q10. Most important lesson before real funds?
A) Max slippage B) Testnet practice C) Avoid LP D) Only CEX

Quiz (2/2)

Q6. What do LPs earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens
Answer: B – Proportional share of trading fees.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – Occurs when token prices change vs deposit.

Q8. What must you deposit to provide liquidity?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio
Answer: C – AMMs require balanced deposits.

Q9. What are tx hashes used for in the lab?
A) Verify on-chain activity B) Claim rewards C) Increase grades D) Mine blocks
Answer: A – Allow verification via Etherscan.

Q10. Most important lesson before real funds?
A) Max slippage B) Testnet practice C) Avoid LP D) Only CEX
Answer: B – Practice builds understanding without risk.

Thank you

Questions?

Next: L37 – Lending Protocols

Lab Session: Testnet Swap

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module E: DeFi Ecosystem

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Set up MetaMask wallet on Sepolia testnet
- Execute token swaps on Uniswap
- Analyze and understand slippage
- Provide and remove liquidity from AMM pools
- Track impermanent loss in practice

(c) Joerg Osterrieder 2025

The Problem: Understanding DeFi Through Practice

The Challenge
How can students safely learn DEX mechanics, slippage dynamics, and liquidity provision without risking real funds or facing prohibitive transaction costs?

Why It Matters

- Real DeFi mistakes can cost hundreds in gas fees or lost funds
- Understanding AMM mechanics is critical before mainnet usage

What You'll Explore

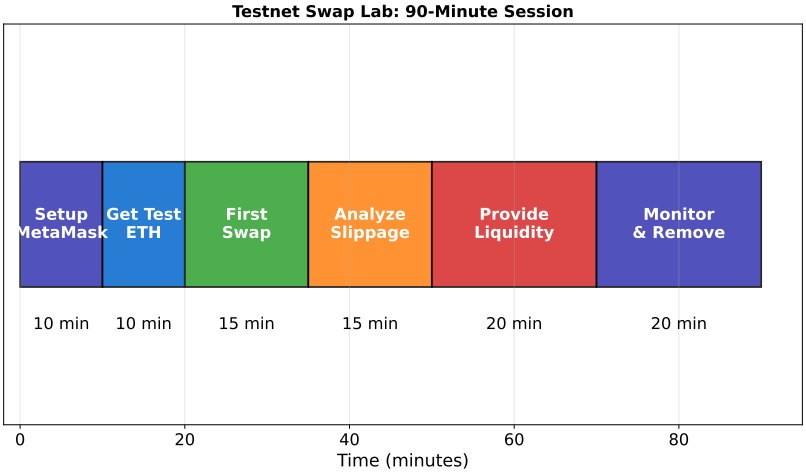
- Connecting wallet to testnet
- Executing swaps and analyzing slippage
- Providing liquidity and tracking impermanent loss
- Comparing theory to hands-on experience

The Cryptoeconomics Question
How do testnets enable risk-free learning while maintaining realistic incentive structures?

Today's lab: Hands-on DeFi experience reveals the economics beneath the interface

(c) Joerg Osterrieder 2025

Lab Session Structure



Hands-on DeFi experience with zero financial risk

Step 1: Setup MetaMask

Actions:

1. Install MetaMask browser extension
2. Create new wallet and save seed phrase
3. Enable test networks in settings
4. Switch to Sepolia Test Network

Safety Reminders:

- Testnet funds have NO real value
- Never share seed phrase
- Do NOT send real ETH to testnet address

Step 2: Acquire Testnet ETH

Sepolia Faucets:

- `https://sepoliafaucet.com`
- `https://www.alchemy.com/faucets/ethereum-sepolia`

Process:

1. Copy Sepolia address from MetaMask
2. Paste into faucet and complete captcha
3. Request 0.5-1 testnet ETH
4. Wait for transaction confirmation

Step 3: Execute First Swap

Goal: Swap 0.1 ETH for USDC on Uniswap

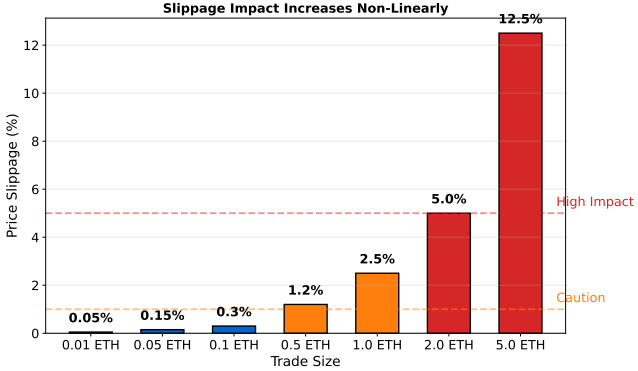
Process:

1. Connect wallet at `https://app.uniswap.org`
2. Select ETH to USDC swap
3. Enter amount and review rate
4. Confirm in MetaMask

Record:

- Exchange rate received
- Gas fee paid
- Transaction hash

Understanding Slippage



Larger trades face exponentially higher slippage - AMM fundamental

Step 4: Analyze Slippage

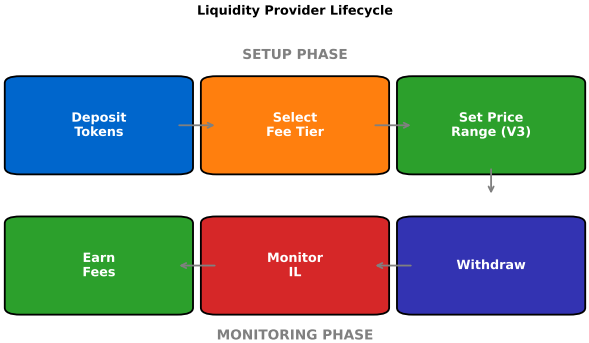
Experiment (DO NOT execute):

1. Quote 0.01 ETH swap - note price
2. Quote 0.1 ETH swap - note price
3. Quote 1 ETH swap - note price
4. Compare the three rates

Questions:

- How does price change with swap size?
- What causes non-linear slippage?
- How does pool liquidity affect slippage?

Liquidity Provider Lifecycle



LPs earn fees but face impermanent loss risk

Step 5: Provide Liquidity

Goal: Become a liquidity provider

Process:

1. Click “Pool” tab on Uniswap
2. Select ETH/USDC pair
3. Choose fee tier (0.3% recommended)
4. Enter token amounts
5. Approve and confirm transaction

Record:

- ETH and USDC deposited
- Fee tier selected
- Initial position value

Step 6: Monitor and Remove Liquidity

After providing liquidity:

- Check pool share percentage
- Monitor fees earned
- Execute a swap to see fees accrue

Remove Liquidity:

1. Click on your position
2. Select "Remove Liquidity"
3. Confirm withdrawal
4. Compare final amounts to initial deposit

Lab Deliverables

Submit:

1. **Lab Report (3-4 pages):**
   - Swap details and exchange rates
   - Slippage analysis observations
   - LP position and impermanent loss calculation
   - Reflection on DeFi user experience
2. **Supporting Evidence:**
   - Transaction hashes (Etherscan links)
   - Screenshots of key steps

Problem Solved? Testnet Learning Model

The Original Problem

How to learn DeFi mechanics without financial risk?

How Testnets Solve It

- Free testnet ETH from faucets eliminates capital requirements
- Identical smart contracts to mainnet enable realistic practice
- Mistakes cost nothing - failure becomes valuable learning

Remaining Limitations

- Testnet liquidity is shallow - slippage unrealistically high
- No real economic incentives - LP behavior differs from mainnet

Open Questions

- What behaviors change when real money is at stake?
- Risk: Overconfidence from testnet success leads to mainnet losses

Testnets solve the learning problem but cannot fully simulate mainnet incentive structures

(c) Joerg Osterrieder 2025

Key Takeaways

- Testnets enable risk-free DeFi experimentation
- Slippage increases non-linearly with trade size
- Liquidity providers earn fees but face impermanent loss
- DEX UX has improved but remains more complex than CEX
- Understanding mechanics is essential before using real funds

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of using Sepolia testnet for this lab?
A) To earn real cryptocurrency B) To practice DeFi without financial risk
C) To mine test Ethereum D) To bypass gas fees permanently
Answer: B – Testnet funds have no real value, enabling risk-free experimentation.

Q2. Which critical information should NEVER be shared?
A) Testnet address B) Transaction hash
C) Wallet seed phrase D) Sepolia ETH balance
Answer: C – Seed phrases grant full wallet access and must remain confidential.

Q3. What happens when you send real ETH to a testnet address?
A) It gets converted to testnet ETH B) The funds are permanently lost
C) The network refunds you D) It appears on mainnet instead
Answer: B – Mainnet and testnet are separate; real ETH sent to testnet is unrecoverable.

Q4. What is the typical amount of testnet ETH you can request from a faucet?
A) 0.001-0.01 ETH B) 0.5-1 ETH
C) 10-50 ETH D) Unlimited amounts
Answer: B – Most faucets distribute 0.5-1 testnet ETH per request to prevent abuse.

Q5. Why must you enable test networks in MetaMask settings?
A) Test networks are hidden by default B) To increase security
C) To mine testnet coins D) To reduce gas fees
Answer: A – MetaMask hides testnets by default to prevent accidental mainnet confusion.

Quiz Questions (6–10)

Q6. What does slippage measure in an AMM swap?
A) Gas fee variation B) Difference between expected and executed price
C) Network congestion D) LP fee percentage
Answer: B – Slippage is the price difference due to trade impact on the pool.

Q7. How does slippage change as swap size increases?
A) Remains constant B) Decreases linearly
C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete pool reserves faster, causing exponential slippage.

Q8. Which factor MOST affects slippage for a given trade size?
A) Time of day B) Pool liquidity depth
C) Token age D) Number of LP providers
Answer: B – Deeper liquidity pools absorb larger trades with less price impact.

Q9. When quoting different swap sizes, why should you NOT execute all of them?
A) Gas fees would be too high B) To conserve limited testnet ETH
C) Uniswap blocks rapid swaps D) MetaMask prevents it
Answer: B – Testnet ETH is limited; multiple large swaps would deplete your balance.

Q10. What does the Uniswap constant product formula ($x * y = k$) ensure?
A) Prices remain fixed B) Pool reserves maintain a product constant
C) No slippage occurs D) Gas fees are minimized
Answer: B – The formula ensures total liquidity (k) remains constant after swaps.

Quiz Questions (11–15)

Q11. What do liquidity providers (LPs) earn in exchange for depositing tokens?
A) Mining rewards B) Trading fee share
C) Staking yields D) Governance tokens only
Answer: B – LPs earn a percentage of trading fees proportional to their pool share.

Q12. What is impermanent loss?
A) Temporary network downtime B) Loss from price divergence between deposited assets
C) Gas fees paid D) Slippage on withdrawal
Answer: B – Impermanent loss occurs when token prices change relative to deposit time.

Q13. Which fee tier is recommended for the ETH/USDC pool in this lab?
A) 0.01% B) 0.05% C) 0.3% D) 1%
Answer: C – 0.3% is standard for medium volatility pairs like ETH/USDC.

Q14. When providing liquidity, what must you deposit?
A) Only ETH B) Only USDC
C) Equal USD value of both tokens D) Any ratio you choose
Answer: C – AMMs require balanced deposits to maintain the pool ratio.

Q15. How do you benefit from executing a swap after providing liquidity?
A) You get free tokens B) Fees accrue to your position
C) Slippage decreases D) Gas fees are refunded
Answer: B – Swaps generate fees that are distributed to LPs proportionally.

Quiz Questions (16–20)

Q16. What should you compare when removing liquidity?
A) Gas fees paid vs earned B) Final token amounts vs initial deposit
C) Pool size at start vs end D) Number of swaps executed
Answer: B – Comparing amounts reveals impermanent loss and fee earnings.

Q17. What is required in the lab report deliverable?
A) Only transaction hashes B) Swap details, slippage analysis, LP position
C) Smart contract code D) Full wallet seed phrase
Answer: B – The report must include swap rates, slippage observations, and IL calculations.

Q18. Why are transaction hashes included as supporting evidence?
A) To verify on-chain activity B) To claim rewards
C) To increase grades D) To mine blocks
Answer: A – Transaction hashes allow verification via Etherscan that steps were completed.

Q19. What does "DEX UX remains more complex than CEX" mean?
A) DEXs have worse interfaces B) Self-custody adds complexity vs centralized exchanges
C) DEXs are slower D) CEXs have more features
Answer: B – DEXs require wallet management, gas fees, and slippage understanding.

Q20. What is the MOST important lesson before using real funds in DeFi?
A) Always use maximum slippage B) Understand mechanics through testnet practice
C) Avoid all liquidity provision D) Only trade on centralized exchanges
Answer: B – Testnet practice builds understanding without financial risk.

Lab Session: Testnet Swap

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module E: DeFi Ecosystem

(c) Joerg Osterrieder 2025

Use Testnet First!

[COMIC: Use testnet first!]

Placeholder for comic showing two paths: one person confidently using mainnet and losing real ETH, another person practicing on testnet with fake money and learning safely

The Setup

- "I watched a YouTube tutorial"
- "How hard can DeFi be?"
- "I'll just figure it out on mainnet"

The Punchline

- Testnet: mistakes cost nothing
- Mainnet: mistakes cost real money
- Same interface, zero financial risk

The only difference between testnet and mainnet is whether your mistakes cost money

Learning Objectives

By the end of this lab session, you will be able to:

- Set up MetaMask wallet on Sepolia testnet
- Execute token swaps on Uniswap
- Analyze and understand slippage
- Provide and remove liquidity from AMM pools
- Track impermanent loss in practice

Building on L35: Uniswap Deep Dive

The Problem: Understanding DeFi Through Practice

The Challenge
How can students safely learn DEX mechanics, slippage dynamics, and liquidity provision without risking real funds or facing prohibitive transaction costs?

Why It Matters

- Real DeFi mistakes can cost hundreds in gas fees or lost funds
- Understanding AMM mechanics is critical before mainnet usage

What You'll Explore

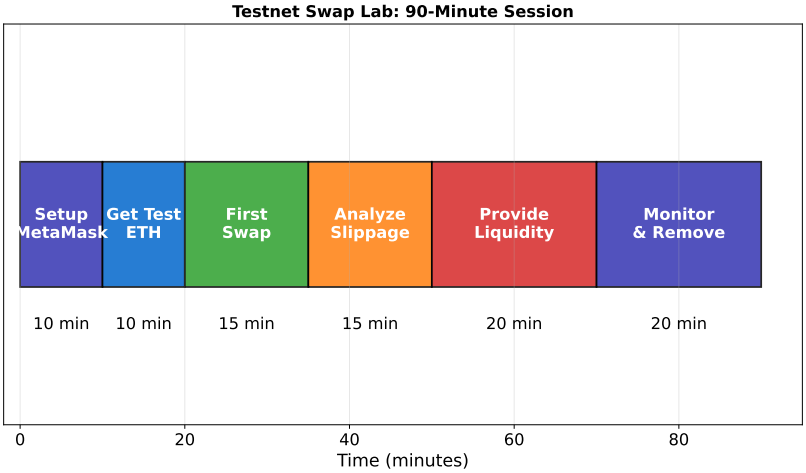
- Connecting wallet to testnet
- Executing swaps and analyzing slippage
- Providing liquidity and tracking impermanent loss
- Comparing theory to hands-on experience

The Cryptoeconomics Question
How do testnets enable risk-free learning while maintaining realistic incentive structures?

Today's lab: Hands-on DeFi experience reveals the economics beneath the interface

(c) Joerg Osterrieder 2025

What Are the Key Steps in This Lab?



Hands-on DeFi experience with zero financial risk

How Do You Set Up MetaMask for Testing?

Actions:

1. Install MetaMask browser extension
2. Create new wallet and save seed phrase
3. Enable test networks in settings
4. Switch to Sepolia Test Network

Safety Reminders:

- Testnet funds have NO real value
- Never share seed phrase
- Do NOT send real ETH to testnet address

Where Do You Get Testnet ETH?

Sepolia Faucets:

- `https://sepoliafaucet.com`
- `https://www.alchemy.com/faucets/ethereum-sepolia`

Process:

1. Copy Sepolia address from MetaMask
2. Paste into faucet and complete captcha
3. Request 0.5-1 testnet ETH
4. Wait for transaction confirmation

How Do You Execute Your First Swap?

Goal: Swap 0.1 ETH for USDC on Uniswap

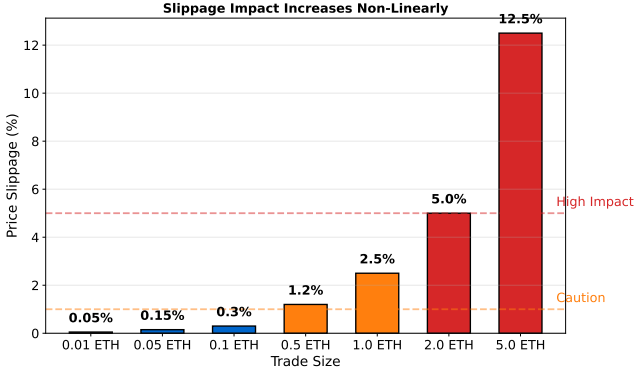
Process:

1. Connect wallet at `https://app.uniswap.org`
2. Select ETH to USDC swap
3. Enter amount and review rate
4. Confirm in MetaMask

Record:

- Exchange rate received
- Gas fee paid
- Transaction hash

Why Does Slippage Increase with Trade Size?



Larger trades face exponentially higher slippage - AMM fundamental

How Does Trade Size Affect Slippage?

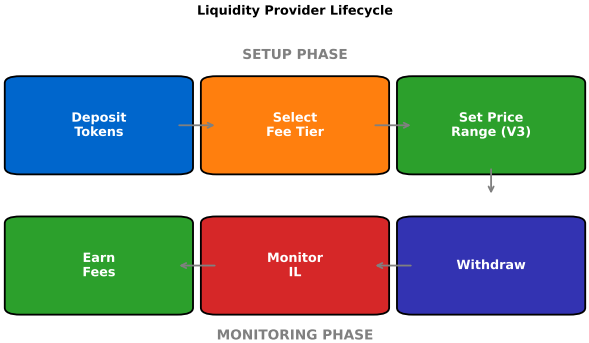
Experiment (DO NOT execute):

1. Quote 0.01 ETH swap - note price
2. Quote 0.1 ETH swap - note price
3. Quote 1 ETH swap - note price
4. Compare the three rates

Questions:

- How does price change with swap size?
- What causes non-linear slippage?
- How does pool liquidity affect slippage?

What Is the Liquidity Provider Lifecycle?



LPs earn fees but face impermanent loss risk

How Do You Provide Liquidity?

Goal: Become a liquidity provider

Process:

1. Click “Pool” tab on Uniswap
2. Select ETH/USDC pair
3. Choose fee tier (0.3% recommended)
4. Enter token amounts
5. Approve and confirm transaction

Record:

- ETH and USDC deposited
- Fee tier selected
- Initial position value

How Do You Remove Liquidity?

After providing liquidity:

- Check pool share percentage
- Monitor fees earned
- Execute a swap to see fees accrue

Remove Liquidity:

1. Click on your position
2. Select “Remove Liquidity”
3. Confirm withdrawal
4. Compare final amounts to initial deposit

What Should You Submit?

Submit:

1. **Lab Report (3-4 pages):**
   - Swap details and exchange rates
   - Slippage analysis observations
   - LP position and impermanent loss calculation
   - Reflection on DeFi user experience
2. **Supporting Evidence:**
   - Transaction hashes (Etherscan links)
   - Screenshots of key steps

Problem Solved? Testnet Learning Model

The Original Problem

How to learn DeFi mechanics without financial risk?

How Testnets Solve It

- Free testnet ETH from faucets eliminates capital requirements
- Identical smart contracts to mainnet enable realistic practice
- Mistakes cost nothing - failure becomes valuable learning

Remaining Limitations

- Testnet liquidity is shallow - slippage unrealistically high
- No real economic incentives - LP behavior differs from mainnet

Open Questions

- What behaviors change when real money is at stake?
- Risk: Overconfidence from testnet success leads to mainnet losses

Testnets solve the learning problem but cannot fully simulate mainnet incentive structures

(c) Joerg Osterrieder 2025

The Economics of Testnet Swap

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Testnet Swap

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Testnet Swap

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Slippage Surprise

[COMIC: Slippage surprise]

Placeholder for comic showing trader expecting to receive 100 tokens, then shocked face when they only receive 85 due to slippage and price impact

The Hidden Cost

- Quoted price is not execution price
- Larger trades = worse prices
- Low liquidity pools = massive slippage

Protect Yourself

- Set slippage tolerance
- Check price impact before confirming
- Split large trades into smaller ones

The price you see is not always the price you get – especially for large trades

(c) Joerg Osterrieder 2025

Key Takeaways

- Testnets enable risk-free DeFi experimentation
- Slippage increases non-linearly with trade size
- Liquidity providers earn fees but face impermanent loss
- DEX UX has improved but remains more complex than CEX
- Understanding mechanics is essential before using real funds

Next Lesson: L37 – Lending Protocols

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of using Sepolia testnet for this lab?
A) To earn real cryptocurrency B) To practice DeFi without financial risk
C) To mine test Ethereum D) To bypass gas fees permanently
Answer: B – Testnet funds have no real value, enabling risk-free experimentation.

Q2. Which critical information should NEVER be shared?
A) Testnet address B) Transaction hash
C) Wallet seed phrase D) Sepolia ETH balance
Answer: C – Seed phrases grant full wallet access and must remain confidential.

Q3. What happens when you send real ETH to a testnet address?
A) It gets converted to testnet ETH B) The funds are permanently lost
C) The network refunds you D) It appears on mainnet instead
Answer: B – Mainnet and testnet are separate; real ETH sent to testnet is unrecoverable.

Q4. What is the typical amount of testnet ETH you can request from a faucet?
A) 0.001-0.01 ETH B) 0.5-1 ETH
C) 10-50 ETH D) Unlimited amounts
Answer: B – Most faucets distribute 0.5-1 testnet ETH per request to prevent abuse.

Q5. Why must you enable test networks in MetaMask settings?
A) Test networks are hidden by default B) To increase security
C) To mine testnet coins D) To reduce gas fees
Answer: A – MetaMask hides testnets by default to prevent accidental mainnet confusion.

Quiz Questions (6–10)

Q6. What does slippage measure in an AMM swap?
A) Gas fee variation B) Difference between expected and executed price
C) Network congestion D) LP fee percentage
Answer: B – Slippage is the price difference due to trade impact on the pool.

Q7. How does slippage change as swap size increases?
A) Remains constant B) Decreases linearly
C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete pool reserves faster, causing exponential slippage.

Q8. Which factor MOST affects slippage for a given trade size?
A) Time of day B) Pool liquidity depth
C) Token age D) Number of LP providers
Answer: B – Deeper liquidity pools absorb larger trades with less price impact.

Q9. When quoting different swap sizes, why should you NOT execute all of them?
A) Gas fees would be too high B) To conserve limited testnet ETH
C) Uniswap blocks rapid swaps D) MetaMask prevents it
Answer: B – Testnet ETH is limited; multiple large swaps would deplete your balance.

Q10. What does the Uniswap constant product formula ($x * y = k$) ensure?
A) Prices remain fixed B) Pool reserves maintain a product constant
C) No slippage occurs D) Gas fees are minimized
Answer: B – The formula ensures total liquidity (k) remains constant after swaps.

Quiz Questions (11–15)

Q11. What do liquidity providers (LPs) earn in exchange for depositing tokens?
A) Mining rewards B) Trading fee share
C) Staking yields D) Governance tokens only
Answer: B – LPs earn a percentage of trading fees proportional to their pool share.

Q12. What is impermanent loss?
A) Temporary network downtime B) Loss from price divergence between deposited assets
C) Gas fees paid D) Slippage on withdrawal
Answer: B – Impermanent loss occurs when token prices change relative to deposit time.

Q13. Which fee tier is recommended for the ETH/USDC pool in this lab?
A) 0.01% B) 0.05% C) 0.3% D) 1%
Answer: C – 0.3% is standard for medium volatility pairs like ETH/USDC.

Q14. When providing liquidity, what must you deposit?
A) Only ETH B) Only USDC
C) Equal USD value of both tokens D) Any ratio you choose
Answer: C – AMMs require balanced deposits to maintain the pool ratio.

Q15. How do you benefit from executing a swap after providing liquidity?
A) You get free tokens B) Fees accrue to your position
C) Slippage decreases D) Gas fees are refunded
Answer: B – Swaps generate fees that are distributed to LPs proportionally.

Quiz Questions (16–20)

Q16. What should you compare when removing liquidity?
A) Gas fees paid vs earned B) Final token amounts vs initial deposit
C) Pool size at start vs end D) Number of swaps executed
Answer: B – Comparing amounts reveals impermanent loss and fee earnings.

Q17. What is required in the lab report deliverable?
A) Only transaction hashes B) Swap details, slippage analysis, LP position
C) Smart contract code D) Full wallet seed phrase
Answer: B – The report must include swap rates, slippage observations, and IL calculations.

Q18. Why are transaction hashes included as supporting evidence?
A) To verify on-chain activity B) To claim rewards
C) To increase grades D) To mine blocks
Answer: A – Transaction hashes allow verification via Etherscan that steps were completed.

Q19. What does "DEX UX remains more complex than CEX" mean?
A) DEXs have worse interfaces B) Self-custody adds complexity vs centralized exchanges
C) DEXs are slower D) CEXs have more features
Answer: B – DEXs require wallet management, gas fees, and slippage understanding.

Q20. What is the MOST important lesson before using real funds in DeFi?
A) Always use maximum slippage B) Understand mechanics through testnet practice
C) Avoid all liquidity provision D) Only trade on centralized exchanges
Answer: B – Testnet practice builds understanding without financial risk.

Quiz: Lab Testnet Swap

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of using Sepolia testnet?
A) Earn real crypto B) Practice DeFi risk-free C) Mine ETH D) Bypass gas fees

Quiz (1–5)

Q1. What is the primary purpose of using Sepolia testnet?
A) Earn real crypto B) Practice DeFi risk-free C) Mine ETH D) Bypass gas fees
Answer: B – Testnet funds have no value, enabling safe experimentation.

Q2. Which information should NEVER be shared?
A) Testnet address B) Transaction hash C) Wallet seed phrase D) ETH balance

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of using Sepolia testnet?
A) Earn real crypto B) Practice DeFi risk-free C) Mine ETH D) Bypass gas fees
Answer: B – Testnet funds have no value, enabling safe experimentation.

Q2. Which information should NEVER be shared?
A) Testnet address B) Transaction hash C) Wallet seed phrase D) ETH balance
Answer: C – Seed phrases grant full wallet access and must stay confidential.

Q3. How does slippage change as swap size increases?
A) Stays constant B) Decreases C) Increases non-linearly D) Becomes negative

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of using Sepolia testnet?
A) Earn real crypto B) Practice DeFi risk-free C) Mine ETH D) Bypass gas fees
Answer: B – Testnet funds have no value, enabling safe experimentation.

Q2. Which information should NEVER be shared?
A) Testnet address B) Transaction hash C) Wallet seed phrase D) ETH balance
Answer: C – Seed phrases grant full wallet access and must stay confidential.

Q3. How does slippage change as swap size increases?
A) Stays constant B) Decreases C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete reserves faster, causing exponential slippage.

Q4. What does the constant product formula $x \times y = k$ ensure?
A) Fixed prices B) Pool reserves maintain constant product C) No slippage D) Zero fees

Quiz (1–5)

Q1. What is the primary purpose of using Sepolia testnet?
A) Earn real crypto B) Practice DeFi risk-free C) Mine ETH D) Bypass gas fees
Answer: B – Testnet funds have no value, enabling safe experimentation.

Q2. Which information should NEVER be shared?
A) Testnet address B) Transaction hash C) Wallet seed phrase D) ETH balance
Answer: C – Seed phrases grant full wallet access and must stay confidential.

Q3. How does slippage change as swap size increases?
A) Stays constant B) Decreases C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete reserves faster, causing exponential slippage.

Q4. What does the constant product formula $x \times y = k$ ensure?
A) Fixed prices B) Pool reserves maintain constant product C) No slippage D) Zero fees
Answer: B – The formula keeps total liquidity (k) constant after swaps.

Q5. Which fee tier is recommended for ETH/USDC pool?
A) 0.01% B) 0.05% C) 0.3% D) 1%

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary purpose of using Sepolia testnet?
A) Earn real crypto B) Practice DeFi risk-free C) Mine ETH D) Bypass gas fees
Answer: B – Testnet funds have no value, enabling safe experimentation.

Q2. Which information should NEVER be shared?
A) Testnet address B) Transaction hash C) Wallet seed phrase D) ETH balance
Answer: C – Seed phrases grant full wallet access and must stay confidential.

Q3. How does slippage change as swap size increases?
A) Stays constant B) Decreases C) Increases non-linearly D) Becomes negative
Answer: C – Larger trades deplete reserves faster, causing exponential slippage.

Q4. What does the constant product formula $x \times y = k$ ensure?
A) Fixed prices B) Pool reserves maintain constant product C) No slippage D) Zero fees
Answer: B – The formula keeps total liquidity (k) constant after swaps.

Q5. Which fee tier is recommended for ETH/USDC pool?
A) 0.01% B) 0.05% C) 0.3% D) 1%
Answer: C – 0.3% is standard for medium volatility pairs.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What do liquidity providers earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens only

Quiz (6–10)

Q6. What do liquidity providers earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens only
Answer: B – LPs earn fees proportional to their pool share.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage

Quiz (6–10)

Q6. What do liquidity providers earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens only
Answer: B – LPs earn fees proportional to their pool share.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – IL occurs when token prices change relative to deposit time.

Q8. Which factor MOST affects slippage for a given trade?
A) Time of day B) Pool liquidity depth C) Token age D) Number of LPs

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What do liquidity providers earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens only
Answer: B – LPs earn fees proportional to their pool share.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – IL occurs when token prices change relative to deposit time.

Q8. Which factor MOST affects slippage for a given trade?
A) Time of day B) Pool liquidity depth C) Token age D) Number of LPs
Answer: B – Deeper pools absorb larger trades with less price impact.

Q9. When providing liquidity, what must you deposit?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What do liquidity providers earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens only
Answer: B – LPs earn fees proportional to their pool share.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – IL occurs when token prices change relative to deposit time.

Q8. Which factor MOST affects slippage for a given trade?
A) Time of day B) Pool liquidity depth C) Token age D) Number of LPs
Answer: B – Deeper pools absorb larger trades with less price impact.

Q9. When providing liquidity, what must you deposit?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio
Answer: C – AMMs require balanced deposits to maintain pool ratio.

Q10. What should you compare when removing liquidity?
A) Gas fees paid B) Final amounts vs initial deposit C) Pool size D) Swap count

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What do liquidity providers earn?
A) Mining rewards B) Trading fee share C) Staking yields D) Governance tokens only
Answer: B – LPs earn fees proportional to their pool share.

Q7. What is impermanent loss?
A) Network downtime B) Loss from price divergence C) Gas fees D) Slippage
Answer: B – IL occurs when token prices change relative to deposit time.

Q8. Which factor MOST affects slippage for a given trade?
A) Time of day B) Pool liquidity depth C) Token age D) Number of LPs
Answer: B – Deeper pools absorb larger trades with less price impact.

Q9. When providing liquidity, what must you deposit?
A) Only ETH B) Only USDC C) Equal USD value of both D) Any ratio
Answer: C – AMMs require balanced deposits to maintain pool ratio.

Q10. What should you compare when removing liquidity?
A) Gas fees paid B) Final amounts vs initial deposit C) Pool size D) Swap count
Answer: B – Comparing amounts reveals impermanent loss and fee earnings.

(c) Joerg Osterrieder 2025

L37: Lending Protocols

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

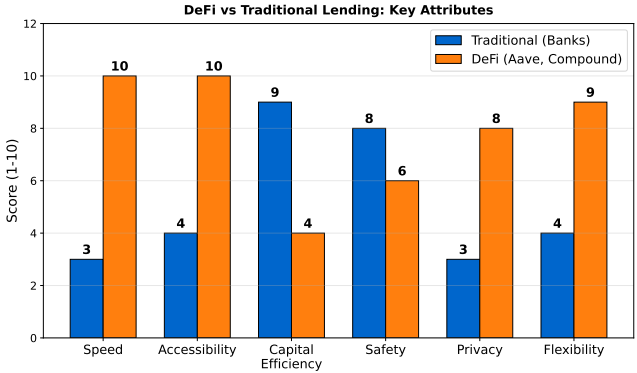
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Explain how DeFi lending protocols work (Aave, Compound)
- Calculate health factors and liquidation thresholds
- Analyze utilization-based interest rate models
- Compare DeFi lending to traditional finance

DeFi vs Traditional Lending



Trade-off: DeFi offers accessibility but requires overcollateralization.

How DeFi Lending Works

Core Mechanism:

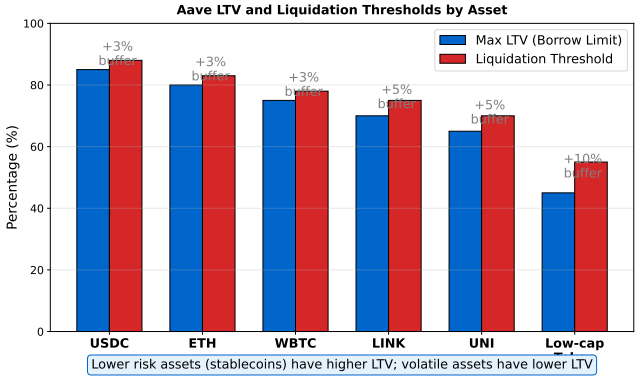
1. **Lenders:** Deposit assets, earn interest (variable APY)
2. **Borrowers:** Deposit collateral, borrow up to LTV%, pay interest
3. **Protocol:** Matches via smart contracts, manages liquidations

Example (Aave):

- Deposit 10 ETH ($20,000), receive aETH tokens
- ETH has 80% LTV: max borrow = $16,000
- Borrow $10,000 USDC at 5% APY

(c) Joerg Osterrieder 2025

LTV and Liquidation Thresholds



Buffer between LTV and liquidation threshold protects against immediate liquidation.

Health Factor Calculation

Formula (Aave):

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liq. Threshold}}{\text{Borrowed Value}}$$

Interpretation:

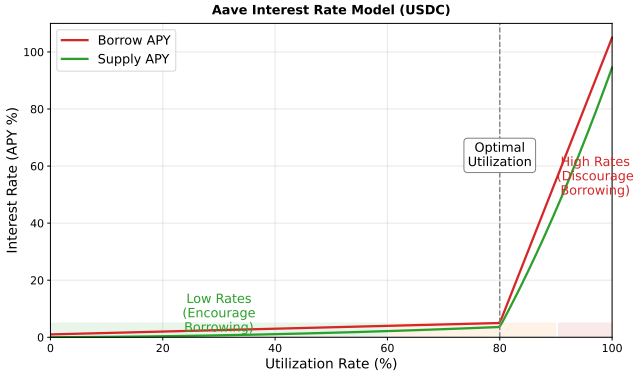
- HF ¿ 1.5: Safe (comfortable buffer)
- HF 1.0-1.5: Warning zone
- HF ¡ 1: Liquidation occurs

Example:

- Collateral: $20,000, Borrowed: $12,000, Liq threshold: 83%
- HF $= \frac{20{,}000 \times 0.83}{12{,}000} = 1.38$ (safe)

(c) Joerg Osterrieder 2025

Interest Rate Model



High utilization triggers steep rate increases to prevent liquidity crises.

Aave vs Compound

Aave (Market Leader):

- Flash loans (no collateral, same-tx repay)
- Stable/variable rate choice
- $31B TVL (Dec 2025), 60%+ market share

Compound (Pioneer):

- cTokens (interest-bearing)
- Simpler, fewer features
- COMP mining sparked “DeFi Summer” 2020

Flash Loans

Definition: Borrow any amount without collateral, repay in same tx.

How It Works:

1. Borrow $1M USDC from Aave
2. Use for arbitrage, collateral swap, or liquidation
3. Repay $1M + 0.09% fee
4. All atomic (succeeds or reverts entirely)

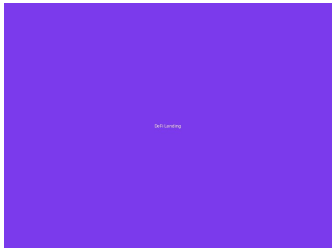
Risk: Used in many DeFi exploits (oracle manipulation attacks).

Key Takeaways

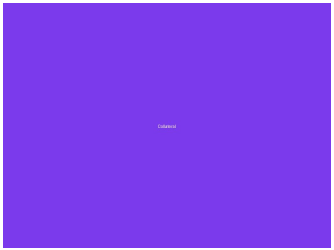
1. **DeFi Lending:** Permissionless but requires overcollateralization
2. **LTV Ratios:** Vary by asset risk (ETH 80%, altcoins 45%)
3. **Health Factor:** Must stay above 1 to avoid liquidation
4. **Interest Rates:** Adjust algorithmically based on utilization
5. **Aave Dominates:** $31B TVL; flash loans are unique feature

Next: L38 – Stablecoin Mechanisms

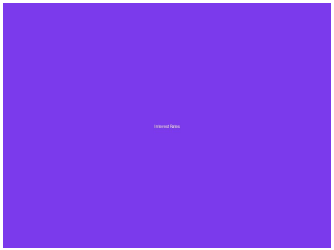
Lending Protocols in Practice



DeFi Lending



Collateral



Interest Rates

Images: Unsplash (CC0)

Quiz (1/2)

Q1. Main difference between traditional and DeFi lending?
A) Traditional requires KYC B) Traditional is faster C) DeFi allows undercollateralized D) Traditional is 24/7

Quiz (1/2)

Q1. Main difference between traditional and DeFi lending?
A) Traditional requires KYC B) Traditional is faster C) DeFi allows undercollateralized D) Traditional is 24/7
Answer: A – DeFi is permissionless, no KYC required.

Q2. 10 ETH worth $20,000 with 80% LTV. Max borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000

Quiz (1/2)

Q1. Main difference between traditional and DeFi lending?
A) Traditional requires KYC B) Traditional is faster C) DeFi allows undercollateralized D) Traditional is 24/7
Answer: A – DeFi is permissionless, no KYC required.

Q2. 10 ETH worth $20,000 with 80% LTV. Max borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – $20,000 x 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Position liquidated D) Nothing

Quiz (1/2)

Q1. Main difference between traditional and DeFi lending?
A) Traditional requires KYC B) Traditional is faster C) DeFi allows undercollateralized D) Traditional is 24/7
Answer: A – DeFi is permissionless, no KYC required.

Q2. 10 ETH worth $20,000 with 80% LTV. Max borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – $20,000 x 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Position liquidated D) Nothing
Answer: C – HF ¡ 1 triggers liquidation.

Q4. Why do volatile assets have lower LTV ratios?
A) Less popular B) Higher price risk C) Lower liquidity D) Regulatory

Quiz (1/2)

Q1. Main difference between traditional and DeFi lending?
A) Traditional requires KYC B) Traditional is faster C) DeFi allows undercollateralized D) Traditional is 24/7
Answer: A – DeFi is permissionless, no KYC required.

Q2. 10 ETH worth $20,000 with 80% LTV. Max borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – $20,000 x 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Position liquidated D) Nothing
Answer: C – HF ¡ 1 triggers liquidation.

Q4. Why do volatile assets have lower LTV ratios?
A) Less popular B) Higher price risk C) Lower liquidity D) Regulatory
Answer: B – Need larger buffers against price swings.

Q5. $30k collateral, $20k borrowed, 85% liq threshold. HF?
A) 1.00 B) 1.28 C) 1.50 D) 0.67

Quiz (1/2)

Q1. Main difference between traditional and DeFi lending?
A) Traditional requires KYC B) Traditional is faster C) DeFi allows undercollateralized D) Traditional is 24/7
Answer: A – DeFi is permissionless, no KYC required.

Q2. 10 ETH worth $20,000 with 80% LTV. Max borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – $20,000 x 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Position liquidated D) Nothing
Answer: C – HF ¡ 1 triggers liquidation.

Q4. Why do volatile assets have lower LTV ratios?
A) Less popular B) Higher price risk C) Lower liquidity D) Regulatory
Answer: B – Need larger buffers against price swings.

Q5. $30k collateral, $20k borrowed, 85% liq threshold. HF?
A) 1.00 B) 1.28 C) 1.50 D) 0.67
Answer: B – (30,000 x 0.85) / 20,000 = 1.275.

Quiz (2/2)

Q6. What is the liquidation penalty on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%

Quiz (2/2)

Q6. What is the liquidation penalty on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive 5-10% bonus.

Q7. How is utilization rate calculated?
A) Supplied/Borrowed B) Borrowed/Supplied C) Borrowed - Supplied D) Rate/LTV

Quiz (2/2)

Q6. What is the liquidation penalty on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive 5-10% bonus.

Q7. How is utilization rate calculated?
A) Supplied/Borrowed B) Borrowed/Supplied C) Borrowed - Supplied D) Rate/LTV
Answer: B – Total Borrowed / Total Supplied.

Q8. What happens when utilization exceeds 90%?
A) Rates decrease B) Constant C) Rates increase steeply D) Shutdown

Quiz (2/2)

Q6. What is the liquidation penalty on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive 5-10% bonus.

Q7. How is utilization rate calculated?
A) Supplied/Borrowed B) Borrowed/Supplied C) Borrowed - Supplied D) Rate/LTV
Answer: B – Total Borrowed / Total Supplied.

Q8. What happens when utilization exceeds 90%?
A) Rates decrease B) Constant C) Rates increase steeply D) Shutdown
Answer: C – High utilization triggers steep increases.

Q9. Unique Aave feature not in Compound?
A) cTokens B) Flash loans C) Governance token D) Overcollateralized loans

Quiz (2/2)

Q6. What is the liquidation penalty on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive 5-10% bonus.

Q7. How is utilization rate calculated?
A) Supplied/Borrowed B) Borrowed/Supplied C) Borrowed - Supplied D) Rate/LTV
Answer: B – Total Borrowed / Total Supplied.

Q8. What happens when utilization exceeds 90%?
A) Rates decrease B) Constant C) Rates increase steeply D) Shutdown
Answer: C – High utilization triggers steep increases.

Q9. Unique Aave feature not in Compound?
A) cTokens B) Flash loans C) Governance token D) Overcollateralized loans
Answer: B – Aave pioneered flash loans.

Q10. What is the typical flash loan fee on Aave?
A) 0.09% B) 1% C) 5% D) 10%

Quiz (2/2)

Q6. What is the liquidation penalty on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive 5-10% bonus.

Q7. How is utilization rate calculated?
A) Supplied/Borrowed B) Borrowed/Supplied C) Borrowed - Supplied D) Rate/LTV
Answer: B – Total Borrowed / Total Supplied.

Q8. What happens when utilization exceeds 90%?
A) Rates decrease B) Constant C) Rates increase steeply D) Shutdown
Answer: C – High utilization triggers steep increases.

Q9. Unique Aave feature not in Compound?
A) cTokens B) Flash loans C) Governance token D) Overcollateralized loans
Answer: B – Aave pioneered flash loans.

Q10. What is the typical flash loan fee on Aave?
A) 0.09% B) 1% C) 5% D) 10%
Answer: A – 0.09% fee per flash loan.

(c) Joerg Osterrieder 2025

Thank you

Questions?

Next: L38 – Stablecoin Mechanisms

L37: Lending Protocols

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Explain how DeFi lending protocols work (Aave, Compound)
- Analyze overcollateralization and its necessity
- Calculate health factors and liquidation thresholds
- Explore interest rate models (utilization-based)
- Compare DeFi lending to traditional finance

(c) Joerg Osterrieder 2025

The Problem: How do we lend without credit scores?

The Challenge
How can we create a lending system without banks, credit scores, or identity verification? Traditional finance relies on centralized institutions to assess borrower creditworthiness and enforce repayment through legal systems.

Why It Matters

- Without credit infrastructure, billions are excluded from lending markets
- Traditional lending requires KYC, credit history, geographic presence, and legal recourse

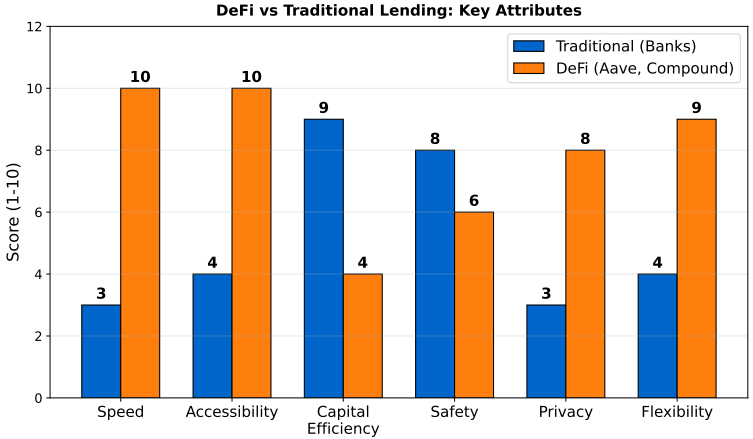
What We Need

- System that eliminates default risk without identity
- Automated liquidation mechanism that doesn't rely on courts
- Algorithmic interest rates that balance supply and demand

The Cryptoeconomics Question
Creating systems with desired properties: How do we align incentives so borrowers never default?

Today's lesson: How overcollateralized lending protocols address this challenge

DeFi vs Traditional Lending



DeFi trades capital efficiency for accessibility and speed

Traditional vs DeFi Lending

Traditional Lending

- Credit checks, KYC required
- Undercollateralized possible
- Long approval process
- Geographic restrictions

DeFi Lending

- No credit checks
- Overcollateralized only
- Instant approval
- Global access, 24/7

Key Trade-off: DeFi accessibility vs. capital efficiency (must lock more than you borrow).

(c) Joerg Osterrieder 2025

How DeFi Lending Works

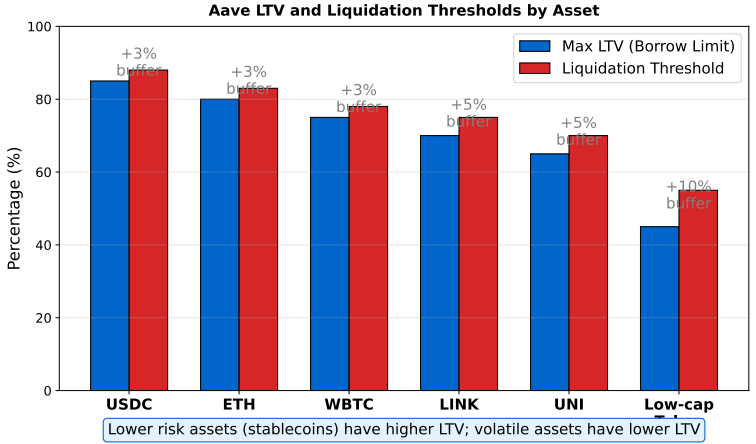
Core Mechanism:

1. **Lenders (Suppliers):** Deposit assets, earn interest (APY varies)
2. **Borrowers:** Deposit collateral, borrow up to LTV%, pay interest
3. **Protocol:** Matches via smart contracts, manages liquidations

Example: Borrowing on Aave

- Deposit 10 ETH ($20,000), receive aETH tokens
- ETH has 80% LTV: max borrow = $16,000
- Borrow $10,000 USDC (safe margin)
- Pay 5% APY on debt, earn 2% on collateral

LTV and Liquidation Thresholds



Buffer between LTV and liquidation threshold protects against immediate liquidation

Loan-to-Value (LTV) Explained

Definition:

$$\text{LTV} = \frac{\text{Borrowed Value}}{\text{Collateral Value}} \times 100\%$$

Why Different LTVs?

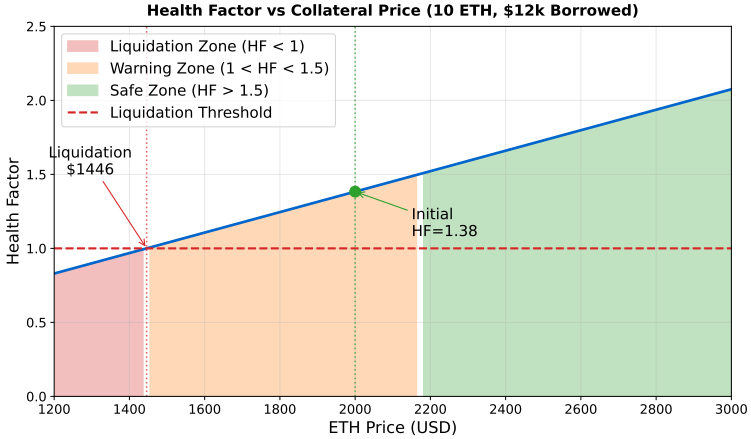
- Volatile assets = lower LTV (more buffer for price swings)
- Stable assets = higher LTV (minimal price risk)

Example Calculation:

- Collateral: 10 ETH at \$2,000 = \$20,000
- Borrowed: \$12,000 USDC
- LTV: $\frac{12{,}000}{20{,}000} = 60\%$ (safe, under 80% max)

(c) Joerg Osterrieder 2025

Health Factor Dynamics



Health factor must stay above 1; monitor closely during volatility

Health Factor Calculation

Formula (Aave):

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Borrowed Value}}$$

Interpretation:

- HF ¿ 1.5: Safe (comfortable buffer)
- HF 1.0-1.5: Warning zone
- HF ¡ 1: Liquidation occurs

Example:

- Collateral: $20,000 (ETH), Borrowed: $12,000
- Liquidation threshold: 83%
- HF $= \frac{20{,}000 \times 0.83}{12{,}000} = 1.38$ (safe)

(c) Joerg Osterrieder 2025

Liquidation Process

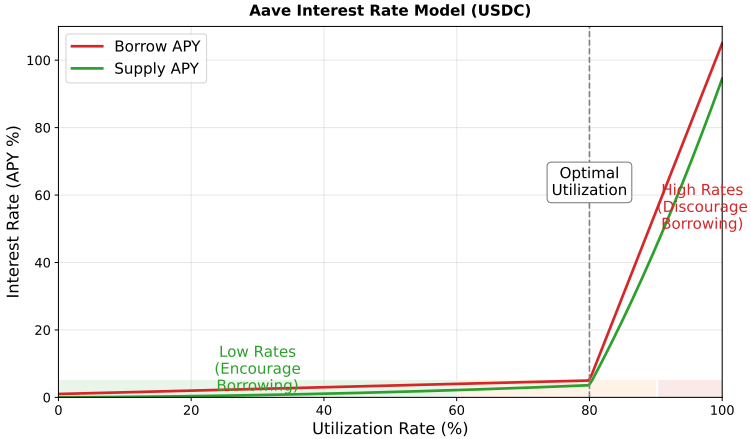
When Health Factor ¡ 1:

1. **Liquidator Bot Detects** unhealthy position
2. **Liquidator Repays** portion of debt (up to 50%)
3. **Liquidator Receives** equivalent collateral + 5-10% bonus
4. **Borrower Loses** liquidation penalty

Example:

- Debt: $12,000, Collateral: $14,460
- Liquidator repays 50% ($6,000), receives $6,300 in ETH
- Borrower loses $300 penalty (5%)

Interest Rate Model



High utilization triggers steep rate increase to prevent liquidity crises

Utilization-Based Interest Rates

Utilization Rate:

$$U = \frac{\text{Total Borrowed}}{\text{Total Supplied}}$$

Rate Behavior:

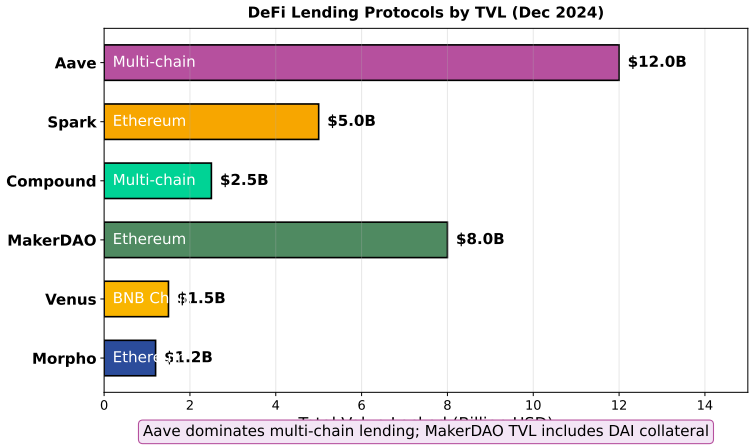
- Low utilization (0-60%): Low rates (encourage borrowing)
- Optimal (80%): Moderate rates (balanced)
- High (¿90%): Very high rates (discourage borrowing)

Supply APY Formula:

$$\text{Supply APY} = \text{Borrow APY} \times U \times (1 - \text{Reserve Factor})$$

Key Insight: Supply APY always lower than borrow APY.

Lending Protocol Market Share



Aave leads through multi-chain expansion; Compound pioneered the model

Aave vs Compound

Aave

- Flash loans (no collateral)
- Stable/variable rate choice
- Credit delegation
- E-Mode for correlated assets
- $31B TVL (Dec 2025), 60%+ DeFi lending market share

Compound

- cTokens (interest-bearing)
- Simpler, fewer features
- Pioneered DeFi lending
- COMP governance token
- $2.5B TVL

Historical Note: Compound launched 2018, Aave 2020. Compound's COMP mining sparked "DeFi Summer" 2020.

Flash Loans

Definition: Borrow any amount without collateral, repay in same transaction.

How It Works:

1. Borrow $1M USDC from Aave
2. Use for arbitrage, collateral swap, or liquidation
3. Repay $1M + 0.09% fee
4. All atomic (succeeds or reverts entirely)

Use Cases:

- Arbitrage across DEXs
- Collateral swaps without closing position
- Self-liquidation to avoid penalty

Risk: Used in many DeFi exploits (oracle manipulation attacks).

Risks in DeFi Lending

1. **Smart Contract Risk**
   - Bugs or exploits (Rari Capital, Cream Finance hacks)
2. **Liquidation Risk**
   - Volatile markets, network congestion prevents adding collateral
3. **Oracle Risk**
   - Price feed manipulation, stale prices
4. **Liquidity Risk**
   - High utilization prevents withdrawals

2022 Lesson: CeFi lenders (Celsius, BlockFi) collapsed; DeFi protocols survived.

(c) Joerg Osterrieder 2025

Future: Undercollateralized Lending

Current Limitation: Overcollateralization is capital inefficient.

Emerging Solutions:

1. **On-Chain Credit Scores:** Track repayment history (Credora, ARCx)
2. **Real-World Identity:** KYC-linked, legal recourse (Goldfinch, TrueFi)
3. **Social Collateral:** Community vouching (Teller Protocol)

Trade-off: Undercollateralization requires identity or trust, reducing permissionlessness.

Problem Solved? Lending Protocols

The Original Problem

How do we lend without credit scores?

How Lending Protocols Solves It

- **Overcollateralization:** Borrowers deposit more value than they borrow, eliminating default risk entirely
- **Automated liquidation:** Smart contracts enforce liquidation when health factor ¡ 1, no courts needed
- **Algorithmic interest rates:** Utilization-based models adjust rates to balance supply/demand without central authority

Remaining Limitations

- **Capital inefficiency:** Must lock $150 to borrow $100 (vs traditional lending at 20-30% down payment)
- **Liquidation cascades:** Market volatility can trigger mass liquidations, amplifying price drops

Open Questions

- Can undercollateralized DeFi lending work without sacrificing permissionlessness?
- Risk: Identity-based credit systems (Goldfinch, TrueFi) reintroduce centralization and exclusion

Lending protocols solve trustless lending but trade capital efficiency for permissionless access

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- DeFi lending: permissionless but requires overcollateralization
- LTV ratios vary by asset risk (ETH 80%, low-cap 45%)
- Health factor must stay above 1 to avoid liquidation
- Interest rates adjust algorithmically based on utilization
- Flash loans enable zero-collateral borrowing within one tx
- Aave dominates ($31B TVL); Compound pioneered the model
- Future: undercollateralized lending via credit scoring

Next Lecture: Stablecoin Mechanisms.

Questions for Reflection

1. Calculate health factor: $30k collateral, $20k borrowed, 85% liq threshold.
2. Why is overcollateralization necessary in DeFi lending?
3. How do interest rates adjust to prevent bank runs?
4. What risks do flash loans pose to DeFi protocols?
5. Variable or stable rates for 1-year borrow?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the main difference between traditional lending and DeFi lending?
A) Traditional requires KYC, DeFi doesn't B) Traditional is faster C) DeFi allows undercollateralized loans D) Traditional is 24/7
Answer: A – DeFi lending is permissionless with no KYC, while traditional requires credit checks and identity verification.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, what is the maximum you can borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – Maximum borrow = Collateral Value $\times$ LTV = $20,000 $\times$ 0.80 = $16,000.

Q3. What happens when your health factor drops below 1?
A) Interest rate increases B) You get a warning email C) Your position gets liquidated D) Nothing happens
Answer: C – Health factor ¡ 1 triggers liquidation; liquidators repay debt and receive collateral plus a bonus.

Q4. Why do volatile assets like altcoins have lower LTV ratios than stablecoins?
A) Less popular B) Higher price volatility risk C) Lower liquidity D) Regulatory restrictions
Answer: B – Volatile assets need larger buffers (lower LTV) to protect against price swings and prevent immediate liquidations.

Q5. What is the health factor for $30,000 collateral, $20,000 borrowed, 85% liquidation threshold?
A) 1.00 B) 1.28 C) 1.50 D) 0.67
Answer: B – HF = (30,000 $\times$ 0.85) / 20,000 = 25,500 / 20,000 = 1.275 $\approx$ 1.28.

Quiz Questions (6–10)

Q6. What is the liquidation penalty received by liquidators on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive a 5-10% bonus on top of the collateral they claim as incentive for maintaining protocol solvency.

Q7. How is the utilization rate calculated?
A) Total Supplied / Total Borrowed B) Total Borrowed / Total Supplied C) Total Borrowed - Total Supplied D) Interest Rate / LTV
Answer: B – Utilization Rate = Total Borrowed / Total Supplied, measuring what percentage of available liquidity is being used.

Q8. What happens to borrow interest rates when utilization exceeds 90%?
A) They decrease B) They stay constant C) They increase steeply D) Protocol shuts down
Answer: C – High utilization triggers steep rate increases to discourage borrowing and encourage repayment, preventing liquidity crises.

Q9. Which protocol has the largest DeFi lending market share as of December 2025?
A) Compound B) MakerDAO C) Aave D) dYdX
Answer: C – Aave leads with $31B TVL and 60%+ market share through multi-chain expansion and innovative features.

Q10. What unique feature does Aave offer that Compound does not?
A) Interest-bearing tokens B) Flash loans C) Governance token D) Overcollateralized loans
Answer: B – Aave pioneered flash loans (uncollateralized borrowing within one transaction), which Compound does not offer.

Quiz Questions (11–15)

Q11. What must happen for a flash loan to succeed?
A) Collateral must be posted B) Loan must be repaid within same transaction C) Loan duration must be 1 block D) KYC verification
Answer: B – Flash loans are atomic: borrow, use, and repay (plus fee) must all happen in the same transaction or the entire transaction reverts.

Q12. What is the typical flash loan fee on Aave?
A) 0.09% B) 1% C) 5% D) 10%
Answer: A – Aave charges a 0.09% fee on flash loans, making them very capital-efficient for arbitrage and other single-transaction strategies.

Q13. Why is Supply APY always lower than Borrow APY in lending protocols?
A) Protocol keeps the difference as revenue B) Gas costs C) Reserve factor and utilization D) Regulatory requirements
Answer: C – Supply APY = Borrow APY $\times$ Utilization $\times$ (1 - Reserve Factor); the reserve factor and ¡100% utilization ensure supply rates are lower.

Q14. What tokens do lenders receive when depositing assets on Aave?
A) cTokens B) aTokens C) COMP tokens D) LP tokens
Answer: B – Aave issues aTokens (e.g., aETH, aUSDC) that accrue interest in real-time and represent the deposited assets plus earned interest.

Q15. Which event sparked "DeFi Summer" in 2020?
A) Aave launch B) Compound COMP mining C) Uniswap v2 D) Bitcoin halving
Answer: B – Compound's COMP token liquidity mining program in June 2020 sparked explosive DeFi growth known as "DeFi Summer."

Quiz Questions (16–20)

Q16. What is the main risk that flash loans pose to DeFi protocols?
A) High gas costs B) Oracle manipulation attacks C) Regulatory scrutiny D) Network congestion
Answer: B – Flash loans provide large capital for oracle manipulation attacks, allowing attackers to distort price feeds and exploit protocols.

Q17. What is Aave's E-Mode designed for?
A) Emergency shutdowns B) Higher LTV for correlated assets C) Lower gas costs D) Faster liquidations
Answer: B – E-Mode allows higher LTV ratios for highly correlated assets (e.g., ETH-stETH), improving capital efficiency for low-risk pairs.

Q18. What happened to CeFi lenders Celsius and BlockFi in 2022?
A) They merged B) They went public C) They collapsed D) They launched tokens
Answer: C – Both Celsius and BlockFi collapsed in 2022 due to mismanagement and contagion, while DeFi protocols remained operational.

Q19. What is needed for undercollateralized DeFi lending to work?
A) Higher interest rates B) Credit scores or identity systems C) Longer loan terms D) More liquidators
Answer: B – Undercollateralized lending requires reputation, on-chain credit scores, or KYC/identity to enable legal recourse.

Q20. What is the trade-off of introducing identity-based undercollateralized lending?
A) Higher fees B) Slower transactions C) Reduced permissionlessness D) Lower yields
Answer: C – Adding identity or credit requirements reduces DeFi's core benefit of permissionless access, trading accessibility for capital efficiency.

L37: Lending Protocols

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Why Lock Up Assets to Borrow Money?

[COMIC: Collateralized borrowing]

Placeholder for comic showing person handing over car keys (collateral) to borrow money, with the lender holding keys until loan is repaid

The Setup

- Traditional bank: credit score required
- Years of history, identity verification
- Banks decide who deserves a loan

The Punchline

- DeFi: your collateral is your credit
- Lock up ETH, borrow stablecoins
- No credit check, no bank approval

In DeFi, your assets are your credit score – lock them up and borrow instantly

Learning Objectives

- Explain how DeFi lending protocols work (Aave, Compound)
- Analyze overcollateralization and its necessity
- Calculate health factors and liquidation thresholds
- Explore interest rate models (utilization-based)
- Compare DeFi lending to traditional finance

Building on L36: Lab: Testnet Swap

The Problem: How do we lend without credit scores?

The Challenge
How can we create a lending system without banks, credit scores, or identity verification? Traditional finance relies on centralized institutions to assess borrower creditworthiness and enforce repayment through legal systems.

Why It Matters

- Without credit infrastructure, billions are excluded from lending markets
- Traditional lending requires KYC, credit history, geographic presence, and legal recourse

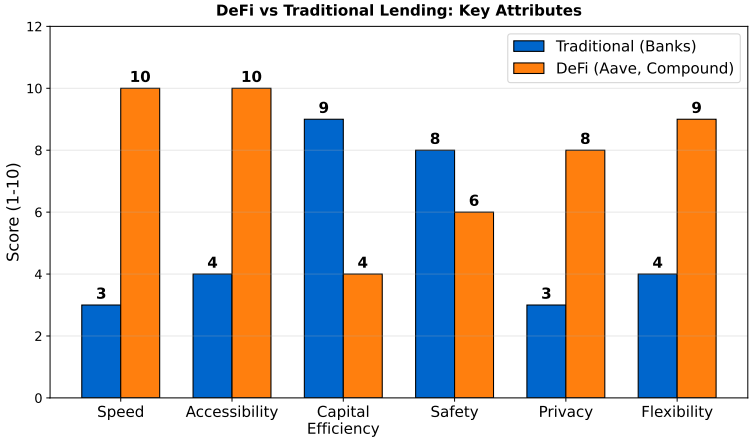
What We Need

- System that eliminates default risk without identity
- Automated liquidation mechanism that doesn't rely on courts
- Algorithmic interest rates that balance supply and demand

The Cryptoeconomics Question
Creating systems with desired properties: How do we align incentives so borrowers never default?

Today's lesson: How overcollateralized lending protocols address this challenge

How Does DeFi Lending Differ From Banks?



DeFi trades efficiency for accessibility – overcollateralize, but anyone can participate.

What Are the Key Trade-offs?

Traditional Lending

- Credit checks, KYC required
- Undercollateralized possible
- Long approval process
- Geographic restrictions

DeFi Lending

- No credit checks
- Overcollateralized only
- Instant approval
- Global access, 24/7

Key Trade-off: DeFi accessibility vs. capital efficiency (must lock more than you borrow).

How Do You Borrow Without a Bank?

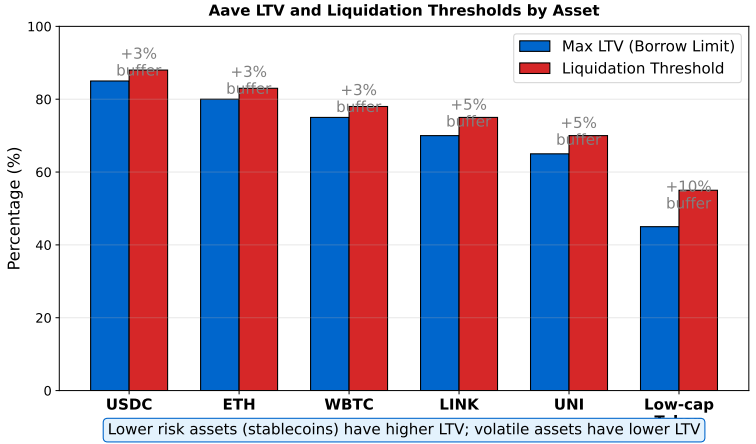
Core Mechanism:

1. **Lenders (Suppliers):** Deposit assets, earn interest (APY varies)
2. **Borrowers:** Deposit collateral, borrow up to LTV%, pay interest
3. **Protocol:** Matches via smart contracts, manages liquidations

Example: Borrowing on Aave

- Deposit 10 ETH ($20,000), receive aETH tokens
- ETH has 80% LTV: max borrow = $16,000
- Borrow $10,000 USDC (safe margin)
- Pay 5% APY on debt, earn 2% on collateral

How Much Can You Borrow Against Your Collateral?



LTV replaces credit scores – protocol trusts collateral, not you. If ETH drops, liquidation.

What Determines Your Borrowing Limit?

Definition:

$$\text{LTV} = \frac{\text{Borrowed Value}}{\text{Collateral Value}} \times 100\%$$

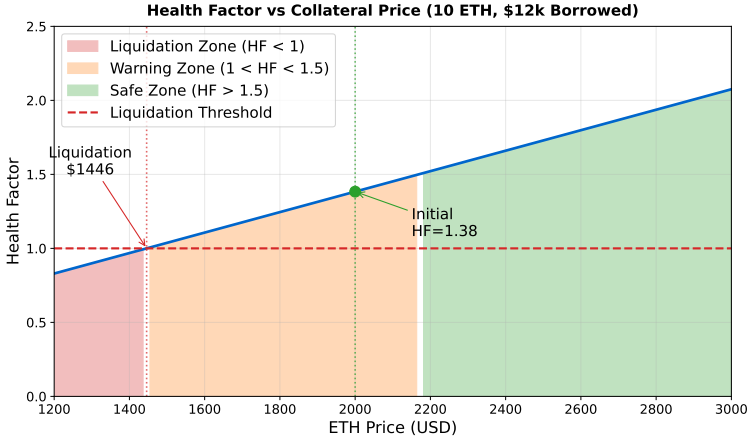
Why Different LTVs?

- Volatile assets = lower LTV (more buffer for price swings)
- Stable assets = higher LTV (minimal price risk)

Example Calculation:

- Collateral: 10 ETH at \$2,000 = \$20,000
- Borrowed: \$12,000 USDC
- LTV: $\frac{12{,}000}{20{,}000} = 60\%$ (safe, under 80% max)

How Safe Is Your Loan Position?



Health factor must stay above 1; monitor closely during volatility

How Is Loan Safety Measured?

Formula (Aave):

$$\text{Health Factor} = \frac{\text{Collateral Value} \times \text{Liquidation Threshold}}{\text{Borrowed Value}}$$

Health factor (loan safety metric: above 1 = safe, below 1 = liquidation):

Interpretation:

- HF ¿ 1.5: Safe (comfortable buffer)
- HF 1.0-1.5: Warning zone
- HF ¡ 1: Liquidation occurs

Example:

- Collateral: $20,000 (ETH), Borrowed: $12,000
- Liquidation threshold: 83%
- HF $= \frac{20{,}000 \times 0.83}{12{,}000} = 1.38$ (safe)

What Happens When Your Health Factor Drops?

Liquidation (automatic seizure of collateral when loan becomes unsafe):
When Health Factor ¡ 1:

1. **Liquidator Bot Detects** unhealthy position
2. **Liquidator Repays** portion of debt (up to 50%)
3. **Liquidator Receives** equivalent collateral + 5-10% bonus
4. **Borrower Loses** liquidation penalty

Example:

- Debt: $12,000, Collateral: $14,460
- Liquidator repays 50% ($6,000), receives $6,300 in ETH
- Borrower loses $300 penalty (5%)

Liquidation replaces courts – bots seize collateral, ensuring debts are always repaid.

Pseudocode: Liquidation Check

Aave-Style Liquidation Logic

```
function check_liquidation(position):
  health = (collateral_value * liq_threshold)
         / borrowed_value
  if health < 1.0:
    // Position is underwater
    repay_amount = borrowed_value * 0.5
    bonus = repay_amount * 0.05 // 5% liquidation bonus
    seize_collateral(repay_amount + bonus)
    reduce_debt(repay_amount)
    emit Liquidation(position, repay_amount)
```

Key Insight: The 5% bonus incentivizes liquidator bots to act instantly. Without this profit motive, unhealthy positions would linger and threaten protocol solvency.

Smart contracts replace courts: automated liquidation ensures debts are always repaid without legal action

Problem Check-In: Lending Protocols

Recall Our Problem

How do we lend without credit scores?

What We've Learned So Far

- Overcollateralization: deposit $150 to borrow $100 – eliminates default risk without credit history
- Health factor tracks loan safety: HF ¿ 1 is safe, HF ¡ 1 triggers automatic liquidation
- Math replaces credit checks: collateral + liquidation = guaranteed repayment without courts

Still to Address

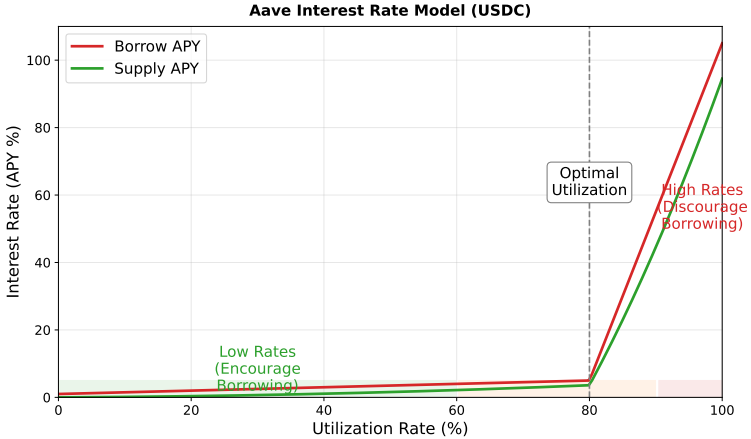
- Interest rate models: how supply/demand automatically sets borrowing costs
- Can DeFi ever offer undercollateralized loans while staying permissionless?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we lend without credit scores?"?

How Are Interest Rates Determined?



High utilization triggers steep rate increase to prevent liquidity crises

How Do Interest Rates Adjust Automatically?

Utilization Rate:

$$U = \frac{\text{Total Borrowed}}{\text{Total Supplied}}$$

Rate Behavior:

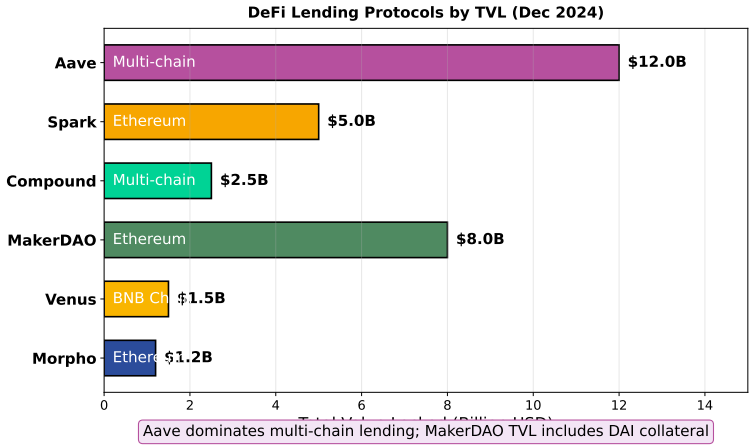
- Low utilization (0-60%): Low rates (encourage borrowing)
- Optimal (80%): Moderate rates (balanced)
- High (¿90%): Very high rates (discourage borrowing)

Supply APY Formula:

$$\text{Supply APY} = \text{Borrow APY} \times U \times (1 - \text{Reserve Factor})$$

Key Insight: Supply APY always lower than borrow APY.

Which Protocols Dominate DeFi Lending?



Aave leads through multi-chain expansion; Compound pioneered the model

How Do Aave and Compound Compare?

Aave

- Flash loans (no collateral)
- Stable/variable rate choice
- Credit delegation
- E-Mode for correlated assets
- $31B TVL (Dec 2025), 60%+ DeFi lending market share

Compound

- cTokens (interest-bearing)
- Simpler, fewer features
- Pioneered DeFi lending
- COMP governance token
- $2.5B TVL

Historical Note: Compound launched 2018, Aave 2020. Compound's COMP mining sparked "DeFi Summer" 2020.

Aave vs Compound: both solve creditless lending, but Aave adds flash loans and stable rates.

How Can You Borrow Without Collateral?

Definition: Borrow any amount without collateral, repay in same transaction.

How It Works:

1. Borrow $1M USDC from Aave
2. Use for arbitrage, collateral swap, or liquidation
3. Repay $1M + 0.09% fee
4. All atomic (succeeds or reverts entirely)

Use Cases:

- Arbitrage across DEXs
- Collateral swaps without closing position
- Self-liquidation to avoid penalty

Risk: Used in many DeFi exploits (oracle manipulation attacks).

What Can Go Wrong in DeFi Lending?

1. **Smart Contract Risk**
   - Bugs or exploits (Rari Capital, Cream Finance hacks)
2. **Liquidation Risk**
   - Volatile markets, network congestion prevents adding collateral
3. **Oracle Risk**
   - Price feed manipulation, stale prices
4. **Liquidity Risk**
   - High utilization prevents withdrawals

2022 Lesson: CeFi lenders (Celsius, BlockFi) collapsed; DeFi protocols survived.

Can DeFi Ever Lend Without Overcollateralization?

Current Limitation: Overcollateralization is capital inefficient.

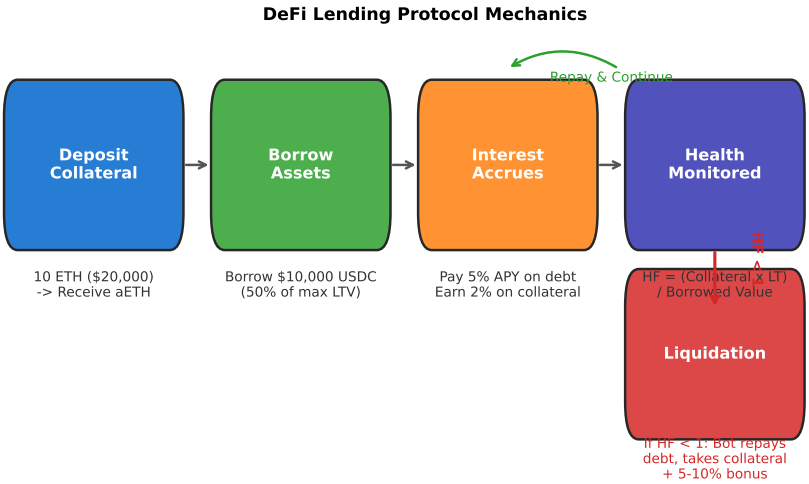
Emerging Solutions:

1. **On-Chain Credit Scores:** Track repayment history (Credora, ARCx)
2. **Real-World Identity:** KYC-linked, legal recourse (Goldfinch, TrueFi)
3. **Social Collateral:** Community vouching (Teller Protocol)

Trade-off: Undercollateralization requires identity or trust, reducing permissionlessness.

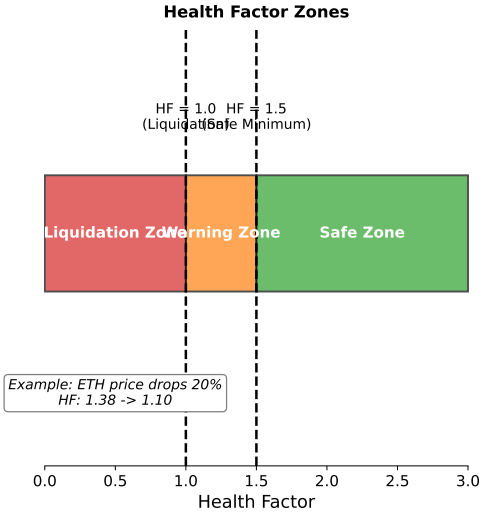
(c) Joerg Osterrieder 2025

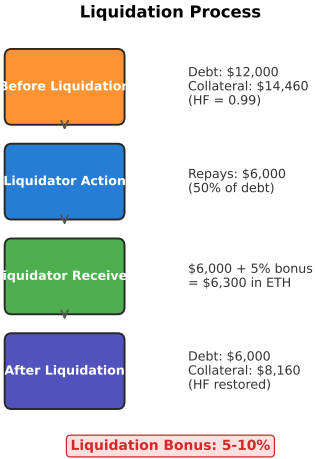
How Does the Complete Lending Cycle Work?



Complete lifecycle: deposit collateral, borrow assets, accrue interest, monitor health, avoid liquidation.

How Does Liquidation Actually Work?





Liquidators profit from the 5-10% bonus, incentivizing them to maintain protocol solvency.

Problem Solved? Lending Protocols

The Original Problem

How do we lend without credit scores?

How Lending Protocols Solves It

- **Overcollateralization:** Borrowers deposit more value than they borrow, eliminating default risk entirely
- **Automated liquidation:** Smart contracts enforce liquidation when health factor ¡ 1, no courts needed
- **Algorithmic interest rates:** Utilization-based models adjust rates to balance supply/demand without central authority

Remaining Limitations

- **Capital inefficiency:** Must lock $150 to borrow $100 (vs traditional lending at 20-30% down payment)
- **Liquidation cascades:** Market volatility can trigger mass liquidations, amplifying price drops

Open Questions

- Can undercollateralized DeFi lending work without sacrificing permissionlessness?
- Risk: Identity-based credit systems (Goldfinch, TrueFi) reintroduce centralization and exclusion

Lending protocols solve trustless lending but trade capital efficiency for permissionless access

(c) Joerg Osterrieder 2025

The Economics of Lending Protocols

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Lending Protocols

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Lending Protocols

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Why Do Liquidations Cascade?

[COMIC: Liquidation cascade]

Placeholder for comic showing dominos falling: ETH price drops, triggers liquidation, forced selling drops price more, triggers more liquidations – cascade effect

The Danger

- One liquidation = forced selling
- Forced selling = price drops further
- More price drops = more liquidations

Protect Yourself

- Keep health factor above 1.5
- Set alerts for price drops
- Have collateral ready to add

In a cascade, your safe health factor can become unsafe in minutes

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- DeFi lending: permissionless but requires overcollateralization
- LTV ratios vary by asset risk (ETH 80%, low-cap 45%)
- Health factor must stay above 1 to avoid liquidation
- Interest rates adjust algorithmically based on utilization
- Flash loans enable zero-collateral borrowing within one tx
- Aave dominates ($31B TVL); Compound pioneered the model
- Future: undercollateralized lending via credit scoring

Next Lecture: Stablecoin Mechanisms.

Next Lesson: L38 – Stablecoin Mechanisms

Questions for Reflection

1. Calculate health factor: $30k collateral, $20k borrowed, 85% liq threshold.
2. Why is overcollateralization necessary in DeFi lending?
3. How do interest rates adjust to prevent bank runs?
4. What risks do flash loans pose to DeFi protocols?
5. Variable or stable rates for 1-year borrow?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the main difference between traditional lending and DeFi lending?
A) Traditional requires KYC, DeFi doesn't B) Traditional is faster C) DeFi allows undercollateralized loans D) Traditional is 24/7
Answer: A – DeFi lending is permissionless with no KYC, while traditional requires credit checks and identity verification.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, what is the maximum you can borrow?
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – Maximum borrow = Collateral Value $\times$ LTV = $20,000 $\times$ 0.80 = $16,000.

Q3. What happens when your health factor drops below 1?
A) Interest rate increases B) You get a warning email C) Your position gets liquidated D) Nothing happens
Answer: C – Health factor ¡ 1 triggers liquidation; liquidators repay debt and receive collateral plus a bonus.

Q4. Why do volatile assets like altcoins have lower LTV ratios than stablecoins?
A) Less popular B) Higher price volatility risk C) Lower liquidity D) Regulatory restrictions
Answer: B – Volatile assets need larger buffers (lower LTV) to protect against price swings and prevent immediate liquidations.

Q5. What is the health factor for $30,000 collateral, $20,000 borrowed, 85% liquidation threshold?
A) 1.00 B) 1.28 C) 1.50 D) 0.67
Answer: B – HF = (30,000 $\times$ 0.85) / 20,000 = 25,500 / 20,000 = 1.275 $\approx$ 1.28.

Quiz Questions (6–10)

Q6. What is the liquidation penalty received by liquidators on Aave?
A) 1-2% B) 5-10% C) 15-20% D) 25-30%
Answer: B – Liquidators receive a 5-10% bonus on top of the collateral they claim as incentive for maintaining protocol solvency.

Q7. How is the utilization rate calculated?
A) Total Supplied / Total Borrowed B) Total Borrowed / Total Supplied C) Total Borrowed - Total Supplied D) Interest Rate / LTV
Answer: B – Utilization Rate = Total Borrowed / Total Supplied, measuring what percentage of available liquidity is being used.

Q8. What happens to borrow interest rates when utilization exceeds 90%?
A) They decrease B) They stay constant C) They increase steeply D) Protocol shuts down
Answer: C – High utilization triggers steep rate increases to discourage borrowing and encourage repayment, preventing liquidity crises.

Q9. Which protocol has the largest DeFi lending market share as of December 2025?
A) Compound B) MakerDAO C) Aave D) dYdX
Answer: C – Aave leads with $31B TVL and 60%+ market share through multi-chain expansion and innovative features.

Q10. What unique feature does Aave offer that Compound does not?
A) Interest-bearing tokens B) Flash loans C) Governance token D) Overcollateralized loans
Answer: B – Aave pioneered flash loans (uncollateralized borrowing within one transaction), which Compound does not offer.

Quiz Questions (11–15)

Q11. What must happen for a flash loan to succeed?
A) Collateral must be posted B) Loan must be repaid within same transaction C) Loan duration must be 1 block D) KYC verification
Answer: B – Flash loans are atomic: borrow, use, and repay (plus fee) must all happen in the same transaction or the entire transaction reverts.

Q12. What is the typical flash loan fee on Aave?
A) 0.09% B) 1% C) 5% D) 10%
Answer: A – Aave charges a 0.09% fee on flash loans, making them very capital-efficient for arbitrage and other single-transaction strategies.

Q13. Why is Supply APY always lower than Borrow APY in lending protocols?
A) Protocol keeps the difference as revenue B) Gas costs C) Reserve factor and utilization D) Regulatory requirements
Answer: C – Supply APY = Borrow APY $\times$ Utilization $\times$ (1 - Reserve Factor); the reserve factor and ¡100% utilization ensure supply rates are lower.

Q14. What tokens do lenders receive when depositing assets on Aave?
A) cTokens B) aTokens C) COMP tokens D) LP tokens
Answer: B – Aave issues aTokens (e.g., aETH, aUSDC) that accrue interest in real-time and represent the deposited assets plus earned interest.

Q15. Which event sparked "DeFi Summer" in 2020?
A) Aave launch B) Compound COMP mining C) Uniswap v2 D) Bitcoin halving
Answer: B – Compound's COMP token liquidity mining program in June 2020 sparked explosive DeFi growth known as "DeFi Summer."

Quiz Questions (16–20)

Q16. What is the main risk that flash loans pose to DeFi protocols?
A) High gas costs B) Oracle manipulation attacks C) Regulatory scrutiny D) Network congestion
Answer: B – Flash loans provide large capital for oracle manipulation attacks, allowing attackers to distort price feeds and exploit protocols.

Q17. What is Aave's E-Mode designed for?
A) Emergency shutdowns B) Higher LTV for correlated assets C) Lower gas costs D) Faster liquidations
Answer: B – E-Mode allows higher LTV ratios for highly correlated assets (e.g., ETH-stETH), improving capital efficiency for low-risk pairs.

Q18. What happened to CeFi lenders Celsius and BlockFi in 2022?
A) They merged B) They went public C) They collapsed D) They launched tokens
Answer: C – Both Celsius and BlockFi collapsed in 2022 due to mismanagement and contagion, while DeFi protocols remained operational.

Q19. What is needed for undercollateralized DeFi lending to work?
A) Higher interest rates B) Credit scores or identity systems C) Longer loan terms D) More liquidators
Answer: B – Undercollateralized lending requires reputation, on-chain credit scores, or KYC/identity to enable legal recourse.

Q20. What is the trade-off of introducing identity-based undercollateralized lending?
A) Higher fees B) Slower transactions C) Reduced permissionlessness D) Lower yields
Answer: C – Adding identity or credit requirements reduces DeFi's core benefit of permissionless access, trading accessibility for capital efficiency.

Quiz: Lending Protocols

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the main difference between traditional and DeFi lending?
A) Traditional is faster B) DeFi requires KYC C) DeFi is permissionless D) Traditional is 24/7

Quiz (1–5)

Q1. What is the main difference between traditional and DeFi lending?
A) Traditional is faster B) DeFi requires KYC C) DeFi is permissionless D) Traditional is 24/7
Answer: C – DeFi lending is permissionless with no KYC or credit checks required.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, max borrow is:
A) $20,000 B) $16,000 C) $10,000 D) $25,000

Quiz (1–5)

Q1. What is the main difference between traditional and DeFi lending?
A) Traditional is faster B) DeFi requires KYC C) DeFi is permissionless D) Traditional is 24/7
Answer: C – DeFi lending is permissionless with no KYC or credit checks required.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, max borrow is:
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – Max borrow = $20,000 $\times$ 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Liquidation occurs D) Nothing

Quiz (1–5)

Q1. What is the main difference between traditional and DeFi lending?
A) Traditional is faster B) DeFi requires KYC C) DeFi is permissionless D) Traditional is 24/7
Answer: C – DeFi lending is permissionless with no KYC or credit checks required.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, max borrow is:
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – Max borrow = $20,000 $\times$ 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Liquidation occurs D) Nothing
Answer: C – HF < 1 triggers liquidation; bots repay debt and claim collateral + bonus.

Q4. Health factor for $30k collateral, $20k borrowed, 85% threshold?
A) 1.00 B) 1.28 C) 1.50 D) 0.67

Quiz (1–5)

Q1. What is the main difference between traditional and DeFi lending?
A) Traditional is faster B) DeFi requires KYC C) DeFi is permissionless D) Traditional is 24/7
Answer: C – DeFi lending is permissionless with no KYC or credit checks required.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, max borrow is:
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – Max borrow = $20,000 $\times$ 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Liquidation occurs D) Nothing
Answer: C – HF < 1 triggers liquidation; bots repay debt and claim collateral + bonus.

Q4. Health factor for $30k collateral, $20k borrowed, 85% threshold?
A) 1.00 B) 1.28 C) 1.50 D) 0.67
Answer: B – HF = (30,000 $\times$ 0.85) / 20,000 = 1.275 $\approx$ 1.28.

Q5. Why do volatile assets have lower LTV ratios?
A) Less popular B) Higher price risk C) Lower liquidity D) Regulations

Quiz (1–5)

Q1. What is the main difference between traditional and DeFi lending?
A) Traditional is faster B) DeFi requires KYC C) DeFi is permissionless D) Traditional is 24/7
Answer: C – DeFi lending is permissionless with no KYC or credit checks required.

Q2. If you deposit 10 ETH worth $20,000 with 80% LTV, max borrow is:
A) $20,000 B) $16,000 C) $10,000 D) $25,000
Answer: B – Max borrow = $20,000 $\times$ 0.80 = $16,000.

Q3. What happens when health factor drops below 1?
A) Interest increases B) Warning email C) Liquidation occurs D) Nothing
Answer: C – HF < 1 triggers liquidation; bots repay debt and claim collateral + bonus.

Q4. Health factor for $30k collateral, $20k borrowed, 85% threshold?
A) 1.00 B) 1.28 C) 1.50 D) 0.67
Answer: B – HF = (30,000 $\times$ 0.85) / 20,000 = 1.275 $\approx$ 1.28.

Q5. Why do volatile assets have lower LTV ratios?
A) Less popular B) Higher price risk C) Lower liquidity D) Regulations
Answer: B – Volatile assets need larger buffers to prevent immediate liquidation.

Quiz (6–10)

Q6. What is the liquidation bonus typically on Aave?
A) 1–2% B) 5–10% C) 15–20% D) 25–30%

Quiz (6–10)

Q6. What is the liquidation bonus typically on Aave?
A) 1–2% B) 5–10% C) 15–20% D) 25–30%
Answer: B – Liquidators receive 5–10% bonus as incentive to maintain protocol solvency.

Q7. What happens to borrow rates when utilization exceeds 90%?
A) Decrease B) Stay constant C) Increase steeply D) Protocol pauses

Quiz (6–10)

Q6. What is the liquidation bonus typically on Aave?
A) 1–2% B) 5–10% C) 15–20% D) 25–30%
Answer: B – Liquidators receive 5–10% bonus as incentive to maintain protocol solvency.

Q7. What happens to borrow rates when utilization exceeds 90%?
A) Decrease B) Stay constant C) Increase steeply D) Protocol pauses
Answer: C – High utilization triggers steep rate increase to prevent liquidity crises.

Q8. Which protocol has largest DeFi lending market share (Dec 2025)?
A) Compound B) MakerDAO C) Aave D) dYdX

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation bonus typically on Aave?
A) 1–2% B) 5–10% C) 15–20% D) 25–30%
Answer: B – Liquidators receive 5–10% bonus as incentive to maintain protocol solvency.

Q7. What happens to borrow rates when utilization exceeds 90%?
A) Decrease B) Stay constant C) Increase steeply D) Protocol pauses
Answer: C – High utilization triggers steep rate increase to prevent liquidity crises.

Q8. Which protocol has largest DeFi lending market share (Dec 2025)?
A) Compound B) MakerDAO C) Aave D) dYdX
Answer: C – Aave leads with $31B TVL and 60%+ market share.

Q9. What unique feature does Aave offer that Compound does not?
A) Interest-bearing tokens B) Flash loans C) Governance token D) Overcollateralization

Quiz (6–10)

Q6. What is the liquidation bonus typically on Aave?
A) 1–2% B) 5–10% C) 15–20% D) 25–30%
Answer: B – Liquidators receive 5–10% bonus as incentive to maintain protocol solvency.

Q7. What happens to borrow rates when utilization exceeds 90%?
A) Decrease B) Stay constant C) Increase steeply D) Protocol pauses
Answer: C – High utilization triggers steep rate increase to prevent liquidity crises.

Q8. Which protocol has largest DeFi lending market share (Dec 2025)?
A) Compound B) MakerDAO C) Aave D) dYdX
Answer: C – Aave leads with $31B TVL and 60%+ market share.

Q9. What unique feature does Aave offer that Compound does not?
A) Interest-bearing tokens B) Flash loans C) Governance token D) Overcollateralization
Answer: B – Aave pioneered flash loans (uncollateralized single-tx borrowing).

Q10. What is needed for undercollateralized DeFi lending to work?
A) Higher rates B) Credit scores or identity C) Longer terms D) More liquidators

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation bonus typically on Aave?
A) 1–2% B) 5–10% C) 15–20% D) 25–30%
Answer: B – Liquidators receive 5–10% bonus as incentive to maintain protocol solvency.

Q7. What happens to borrow rates when utilization exceeds 90%?
A) Decrease B) Stay constant C) Increase steeply D) Protocol pauses
Answer: C – High utilization triggers steep rate increase to prevent liquidity crises.

Q8. Which protocol has largest DeFi lending market share (Dec 2025)?
A) Compound B) MakerDAO C) Aave D) dYdX
Answer: C – Aave leads with $31B TVL and 60%+ market share.

Q9. What unique feature does Aave offer that Compound does not?
A) Interest-bearing tokens B) Flash loans C) Governance token D) Overcollateralization
Answer: B – Aave pioneered flash loans (uncollateralized single-tx borrowing).

Q10. What is needed for undercollateralized DeFi lending to work?
A) Higher rates B) Credit scores or identity C) Longer terms D) More liquidators
Answer: B – Undercollateralized lending requires reputation or KYC for legal recourse.

L38: Stablecoin Mechanisms

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

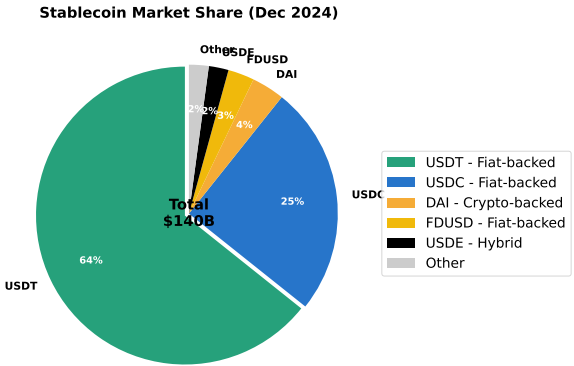
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

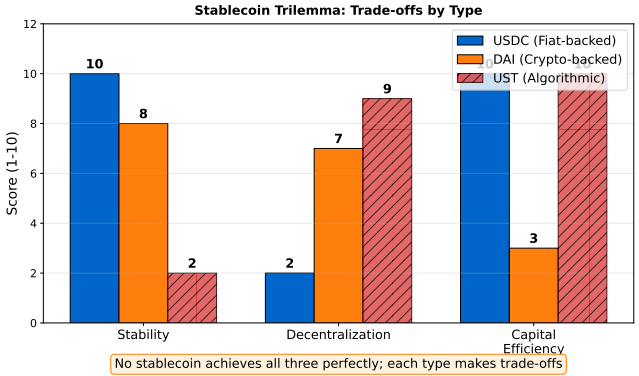
- Classify stablecoin types (fiat-backed, crypto-backed, algorithmic)
- Analyze fiat-backed stablecoins (USDC, USDT)
- Explore crypto-backed stablecoins (DAI, MakerDAO)
- Evaluate algorithmic stablecoins and failure modes

Stablecoin Market Share



Market Cap: $310B (Dec 2025); USDT 59%, USDC 24%; fiat-backed = 90%+.

Stablecoin Trilemma



Each type sacrifices one property: No perfect stablecoin exists.

Type 1: Fiat-Backed Stablecoins

Mechanism: 1 stablecoin backed by $1 in bank account.

Examples:

- **USDC:** Fully backed by cash + T-bills, monthly attestations
- **USDT:** Largest ($142B), less transparent, shifted to 80%+ Treasuries

Advantages: Strong peg, capital efficient
Disadvantages: Centralized, can freeze addresses, counterparty risk

SVB Collapse (Mar 2023): USDC depegged to $0.87 when Circle's bank failed.

Type 2: Crypto-Backed (DAI)

Mechanism: Overcollateralized by crypto (150%+).

How It Works:

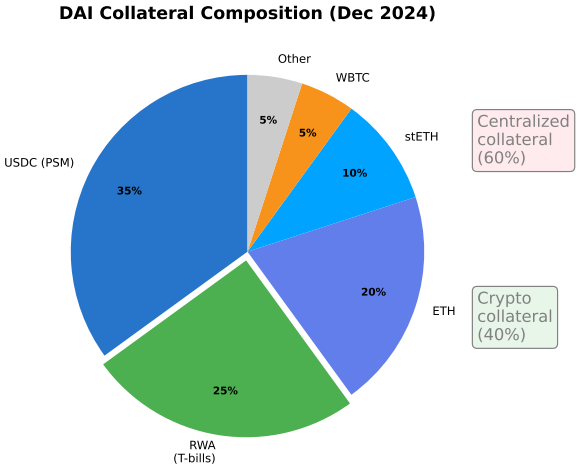
1. Deposit $150 ETH as collateral
2. Mint $100 DAI (150% collateralization)
3. If ETH drops, position liquidated to protect peg

DAI (MakerDAO):

- Largest decentralized stablecoin ($5B)
- Backed by ETH, WBTC, USDC, RWAs
- Governed by MKR token holders

Trade-off: Decentralized but capital inefficient.

DAI Collateral Composition



Decentralization reduced: USDC and RWA backing adds centralization.

Type 3: Algorithmic Stablecoins

Mechanism: Maintain peg through supply adjustments (no/minimal collateral).

How It Works (Theory):

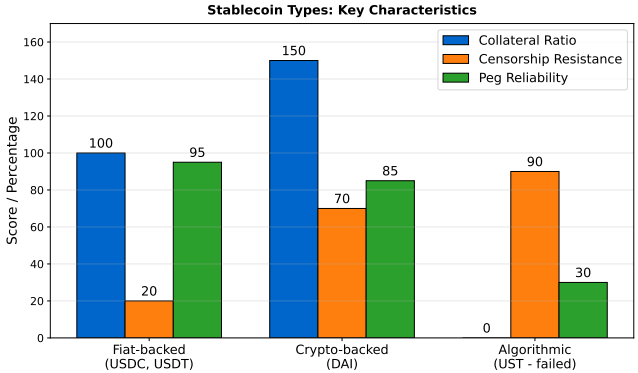
- Price ¿ $1: Increase supply (mint, sell)
- Price ¡ $1: Decrease supply (buy, burn)

Examples:

- **Terra UST:** Failed spectacularly (May 2022)
- **FRAX:** Hybrid (partially collateralized)

Reality: Most pure algo stablecoins have failed (death spirals).

Stablecoin Types Comparison



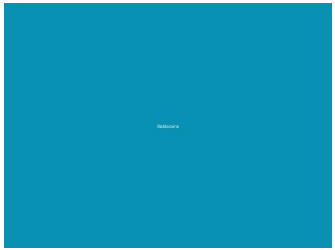
Key Trade-offs: Decentralization vs. capital efficiency vs. stability.

Key Takeaways

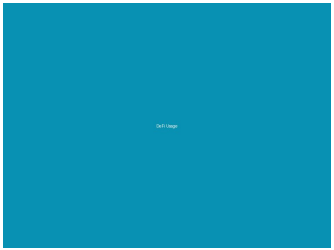
1. **Fiat-Backed:** USDT (59%), USDC (24%); strong peg but centralized
2. **Crypto-Backed:** DAI; decentralized but capital inefficient (150%+)
3. **Algorithmic:** Capital efficient theory; death spiral reality (Terra UST)
4. **Trilemma:** Cannot optimize all three: decentralization, stability, efficiency
5. **Market:** $310B (Dec 2025); fiat-backed dominates 90%+

Next: L39 – Terra Luna Case Study

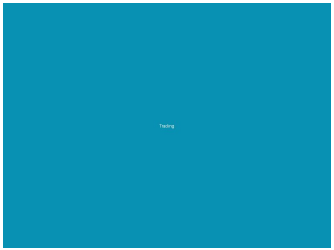
Stablecoins in Practice



Stablecoins



DeFi Usage



Trading

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is a stablecoin?
A) High volatility token B) Crypto pegged to $1 C) Mining reward D) Governance token

Quiz (1/2)

Q1. What is a stablecoin?
A) High volatility token B) Crypto pegged to $1 C) Mining reward D) Governance token
Answer: B – Designed to maintain stable $1 value.

Q2. Total stablecoin market cap (Dec 2025)?
A) $50B B) $140B C) $310B D) $500B

Quiz (1/2)

Q1. What is a stablecoin?
A) High volatility token B) Crypto pegged to $1 C) Mining reward D) Governance token
Answer: B – Designed to maintain stable $1 value.

Q2. Total stablecoin market cap (Dec 2025)?
A) $50B B) $140B C) $310B D) $500B
Answer: C – $310B, up from $140B in Dec 2024.

Q3. Which stablecoin has largest market share?
A) USDC B) USDT C) DAI D) FRAX

Quiz (1/2)

Q1. What is a stablecoin?
A) High volatility token B) Crypto pegged to $1 C) Mining reward D) Governance token
Answer: B – Designed to maintain stable $1 value.

Q2. Total stablecoin market cap (Dec 2025)?
A) $50B B) $140B C) $310B D) $500B
Answer: C – $310B, up from $140B in Dec 2024.

Q3. Which stablecoin has largest market share?
A) USDC B) USDT C) DAI D) FRAX
Answer: B – USDT at 59% ($142B).

Q4. What backs fiat-backed stablecoins?
A) Crypto B) Algorithms C) Bank deposits/Treasuries D) Nothing

Quiz (1/2)

Q1. What is a stablecoin?
A) High volatility token B) Crypto pegged to $1 C) Mining reward D) Governance token
Answer: B – Designed to maintain stable $1 value.

Q2. Total stablecoin market cap (Dec 2025)?
A) $50B B) $140B C) $310B D) $500B
Answer: C – $310B, up from $140B in Dec 2024.

Q3. Which stablecoin has largest market share?
A) USDC B) USDT C) DAI D) FRAX
Answer: B – USDT at 59% ($142B).

Q4. What backs fiat-backed stablecoins?
A) Crypto B) Algorithms C) Bank deposits/Treasuries D) Nothing
Answer: C – Cash and T-bills in bank accounts.

Q5. Why is DAI overcollateralized at 150%?
A) Higher profits B) Buffer for crypto volatility C) Regulatory requirement D) Gas savings

Quiz (1/2)

Q1. What is a stablecoin?
A) High volatility token B) Crypto pegged to $1 C) Mining reward D) Governance token
Answer: B – Designed to maintain stable $1 value.

Q2. Total stablecoin market cap (Dec 2025)?
A) $50B B) $140B C) $310B D) $500B
Answer: C – $310B, up from $140B in Dec 2024.

Q3. Which stablecoin has largest market share?
A) USDC B) USDT C) DAI D) FRAX
Answer: B – USDT at 59% ($142B).

Q4. What backs fiat-backed stablecoins?
A) Crypto B) Algorithms C) Bank deposits/Treasuries D) Nothing
Answer: C – Cash and T-bills in bank accounts.

Q5. Why is DAI overcollateralized at 150%?
A) Higher profits B) Buffer for crypto volatility C) Regulatory requirement D) Gas savings
Answer: B – Protects peg against collateral price drops.

Quiz (2/2)

Q6. What is the stablecoin trilemma?
A) Three stablecoin types B) Cannot optimize decentralization + stability + efficiency C) Three backing assets D) Three price points

Quiz (2/2)

Q6. What is the stablecoin trilemma?
A) Three stablecoin types B) Cannot optimize decentralization + stability + efficiency C) Three backing assets D) Three price points
Answer: B – Each type sacrifices one property.

Q7. What happened to USDC in March 2023?
A) Doubled in value B) Depegged to $0.87 (SVB collapse) C) Was acquired D) Launched V2

Quiz (2/2)

Q6. What is the stablecoin trilemma?
A) Three stablecoin types B) Cannot optimize decentralization + stability + efficiency C) Three backing assets D) Three price points
Answer: B – Each type sacrifices one property.

Q7. What happened to USDC in March 2023?
A) Doubled in value B) Depegged to \$0.87 (SVB collapse) C) Was acquired D) Launched V2
Answer: B – Circle had \$3.3B at failed Silicon Valley Bank.

Q8. Why do most algorithmic stablecoins fail?
A) Too complex B) Death spirals C) High gas fees D) Regulatory issues

Quiz (2/2)

Q6. What is the stablecoin trilemma?
A) Three stablecoin types B) Cannot optimize decentralization + stability + efficiency C) Three backing assets D) Three price points
Answer: B – Each type sacrifices one property.

Q7. What happened to USDC in March 2023?
A) Doubled in value B) Depegged to $0.87 (SVB collapse) C) Was acquired D) Launched V2
Answer: B – Circle had $3.3B at failed Silicon Valley Bank.

Q8. Why do most algorithmic stablecoins fail?
A) Too complex B) Death spirals C) High gas fees D) Regulatory issues
Answer: B – Depeg causes selling spiral to zero.

Q9. Which stablecoin failed in May 2022?
A) USDC B) USDT C) DAI D) Terra UST

Quiz (2/2)

Q6. What is the stablecoin trilemma?
A) Three stablecoin types B) Cannot optimize decentralization + stability + efficiency C) Three backing assets D) Three price points
Answer: B – Each type sacrifices one property.

Q7. What happened to USDC in March 2023?
A) Doubled in value B) Depegged to $0.87 (SVB collapse) C) Was acquired D) Launched V2
Answer: B – Circle had $3.3B at failed Silicon Valley Bank.

Q8. Why do most algorithmic stablecoins fail?
A) Too complex B) Death spirals C) High gas fees D) Regulatory issues
Answer: B – Depeg causes selling spiral to zero.

Q9. Which stablecoin failed in May 2022?
A) USDC B) USDT C) DAI D) Terra UST
Answer: D – $40B collapse, algorithmic death spiral.

Q10. What percentage of stablecoins are fiat-backed?
A) 50% B) 70% C) 90%+ D) 100%

Quiz (2/2)

Q6. What is the stablecoin trilemma?
A) Three stablecoin types B) Cannot optimize decentralization + stability + efficiency C) Three backing assets D) Three price points
Answer: B – Each type sacrifices one property.

Q7. What happened to USDC in March 2023?
A) Doubled in value B) Depegged to $0.87 (SVB collapse) C) Was acquired D) Launched V2
Answer: B – Circle had $3.3B at failed Silicon Valley Bank.

Q8. Why do most algorithmic stablecoins fail?
A) Too complex B) Death spirals C) High gas fees D) Regulatory issues
Answer: B – Depeg causes selling spiral to zero.

Q9. Which stablecoin failed in May 2022?
A) USDC B) USDT C) DAI D) Terra UST
Answer: D – $40B collapse, algorithmic death spiral.

Q10. What percentage of stablecoins are fiat-backed?
A) 50% B) 70% C) 90%+ D) 100%
Answer: C – USDT + USDC alone = 83%.

Thank you

Questions?

Next: L39 – Terra Luna Case Study

L38: Stablecoin Mechanisms

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Classify different stablecoin mechanism types (fiat-backed, crypto-backed, algorithmic)
- Analyze fiat-backed stablecoins (USDC, USDT)
- Explore crypto-backed stablecoins (DAI, MakerDAO)
- Evaluate algorithmic stablecoins and their failure modes
- Compare stablecoin trade-offs (decentralization, stability, efficiency)

The Problem: How do we create stable value on-chain?

The Challenge
Cryptocurrencies are highly volatile (BTC: $69k to $15k in 2022). DeFi needs price-stable assets for payments, lending, and savings, but blockchain systems lack native connection to fiat currencies.

Why It Matters

- Volatility makes crypto unusable for everyday payments and savings
- Historical example: Tether (2014), DAI (2017), algorithmic failures (Terra/Luna 2022)

What We Need

- System design principles
- Price stability mechanism resistant to market shocks and attacks

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How Stablecoin Mechanisms addresses this challenge

What is a Stablecoin?

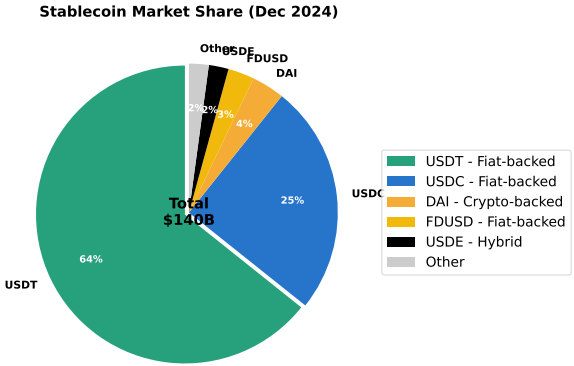
Definition: A cryptocurrency designed to maintain a stable value relative to $1 USD.

Why Stablecoins?

- Price stability (avoid crypto volatility)
- Medium of exchange, store of value
- DeFi building block (lending, trading, yield)
- Fast, cheap cross-border payments

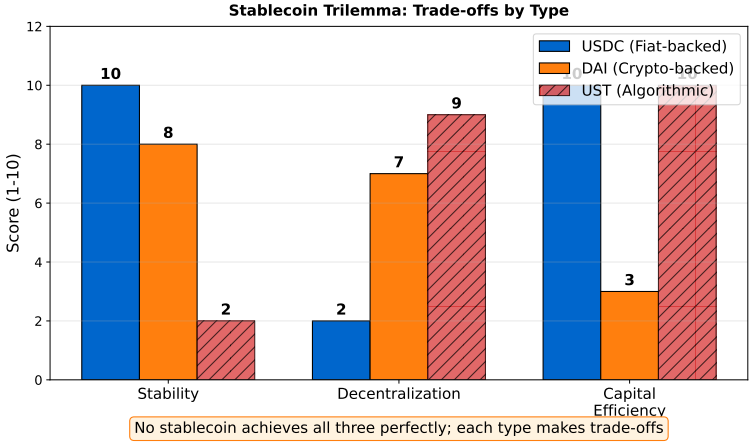
Total Market Cap: $310B (Dec 2025), up from $140B in Dec 2024

Stablecoin Market Share



USDT dominates (59%, $142B); USDC 24% ($52B); fiat-backed = 90%+ of market

Stablecoin Trilemma



Each type sacrifices one property; no perfect stablecoin exists

Type 1: Fiat-Backed Stablecoins

Mechanism: 1 stablecoin backed by $1 in bank account.

How It Works:

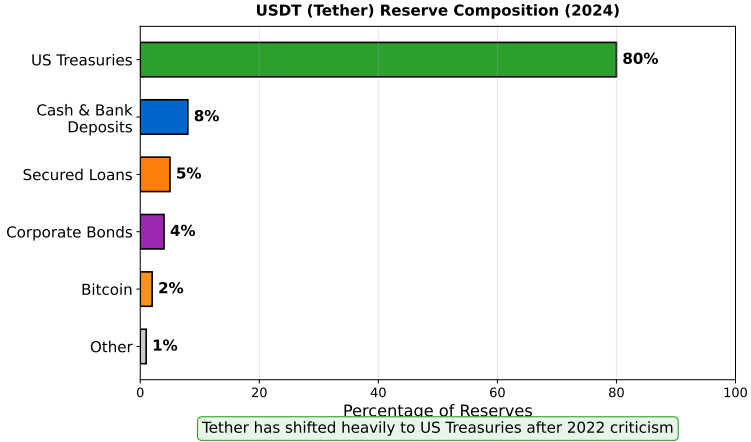
1. User deposits $100 fiat to issuer
2. Issuer mints 100 tokens, holds reserves
3. User can redeem 100 tokens for $100 anytime

Examples:

- **USDC:** Fully backed by cash + T-bills, monthly attestations
- **USDT:** Mixed reserves, largest but less transparent

Advantages: Strong peg, capital efficient, easy to understand
Disadvantages: Centralized, censorship risk, counterparty risk

USDT Reserve Composition



Tether has shifted to 80%+ US Treasuries after 2022 criticism

Fiat-Backed: Key Risks

Centralization: Issuer can freeze addresses (OFAC compliance)
Counterparty Risk: Trust issuer to maintain reserves

Black Swan Example: SVB Collapse (March 2023)

- Circle had $3.3B deposited at Silicon Valley Bank
- Bank failure caused USDC to depeg to $0.87
- Recovered after Fed guarantee on deposits

Lesson: Even "safe" fiat-backed stablecoins have counterparty risk.

Type 2: Crypto-Backed Stablecoins

Mechanism: Backed by crypto collateral (overcollateralized).

How It Works:

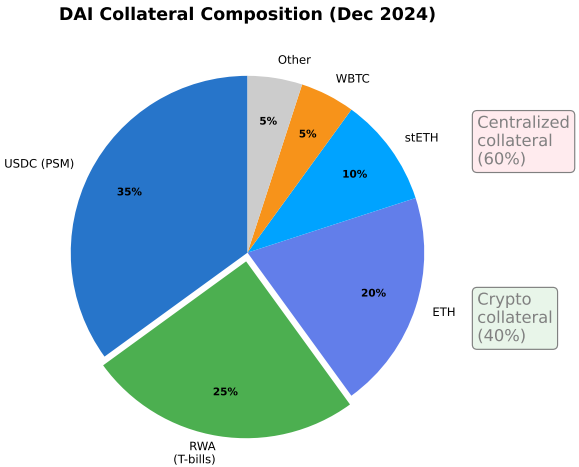
1. User deposits $150 ETH as collateral
2. Protocol mints $100 DAI (150% collateralization)
3. If ETH drops, position liquidated to protect peg

Example: DAI (MakerDAO)

- Largest decentralized stablecoin ($5B)
- Backed by ETH, WBTC, USDC, RWAs
- Governed by MKR token holders

Advantages: Decentralized, transparent, censorship-resistant

DAI Collateral Composition



DAI's decentralization reduced by USDC and RWA backing (centralized collateral)

MakerDAO: DAI Stability Mechanisms

1. **Arbitrage**
   - DAI ¿ $1: Mint DAI, sell for profit
   - DAI ¡ $1: Buy DAI, repay vault for profit
2. **Stability Fee (Interest Rate)**
   - High fee: Reduces supply (repayments)
   - Low fee: Increases supply (more minting)
3. **Peg Stability Module (PSM)**
   - Swap USDC for DAI 1:1 (backstop for large depegs)

Trade-off: PSM improves stability but increases centralization.

Type 3: Algorithmic Stablecoins

Mechanism: Maintain peg through supply adjustments (no/minimal collateral).

How It Works (Theoretically):

- Price ¿ $1: Increase supply (mint, sell)
- Price ¡ $1: Decrease supply (buy, burn)

Examples:

- **Terra UST:** Failed spectacularly (May 2022)
- **FRAX:** Hybrid (partially collateralized)

Theoretical Advantage: Capital efficient, decentralized, scalable
Reality: Most pure algorithmic stablecoins have failed (death spirals).

Why Algorithmic Stablecoins Fail

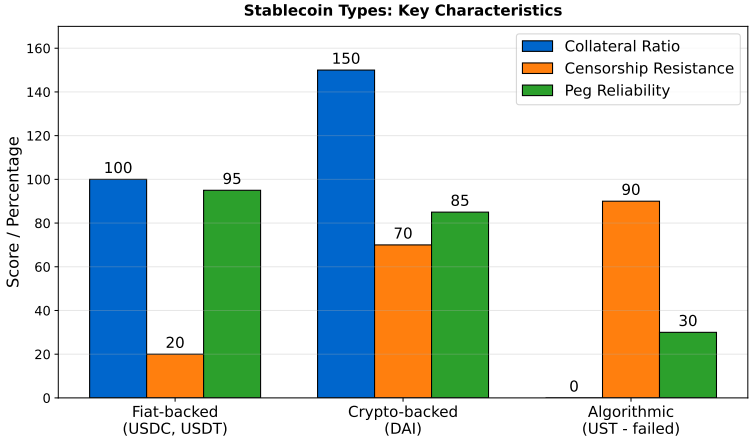
Death Spiral Scenario:

1. Stablecoin depegs below $1
2. Protocol mints sister token to incentivize buying
3. Sister token crashes from dilution
4. Loss of confidence accelerates selling
5. Spiral to zero, total collapse

Root Cause: No intrinsic backing or demand floor.
Lesson: Algorithmic stability relies entirely on confidence. Once lost, irrecoverable.

(c) Joerg Osterrieder 2025

Stablecoin Types Comparison



Fiat-backed wins on reliability; crypto-backed best censorship resistance

Stablecoin Comparison Table

Type	Example	Backing	Decent.	Efficient
Fiat-backed	USDC	USD (1:1)	No	Yes
Fiat-backed	USDT	Mixed	No	Yes
Crypto-backed	DAI	ETH+USDC	Partial	No
Algorithmic	UST	None	Yes	Yes
Hybrid	FRAX	USDC+FXS	Partial	Partial

Key Insight: No stablecoin achieves all three properties (trilemma).

Regulatory Landscape

US:

- SEC scrutiny (some stablecoins may be securities)
- Bank-like regulation proposed (reserve requirements)

EU (MiCA):

- Stablecoin issuers need authorization
- Reserve and redemption requirements
- Significant stablecoins face additional rules

Impact (Dec 2024):

- BUSD shut down (Feb 2023, regulatory pressure)
- MiCA full effect: USDT delisted from EU exchanges (Coinbase, Kraken EU)
- Circle USDC MiCA-compliant (EMI license July 2024)
- Increasing compliance costs favor large, regulated players

Problem Solved? Stablecoin Mechanisms

The Original Problem

How do we create stable value on-chain?

How Stablecoin Mechanisms Solves It

- Fiat-backed (USDC, USDT): Simple 1:1 reserves – strong peg but centralized
- Crypto-collateralized (DAI): Overcollateralization + arbitrage + PSM – decentralized but capital inefficient
- Algorithmic: Supply adjustments – capital efficient but unstable (most failed)

Remaining Limitations

- Centralization risk: Fiat-backed requires trust in issuer; DAI increasingly uses USDC
- Depeg events: SVB collapse (USDC), death spirals (Terra/Luna)
- Regulatory pressure: MiCA compliance, USDT delistings

Open Questions

- Is fully decentralized stable value achievable without centralized collateral?
- Risk: Regulatory crackdown on unregulated stablecoins, confidence crises

Stablecoin Mechanisms partially solves "create stable value on-chain" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- Stablecoins maintain $1 peg; $310B market cap (Dec 2025)
- Fiat-backed (USDC, USDT): Stable but centralized
- Crypto-backed (DAI): Decentralized but capital inefficient
- Algorithmic: Capital efficient but unstable (most failed)
- Stablecoin trilemma: Can't have stability + decentralization + efficiency
- DAI's centralization debate: USDC backing vs. pure crypto
- Regulation increasing (MiCA, US proposals)

Next Lecture: Terra/Luna Case Study.

Questions for Reflection

1. Why do algorithmic stablecoins tend to fail during market stress?
2. How does the PSM help DAI maintain its peg? What's the trade-off?
3. Would you trust a stablecoin backed by 80% US Treasuries?
4. How might stablecoin regulation impact DeFi?
5. Is perfect decentralization compatible with price stability?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of a stablecoin?
A) To maximize returns B) To maintain a stable value relative to $1 USD
C) To replace Bitcoin D) To eliminate transaction fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. What was the approximate total stablecoin market cap in December 2025?
A) $50B B) $150B C) $310B D) $500B
Answer: C – The market cap reached $310B (USDT $187B, USDC $77B), up from $140B in Dec 2024.

Q3. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) dominates with 59% market share ($142B).

Q4. What does the stablecoin trilemma state?
A) All stablecoins will fail B) Only 3 stablecoins can exist
C) No stablecoin can achieve stability, decentralization, and efficiency D) Stablecoins need 3 types of collateral
Answer: C – Each stablecoin type sacrifices one of the three properties.

Q5. How does a fiat-backed stablecoin maintain its peg?
A) Algorithmic supply adjustments B) 1:1 backing with USD reserves
C) Overcollateralized crypto D) Community voting
Answer: B – Users deposit $1 fiat, issuer mints 1 token backed by reserves.

Quiz Questions (6–10)

Q6. What is the main disadvantage of fiat-backed stablecoins?
A) High volatility B) Centralization and counterparty risk
C) Low liquidity D) No use case
Answer: B – They are centralized and require trust in the issuer to maintain reserves.

Q7. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure
C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q8. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets
C) No collateral D) Government bonds
Answer: B – Users deposit $150 ETH to mint $100 DAI (150% collateralization).

Q9. What is DAI's approximate market cap?
A) $1B B) $5B C) $50B D) $100B
Answer: B – DAI is the largest decentralized stablecoin at $5B.

Q10. What collateral types back DAI?
A) Only ETH B) ETH, WBTC, USDC, RWAs
C) Only USDC D) Gold and silver
Answer: B – DAI uses diversified collateral including crypto and real-world assets.

Quiz Questions (11–15)

Q11. What is the Peg Stability Module (PSM)?
A) A voting mechanism B) 1:1 swap between USDC and DAI
C) An insurance fund D) A liquidation bot
Answer: B – PSM allows swapping USDC for DAI 1:1, backstopping large depegs.

Q12. What is the trade-off of using the PSM in MakerDAO?
A) Higher fees B) Lower liquidity
C) Improved stability but increased centralization D) Faster transactions
Answer: C – PSM relies on USDC (centralized), reducing DAI's decentralization.

Q13. How do algorithmic stablecoins theoretically maintain their peg?
A) Fiat reserves B) Supply adjustments (mint/burn)
C) Overcollateralization D) Central bank intervention
Answer: B – They increase supply when price ¿ \$1, decrease when price ¡ \$1.

Q14. Which algorithmic stablecoin failed spectacularly in May 2022?
A) USDC B) DAI C) Terra UST D) FRAX
Answer: C – Terra UST collapsed in a death spiral, losing its peg completely.

Q15. What is a "death spiral" in algorithmic stablecoins?
A) Slow decline in price B) Depeg triggers sister token dilution, accelerating collapse
C) Government shutdown D) Network congestion
Answer: B – Loss of confidence causes selling, sister token crashes, spiral to zero.

Quiz Questions (16–20)

Q16. What is the root cause of algorithmic stablecoin failures?
A) Poor marketing B) No intrinsic backing or demand floor
C) High transaction fees D) Slow block times
Answer: B – They rely entirely on confidence; once lost, there's no recovery mechanism.

Q17. What percentage of Tether's (USDT) reserves are in US Treasuries?
A) 20% B) 50% C) 80%+ D) 0%
Answer: C – Tether shifted to 80%+ US Treasuries after 2022 criticism.

Q18. Which stablecoin was shut down in February 2023 due to regulatory pressure?
A) USDT B) USDC C) DAI D) BUSD
Answer: D – BUSD was shut down following regulatory action.

Q19. Under EU MiCA regulation (Dec 2024), what happened to USDT?
A) Approved for all EU exchanges B) Delisted from major EU exchanges
C) Given special exemption D) Banned globally
Answer: B – USDT was delisted from EU exchanges like Coinbase and Kraken EU.

Q20. Which stablecoin became MiCA-compliant with an EMI license in July 2024?
A) USDT B) DAI C) USDC D) FRAX
Answer: C – Circle's USDC obtained EMI license and became MiCA-compliant.

L38: Stablecoin Mechanisms

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Why Put a Dollar On Blockchain?

[COMIC: Dollar but on blockchain]

Placeholder for comic showing confused person asking "Why do we need a dollar on blockchain?" while another shows instant global transfers, 24/7 availability, and programmable money

The Setup

- Crypto is too volatile for payments
- BTC: $69k to $15k in one year
- Can't price coffee in something that moves 10%/day

The Punchline

- Stablecoins: crypto stability
- Dollar value, blockchain speed
- Best of both worlds

Stablecoins solve the "I can't buy coffee with BTC" problem

Learning Objectives

- Classify different stablecoin mechanism types (fiat-backed, crypto-backed, algorithmic)
- Analyze fiat-backed stablecoins (USDC, USDT)
- Explore crypto-backed stablecoins (DAI, MakerDAO)
- Evaluate algorithmic stablecoins and their failure modes
- Compare stablecoin trade-offs (decentralization, stability, efficiency)

Building on L37: Lending Protocols

The Problem: How do we create stable value on-chain?

The Challenge
Cryptocurrencies are highly volatile (BTC: $69k to $15k in 2022). DeFi needs price-stable assets for payments, lending, and savings, but blockchain systems lack native connection to fiat currencies.

Why It Matters

- Volatility makes crypto unusable for everyday payments and savings
- Historical example: Tether (2014), DAI (2017), algorithmic failures (Terra/Luna 2022)

What We Need

- System design principles
- Price stability mechanism resistant to market shocks and attacks

The Cryptoeconomics Question
Creating systems with desired properties

Today's lesson: How Stablecoin Mechanisms addresses this challenge

What Are Stablecoins and Why Do We Need Them?

Definition: A cryptocurrency designed to maintain a stable value relative to $1 USD.

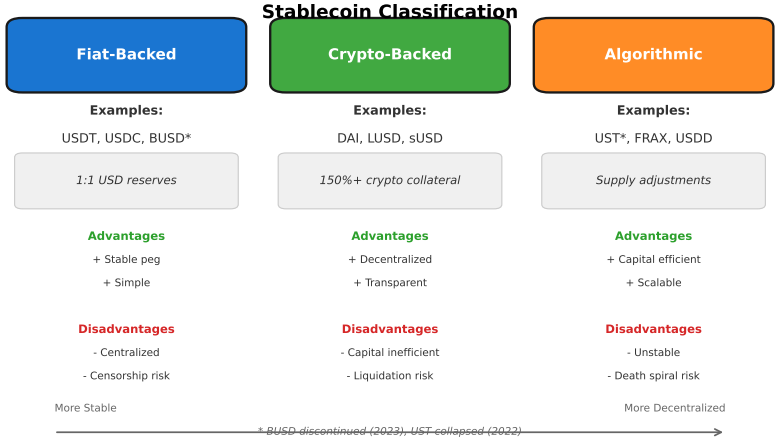
Why Stablecoins?

- Price stability (avoid crypto volatility)
- Medium of exchange, store of value
- DeFi building block (lending, trading, yield)
- Fast, cheap cross-border payments

Total Market Cap: $310B (Dec 2025), up from $140B in Dec 2024

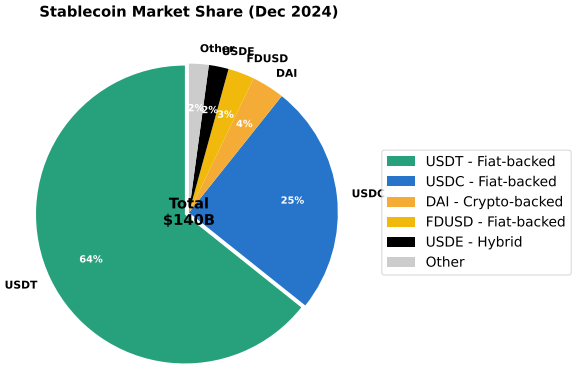
*Stablecoins maintain **$1** value on-chain, enabling saving and trading without crypto volatility.*

What Types of Stablecoins Exist?



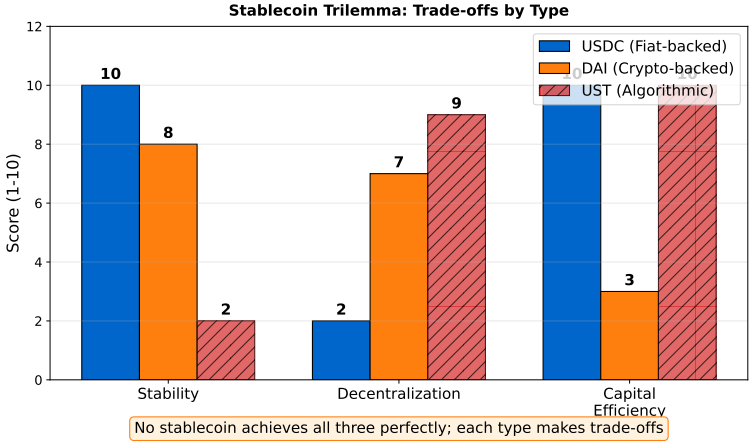
Three main types: fiat-backed (stable, centralized), crypto-backed (decentralized, inefficient), algorithmic (scalable, risky)

Which Stablecoins Dominate the Market?



USDT dominates (59%, $142B); USDC 24% ($52B); fiat-backed = 90%+ of market

What Trade-offs Do Stablecoins Face?



Each type sacrifices one property; no perfect stablecoin exists

How Do Fiat-Backed Stablecoins Work?

Mechanism: 1 stablecoin backed by $1 in bank account.

How It Works:

1. User deposits $100 fiat to issuer
2. Issuer mints 100 tokens, holds reserves
3. User can redeem 100 tokens for $100 anytime

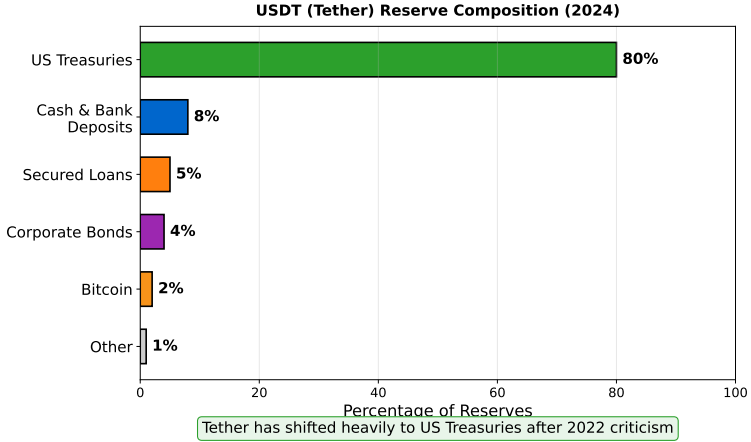
Examples:

- **USDC:** Fully backed by cash + T-bills, monthly attestations
- **USDT:** Mixed reserves, largest but less transparent

Advantages: Strong peg, capital efficient, easy to understand
Disadvantages: Centralized, censorship risk, counterparty risk

Fiat-backed = 1 token backed by $1 in bank. Trade-off: trusting a centralized issuer.

What Backs Tether (USDT)?



Tether has shifted to 80%+ US Treasuries after 2022 criticism

What Are the Risks of Fiat-Backed Stablecoins?

Centralization: Issuer can freeze addresses (OFAC compliance)
Counterparty Risk: Trust issuer to maintain reserves

Black Swan Example: SVB Collapse (March 2023)

- Circle had $3.3B deposited at Silicon Valley Bank
- Bank failure caused USDC to depeg to $0.87
- Recovered after Fed guarantee on deposits

Lesson: Even "safe" fiat-backed stablecoins have counterparty risk.

How Do Crypto-Backed Stablecoins Maintain Their Peg?

Mechanism: Backed by crypto collateral (overcollateralized – deposit more value than borrowed, e.g., $150 for $100).

How It Works:

1. User deposits $150 ETH as collateral
2. Protocol mints $100 DAI (150% collateralization)
3. If ETH drops, position liquidated to protect peg

Example: DAI (MakerDAO)

- Largest decentralized stablecoin ($5B)
- Backed by ETH, WBTC, USDC, RWAs
- Governed by MKR token holders

Advantages: Decentralized, transparent, censorship-resistant

Problem Check-In: Stablecoin Mechanisms

Recall Our Problem

How do we create stable value on-chain?

What We've Learned So Far

- Three stablecoin types: fiat-backed (USDC), crypto-backed (DAI), algorithmic (failed UST)
- The stablecoin trilemma: no design achieves stability + decentralization + capital efficiency
- Different mechanisms = different trade-offs. Fiat-backed is stable but centralized.

Still to Address

- Algorithmic stablecoins: why most have failed (death spiral risk)
- Is true decentralization compatible with price stability?

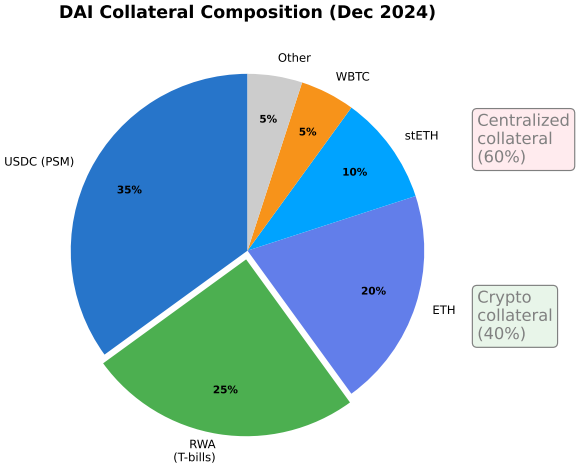
Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we create stable value on-chain?"?

(c) Joerg Osterrieder 2025

What Assets Back DAI?



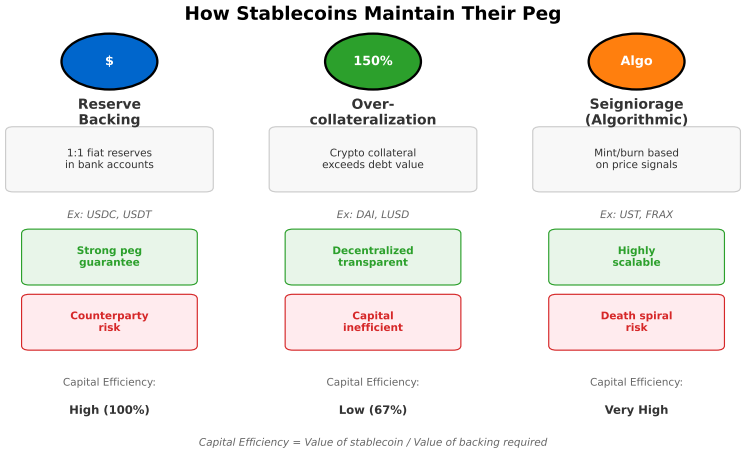
DAI's collateral mix reveals the trilemma: adding USDC improves stability but reduces decentralization.

How Does DAI Maintain Its Peg?

1. **Arbitrage**
   - DAI ¿ $1: Mint DAI, sell for profit
   - DAI ¡ $1: Buy DAI, repay vault for profit
2. **Stability Fee (Interest Rate)**
   - High fee: Reduces supply (repayments)
   - Low fee: Increases supply (more minting)
3. **Peg Stability Module (PSM)**
   - Swap USDC for DAI 1:1 (backstop for large depegs)

Trade-off: PSM improves stability but increases centralization.

How Do Different Stability Mechanisms Compare?



Each mechanism trades off between stability, decentralization, and capital efficiency

How Do Algorithmic Stablecoins Work?

Mechanism: Maintain peg through supply adjustments (no/minimal collateral).

How It Works (Theoretically):

- Price ¿ $1: Increase supply (mint, sell)
- Price ¡ $1: Decrease supply (buy, burn)

Examples:

- **Terra UST:** Failed spectacularly (May 2022)
- **FRAX:** Hybrid (partially collateralized)

Theoretical Advantage: Capital efficient, decentralized, scalable
Reality: Most pure algorithmic stablecoins have failed (death spirals).

Pseudocode: Algorithmic Peg Mechanism

Mint-and-Burn Stabilization (Terra-style)

```
function stabilize(stablecoin_price):
  if stablecoin_price > $1.00:
    // Above peg:  increase supply
    mint_stablecoin(excess_demand)
    burn_governance_token(equivalent_value)
  if stablecoin_price < $1.00:
    // Below peg:  decrease supply
    burn_stablecoin(excess_supply)
    mint_governance_token(equivalent_value)
    // DANGER: governance token dilution
    // If confidence drops, death spiral begins
```

Key Insight: The mint-and-burn loop works *only while confidence holds*. When the governance token loses value, minting more cannot restore the peg – each mint dilutes further, accelerating collapse.

Terra/Luna's $40B collapse in May 2022 demonstrated exactly this death spiral in practice

Why Do Algorithmic Stablecoins Keep Failing?

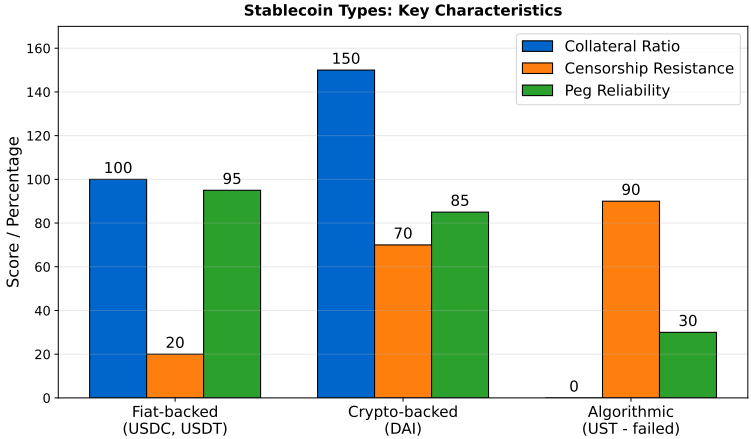
Death Spiral Scenario:
(Death spiral = self-reinforcing collapse where falling prices trigger more selling)

1. Stablecoin depegs below $1
2. Protocol mints sister token to incentivize buying
3. Sister token crashes from dilution
4. Loss of confidence accelerates selling
5. Spiral to zero, total collapse

Root Cause: No intrinsic backing or demand floor.
Lesson: Algorithmic stability relies entirely on confidence. Once lost, irrecoverable.

Death spirals explain algo failures: no backing means confidence loss triggers collapse.

How Do the Three Stablecoin Types Compare?



Fiat-backed wins on reliability; crypto-backed best censorship resistance

How Do Specific Stablecoins Compare?

Type	Example	Backing	Decent.	Efficient
Fiat-backed	USDC	USD (1:1)	No	Yes
Fiat-backed	USDT	Mixed	No	Yes
Crypto-backed	DAI	ETH+USDC	Partial	No
Algorithmic	UST	None	Yes	Yes
Hybrid	FRAX	USDC+FXS	Partial	Partial

Key Insight: No stablecoin achieves all three properties (trilemma).

(c) Joerg Osterrieder 2025

How Is Stablecoin Regulation Evolving?

US:

- SEC scrutiny (some stablecoins may be securities)
- Bank-like regulation proposed (reserve requirements)

EU (MiCA):

- Stablecoin issuers need authorization
- Reserve and redemption requirements
- Significant stablecoins face additional rules

Impact (Dec 2024):

- BUSD shut down (Feb 2023, regulatory pressure)
- MiCA full effect: USDT delisted from EU exchanges (Coinbase, Kraken EU)
- Circle USDC MiCA-compliant (EMI license July 2024)
- Increasing compliance costs favor large, regulated players

Problem Solved? Stablecoin Mechanisms

The Original Problem

How do we create stable value on-chain?

How Stablecoin Mechanisms Solves It

- Fiat-backed (USDC, USDT): Simple 1:1 reserves – strong peg but centralized
- Crypto-collateralized (DAI): Overcollateralization + arbitrage + PSM – decentralized but capital inefficient
- Algorithmic: Supply adjustments – capital efficient but unstable (most failed)

Remaining Limitations

- Centralization risk: Fiat-backed requires trust in issuer; DAI increasingly uses USDC
- Depeg events: SVB collapse (USDC), death spirals (Terra/Luna)
- Regulatory pressure: MiCA compliance, USDT delistings

Open Questions

- Is fully decentralized stable value achievable without centralized collateral?
- Risk: Regulatory crackdown on unregulated stablecoins, confidence crises

Stablecoin Mechanisms partially solves "create stable value on-chain" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Stablecoin Mechanisms

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Stablecoin Mechanisms

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Stablecoin Mechanisms

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Can We Trust Stablecoin Reserve Claims?

[COMIC: Reserve transparency issues]

Placeholder for comic showing user asking "Is my stablecoin really backed 1:1?" while issuer nervously hides a pie chart showing commercial paper, loans, and "other"

The Trust Problem

- Fiat-backed = trust the issuer
- "Trust us, the money is there"
- Attestation is not an audit

Historical Examples

- USDT reserve composition debates
- USDC SVB depeg ($0.87)
- Counterparty risk is real

"Fully backed" means different things to different issuers

Summary

Key Takeaways:

- Stablecoins maintain $1 peg; $310B market cap (Dec 2025)
- Fiat-backed (USDC, USDT): Stable but centralized
- Crypto-backed (DAI): Decentralized but capital inefficient
- Algorithmic: Capital efficient but unstable (most failed)
- Stablecoin trilemma: Can't have stability + decentralization + efficiency
- DAI's centralization debate: USDC backing vs. pure crypto
- Regulation increasing (MiCA, US proposals)

Next Lecture: Terra/Luna Case Study.

Next Lesson: L39 – Terra/Luna Case Study

Questions for Reflection

1. Why do algorithmic stablecoins tend to fail during market stress?
2. How does the PSM help DAI maintain its peg? What's the trade-off?
3. Would you trust a stablecoin backed by 80% US Treasuries?
4. How might stablecoin regulation impact DeFi?
5. Is perfect decentralization compatible with price stability?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of a stablecoin?
A) To maximize returns B) To maintain a stable value relative to $1 USD
C) To replace Bitcoin D) To eliminate transaction fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. What was the approximate total stablecoin market cap in December 2025?
A) $50B B) $150B C) $310B D) $500B
Answer: C – The market cap reached $310B (USDT $187B, USDC $77B), up from $140B in Dec 2024.

Q3. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) dominates with 59% market share ($142B).

Q4. What does the stablecoin trilemma state?
A) All stablecoins will fail B) Only 3 stablecoins can exist
C) No stablecoin can achieve stability, decentralization, and efficiency D) Stablecoins need 3 types of collateral
Answer: C – Each stablecoin type sacrifices one of the three properties.

Q5. How does a fiat-backed stablecoin maintain its peg?
A) Algorithmic supply adjustments B) 1:1 backing with USD reserves
C) Overcollateralized crypto D) Community voting
Answer: B – Users deposit $1 fiat, issuer mints 1 token backed by reserves.

Quiz Questions (6–10)

Q6. What is the main disadvantage of fiat-backed stablecoins?
A) High volatility B) Centralization and counterparty risk
C) Low liquidity D) No use case
Answer: B – They are centralized and require trust in the issuer to maintain reserves.

Q7. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure
C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q8. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets
C) No collateral D) Government bonds
Answer: B – Users deposit $150 ETH to mint $100 DAI (150% collateralization).

Q9. What is DAI's approximate market cap?
A) $1B B) $5B C) $50B D) $100B
Answer: B – DAI is the largest decentralized stablecoin at $5B.

Q10. What collateral types back DAI?
A) Only ETH B) ETH, WBTC, USDC, RWAs
C) Only USDC D) Gold and silver
Answer: B – DAI uses diversified collateral including crypto and real-world assets.

Quiz Questions (11–15)

Q11. What is the Peg Stability Module (PSM)?
A) A voting mechanism B) 1:1 swap between USDC and DAI
C) An insurance fund D) A liquidation bot
Answer: B – PSM allows swapping USDC for DAI 1:1, backstopping large depegs.

Q12. What is the trade-off of using the PSM in MakerDAO?
A) Higher fees B) Lower liquidity
C) Improved stability but increased centralization D) Faster transactions
Answer: C – PSM relies on USDC (centralized), reducing DAI's decentralization.

Q13. How do algorithmic stablecoins theoretically maintain their peg?
A) Fiat reserves B) Supply adjustments (mint/burn)
C) Overcollateralization D) Central bank intervention
Answer: B – They increase supply when price ¿ \$1, decrease when price ¡ \$1.

Q14. Which algorithmic stablecoin failed spectacularly in May 2022?
A) USDC B) DAI C) Terra UST D) FRAX
Answer: C – Terra UST collapsed in a death spiral, losing its peg completely.

Q15. What is a "death spiral" in algorithmic stablecoins?
A) Slow decline in price B) Depeg triggers sister token dilution, accelerating collapse
C) Government shutdown D) Network congestion
Answer: B – Loss of confidence causes selling, sister token crashes, spiral to zero.

Quiz Questions (16–20)

Q16. What is the root cause of algorithmic stablecoin failures?
A) Poor marketing B) No intrinsic backing or demand floor
C) High transaction fees D) Slow block times
Answer: B – They rely entirely on confidence; once lost, there's no recovery mechanism.

Q17. What percentage of Tether's (USDT) reserves are in US Treasuries?
A) 20% B) 50% C) 80%+ D) 0%
Answer: C – Tether shifted to 80%+ US Treasuries after 2022 criticism.

Q18. Which stablecoin was shut down in February 2023 due to regulatory pressure?
A) USDT B) USDC C) DAI D) BUSD
Answer: D – BUSD was shut down following regulatory action.

Q19. Under EU MiCA regulation (Dec 2024), what happened to USDT?
A) Approved for all EU exchanges B) Delisted from major EU exchanges
C) Given special exemption D) Banned globally
Answer: B – USDT was delisted from EU exchanges like Coinbase and Kraken EU.

Q20. Which stablecoin became MiCA-compliant with an EMI license in July 2024?
A) USDT B) DAI C) USDC D) FRAX
Answer: C – Circle's USDC obtained EMI license and became MiCA-compliant.

Quiz: Stablecoin Mechanisms

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of a stablecoin?

A) Maximize returns B) Maintain stable value relative to $1 USD C) Replace Bitcoin D) Eliminate fees

Quiz (1–5)

Q1. What is the primary purpose of a stablecoin?
A) Maximize returns B) Maintain stable value relative to $1 USD C) Replace Bitcoin D) Eliminate fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD

Quiz (1–5)

Q1. What is the primary purpose of a stablecoin?
A) Maximize returns B) Maintain stable value relative to $1 USD C) Replace Bitcoin D) Eliminate fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) dominates with 59% market share ($187B).

Q3. What does the stablecoin trilemma state?
A) All stablecoins will fail B) Only 3 can exist C) Can't achieve stability + decentralization + efficiency
D) Need 3 collateral types

Quiz (1–5)

Q1. What is the primary purpose of a stablecoin?
A) Maximize returns B) Maintain stable value relative to $1 USD C) Replace Bitcoin D) Eliminate fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) dominates with 59% market share ($187B).

Q3. What does the stablecoin trilemma state?
A) All stablecoins will fail B) Only 3 can exist C) Can't achieve stability + decentralization + efficiency
D) Need 3 collateral types
Answer: C – Each stablecoin type sacrifices one of the three properties.

Q4. How does a fiat-backed stablecoin maintain its peg?
A) Algorithmic supply adjustments B) 1:1 backing with USD reserves C) Overcollateralized crypto D) Community voting

Quiz (1–5)

Q1. What is the primary purpose of a stablecoin?
A) Maximize returns B) Maintain stable value relative to $1 USD C) Replace Bitcoin D) Eliminate fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) dominates with 59% market share ($187B).

Q3. What does the stablecoin trilemma state?
A) All stablecoins will fail B) Only 3 can exist C) Can't achieve stability + decentralization + efficiency
D) Need 3 collateral types
Answer: C – Each stablecoin type sacrifices one of the three properties.

Q4. How does a fiat-backed stablecoin maintain its peg?
A) Algorithmic supply adjustments B) 1:1 backing with USD reserves C) Overcollateralized crypto D) Community voting
Answer: B – Users deposit $1 fiat, issuer mints 1 token backed by reserves.

Q5. What is the main disadvantage of fiat-backed stablecoins?
A) High volatility B) Centralization and counterparty risk C) Low liquidity D) No use case

Quiz (1–5)

Q1. What is the primary purpose of a stablecoin?
A) Maximize returns B) Maintain stable value relative to $1 USD C) Replace Bitcoin D) Eliminate fees
Answer: B – Stablecoins are designed to maintain price stability, avoiding crypto volatility.

Q2. Which stablecoin has the largest market share?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) dominates with 59% market share ($187B).

Q3. What does the stablecoin trilemma state?
A) All stablecoins will fail B) Only 3 can exist C) Can't achieve stability + decentralization + efficiency
D) Need 3 collateral types
Answer: C – Each stablecoin type sacrifices one of the three properties.

Q4. How does a fiat-backed stablecoin maintain its peg?
A) Algorithmic supply adjustments B) 1:1 backing with USD reserves C) Overcollateralized crypto D) Community voting
Answer: B – Users deposit $1 fiat, issuer mints 1 token backed by reserves.

Q5. What is the main disadvantage of fiat-backed stablecoins?
A) High volatility B) Centralization and counterparty risk C) Low liquidity D) No use case
Answer: B – They are centralized and require trust in the issuer to maintain reserves.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure C) Silicon Valley Bank collapse D) Regulatory ban

Quiz (6–10)

Q6. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q7. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets C) No collateral D) Government bonds

Quiz (6–10)

Q6. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q7. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets C) No collateral D) Government bonds
Answer: B – Users deposit $150 ETH to mint $100 DAI (150% collateralization).

Q8. Which algorithmic stablecoin failed spectacularly in May 2022?
A) USDC B) DAI C) Terra UST D) FRAX

Quiz (6–10)

Q6. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q7. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets C) No collateral D) Government bonds
Answer: B – Users deposit $150 ETH to mint $100 DAI (150% collateralization).

Q8. Which algorithmic stablecoin failed spectacularly in May 2022?
A) USDC B) DAI C) Terra UST D) FRAX
Answer: C – Terra UST collapsed in a death spiral, destroying $40B+.

Q9. What is a "death spiral" in algorithmic stablecoins?
A) Slow decline B) Depeg triggers sister token dilution, accelerating collapse C) Government shutdown
D) Network congestion

Quiz (6–10)

Q6. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q7. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets C) No collateral D) Government bonds
Answer: B – Users deposit $150 ETH to mint $100 DAI (150% collateralization).

Q8. Which algorithmic stablecoin failed spectacularly in May 2022?
A) USDC B) DAI C) Terra UST D) FRAX
Answer: C – Terra UST collapsed in a death spiral, destroying $40B+.

Q9. What is a "death spiral" in algorithmic stablecoins?
A) Slow decline B) Depeg triggers sister token dilution, accelerating collapse C) Government shutdown
D) Network congestion
Answer: B – Loss of confidence causes selling, sister token crashes, spiral to zero.

Q10. Which stablecoin became MiCA-compliant with an EMI license in July 2024?
A) USDT B) DAI C) USDC D) FRAX

Quiz (6–10)

Q6. What caused USDC to depeg to $0.87 in March 2023?
A) Hacker attack B) Algorithmic failure C) Silicon Valley Bank collapse D) Regulatory ban
Answer: C – Circle had $3.3B at SVB; recovered after Fed guarantee.

Q7. How does a crypto-backed stablecoin like DAI work?
A) 1:1 fiat backing B) Overcollateralized with crypto assets C) No collateral D) Government bonds
Answer: B – Users deposit $150 ETH to mint $100 DAI (150% collateralization).

Q8. Which algorithmic stablecoin failed spectacularly in May 2022?
A) USDC B) DAI C) Terra UST D) FRAX
Answer: C – Terra UST collapsed in a death spiral, destroying $40B+.

Q9. What is a "death spiral" in algorithmic stablecoins?
A) Slow decline B) Depeg triggers sister token dilution, accelerating collapse C) Government shutdown
D) Network congestion
Answer: B – Loss of confidence causes selling, sister token crashes, spiral to zero.

Q10. Which stablecoin became MiCA-compliant with an EMI license in July 2024?
A) USDT B) DAI C) USDC D) FRAX
Answer: C – Circle's USDC obtained EMI license and became MiCA-compliant.

L39: Terra/Luna Case Study

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

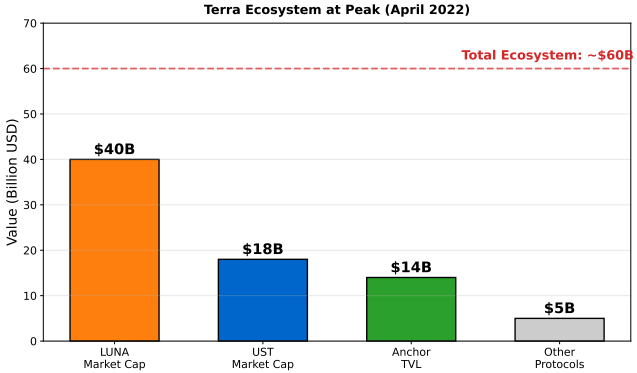
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Describe the Terra/Luna mechanism (UST + LUNA)
- Analyze Anchor Protocol's 20% APY promise
- Trace the death spiral timeline (May 2022)
- Extract lessons for algorithmic stablecoin design

Terra Ecosystem at Peak



Peak (April 2022): UST $18B, LUNA $40B. Collapsed in 72 hours.

The UST-LUNA Mechanism

Algorithmic Stability: UST pegged to $1 through arbitrage with LUNA.

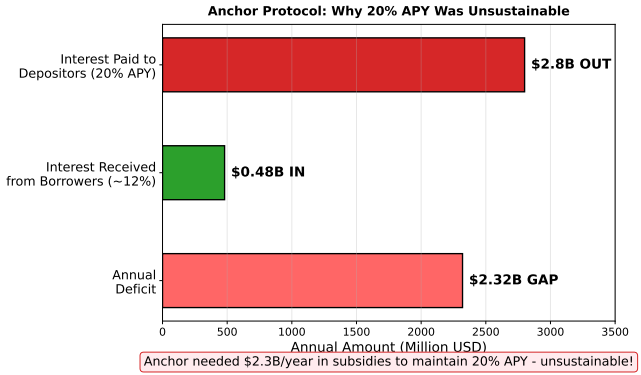
Mechanism:

1. **Mint UST:** Burn $1 of LUNA, create 1 UST
2. **Burn UST:** Burn 1 UST, create $1 of LUNA

If UST ¿ $1: Burn LUNA → mint UST → sell → profit
If UST ¡ $1: Buy UST → burn → mint LUNA → profit

Fatal Flaw: Only works if LUNA maintains value!

Anchor Protocol: The 20% APY Trap



Reality: Borrowers paid 10-15%; Anchor subsidized gap. Yield reserve burning \$50-100M/month.

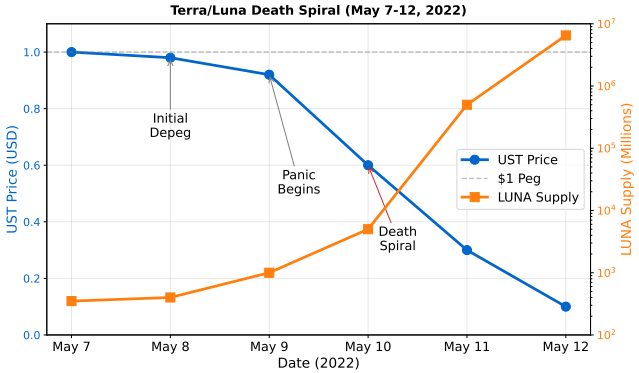
The Death Spiral

Death Spiral Logic:

1. UST depegs below $1 (e.g., $0.90)
2. Arbitrageurs burn UST, mint LUNA
3. Massive LUNA supply increase (dilution)
4. LUNA price crashes
5. Confidence in UST collapses
6. More UST selling, deeper depeg
7. Cycle repeats, accelerating downward

Analogy: Defending currency by printing more currency.

Death Spiral Timeline



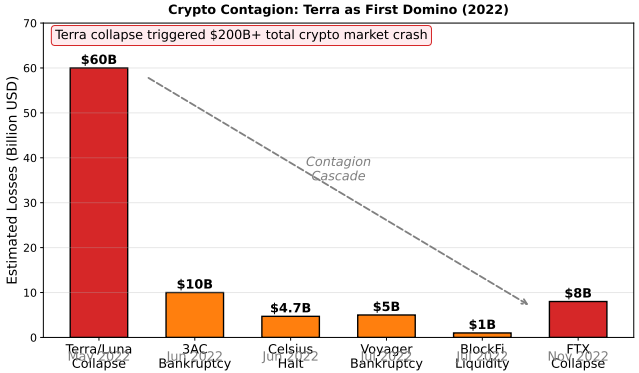
LUNA supply: 350M $\rightarrow$ 6.5 trillion tokens in 5 days.

The Collapse (May 7-12, 2022)

May 7-8: Large UST withdrawals ($2B+), UST briefly at $0.98
May 9: Panic begins. UST $0.92, LUNA drops 30%
May 10: Death spiral accelerates. UST $0.60, LUNA from $60 to $1
May 11-12: Total collapse. UST $0.01, LUNA $0.0001. Chain halted.

Losses: $40B+ in investor losses. Bitcoin reserve ($1.5B) failed to save peg.

Contagion Cascade



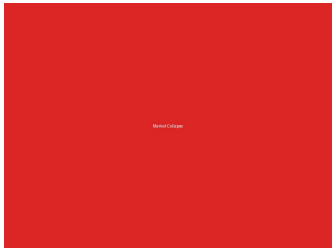
Terra → 3AC → Celsius/Voyager/BlockFi: First domino of 2022 crypto crisis.

Key Takeaways

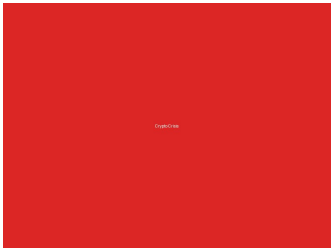
1. **Death Spiral:** Pure algorithmic stablecoins have no demand floor
2. **20% APY:** Unsustainable yield was Ponzi-like (new deposits paid old)
3. **Collapse:** $60B ecosystem destroyed in 72 hours (May 2022)
4. **Reserves Failed:** $3B BTC reserve couldn't stop panic
5. **Contagion:** Terra collapse triggered 3AC, Celsius, Voyager failures

Lesson: Sustainable yield ¡ protocol revenue; collateral ¿ algorithmic promises.

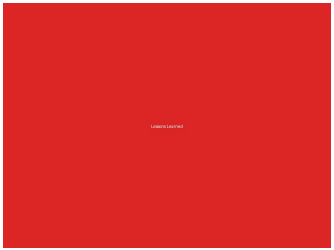
Terra Luna Collapse



Market Collapse



Crypto Crisis



Lessons Learned

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What was UST?
A) Fiat-backed stablecoin B) Algorithmic stablecoin C) Crypto-backed D) CBDC

Quiz (1/2)

Q1. What was UST?
A) Fiat-backed stablecoin B) Algorithmic stablecoin C) Crypto-backed D) CBDC
Answer: B – UST was an algorithmic stablecoin pegged via LUNA.

Q2. Peak combined market cap of UST + LUNA?
A) $10B B) $30B C) $60B D) $100B

Quiz (1/2)

Q1. What was UST?
A) Fiat-backed stablecoin B) Algorithmic stablecoin C) Crypto-backed D) CBDC
Answer: B – UST was an algorithmic stablecoin pegged via LUNA.

Q2. Peak combined market cap of UST + LUNA?
A) $10B B) $30B C) $60B D) $100B
Answer: C – UST $18B + LUNA $40B = $60B.

Q3. What APY did Anchor Protocol promise?
A) 5% B) 10% C) 20% D) 50%

Quiz (1/2)

Q1. What was UST?
A) Fiat-backed stablecoin B) Algorithmic stablecoin C) Crypto-backed D) CBDC
Answer: B – UST was an algorithmic stablecoin pegged via LUNA.

Q2. Peak combined market cap of UST + LUNA?
A) $10B B) $30B C) $60B D) $100B
Answer: C – UST $18B + LUNA $40B = $60B.

Q3. What APY did Anchor Protocol promise?
A) 5% B) 10% C) 20% D) 50%
Answer: C – 20% APY on UST deposits.

Q4. Why was 20% APY unsustainable?
A) Too many users B) Borrowers only paid 10-15% C) Gas fees D) Regulations

Quiz (1/2)

Q1. What was UST?
A) Fiat-backed stablecoin B) Algorithmic stablecoin C) Crypto-backed D) CBDC
Answer: B – UST was an algorithmic stablecoin pegged via LUNA.

Q2. Peak combined market cap of UST + LUNA?
A) $10B B) $30B C) $60B D) $100B
Answer: C – UST $18B + LUNA $40B = $60B.

Q3. What APY did Anchor Protocol promise?
A) 5% B) 10% C) 20% D) 50%
Answer: C – 20% APY on UST deposits.

Q4. Why was 20% APY unsustainable?
A) Too many users B) Borrowers only paid 10-15% C) Gas fees D) Regulations
Answer: B – Anchor subsidized the gap; yield reserve burning $50-100M/month.

Q5. What caused the death spiral?
A) Hack B) Minting LUNA diluted its value C) Regulation D) Team exit

Quiz (1/2)

Q1. What was UST?
A) Fiat-backed stablecoin B) Algorithmic stablecoin C) Crypto-backed D) CBDC
Answer: B – UST was an algorithmic stablecoin pegged via LUNA.

Q2. Peak combined market cap of UST + LUNA?
A) $10B B) $30B C) $60B D) $100B
Answer: C – UST $18B + LUNA $40B = $60B.

Q3. What APY did Anchor Protocol promise?
A) 5% B) 10% C) 20% D) 50%
Answer: C – 20% APY on UST deposits.

Q4. Why was 20% APY unsustainable?
A) Too many users B) Borrowers only paid 10-15% C) Gas fees D) Regulations
Answer: B – Anchor subsidized the gap; yield reserve burning $50-100M/month.

Q5. What caused the death spiral?
A) Hack B) Minting LUNA diluted its value C) Regulation D) Team exit
Answer: B – UST depeg $\rightarrow$ mint LUNA $\rightarrow$ LUNA crashes $\rightarrow$ deeper depeg.

Quiz (2/2)

Q6. How long did the collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month

Quiz (2/2)

Q6. How long did the collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – $60B ecosystem collapsed in about 72 hours.

Q7. What did LFG deploy to save the peg?
A) More LUNA B) Bitcoin reserves C) USDC D) Nothing

Quiz (2/2)

Q6. How long did the collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – $60B ecosystem collapsed in about 72 hours.

Q7. What did LFG deploy to save the peg?
A) More LUNA B) Bitcoin reserves C) USDC D) Nothing
Answer: B – $1.5B in BTC, but failed to stop panic.

Q8. What happened to LUNA supply during collapse?
A) Stayed same B) Decreased C) Grew from 350M to 6.5T D) Burned

Quiz (2/2)

Q6. How long did the collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – $60B ecosystem collapsed in about 72 hours.

Q7. What did LFG deploy to save the peg?
A) More LUNA B) Bitcoin reserves C) USDC D) Nothing
Answer: B – $1.5B in BTC, but failed to stop panic.

Q8. What happened to LUNA supply during collapse?
A) Stayed same B) Decreased C) Grew from 350M to 6.5T D) Burned
Answer: C – Massive hyperinflation from arbitrage minting.

Q9. Which fund collapsed after Terra?
A) Binance B) Three Arrows Capital (3AC) C) Coinbase D) Kraken

Quiz (2/2)

Q6. How long did the collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – $60B ecosystem collapsed in about 72 hours.

Q7. What did LFG deploy to save the peg?
A) More LUNA B) Bitcoin reserves C) USDC D) Nothing
Answer: B – $1.5B in BTC, but failed to stop panic.

Q8. What happened to LUNA supply during collapse?
A) Stayed same B) Decreased C) Grew from 350M to 6.5T D) Burned
Answer: C – Massive hyperinflation from arbitrage minting.

Q9. Which fund collapsed after Terra?
A) Binance B) Three Arrows Capital (3AC) C) Coinbase D) Kraken
Answer: B – 3AC had billions in LUNA exposure; went bankrupt.

Q10. Key lesson from Terra collapse?
A) Algorithms are perfect B) 20% APY is safe C) Collateral ¿ algorithmic promises D) BTC always saves pegs

Quiz (2/2)

Q6. How long did the collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – $60B ecosystem collapsed in about 72 hours.

Q7. What did LFG deploy to save the peg?
A) More LUNA B) Bitcoin reserves C) USDC D) Nothing
Answer: B – $1.5B in BTC, but failed to stop panic.

Q8. What happened to LUNA supply during collapse?
A) Stayed same B) Decreased C) Grew from 350M to 6.5T D) Burned
Answer: C – Massive hyperinflation from arbitrage minting.

Q9. Which fund collapsed after Terra?
A) Binance B) Three Arrows Capital (3AC) C) Coinbase D) Kraken
Answer: B – 3AC had billions in LUNA exposure; went bankrupt.

Q10. Key lesson from Terra collapse?
A) Algorithms are perfect B) 20% APY is safe C) Collateral ¿ algorithmic promises D) BTC always saves pegs
Answer: C – Sustainable yield must be ¡ protocol revenue; need real collateral.

Thank you

Questions?

Next: L40 Lab – Testnet Lending

L39: Case Study - Terra/Luna Collapse

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Describe the Terra/Luna mechanism (UST stablecoin + LUNA token)
- Analyze the Anchor Protocol's 20% APY promise
- Trace the death spiral timeline (May 2022)
- Identify systemic risks and warning signs
- Extract lessons for DeFi stability and sustainability

(c) Joerg Osterrieder 2025

The Problem: What happens when stablecoins fail?

The Challenge
What happens when a $60 billion stablecoin ecosystem collapses in 72 hours? Terra/Luna's death spiral represents the largest cryptoeconomic failure mode in DeFi history – a case study in systemic risk, reflexive dynamics, and misaligned incentives.

Why It Matters

- $40B+ investor losses, triggering crypto contagion (3AC, Celsius, Voyager)
- Regulatory catalyst: MiCA reserve requirements, SEC fraud charges
- Historical lesson: Anchor's 20% APY, algorithmic peg failure, death spiral mechanics

What We Need

- Risk management and mitigation
- Understanding of reflexive feedback loops in algorithmic stablecoins
- Ability to distinguish sustainable vs. unsustainable yield mechanisms

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks: How do we design stable value without collateral?

Today's lesson: How Terra/Luna's cryptoeconomic design flaws led to catastrophic failure

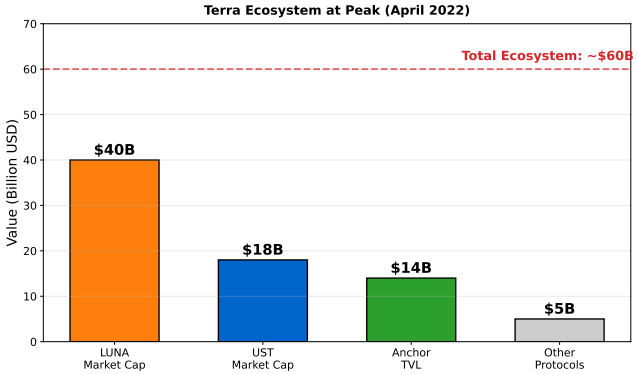
Terra Ecosystem Overview

Key Components:

- **UST (TerraUSD):** Algorithmic stablecoin pegged to $1
- **LUNA:** Native token of Terra blockchain, used to stabilize UST
- **Anchor Protocol:** Lending platform offering 20% APY on UST deposits

Creator: Do Kwon (Terraform Labs)
Peak Market Cap (April 2022): UST: $18B, LUNA: $40B
Collapse (May 2022): Both went to near-zero in 72 hours.

Terra Ecosystem at Peak



Combined $60B ecosystem collapsed in just 72 hours in May 2022

The UST-LUNA Mechanism

Algorithmic Stability: UST maintains $1 peg through arbitrage with LUNA.

Mechanism:

1. **Mint UST:** Burn $1 of LUNA, mint 1 UST
2. **Burn UST:** Burn 1 UST, mint $1 of LUNA

If UST ¿ $1: Burn LUNA $\rightarrow$ mint UST $\rightarrow$ sell UST $\rightarrow$ profit
If UST ¡ $1: Buy UST $\rightarrow$ burn UST $\rightarrow$ mint LUNA $\rightarrow$ profit

Problem: Only works if LUNA maintains value!

(c) Joerg Osterrieder 2025

The Fatal Flaw: Death Spiral

Death Spiral Logic:

1. UST depegs below $1 (e.g., $0.90)
2. Arbitrageurs burn UST, mint LUNA
3. Massive LUNA supply increase (dilution)
4. LUNA price crashes
5. Confidence in UST collapses
6. More UST selling, deeper depeg
7. Cycle repeats, accelerating downward

Analogy: Like a central bank defending currency by printing more currency.
Critical Insight: Pure algorithmic stablecoins have no demand floor.

Anchor Protocol: The 20% APY Trap

Promise: Earn 20% APY by depositing UST.

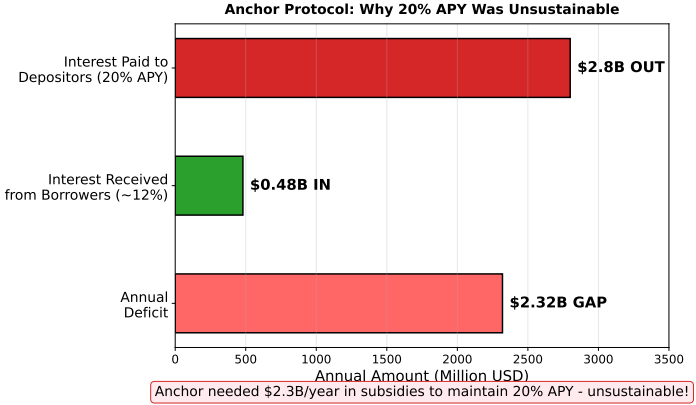
How It Worked:

- Users deposit UST into Anchor
- Anchor lends UST to borrowers (collateralized by staked LUNA)
- Borrowers pay interest (10-15%)
- **Gap:** Anchor subsidized difference to reach 20%

Red Flags:

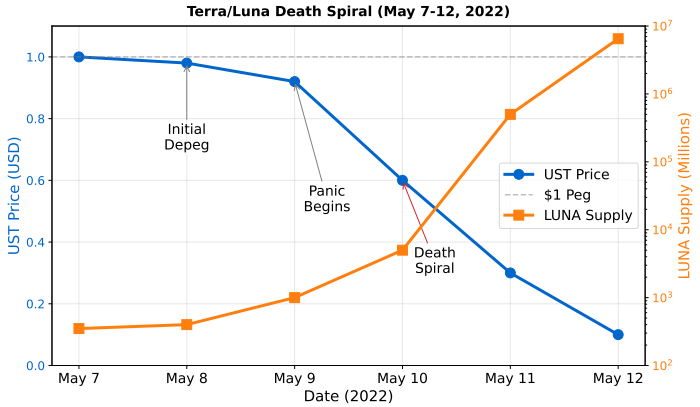
- Yield reserve burning $50-100M per month
- Projected to run out by mid-2022

Why 20% APY Was Unsustainable



Anchor was a Ponzi-like scheme: new deposits paid old depositors

The Death Spiral (May 7-12, 2022)



As UST depegged, LUNA supply exploded from 350M to 6.5 trillion tokens

Timeline: The Collapse

May 7-8: Initial Depeg

- Large UST withdrawals from Anchor ($2B+ in 48 hours)
- UST briefly drops to $0.98

May 9: Panic Begins

- UST falls to $0.92, LUNA drops 30%

May 10: Death Spiral Accelerates

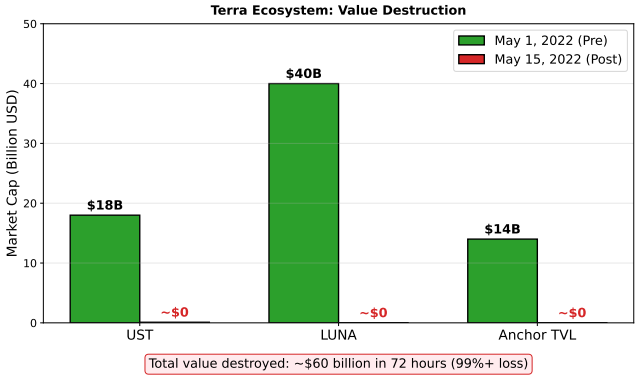
- UST at $0.60, LUNA collapses from $60 to $1

May 11-12: Total Collapse

- UST at $0.01, LUNA at $0.0001
- Terra blockchain halted

(c) Joerg Osterrieder 2025

Value Destruction



Estimated $40B+ in investor losses; triggered broader crypto contagion

Bitcoin Reserve: Failed Rescue

Luna Foundation Guard (LFG):

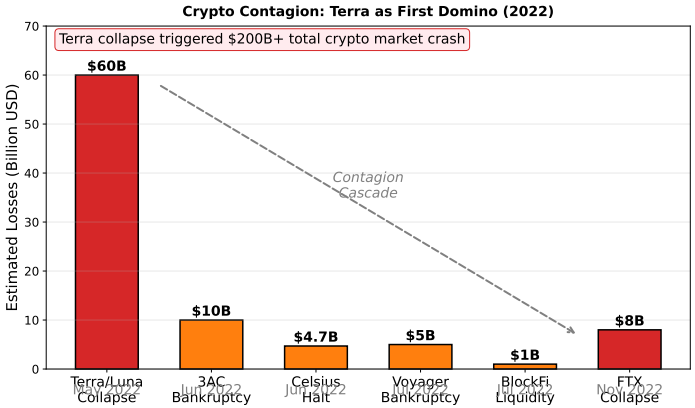
- Reserve fund with $3B+ in Bitcoin, AVAX
- Plan: If UST depegs, sell BTC to buy UST

Reality (May 2022):

- LFG deployed $1.5B BTC to buy UST
- Ineffective: Death spiral too fast
- Lost most of the BTC (sold near bottom)

Lesson: Finite reserves cannot defend algorithmic peg under mass panic.

Contagion: First Domino



Terra collapse caused 3AC bankruptcy, which triggered Celsius/Voyager failures

Three Arrows Capital (3AC) Contagion

Connection:

- 3AC was major LUNA investor (billions in exposure)

Cascade:

1. LUNA collapses (May 2022)
2. 3AC's collateral becomes worthless
3. 3AC fails margin calls on other loans
4. Lenders (BlockFi, Celsius, Voyager) take massive losses
5. 3AC declares bankruptcy (July 2022)

Lesson: Interconnected leverage amplifies failures.

Do Kwon's Hubris

Quotes (Pre-Collapse):

- "I don't debate the poor." (Twitter, responding to critics)
- "95% of stablecoins will fail, UST will win."

Behavior:

- Dismissed warnings from economists, DeFi experts
- Promised unrealistic yields (20% Anchor)

Legal Aftermath:

- SEC charged Do Kwon with fraud (2023)
- Arrested in Montenegro (March 2023), extradited to US
- Sentenced to 15 years in prison (December 2025) for "fraud on epic scale"

Warning Signs (In Hindsight)

Red Flags That Were Ignored:

1. **Unsustainable Yield:** 20% APY with no underlying revenue
2. **Algorithmic Design Flaw:** No collateral, death spiral risk
3. **Concentration Risk:** 78% of UST locked in Anchor
4. **Hubris:** Founder ignored criticism, attacked skeptics
5. **Rapid Growth:** UST grew from $2B to $18B in 6 months
6. **Lack of Stress Testing:** No proven resilience

(c) Joerg Osterrieder 2025

Lessons Learned

For Investors:

- Beware of unsustainable yields (¿10% on stablecoins)
- Algorithmic stablecoins are experimental and risky
- Hubris and dismissiveness are red flags

For Protocols:

- Overcollateralization is necessary for stability
- Stress test designs under extreme scenarios

For Regulators:

- Algorithmic stablecoins pose systemic risk
- Consider reserve requirements for stablecoins

Survivor: DAI vs. UST

Why did DAI survive while UST collapsed?

UST (Failed)

- No collateral
- Pure algorithm
- Death spiral possible
- Unsustainable yield

DAI (Survived)

- 150%+ overcollateralized
- Backed by ETH, USDC
- Liquidations prevent spiral
- No unrealistic yields

Key Difference: Collateral provides demand floor.
Conclusion: Overcollateralization is inefficient but necessary.

(c) Joerg Osterrieder 2025

Terra 2.0: Failed Reboot

Post-Collapse Plan (May 2022):

- Abandon UST stablecoin
- Relaunch Terra blockchain as "Terra 2.0"
- Airdrop to UST/LUNA holders

Result:

- Terra 2.0 launched with minimal adoption
- New LUNA price: \$6 $\rightarrow$ \$0.50 (within months)
- Community fractured, trust destroyed

Lesson: Trust, once broken, is nearly impossible to rebuild.

Regulatory Fallout

US Response:

- SEC charged Do Kwon with fraud
- Proposed legislation requiring reserve backing

Global Response:

- South Korea: Investigation into Terraform Labs
- EU MiCA: Included stablecoin reserve requirements

Industry Impact:

- Algorithmic stablecoins largely abandoned
- FRAX increased collateral ratio to 100%
- Focus shifted to fiat-backed and overcollateralized models

(c) Joerg Osterrieder 2025

Psychological Factors

Why Did People Believe?

1. **Greed:** 20% APY too attractive to pass up
2. **FOMO:** Fear of missing "next big thing"
3. **Herd Mentality:** Everyone else was buying
4. **Confirmation Bias:** Only listened to bulls
5. **Complexity:** Most users didn't understand the mechanism
6. **Charismatic Leader:** Do Kwon's confidence was persuasive

Lesson: If it sounds too good to be true, it probably is.

Problem Solved? Terra/Luna Case Study

The Original Problem

What happens when stablecoins fail? Can algorithmic pegs work without collateral?

How Terra/Luna Attempted to Solve It

- **Algorithmic peg via mint/burn arbitrage:** Burn $1 LUNA → mint 1 UST (and vice versa)
- **Anchor's 20% yield attracted massive deposits:** $18B UST supply (78% locked in Anchor)
- **Bitcoin reserve ($3B LFG):** Intended as emergency backstop for depeg defense

Remaining Limitations

- **Reflexive death spiral:** Depeg → LUNA dilution → confidence collapse → deeper depeg
- **No collateral backing:** Pure algorithmic peg has no demand floor under panic
- **Unsustainable subsidies:** 20% APY required $50-100M/month burn rate

Open Questions

- **Are algorithmic stablecoins inherently unstable?** No successful pure-algorithmic design exists post-Terra
- **Risk:** Black swan events (bank run), cascading contagion (3AC → Celsius), regulatory crackdown

Terra/Luna proved algorithmic stablecoins without collateral cannot survive reflexive runs – $40B lesson learned

Summary

Key Takeaways:

- Terra/Luna was $60B algorithmic stablecoin experiment that collapsed in May 2022
- UST-LUNA mechanism relied on arbitrage but had no collateral backing
- Anchor's 20% APY was unsustainable Ponzi-like scheme
- Death spiral: UST depeg $\rightarrow$ LUNA hyperinflation $\rightarrow$ total collapse
- $40B+ value destroyed, triggering broader crypto contagion
- Lessons: Beware unsustainable yields, algorithmic stablecoins need collateral

Next Lecture: Lab - Testnet Lending (hands-on with Aave).

Questions for Reflection

1. What structural difference between DAI and UST prevented DAI from collapsing?
2. Could the Bitcoin reserve have saved UST if it were larger (e.g., $20B)?
3. Why did Anchor's 20% APY attract deposits despite being unsustainable?
4. How could regulators have prevented Terra collapse without banning innovation?
5. Would you invest in a new algorithmic stablecoin if it had better design?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What was the peak combined market cap of UST and LUNA in April 2022?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA algorithmic peg mechanism work?
A) UST backed by USD reserves B) LUNA backed by gold C) Burn $1 LUNA to mint 1 UST D) Fixed exchange rate
Answer: C – Users could burn $1 worth of LUNA to mint 1 UST, and vice versa, creating arbitrage opportunities.

Q3. What APY did Anchor Protocol promise on UST deposits?
A) 5% B) 10% C) 20% D) 50%
Answer: C – Anchor offered approximately 20% APY, which was unsustainable and required subsidy.

Q4. What percentage of UST supply was concentrated in Anchor Protocol?
A) 25% B) 50% C) 78% D) 90%
Answer: C – About 78% of UST was locked in Anchor, creating massive concentration risk.

Q5. How long did the Terra/Luna collapse take from initial depeg to near-zero?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – The collapse occurred over approximately 72 hours (May 7-12, 2022).

Quiz Questions (6–10)

Q6. What was the fundamental flaw in UST's algorithmic design?
A) Too many validators B) High transaction fees C) No collateral backing D) Slow block times
Answer: C – UST had no collateral; it relied entirely on LUNA's value, which created death spiral risk.

Q7. What happened to LUNA's token supply during the death spiral?
A) Decreased to zero B) Stayed constant C) Increased from 350M to 6.5 trillion D) Halved
Answer: C – LUNA supply exploded from 350 million to 6.5 trillion as UST holders redeemed for LUNA.

Q8. How much Bitcoin did the Luna Foundation Guard deploy to defend the peg?
A) $500M B) $1.5B C) $5B D) $10B
Answer: B – LFG deployed approximately $1.5B in BTC to buy UST, but it was ineffective.

Q9. Which major crypto fund collapsed due to exposure to LUNA?
A) Alameda Research B) Three Arrows Capital (3AC) C) FTX D) Binance
Answer: B – 3AC had billions in LUNA exposure and declared bankruptcy in July 2022.

Q10. At what price did UST fall to during the collapse?
A) $0.50 B) $0.10 C) $0.01 D) Exactly $0
Answer: C – UST fell to approximately $0.01 by May 12, 2022.

Quiz Questions (11–15)

Q11. Who was the founder of Terra/Luna and Terraform Labs?
A) Vitalik Buterin B) Do Kwon C) Charles Hoskinson D) Sam Bankman-Fried
Answer: B – Do Kwon founded Terraform Labs and the Terra ecosystem.

Q12. What was Do Kwon's sentence for fraud in December 2025?
A) 5 years B) 10 years C) 15 years D) 25 years
Answer: C – Do Kwon was sentenced to 15 years in prison for "fraud on epic scale."

Q13. Why was Anchor's 20% APY considered unsustainable?
A) Backed by real revenue B) Required $50-100M/month subsidy C) Too low D) Regulated by SEC
Answer: B – Borrowers only paid 10-15%; Anchor subsidized the gap, burning reserves monthly.

Q14. How does DAI differ from UST in terms of stability mechanism?
A) Both algorithmic B) DAI is 150%+ overcollateralized C) DAI has no collateral D) Same design
Answer: B – DAI is overcollateralized with ETH/USDC, providing a demand floor that UST lacked.

Q15. What happened to Terra 2.0 after the relaunch?
A) Huge success B) Price fell from $6 to $0.50 C) Matched original LUNA D) Still thriving
Answer: B – Terra 2.0 had minimal adoption; price collapsed within months as trust was destroyed.

Quiz Questions (16–20)

Q16. Which regulatory framework included stablecoin reserve requirements after Terra?
A) Dodd-Frank B) Basel III C) EU MiCA D) Sarbanes-Oxley
Answer: C – EU's Markets in Crypto-Assets (MiCA) regulation included stablecoin reserve requirements.

Q17. What is a "death spiral" in the context of algorithmic stablecoins?
A) Rising prices B) Depeg causes LUNA dilution, accelerating collapse C) Stable growth D) Regulatory ban
Answer: B – UST depeg forces LUNA minting (dilution), crashing LUNA price, deepening UST depeg.

Q18. What psychological factor contributed most to Terra's initial growth?
A) Fear B) Regulatory clarity C) Greed (20% APY) D) Technical superiority
Answer: C – The promise of 20% APY was too attractive, driving massive deposits despite red flags.

Q19. Approximately how much value was destroyed in the Terra/Luna collapse?
A) $5B B) $10B C) $40B+ D) $100B
Answer: C – Over $40 billion in investor losses occurred during the May 2022 collapse.

Q20. What key lesson did the industry learn about algorithmic stablecoins?
A) They're superior B) Collateralization is necessary C) 20% yields are achievable D) Regulation is unnecessary
Answer: B – The collapse proved that overcollateralization, though inefficient, is necessary for stability.

L39: Case Study - Terra/Luna Collapse

Module E: DeFi Ecosystem

Blockchain & Cryptocurrency

December 2025

(c) Joerg Osterrieder 2025

Algorithmic Stability Promise

[COMIC: Algorithmic stability promise]

Placeholder for comic showing confident founder promising "Trust the algorithm, no collateral needed!" while skeptics point at math equations with question marks

The Setup

- "We don't need real backing"
- "Arbitrage keeps the peg"
- "The algorithm is self-correcting"

The Punchline

- Confidence-based stability
- Works until it doesn't
- No floor when panic hits

"Trust the algorithm" – famous last words of the $60B collapse

Learning Objectives

- Describe the Terra/Luna mechanism (UST stablecoin + LUNA token)
- Analyze the Anchor Protocol's 20% APY promise
- Trace the death spiral timeline (May 2022)
- Identify systemic risks and warning signs
- Extract lessons for DeFi stability and sustainability

Building on L38: Stablecoin Mechanisms

The Problem: What happens when stablecoins fail?

The Challenge
What happens when a $60 billion stablecoin ecosystem collapses in 72 hours? Terra/Luna's death spiral represents the largest cryptoeconomic failure mode in DeFi history – a case study in systemic risk, reflexive dynamics, and misaligned incentives.

Why It Matters

- $40B+ investor losses, triggering crypto contagion (3AC, Celsius, Voyager)
- Regulatory catalyst: MiCA reserve requirements, SEC fraud charges
- Historical lesson: Anchor's 20% APY, algorithmic peg failure, death spiral mechanics

What We Need

- Risk management and mitigation
- Understanding of reflexive feedback loops in algorithmic stablecoins
- Ability to distinguish sustainable vs. unsustainable yield mechanisms

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks: How do we design stable value without collateral?

Today's lesson: How Terra/Luna's cryptoeconomic design flaws led to catastrophic failure

What Was Terra/Luna?

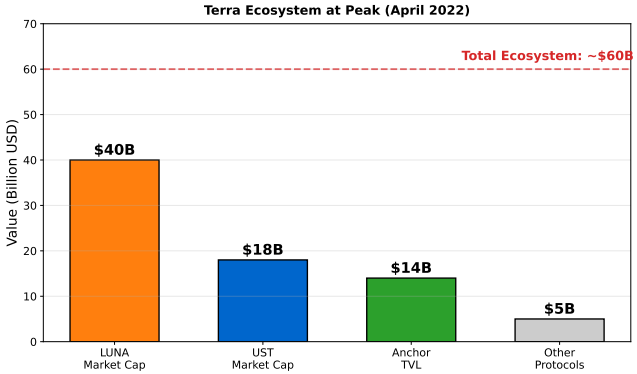
Key Components:

- **UST (TerraUSD):** Algorithmic stablecoin pegged to $1
- **LUNA:** Native token of Terra blockchain, used to stabilize UST
- **Anchor Protocol:** Lending platform offering 20% APY on UST deposits

Creator: Do Kwon (Terraform Labs)
Peak Market Cap (April 2022): UST: $18B, LUNA: $40B
Collapse (May 2022): Both went to near-zero in 72 hours.

→ *Problem: What happens when stablecoins fail? — Terra's $60B collapse shows billions lost in 72 hours.*

How Big Was the Terra Ecosystem?



Combined $60B ecosystem collapsed in just 72 hours in May 2022

How Did the UST-LUNA Peg Work?

Algorithmic Stability: UST maintains $1 peg through arbitrage with LUNA.

Mechanism:

1. **Mint UST:** Burn $1 of LUNA, mint 1 UST
2. **Burn UST:** Burn 1 UST, mint $1 of LUNA

If UST ¿ $1: Burn LUNA → mint UST → sell UST → profit
If UST ¡ $1: Buy UST → burn UST → mint LUNA → profit

Problem: Only works if LUNA maintains value!

What Is the Death Spiral Mechanism?

Death Spiral: A self-reinforcing collapse where falling prices trigger more selling, accelerating the downward spiral (death spiral = self-reinforcing collapse where falling prices trigger more selling).

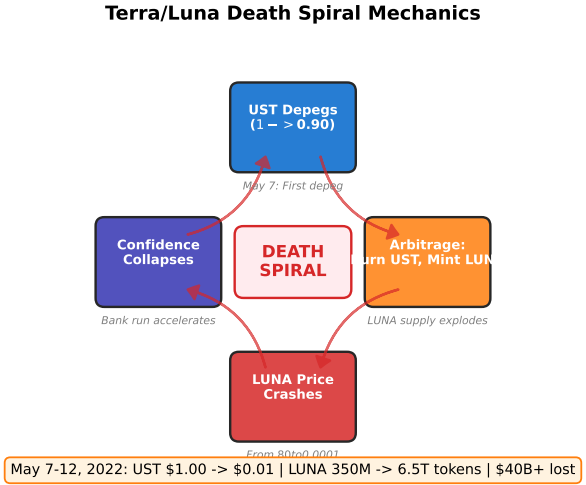
Death Spiral Logic:

1. UST depegs below $1 (e.g., $0.90)
2. Arbitrageurs burn UST, mint LUNA
3. Massive LUNA supply increase (dilution)
4. LUNA price crashes
5. Confidence in UST collapses
6. More UST selling, deeper depeg
7. Cycle repeats, accelerating downward

Analogy: Like a central bank defending currency by printing more currency.
Critical Insight: Pure algorithmic stablecoins have no demand floor.

(c) Joerg Osterrieder 2025

How Does the Death Spiral Work?



Self-reinforcing collapse: UST depeg triggers LUNA dilution, destroying confidence

Why Was 20% APY Too Good to Be True?

Promise: Earn 20% APY by depositing UST.

How It Worked:

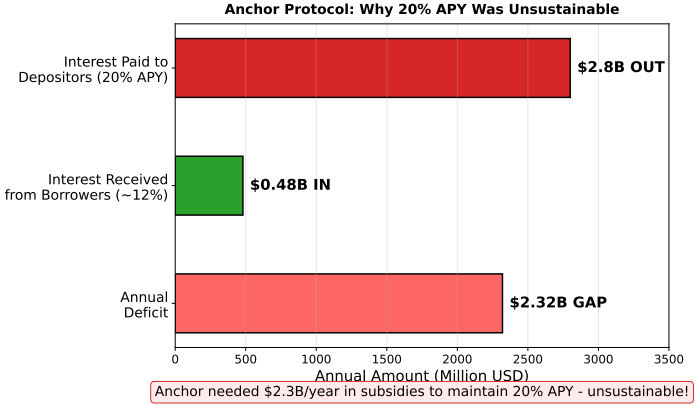
- Users deposit UST into Anchor
- Anchor lends UST to borrowers (collateralized by staked LUNA)
- Borrowers pay interest (10-15%)
- **Gap:** Anchor subsidized difference to reach 20%

Red Flags:

- Yield reserve burning $50-100M per month
- Projected to run out by mid-2022

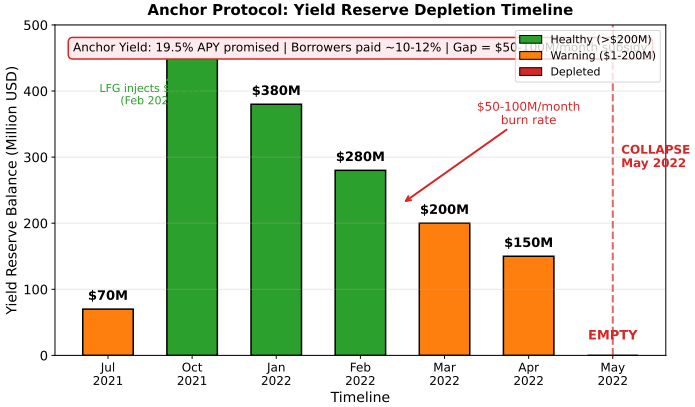
→ *Problem: What happens when stablecoins fail? — Anchor's 20% APY was unsustainable – high yields masked insolvency.*

How Did Anchor's Math Work?



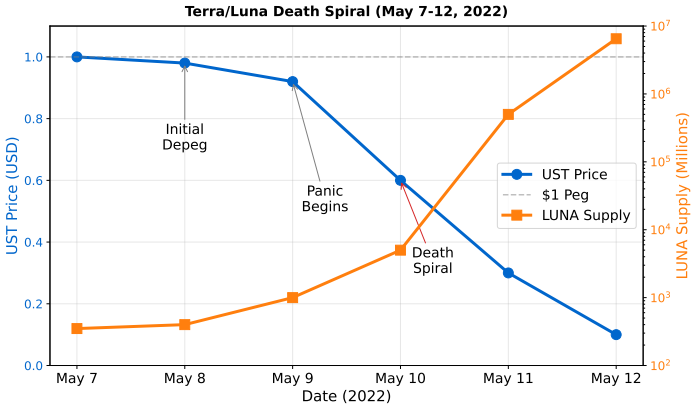
Anchor was a Ponzi-like scheme: new deposits paid old depositors

When Would Anchor's Reserves Run Out?



Yield reserve burned $50-100M/month; projected depletion by mid-2022

What Happened During the Collapse?



As UST depegged, LUNA supply exploded from 350M to 6.5 trillion tokens

How Did the Collapse Unfold?

May 7-8: Initial Depeg

- Large UST withdrawals from Anchor ($2B+ in 48 hours)
- UST briefly drops to $0.98

May 9: Panic Begins

- UST falls to $0.92, LUNA drops 30%

May 10: Death Spiral Accelerates

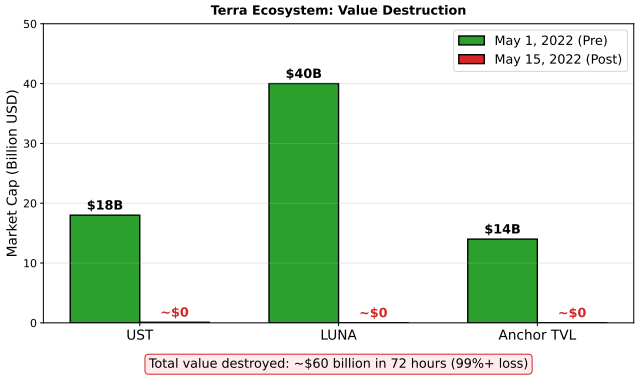
- UST at $0.60, LUNA collapses from $60 to $1

May 11-12: Total Collapse

- UST at $0.01, LUNA at $0.0001
- Terra blockchain halted

(c) Joerg Osterrieder 2025

How Much Value Was Destroyed?



Estimated $40B+ in investor losses; triggered broader crypto contagion

Problem Check-In: Terra/Luna Case Study

Recall Our Problem

What happens when stablecoins fail?

What We've Learned So Far

- UST-LUNA mechanism: burn $1 LUNA to mint 1 UST (and vice versa) – pure algorithm, no collateral
- Death spiral: when UST depegged, LUNA dilution accelerated, destroying confidence and value
- The mechanism explains HOW stablecoins fail: no collateral = no floor = spiral to zero

Still to Address

- Contagion effects: how Terra collapse triggered 3AC, Celsius, and broader crypto crash
- Could any algorithmic stablecoin design be made stable, or are they inherently flawed?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "What happens when stablecoins fail?"?

Why Didn't the Bitcoin Reserve Save UST?

Luna Foundation Guard (LFG):

- Reserve fund with $3B+ in Bitcoin, AVAX
- Plan: If UST depegs, sell BTC to buy UST

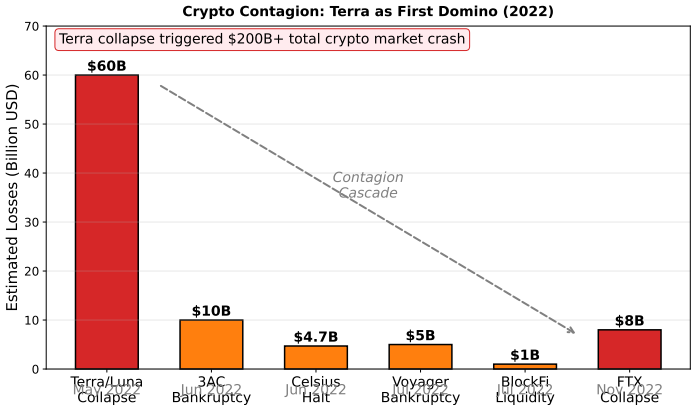
Reality (May 2022):

- LFG deployed $1.5B BTC to buy UST
- Ineffective: Death spiral too fast
- Lost most of the BTC (sold near bottom)

Lesson: Finite reserves cannot defend algorithmic peg under mass panic.

→ *Problem: What happens when stablecoins fail? — $1.5B reserve couldn't stop $60B bank run.*

How Did Contagion Spread?



Terra collapse caused 3AC bankruptcy, which triggered Celsius/Voyager failures

How Did Terra Trigger the Crypto Contagion?

Connection:

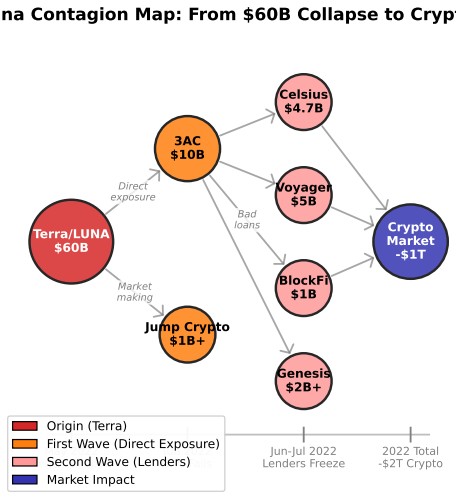
- 3AC was major LUNA investor (billions in exposure)

Cascade:

1. LUNA collapses (May 2022)
2. 3AC's collateral becomes worthless
3. 3AC fails margin calls on other loans
4. Lenders (BlockFi, Celsius, Voyager) take massive losses
5. 3AC declares bankruptcy (July 2022)

Lesson: Interconnected leverage amplifies failures.

Which Firms Failed From Terra?



Terra collapse triggered cascading failures: 3AC, Celsius, Voyager, BlockFi

What Role Did Do Kwon Play?

Quotes (Pre-Collapse):

- "I don't debate the poor." (Twitter, responding to critics)
- "95% of stablecoins will fail, UST will win."

Behavior:

- Dismissed warnings from economists, DeFi experts
- Promised unrealistic yields (20% Anchor)

Legal Aftermath:

- SEC charged Do Kwon with fraud (2023)
- Arrested in Montenegro (March 2023), extradited to US
- Sentenced to 15 years in prison (December 2025) for "fraud on epic scale"

What Were the Warning Signs?

Red Flags That Were Ignored:

1. **Unsustainable Yield:** 20% APY with no underlying revenue
2. **Algorithmic Design Flaw:** No collateral, death spiral risk
3. **Concentration Risk:** 78% of UST locked in Anchor
4. **Hubris:** Founder ignored criticism, attacked skeptics
5. **Rapid Growth:** UST grew from $2B to $18B in 6 months
6. **Lack of Stress Testing:** No proven resilience

(c) Joerg Osterrieder 2025

What Can We Learn From Terra?

For Investors:

- Beware of unsustainable yields (¿10% on stablecoins)
- Algorithmic stablecoins are experimental and risky
- Hubris and dismissiveness are red flags

For Protocols:

- Overcollateralization is necessary for stability
- Stress test designs under extreme scenarios

For Regulators:

- Algorithmic stablecoins pose systemic risk
- Consider reserve requirements for stablecoins

→ *Problem: What happens when stablecoins fail? — These lessons answer: mass losses, contagion, regulatory backlash.*

Why Did DAI Survive While UST Collapsed?

Why did DAI survive while UST collapsed?

UST (Failed)

- No collateral
- Pure algorithm
- Death spiral possible
- Unsustainable yield

DAI (Survived)

- 150%+ overcollateralized
- Backed by ETH, USDC
- Liquidations prevent spiral
- No unrealistic yields

Key Difference: Collateral provides demand floor.
Conclusion: Overcollateralization is inefficient but necessary.

(c) Joerg Osterrieder 2025

Did Terra 2.0 Succeed?

Post-Collapse Plan (May 2022):

- Abandon UST stablecoin
- Relaunch Terra blockchain as "Terra 2.0"
- Airdrop to UST/LUNA holders

Result:

- Terra 2.0 launched with minimal adoption
- New LUNA price: \$6 $\rightarrow$ \$0.50 (within months)
- Community fractured, trust destroyed

Lesson: Trust, once broken, is nearly impossible to rebuild.

How Did Regulators Respond?

US Response:

- SEC charged Do Kwon with fraud
- Proposed legislation requiring reserve backing

Global Response:

- South Korea: Investigation into Terraform Labs
- EU MiCA: Included stablecoin reserve requirements

Industry Impact:

- Algorithmic stablecoins largely abandoned
- FRAX increased collateral ratio to 100%
- Focus shifted to fiat-backed and overcollateralized models

Why Did People Believe in Terra?

Why Did People Believe?

1. **Greed:** 20% APY too attractive to pass up
2. **FOMO:** Fear of missing "next big thing"
3. **Herd Mentality:** Everyone else was buying
4. **Confirmation Bias:** Only listened to bulls
5. **Complexity:** Most users didn't understand the mechanism
6. **Charismatic Leader:** Do Kwon's confidence was persuasive

Lesson: If it sounds too good to be true, it probably is.

Problem Solved? Terra/Luna Case Study

The Original Problem

What happens when stablecoins fail? Can algorithmic pegs work without collateral?

How Terra/Luna Attempted to Solve It

- **Algorithmic peg via mint/burn arbitrage:** Burn $1 LUNA → mint 1 UST (and vice versa)
- **Anchor's 20% yield attracted massive deposits:** $18B UST supply (78% locked in Anchor)
- **Bitcoin reserve ($3B LFG):** Intended as emergency backstop for depeg defense

Remaining Limitations

- **Reflexive death spiral:** Depeg → LUNA dilution → confidence collapse → deeper depeg
- **No collateral backing:** Pure algorithmic peg has no demand floor under panic
- **Unsustainable subsidies:** 20% APY required $50-100M/month burn rate

Open Questions

- **Are algorithmic stablecoins inherently unstable?** No successful pure-algorithmic design exists post-Terra
- **Risk:** Black swan events (bank run), cascading contagion (3AC → Celsius), regulatory crackdown

Terra/Luna proved algorithmic stablecoins without collateral cannot survive reflexive runs – $40B lesson learned

The Economics of Terra/Luna Case Study

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Terra/Luna Case Study

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Terra/Luna Case Study

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Death Spiral Diagram

[COMIC: Death spiral diagram]

Placeholder for comic showing downward spiral: UST depegs → mint LUNA → LUNA crashes → confidence collapses → more UST selling → repeat until zero

The Mechanism of Doom

- UST falls below $1
- Arbitrage mints more LUNA
- LUNA supply explodes (350M → 6.5T)
- LUNA price crashes to zero

No Recovery Possible

- No collateral = no floor
- Confidence lost = game over
- $60B → $0 in 72 hours

When there's no collateral, there's no bottom – the spiral continues until zero

Summary

Key Takeaways:

- Terra/Luna was $60B algorithmic stablecoin experiment that collapsed in May 2022
- UST-LUNA mechanism relied on arbitrage but had no collateral backing
- Anchor's 20% APY was unsustainable Ponzi-like scheme
- Death spiral: UST depeg $\rightarrow$ LUNA hyperinflation $\rightarrow$ total collapse
- $40B+ value destroyed, triggering broader crypto contagion
- Lessons: Beware unsustainable yields, algorithmic stablecoins need collateral

Next Lecture: Lab - Testnet Lending (hands-on with Aave).

Next Lesson: L40 – Lab: Testnet Lending

Questions for Reflection

1. What structural difference between DAI and UST prevented DAI from collapsing?
2. Could the Bitcoin reserve have saved UST if it were larger (e.g., $20B)?
3. Why did Anchor's 20% APY attract deposits despite being unsustainable?
4. How could regulators have prevented Terra collapse without banning innovation?
5. Would you invest in a new algorithmic stablecoin if it had better design?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What was the peak combined market cap of UST and LUNA in April 2022?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA algorithmic peg mechanism work?
A) UST backed by USD reserves B) LUNA backed by gold C) Burn $1 LUNA to mint 1 UST D) Fixed exchange rate
Answer: C – Users could burn $1 worth of LUNA to mint 1 UST, and vice versa, creating arbitrage opportunities.

Q3. What APY did Anchor Protocol promise on UST deposits?
A) 5% B) 10% C) 20% D) 50%
Answer: C – Anchor offered approximately 20% APY, which was unsustainable and required subsidy.

Q4. What percentage of UST supply was concentrated in Anchor Protocol?
A) 25% B) 50% C) 78% D) 90%
Answer: C – About 78% of UST was locked in Anchor, creating massive concentration risk.

Q5. How long did the Terra/Luna collapse take from initial depeg to near-zero?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – The collapse occurred over approximately 72 hours (May 7-12, 2022).

Quiz Questions (6–10)

Q6. What was the fundamental flaw in UST's algorithmic design?
A) Too many validators B) High transaction fees C) No collateral backing D) Slow block times
Answer: C – UST had no collateral; it relied entirely on LUNA's value, which created death spiral risk.

Q7. What happened to LUNA's token supply during the death spiral?
A) Decreased to zero B) Stayed constant C) Increased from 350M to 6.5 trillion D) Halved
Answer: C – LUNA supply exploded from 350 million to 6.5 trillion as UST holders redeemed for LUNA.

Q8. How much Bitcoin did the Luna Foundation Guard deploy to defend the peg?
A) $500M B) $1.5B C) $5B D) $10B
Answer: B – LFG deployed approximately $1.5B in BTC to buy UST, but it was ineffective.

Q9. Which major crypto fund collapsed due to exposure to LUNA?
A) Alameda Research B) Three Arrows Capital (3AC) C) FTX D) Binance
Answer: B – 3AC had billions in LUNA exposure and declared bankruptcy in July 2022.

Q10. At what price did UST fall to during the collapse?
A) $0.50 B) $0.10 C) $0.01 D) Exactly $0
Answer: C – UST fell to approximately $0.01 by May 12, 2022.

Quiz Questions (11–15)

Q11. Who was the founder of Terra/Luna and Terraform Labs?
A) Vitalik Buterin B) Do Kwon C) Charles Hoskinson D) Sam Bankman-Fried
Answer: B – Do Kwon founded Terraform Labs and the Terra ecosystem.

Q12. What was Do Kwon's sentence for fraud in December 2025?
A) 5 years B) 10 years C) 15 years D) 25 years
Answer: C – Do Kwon was sentenced to 15 years in prison for "fraud on epic scale."

Q13. Why was Anchor's 20% APY considered unsustainable?
A) Backed by real revenue B) Required $50-100M/month subsidy C) Too low D) Regulated by SEC
Answer: B – Borrowers only paid 10-15%; Anchor subsidized the gap, burning reserves monthly.

Q14. How does DAI differ from UST in terms of stability mechanism?
A) Both algorithmic B) DAI is 150%+ overcollateralized C) DAI has no collateral D) Same design
Answer: B – DAI is overcollateralized with ETH/USDC, providing a demand floor that UST lacked.

Q15. What happened to Terra 2.0 after the relaunch?
A) Huge success B) Price fell from $6 to $0.50 C) Matched original LUNA D) Still thriving
Answer: B – Terra 2.0 had minimal adoption; price collapsed within months as trust was destroyed.

Quiz Questions (16–20)

Q16. Which regulatory framework included stablecoin reserve requirements after Terra?
A) Dodd-Frank B) Basel III C) EU MiCA D) Sarbanes-Oxley
Answer: C – EU's Markets in Crypto-Assets (MiCA) regulation included stablecoin reserve requirements.

Q17. What is a "death spiral" in the context of algorithmic stablecoins?
A) Rising prices B) Depeg causes LUNA dilution, accelerating collapse C) Stable growth D) Regulatory ban
Answer: B – UST depeg forces LUNA minting (dilution), crashing LUNA price, deepening UST depeg.

Q18. What psychological factor contributed most to Terra's initial growth?
A) Fear B) Regulatory clarity C) Greed (20% APY) D) Technical superiority
Answer: C – The promise of 20% APY was too attractive, driving massive deposits despite red flags.

Q19. Approximately how much value was destroyed in the Terra/Luna collapse?
A) $5B B) $10B C) $40B+ D) $100B
Answer: C – Over $40 billion in investor losses occurred during the May 2022 collapse.

Q20. What key lesson did the industry learn about algorithmic stablecoins?
A) They're superior B) Collateralization is necessary C) 20% yields are achievable D) Regulation is unnecessary
Answer: B – The collapse proved that overcollateralization, though inefficient, is necessary for stability.

Quiz: Terra Luna Case Study

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What was the combined peak market cap of UST and LUNA?
A) $20B B) $40B C) $60B D) $80B

Quiz (1–5)

Q1. What was the combined peak market cap of UST and LUNA?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA peg mechanism work?
A) USD reserves B) Gold backing C) Burn $1 LUNA to mint 1 UST D) Fixed rate

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What was the combined peak market cap of UST and LUNA?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA peg mechanism work?
A) USD reserves B) Gold backing C) Burn $1 LUNA to mint 1 UST D) Fixed rate
Answer: C – Users could burn $1 of LUNA to mint 1 UST, and vice versa.

Q3. What APY did Anchor Protocol promise on UST deposits?
A) 5% B) 10% C) 20% D) 50%

Quiz (1–5)

Q1. What was the combined peak market cap of UST and LUNA?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA peg mechanism work?
A) USD reserves B) Gold backing C) Burn $1 LUNA to mint 1 UST D) Fixed rate
Answer: C – Users could burn $1 of LUNA to mint 1 UST, and vice versa.

Q3. What APY did Anchor Protocol promise on UST deposits?
A) 5% B) 10% C) 20% D) 50%
Answer: C – Anchor offered 20% APY, requiring $50-100M monthly subsidy.

Q4. How long did the Terra/Luna collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What was the combined peak market cap of UST and LUNA?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA peg mechanism work?
A) USD reserves B) Gold backing C) Burn $1 LUNA to mint 1 UST D) Fixed rate
Answer: C – Users could burn $1 of LUNA to mint 1 UST, and vice versa.

Q3. What APY did Anchor Protocol promise on UST deposits?
A) 5% B) 10% C) 20% D) 50%
Answer: C – Anchor offered 20% APY, requiring $50-100M monthly subsidy.

Q4. How long did the Terra/Luna collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – The collapse occurred over 72 hours (May 7-12, 2022).

Q5. What happened to LUNA's supply during the death spiral?
A) Decreased B) Stayed constant C) 350M to 6.5 trillion D) Halved

Quiz (1–5)

Q1. What was the combined peak market cap of UST and LUNA?
A) $20B B) $40B C) $60B D) $80B
Answer: C – UST reached $18B and LUNA $40B, totaling approximately $60B.

Q2. How did the UST-LUNA peg mechanism work?
A) USD reserves B) Gold backing C) Burn $1 LUNA to mint 1 UST D) Fixed rate
Answer: C – Users could burn $1 of LUNA to mint 1 UST, and vice versa.

Q3. What APY did Anchor Protocol promise on UST deposits?
A) 5% B) 10% C) 20% D) 50%
Answer: C – Anchor offered 20% APY, requiring $50-100M monthly subsidy.

Q4. How long did the Terra/Luna collapse take?
A) 24 hours B) 72 hours C) 1 week D) 1 month
Answer: B – The collapse occurred over 72 hours (May 7-12, 2022).

Q5. What happened to LUNA's supply during the death spiral?
A) Decreased B) Stayed constant C) 350M to 6.5 trillion D) Halved
Answer: C – LUNA supply exploded as UST holders redeemed for LUNA.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What was UST's fundamental design flaw?

A) Too many validators B) High fees C) No collateral backing D) Slow blocks

Quiz (6–10)

Q6. What was UST's fundamental design flaw?
A) Too many validators B) High fees C) No collateral backing D) Slow blocks
Answer: C – UST had no collateral; it relied entirely on LUNA's value.

Q7. Which major crypto fund collapsed due to LUNA exposure?
A) Alameda B) Three Arrows Capital C) FTX D) Binance

Quiz (6–10)

Q6. What was UST's fundamental design flaw?
A) Too many validators B) High fees C) No collateral backing D) Slow blocks
Answer: C – UST had no collateral; it relied entirely on LUNA's value.

Q7. Which major crypto fund collapsed due to LUNA exposure?
A) Alameda B) Three Arrows Capital C) FTX D) Binance
Answer: B – 3AC had billions in LUNA exposure and declared bankruptcy July 2022.

Q8. Why does DAI survive while UST collapsed?
A) Both algorithmic B) DAI 150%+ overcollateralized C) Same design D) DAI has no backing

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What was UST's fundamental design flaw?
A) Too many validators B) High fees C) No collateral backing D) Slow blocks
Answer: C – UST had no collateral; it relied entirely on LUNA's value.

Q7. Which major crypto fund collapsed due to LUNA exposure?
A) Alameda B) Three Arrows Capital C) FTX D) Binance
Answer: B – 3AC had billions in LUNA exposure and declared bankruptcy July 2022.

Q8. Why does DAI survive while UST collapsed?
A) Both algorithmic B) DAI 150%+ overcollateralized C) Same design D) DAI has no backing
Answer: B – DAI is overcollateralized with ETH/USDC, providing a demand floor.

Q9. What sentence did Do Kwon receive in December 2025?
A) 5 years B) 10 years C) 15 years D) 25 years

Quiz (6–10)

Q6. What was UST's fundamental design flaw?
A) Too many validators B) High fees C) No collateral backing D) Slow blocks
Answer: C – UST had no collateral; it relied entirely on LUNA's value.

Q7. Which major crypto fund collapsed due to LUNA exposure?
A) Alameda B) Three Arrows Capital C) FTX D) Binance
Answer: B – 3AC had billions in LUNA exposure and declared bankruptcy July 2022.

Q8. Why does DAI survive while UST collapsed?
A) Both algorithmic B) DAI 150%+ overcollateralized C) Same design D) DAI has no backing
Answer: B – DAI is overcollateralized with ETH/USDC, providing a demand floor.

Q9. What sentence did Do Kwon receive in December 2025?
A) 5 years B) 10 years C) 15 years D) 25 years
Answer: C – Do Kwon was sentenced to 15 years for "fraud on epic scale."

Q10. What key lesson did the industry learn?
A) Algorithmic is superior B) Collateralization is necessary C) 20% yields work D) No regulation needed

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What was UST's fundamental design flaw?
A) Too many validators B) High fees C) No collateral backing D) Slow blocks
Answer: C – UST had no collateral; it relied entirely on LUNA's value.

Q7. Which major crypto fund collapsed due to LUNA exposure?
A) Alameda B) Three Arrows Capital C) FTX D) Binance
Answer: B – 3AC had billions in LUNA exposure and declared bankruptcy July 2022.

Q8. Why does DAI survive while UST collapsed?
A) Both algorithmic B) DAI 150%+ overcollateralized C) Same design D) DAI has no backing
Answer: B – DAI is overcollateralized with ETH/USDC, providing a demand floor.

Q9. What sentence did Do Kwon receive in December 2025?
A) 5 years B) 10 years C) 15 years D) 25 years
Answer: C – Do Kwon was sentenced to 15 years for "fraud on epic scale."

Q10. What key lesson did the industry learn?
A) Algorithmic is superior B) Collateralization is necessary C) 20% yields work D) No regulation needed
Answer: B – The collapse proved overcollateralization, though inefficient, is necessary.

(c) Joerg Osterrieder 2025

L40: Lab – Testnet Lending

Mini-Lecture – Module E: DeFi Ecosystem

Blockchain & Cryptocurrency Course

January 2026

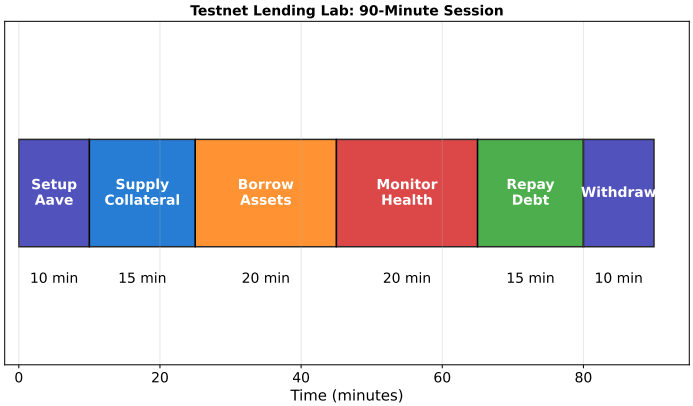
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Supply assets to Aave as collateral
- Borrow against collateral on testnet
- Calculate and monitor health factor
- Explain liquidation mechanics and risk factors

Lab Session Workflow



Goal: Hands-on lending experience with zero financial risk.

Step 1-2: Access Aave and Supply Collateral

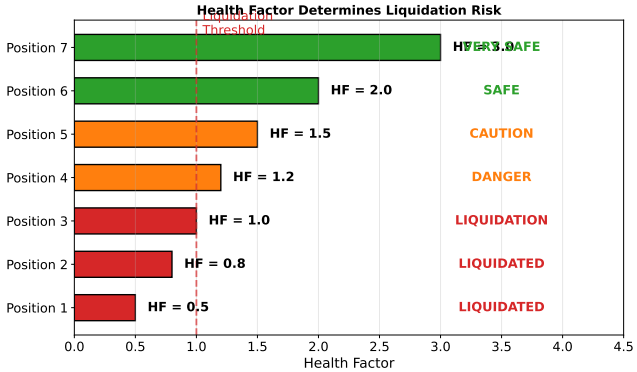
Access Aave Testnet:

1. Connect MetaMask at app.aave.com
2. Switch to Sepolia testnet
3. Use Aave V3 Sepolia interface

Supply Collateral:

1. Click “Supply” on Dashboard
2. Select ETH (0.5 ETH recommended)
3. Enable as collateral, confirm transaction
4. Receive aWETH tokens (interest-bearing)

Understanding Health Factor



Health factor below 1.0 triggers liquidation.

Step 3: Borrow Assets

Health Factor Formula:

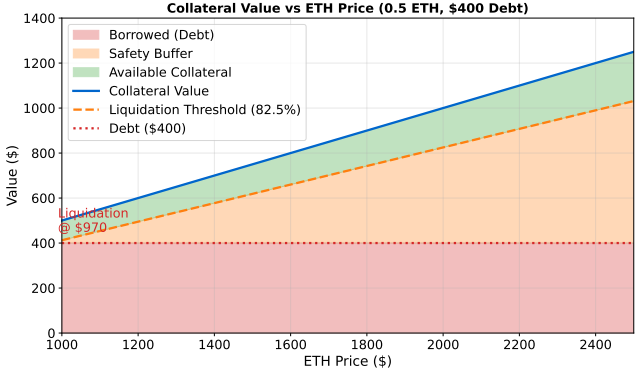
$$\text{HF} = \frac{\text{Collateral} \times \text{Liquidation Threshold}}{\text{Borrowed Amount}}$$

Example:

- Collateral: \$1,000 (0.5 ETH at \$2,000)
- Borrow: \$400 USDC
- $\text{HF} = \frac{1{,}000 \times 0.825}{400} = 2.06$ (safe)

Record: Borrow APY, variable/stable rate choice, HF after borrow.

Collateral vs Liquidation Risk



ETH price drop reduces collateral value; HF approaches 1.0.

Step 4-5: Monitor Position, Repay and Withdraw

Monitor Position:

- Watch health factor on dashboard
- Calculate net cost: Borrow APY - Supply APY
- Add collateral or repay if HF drops

Repay and Withdraw:

1. Click “Repay” to return borrowed USDC
2. Once debt cleared, click “Withdraw”
3. Receive ETH plus earned interest

(c) Joerg Osterrieder 2025

Lab Deliverables

Lab Report (3-4 pages):

1. Supply and borrow details
2. Health factor calculations
3. Liquidation price calculation
4. Interest accrual analysis

Supporting Evidence:

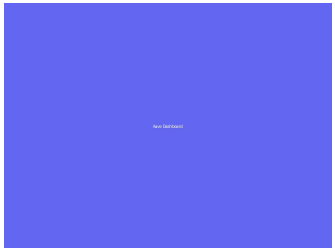
- Dashboard screenshots
- Transaction hashes (Etherscan links)

Key Takeaways

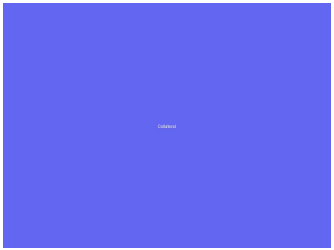
1. **Overcollateralization:** Required to borrow in DeFi
2. **Health Factor:** Must stay above 1.0 to avoid liquidation
3. **aTokens:** Represent interest-bearing deposits
4. **Interest Rates:** Adjust based on pool utilization
5. **Always Test:** Use testnet before real funds

Next Module: F – Advanced Topics

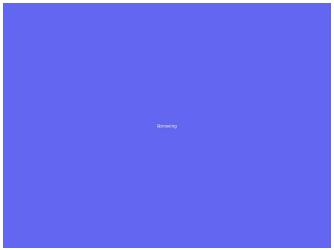
Testnet Lending in Practice



Aave Dashboard



Collateral



Borrowing

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH

Quiz (1/2)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens represent interest-bearing supply.

Q2. Minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0

Quiz (1/2)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens represent interest-bearing supply.

Q2. Minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – HF ¡ 1.0 triggers liquidation.

Q3. $1,000 ETH (LT=82.5%), borrow $500 USDC. Health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0

Quiz (1/2)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens represent interest-bearing supply.

Q2. Minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – HF ¡ 1.0 triggers liquidation.

Q3. $1,000 ETH (LT=82.5%), borrow $500 USDC. Health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – (1000 x 0.825) / 500 = 1.65.

Q4. What increases health factor?
A) Borrow more B) Add collateral C) Wait longer D) Nothing

Quiz (1/2)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens represent interest-bearing supply.

Q2. Minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – HF ¡ 1.0 triggers liquidation.

Q3. $1,000 ETH (LT=82.5%), borrow $500 USDC. Health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – (1000 x 0.825) / 500 = 1.65.

Q4. What increases health factor?
A) Borrow more B) Add collateral C) Wait longer D) Nothing
Answer: B – Adding collateral or repaying debt.

Q5. Why use testnet for this lab?
A) Faster B) Zero financial risk C) More features D) Required by law

Quiz (1/2)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens represent interest-bearing supply.

Q2. Minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – HF ¡ 1.0 triggers liquidation.

Q3. $1,000 ETH (LT=82.5%), borrow $500 USDC. Health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – (1000 x 0.825) / 500 = 1.65.

Q4. What increases health factor?
A) Borrow more B) Add collateral C) Wait longer D) Nothing
Answer: B – Adding collateral or repaying debt.

Q5. Why use testnet for this lab?
A) Faster B) Zero financial risk C) More features D) Required by law
Answer: B – Practice DeFi without losing real money.

Quiz (2/2)

Q6. What happens if ETH price drops 50% while borrowing?
A) Nothing B) HF doubles C) HF drops, liquidation risk D) Debt is forgiven

Quiz (2/2)

Q6. What happens if ETH price drops 50% while borrowing?
A) Nothing B) HF doubles C) HF drops, liquidation risk D) Debt is forgiven
Answer: C – Collateral value drops, HF decreases.

Q7. What is net cost of position?
A) Gas fees B) Borrow APY - Supply APY C) LTV ratio D) Collateral amount

Quiz (2/2)

Q6. What happens if ETH price drops 50% while borrowing?
A) Nothing B) HF doubles C) HF drops, liquidation risk D) Debt is forgiven
Answer: C – Collateral value drops, HF decreases.

Q7. What is net cost of position?
A) Gas fees B) Borrow APY - Supply APY C) LTV ratio D) Collateral amount
Answer: B – You pay borrow rate, earn supply rate.

Q8. Before withdrawing collateral, what must you do?
A) Wait 24 hours B) Repay all debt C) Contact Aave D) Increase HF to 3.0

Quiz (2/2)

Q6. What happens if ETH price drops 50% while borrowing?
A) Nothing B) HF doubles C) HF drops, liquidation risk D) Debt is forgiven
Answer: C – Collateral value drops, HF decreases.

Q7. What is net cost of position?
A) Gas fees B) Borrow APY - Supply APY C) LTV ratio D) Collateral amount
Answer: B – You pay borrow rate, earn supply rate.

Q8. Before withdrawing collateral, what must you do?
A) Wait 24 hours B) Repay all debt C) Contact Aave D) Increase HF to 3.0
Answer: B – Debt must be cleared first.

Q9. What does LT (Liquidation Threshold) represent?
A) Max interest rate B) Max debt-to-collateral before liquidation C) Token price D) Gas limit

Quiz (2/2)

Q6. What happens if ETH price drops 50% while borrowing?
A) Nothing B) HF doubles C) HF drops, liquidation risk D) Debt is forgiven
Answer: C – Collateral value drops, HF decreases.

Q7. What is net cost of position?
A) Gas fees B) Borrow APY - Supply APY C) LTV ratio D) Collateral amount
Answer: B – You pay borrow rate, earn supply rate.

Q8. Before withdrawing collateral, what must you do?
A) Wait 24 hours B) Repay all debt C) Contact Aave D) Increase HF to 3.0
Answer: B – Debt must be cleared first.

Q9. What does LT (Liquidation Threshold) represent?
A) Max interest rate B) Max debt-to-collateral before liquidation C) Token price D) Gas limit
Answer: B – When debt/collateral exceeds LT, liquidation.

Q10. Lab deliverables include?
A) Only screenshots B) Report + tx hashes + screenshots C) Smart contract code D) Video

Quiz (2/2)

Q6. What happens if ETH price drops 50% while borrowing?
A) Nothing B) HF doubles C) HF drops, liquidation risk D) Debt is forgiven
Answer: C – Collateral value drops, HF decreases.

Q7. What is net cost of position?
A) Gas fees B) Borrow APY - Supply APY C) LTV ratio D) Collateral amount
Answer: B – You pay borrow rate, earn supply rate.

Q8. Before withdrawing collateral, what must you do?
A) Wait 24 hours B) Repay all debt C) Contact Aave D) Increase HF to 3.0
Answer: B – Debt must be cleared first.

Q9. What does LT (Liquidation Threshold) represent?
A) Max interest rate B) Max debt-to-collateral before liquidation C) Token price D) Gas limit
Answer: B – When debt/collateral exceeds LT, liquidation.

Q10. Lab deliverables include?
A) Only screenshots B) Report + tx hashes + screenshots C) Smart contract code D) Video
Answer: B – Report with calculations plus evidence.

Thank you

Questions?

Next: Module F – Advanced Topics

Lab Session: Testnet Lending

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module E: DeFi Ecosystem

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Supply assets to Aave as collateral
- Borrow against collateral on testnet
- Calculate and monitor health factor
- Explain liquidation mechanics and risk factors
- Repay debt and withdraw collateral

The Problem: Understanding DeFi Lending Risk

The Challenge
Learning DeFi lending requires hands-on experience, but testing with real capital exposes students to liquidation risk, smart contract vulnerabilities, and costly mistakes that could result in permanent loss of funds.

Why It Matters

- Without practical experience, students misunderstand health factors and get liquidated on mainnet
- Historical example: Terra/Luna collapse highlighted critical importance of understanding lending mechanics

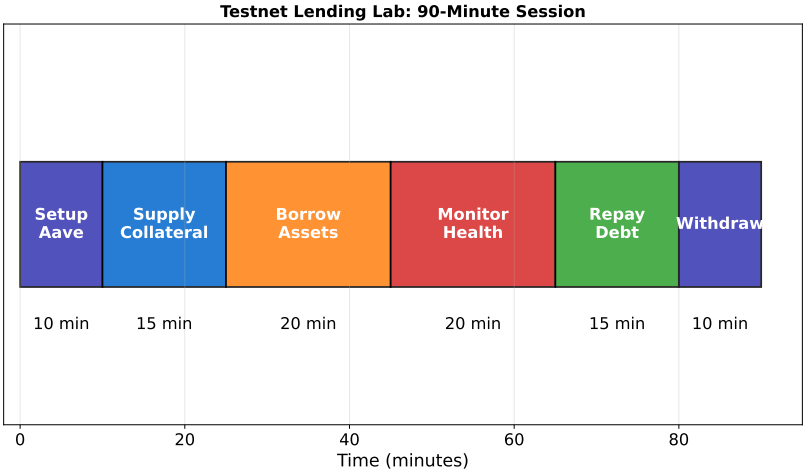
What We Need

- Risk-free environment to practice collateral management
- Real protocol interfaces that mirror production systems
- Ability to safely experiment with liquidation scenarios

The Cryptoeconomics Question
How do we create hands-on learning environments that simulate real financial risk without capital exposure?

Today's lesson: How testnet lending protocols enable risk-free DeFi education

Lab Session Structure



Hands-on lending experience with zero financial risk

Step 1: Access Aave Testnet

URL: `https://app.aave.com`

Actions:

1. Connect MetaMask wallet
2. Switch to Sepolia testnet
3. Verify Aave V3 Sepolia interface

Interface Overview:

- Dashboard: Your supply/borrow positions
- Markets: Available assets
- Health Factor: Your risk indicator

Step 2: Supply Collateral

Goal: Deposit ETH to enable borrowing

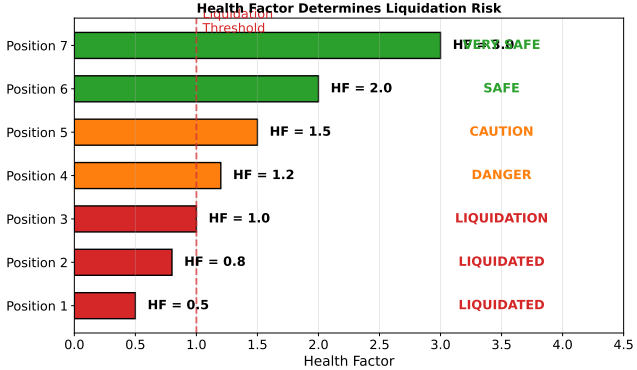
Process:

1. Click “Supply” on Dashboard
2. Select ETH (0.5 ETH recommended)
3. Enable as collateral
4. Confirm transaction

Record:

- Supply APY received
- aWETH tokens received
- Total collateral value

Understanding Health Factor



Health factor below 1.0 triggers liquidation

Step 3: Borrow Assets

Goal: Borrow USDC against ETH collateral

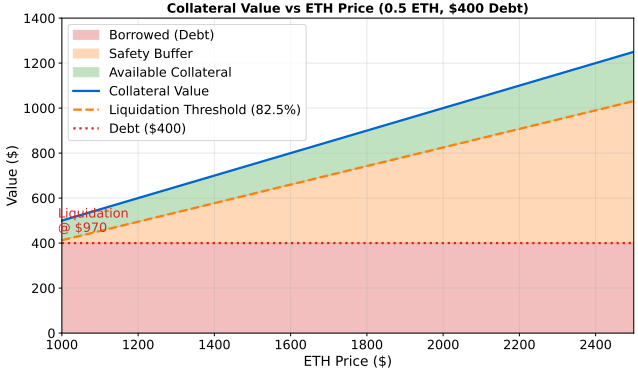
Health Factor Formula:

$$\text{HF} = \frac{\text{Collateral} \times \text{Liquidation Threshold}}{\text{Borrowed Amount}}$$

Example:

- Collateral: \$1,000 (0.5 ETH at \$2,000)
- Borrow: \$400 USDC
- $\text{HF} = \frac{1{,}000 \times 0.825}{400} = 2.06$

Collateral vs Liquidation Risk



ETH price drop reduces collateral value - HF approaches 1.0

Step 4: Monitor Position

Track Over Time:

- Watch health factor on dashboard
- Observe interest accrual (supply vs borrow)
- Calculate net cost: Borrow APY - Supply APY

Risk Management:

- Add collateral if HF drops
- Repay partial debt to increase HF
- Never let HF approach 1.0

(c) Joerg Osterrieder 2025

Step 5: Repay and Withdraw

Repay Debt:

1. Click “Repay” on borrowed asset
2. Select full or partial repayment
3. Approve and confirm

Withdraw Collateral:

1. Ensure debt is fully repaid
2. Click “Withdraw” on supplied asset
3. Receive ETH plus earned interest

Lab Deliverables

Submit:

1. **Lab Report (3-4 pages):**
   - Supply and borrow details
   - Health factor calculations
   - Liquidation price calculation
   - Interest accrual analysis
2. **Supporting Evidence:**
   - Dashboard screenshots
   - Transaction hashes

Problem Solved? Testnet Lending

The Original Problem

How do we enable risk-free hands-on DeFi lending education?

How Testnet Lending Solves It

- **Identical interfaces**: Aave testnet mirrors mainnet exactly - same UI, same formulas, same mechanics
- **Free test assets**: Faucets provide unlimited ETH/USDC for experimentation without capital risk
- **Safe failure**: Students can trigger liquidations, test edge cases, and learn from mistakes with zero financial consequences

Remaining Limitations

- **No real economic incentives**: Testnet lacks genuine market dynamics and emotional pressure of real capital
- **Trade-off**: Perfect safety eliminates the fear/discipline that drives careful risk management

Open Questions

- How much testnet experience is needed before mainnet deployment?
- Risk: Students overconfident after testnet success, underestimate mainnet oracle manipulation and smart contract bugs

Testnet lending solves the capital risk problem but cannot fully replicate mainnet psychological and economic pressures

(c) Joerg Osterrieder 2025

Key Takeaways

- DeFi lending requires overcollateralization
- Health factor must stay above 1.0
- Interest rates adjust based on utilization
- aTokens represent interest-bearing deposits
- Liquidation protects lenders but penalizes borrowers
- Always test on testnet before using real funds

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – Health factor below 1.0 triggers liquidation.

Q3. If you supply $1,000 ETH (LT=82.5%) and borrow $500 USDC, what is your health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – HF $= (1000 \times 0.825) / 500 = 1.65$.

Q4. What happens when your health factor drops below 1.0?
A) You get a warning B) Immediate liquidation C) Trading is disabled D) Nothing
Answer: B – Liquidators can repay your debt and seize collateral.

Q5. Why must DeFi lending be overcollateralized?
A) Regulation requires it B) To pay protocol fees C) No credit checks/KYC D) Higher profits
Answer: C – Without identity verification, collateral protects lenders.

Quiz Questions (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change
Answer: B – Collateral value drops proportionally: $1.5 \times 0.8 = 1.2$.

Q8. What is the primary benefit of supplying assets to Aave?
A) Capital gains B) Earn supply APY C) Free airdrops D) Governance rights
Answer: B – Suppliers earn interest (APY) on their deposits.

Q9. How can you increase your health factor?
A) Borrow more B) Withdraw collateral C) Repay debt D) Wait for liquidation
Answer: C – Repaying debt reduces denominator, increasing HF.

Q10. What network should you use for this lab to avoid losing real funds?
A) Ethereum mainnet B) Polygon C) Sepolia testnet D) Binance Smart Chain
Answer: C – Sepolia testnet uses free test ETH with zero financial risk.

Quiz Questions (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%
Answer: B – Net cost = 5% - 2% = 3% (you pay interest).

Q13. What is the liquidation penalty on Aave?
A) 0% B) 2% C) 5% D) 10%
Answer: C – Liquidators receive a 5% bonus from your collateral.

Q14. Which action does NOT require a transaction on Aave?
A) Supplying ETH B) Borrowing USDC C) Viewing health factor D) Repaying debt
Answer: C – Viewing data is free; state changes require transactions.

Q15. What is the recommended initial borrow amount for this lab?
A) 10% of collateral B) 50% of collateral C) 40% of collateral D) 90% of collateral
Answer: C – $400 USDC on $1,000 collateral (40%) maintains safe HF ¿ 2.0.

Quiz Questions (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation
Answer: B – LTV ¡ 100% ensures collateral covers debt during liquidation.

Q18. What must you do before withdrawing supplied ETH?
A) Wait 7 days B) Pay a fee C) Repay all debt D) Stake AAVE tokens
Answer: C – You cannot withdraw collateral while debt exists.

Q19. How do interest rates adjust on Aave?
A) Fixed by governance B) Based on utilization C) Random D) Daily auctions
Answer: B – Higher utilization increases rates to incentivize supply.

Q20. What is the main deliverable for this lab session?
A) Smart contract code B) 3-4 page lab report C) Video presentation D) Token creation
Answer: B – Submit a lab report with calculations and transaction evidence.

Lab Session: Testnet Lending

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module E: DeFi Ecosystem

(c) Joerg Osterrieder 2025

What Happens While You Sleep?

[COMIC: Aave position management]

Placeholder for comic showing dashboard with health factor gauge, person nervously watching as needle moves toward danger zone during price volatility

The Setup

- Deposit collateral, borrow assets
- Health factor starts safe (2.0+)
- "This is easy, what could go wrong?"

The Punchline

- Price drops while you sleep
- Health factor approaches 1.0
- Liquidation bots don't sleep

Your health factor doesn't care if you're sleeping – but liquidator bots are always awake

Learning Objectives

By the end of this lab session, you will be able to:

- Supply assets to Aave as collateral
- Borrow against collateral on testnet
- Calculate and monitor health factor
- Explain liquidation mechanics and risk factors
- Repay debt and withdraw collateral

Building on L39: Terra/Luna Case Study

The Problem: Understanding DeFi Lending Risk

The Challenge
Learning DeFi lending requires hands-on experience, but testing with real capital exposes students to liquidation risk, smart contract vulnerabilities, and costly mistakes that could result in permanent loss of funds.

Why It Matters

- Without practical experience, students misunderstand health factors and get liquidated on mainnet
- Historical example: Terra/Luna collapse highlighted critical importance of understanding lending mechanics

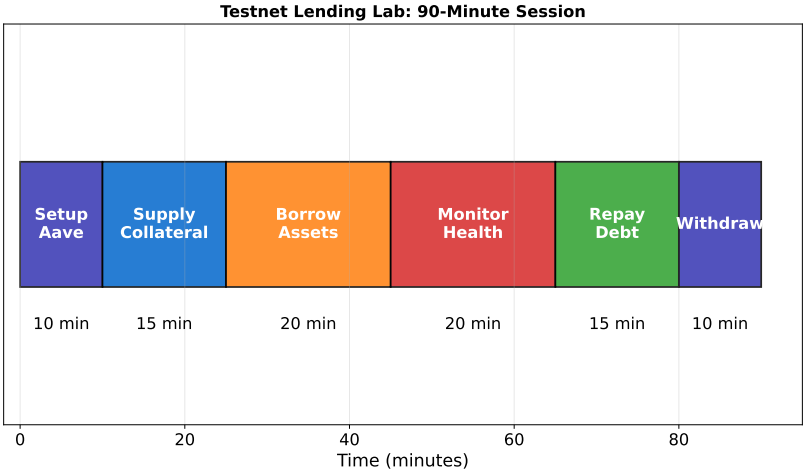
What We Need

- Risk-free environment to practice collateral management
- Real protocol interfaces that mirror production systems
- Ability to safely experiment with liquidation scenarios

The Cryptoeconomics Question
How do we create hands-on learning environments that simulate real financial risk without capital exposure?

Today's lesson: How testnet lending protocols enable risk-free DeFi education

How Does This Lab Work?



Hands-on lending experience with zero financial risk

How Do You Access Aave Testnet?

URL: `https://app.aave.com`

Actions:

1. Connect MetaMask wallet
2. Switch to Sepolia testnet
3. Verify Aave V3 Sepolia interface

Interface Overview:

- Dashboard: Your supply/borrow positions
- Markets: Available assets
- Health Factor: Your risk indicator

How Do You Deposit Collateral?

Goal: Deposit ETH to enable borrowing

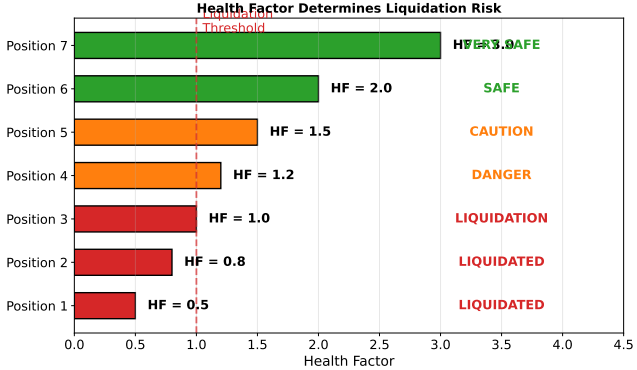
Process:

1. Click “Supply” on Dashboard
2. Select ETH (0.5 ETH recommended)
3. Enable as collateral
4. Confirm transaction

Record:

- Supply APY received
- aWETH tokens received
- Total collateral value

What Is Health Factor?



Health factor below 1.0 triggers liquidation

How Do You Borrow Against Collateral?

Goal: Borrow USDC against ETH collateral

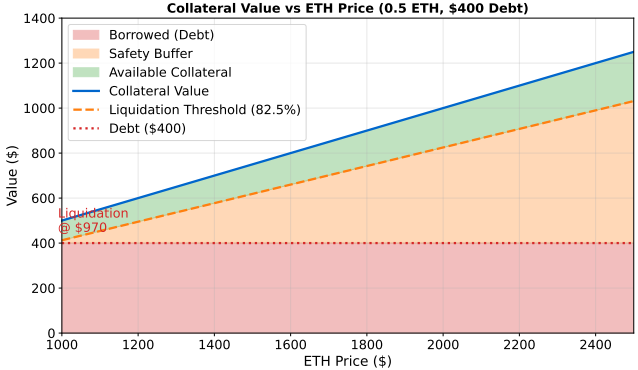
Health Factor Formula:

$$\text{HF} = \frac{\text{Collateral} \times \text{Liquidation Threshold}}{\text{Borrowed Amount}}$$

Example:

- Collateral: \$1,000 (0.5 ETH at \$2,000)
- Borrow: \$400 USDC
- HF $= \frac{1{,}000 \times 0.825}{400} = 2.06$

How Does Price Volatility Affect Your Position?



ETH price drop reduces collateral value - HF approaches 1.0

How Do You Monitor Your Position?

Track Over Time:

- Watch health factor on dashboard
- Observe interest accrual (supply vs borrow)
- Calculate net cost: Borrow APY - Supply APY

Risk Management:

- Add collateral if HF drops
- Repay partial debt to increase HF
- Never let HF approach 1.0

(c) Joerg Osterrieder 2025

How Do You Exit Your Position?

Repay Debt:

1. Click “Repay” on borrowed asset
2. Select full or partial repayment
3. Approve and confirm

Withdraw Collateral:

1. Ensure debt is fully repaid
2. Click “Withdraw” on supplied asset
3. Receive ETH plus earned interest

What Should You Submit?

Submit:

1. **Lab Report (3-4 pages):**
   - Supply and borrow details
   - Health factor calculations
   - Liquidation price calculation
   - Interest accrual analysis
2. **Supporting Evidence:**
   - Dashboard screenshots
   - Transaction hashes

Problem Solved? Testnet Lending

The Original Problem

How do we enable risk-free hands-on DeFi lending education?

How Testnet Lending Solves It

- **Identical interfaces**: Aave testnet mirrors mainnet exactly - same UI, same formulas, same mechanics
- **Free test assets**: Faucets provide unlimited ETH/USDC for experimentation without capital risk
- **Safe failure**: Students can trigger liquidations, test edge cases, and learn from mistakes with zero financial consequences

Remaining Limitations

- **No real economic incentives**: Testnet lacks genuine market dynamics and emotional pressure of real capital
- **Trade-off**: Perfect safety eliminates the fear/discipline that drives careful risk management

Open Questions

- How much testnet experience is needed before mainnet deployment?
- Risk: Students overconfident after testnet success, underestimate mainnet oracle manipulation and smart contract bugs

Testnet lending solves the capital risk problem but cannot fully replicate mainnet psychological and economic pressures

(c) Joerg Osterrieder 2025

The Economics of Testnet Lending

Incentive Structure

- **Core Problem:** Creating systems with desired properties
- **Why act honestly?** Mechanism design for target behaviors
- **Value Flow:** Complexity vs simplicity

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Complexity vs simplicity

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Testnet Lending

Alternatives Considered

1. **Chosen Design:** Architecture patterns, upgrade mechanisms
2. **Alternative:** Alternative design patterns

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Testnet Lending

Critical Failure Mode

- **What breaks:** Unintended consequences, edge cases
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

How Often Should You Check Your Health Factor?

[COMIC: Health factor monitoring]

Placeholder for comic showing person checking health factor once a week vs. professional monitoring 24/7 with alerts, showing different outcomes when market crashes

The Lesson

- Crypto markets run 24/7/365
- Crashes don't wait for you
- Health factor can change fast

Best Practices

- Set up price alerts
- Keep buffer above 1.5 HF
- Have emergency collateral ready

The market doesn't care about your schedule – monitor your health factor or get liquidated

Key Takeaways

- DeFi lending requires overcollateralization
- Health factor must stay above 1.0
- Interest rates adjust based on utilization
- aTokens represent interest-bearing deposits
- Liquidation protects lenders but penalizes borrowers
- Always test on testnet before using real funds

Next Lesson: L41 – Layer 2 Scaling

Quiz Questions (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – Health factor below 1.0 triggers liquidation.

Q3. If you supply $1,000 ETH (LT=82.5%) and borrow $500 USDC, what is your health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – HF $= (1000 \times 0.825) / 500 = 1.65$.

Q4. What happens when your health factor drops below 1.0?
A) You get a warning B) Immediate liquidation C) Trading is disabled D) Nothing
Answer: B – Liquidators can repay your debt and seize collateral.

Q5. Why must DeFi lending be overcollateralized?
A) Regulation requires it B) To pay protocol fees C) No credit checks/KYC D) Higher profits
Answer: C – Without identity verification, collateral protects lenders.

Quiz Questions (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change
Answer: B – Collateral value drops proportionally: $1.5 \times 0.8 = 1.2$.

Q8. What is the primary benefit of supplying assets to Aave?
A) Capital gains B) Earn supply APY C) Free airdrops D) Governance rights
Answer: B – Suppliers earn interest (APY) on their deposits.

Q9. How can you increase your health factor?
A) Borrow more B) Withdraw collateral C) Repay debt D) Wait for liquidation
Answer: C – Repaying debt reduces denominator, increasing HF.

Q10. What network should you use for this lab to avoid losing real funds?
A) Ethereum mainnet B) Polygon C) Sepolia testnet D) Binance Smart Chain
Answer: C – Sepolia testnet uses free test ETH with zero financial risk.

Quiz Questions (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%
Answer: B – Net cost = 5% - 2% = 3% (you pay interest).

Q13. What is the liquidation penalty on Aave?
A) 0% B) 2% C) 5% D) 10%
Answer: C – Liquidators receive a 5% bonus from your collateral.

Q14. Which action does NOT require a transaction on Aave?
A) Supplying ETH B) Borrowing USDC C) Viewing health factor D) Repaying debt
Answer: C – Viewing data is free; state changes require transactions.

Q15. What is the recommended initial borrow amount for this lab?
A) 10% of collateral B) 50% of collateral C) 40% of collateral D) 90% of collateral
Answer: C – $400 USDC on $1,000 collateral (40%) maintains safe HF ¿ 2.0.

Quiz Questions (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation
Answer: B – LTV ¡ 100% ensures collateral covers debt during liquidation.

Q18. What must you do before withdrawing supplied ETH?
A) Wait 7 days B) Pay a fee C) Repay all debt D) Stake AAVE tokens
Answer: C – You cannot withdraw collateral while debt exists.

Q19. How do interest rates adjust on Aave?
A) Fixed by governance B) Based on utilization C) Random D) Daily auctions
Answer: B – Higher utilization increases rates to incentivize supply.

Q20. What is the main deliverable for this lab session?
A) Smart contract code B) 3-4 page lab report C) Video presentation D) Token creation
Answer: B – Submit a lab report with calculations and transaction evidence.

Quiz: Lab Testnet Lending

Instructions: 21 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH

Quiz (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0

Quiz (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – Health factor below 1.0 triggers liquidation.

Q3. If you supply $1,000 ETH (LT=82.5%) and borrow $500 USDC, what is your health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – Health factor below 1.0 triggers liquidation.

Q3. If you supply $1,000 ETH (LT=82.5%) and borrow $500 USDC, what is your health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – HF $= (1000 \times 0.825) / 500 = 1.65$.

Q4. What happens when your health factor drops below 1.0?
A) You get a warning B) Immediate liquidation C) Trading is disabled D) Nothing

Quiz (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – Health factor below 1.0 triggers liquidation.

Q3. If you supply $1,000 ETH (LT=82.5%) and borrow $500 USDC, what is your health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – HF $= (1000 \times 0.825) / 500 = 1.65$.

Q4. What happens when your health factor drops below 1.0?
A) You get a warning B) Immediate liquidation C) Trading is disabled D) Nothing
Answer: B – Liquidators can repay your debt and seize collateral.

Q5. Why must DeFi lending be overcollateralized?
A) Regulation requires it B) To pay protocol fees C) No credit checks/KYC D) Higher profits

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What token do you receive when supplying ETH to Aave?
A) wETH B) aWETH C) stETH D) cETH
Answer: B – aTokens (aWETH) represent your interest-bearing supply position.

Q2. What is the minimum health factor to avoid liquidation?
A) 0.8 B) 1.0 C) 1.5 D) 2.0
Answer: B – Health factor below 1.0 triggers liquidation.

Q3. If you supply $1,000 ETH (LT=82.5%) and borrow $500 USDC, what is your health factor?
A) 0.825 B) 1.0 C) 1.65 D) 2.0
Answer: C – HF $= (1000 \times 0.825) / 500 = 1.65$.

Q4. What happens when your health factor drops below 1.0?
A) You get a warning B) Immediate liquidation C) Trading is disabled D) Nothing
Answer: B – Liquidators can repay your debt and seize collateral.

Q5. Why must DeFi lending be overcollateralized?
A) Regulation requires it B) To pay protocol fees C) No credit checks/KYC D) Higher profits
Answer: C – Without identity verification, collateral protects lenders.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%

Quiz (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change
Answer: B – Collateral value drops proportionally: $1.5 \times 0.8 = 1.2$.

Q8. What is the primary benefit of supplying assets to Aave?
A) Capital gains B) Earn supply APY C) Free airdrops D) Governance rights

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change
Answer: B – Collateral value drops proportionally: $1.5 \times 0.8 = 1.2$.

Q8. What is the primary benefit of supplying assets to Aave?
A) Capital gains B) Earn supply APY C) Free airdrops D) Governance rights
Answer: B – Suppliers earn interest (APY) on their deposits.

Q9. How can you increase your health factor?
A) Borrow more B) Withdraw collateral C) Repay debt D) Wait for liquidation

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change
Answer: B – Collateral value drops proportionally: $1.5 \times 0.8 = 1.2$.

Q8. What is the primary benefit of supplying assets to Aave?
A) Capital gains B) Earn supply APY C) Free airdrops D) Governance rights
Answer: B – Suppliers earn interest (APY) on their deposits.

Q9. How can you increase your health factor?
A) Borrow more B) Withdraw collateral C) Repay debt D) Wait for liquidation
Answer: C – Repaying debt reduces denominator, increasing HF.

Q10. What network should you use for this lab to avoid losing real funds?
A) Ethereum mainnet B) Polygon C) Sepolia testnet D) Binance Smart Chain

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the liquidation threshold for ETH on Aave?
A) 50% B) 65% C) 82.5% D) 100%
Answer: C – ETH has an 82.5% liquidation threshold on Aave V3.

Q7. If ETH price drops 20% and your health factor is 1.5, what happens?
A) Liquidation B) HF drops to 1.2 C) HF increases D) No change
Answer: B – Collateral value drops proportionally: $1.5 \times 0.8 = 1.2$.

Q8. What is the primary benefit of supplying assets to Aave?
A) Capital gains B) Earn supply APY C) Free airdrops D) Governance rights
Answer: B – Suppliers earn interest (APY) on their deposits.

Q9. How can you increase your health factor?
A) Borrow more B) Withdraw collateral C) Repay debt D) Wait for liquidation
Answer: C – Repaying debt reduces denominator, increasing HF.

Q10. What network should you use for this lab to avoid losing real funds?
A) Ethereum mainnet B) Polygon C) Sepolia testnet D) Binance Smart Chain
Answer: C – Sepolia testnet uses free test ETH with zero financial risk.

Quiz (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate

Quiz (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%

Quiz (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%
Answer: B – Net cost = 5% - 2% = 3% (you pay interest).

Q13. What is the liquidation penalty on Aave?
A) 0% B) 2% C) 5% D) 10%

Quiz (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%
Answer: B – Net cost = 5% - 2% = 3% (you pay interest).

Q13. What is the liquidation penalty on Aave?
A) 0% B) 2% C) 5% D) 10%
Answer: C – Liquidators receive a 5% bonus from your collateral.

Q14. Which action does NOT require a transaction on Aave?
A) Supplying ETH B) Borrowing USDC C) Viewing health factor D) Repaying debt

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%
Answer: B – Net cost = 5% - 2% = 3% (you pay interest).

Q13. What is the liquidation penalty on Aave?
A) 0% B) 2% C) 5% D) 10%
Answer: C – Liquidators receive a 5% bonus from your collateral.

Q14. Which action does NOT require a transaction on Aave?
A) Supplying ETH B) Borrowing USDC C) Viewing health factor D) Repaying debt
Answer: C – Viewing data is free; state changes require transactions.

Q15. What is the recommended initial borrow amount for this lab?
A) 10% of collateral B) 50% of collateral C) 40% of collateral D) 90% of collateral

Quiz (11–15)

Q11. What does the utilization rate measure in lending protocols?
A) Profit margin B) Borrowed / Supplied C) Gas fees D) Liquidation rate
Answer: B – Utilization = total borrowed / total supplied.

Q12. If supply APY is 2% and borrow APY is 5%, what is your net cost?
A) -3% B) 3% C) 7% D) 2.5%
Answer: B – Net cost = 5% - 2% = 3% (you pay interest).

Q13. What is the liquidation penalty on Aave?
A) 0% B) 2% C) 5% D) 10%
Answer: C – Liquidators receive a 5% bonus from your collateral.

Q14. Which action does NOT require a transaction on Aave?
A) Supplying ETH B) Borrowing USDC C) Viewing health factor D) Repaying debt
Answer: C – Viewing data is free; state changes require transactions.

Q15. What is the recommended initial borrow amount for this lab?
A) 10% of collateral B) 50% of collateral C) 40% of collateral D) 90% of collateral
Answer: C – $400 USDC on $1,000 collateral (40%) maintains safe HF ¿ 2.0.

Quiz (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH

Quiz (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation

Quiz (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation
Answer: B – LTV ¡ 100% ensures collateral covers debt during liquidation.

Q18. What must you do before withdrawing supplied ETH?
A) Wait 7 days B) Pay a fee C) Repay all debt D) Stake AAVE tokens

Quiz (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation
Answer: B – LTV ¡ 100% ensures collateral covers debt during liquidation.

Q18. What must you do before withdrawing supplied ETH?
A) Wait 7 days B) Pay a fee C) Repay all debt D) Stake AAVE tokens
Answer: C – You cannot withdraw collateral while debt exists.

Q19. How do interest rates adjust on Aave?
A) Fixed by governance B) Based on utilization C) Random D) Daily auctions

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation
Answer: B – LTV ¡ 100% ensures collateral covers debt during liquidation.

Q18. What must you do before withdrawing supplied ETH?
A) Wait 7 days B) Pay a fee C) Repay all debt D) Stake AAVE tokens
Answer: C – You cannot withdraw collateral while debt exists.

Q19. How do interest rates adjust on Aave?
A) Fixed by governance B) Based on utilization C) Random D) Daily auctions
Answer: B – Higher utilization increases rates to incentivize supply.

Q20. What is the main deliverable for this lab session?
A) Smart contract code B) 3-4 page lab report C) Video presentation D) Token creation

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What happens to your aWETH balance over time?
A) Decreases B) Stays constant C) Increases D) Converts to ETH
Answer: C – aTokens accrue interest, increasing your balance.

Q17. Why can't you borrow 100% of your collateral value?
A) Protocol fees B) Liquidation buffer needed C) Gas limits D) Regulation
Answer: B – LTV ¡ 100% ensures collateral covers debt during liquidation.

Q18. What must you do before withdrawing supplied ETH?
A) Wait 7 days B) Pay a fee C) Repay all debt D) Stake AAVE tokens
Answer: C – You cannot withdraw collateral while debt exists.

Q19. How do interest rates adjust on Aave?
A) Fixed by governance B) Based on utilization C) Random D) Daily auctions
Answer: B – Higher utilization increases rates to incentivize supply.

Q20. What is the main deliverable for this lab session?
A) Smart contract code B) 3-4 page lab report C) Video presentation D) Token creation
Answer: B – Submit a lab report with calculations and transaction evidence.

(c) Joerg Osterrieder 2025

Quiz (21–21)

Q21. What network should you use for this lab?
A) Mainnet B) Polygon C) Sepolia testnet D) BSC

Quiz (21–21)

Q21. What network should you use for this lab?
A) Mainnet B) Polygon C) Sepolia testnet D) BSC
Answer: C – Sepolia testnet uses free test ETH with zero financial risk.

L41: Layer 2 Scaling Solutions

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Describe the blockchain scalability trilemma
- Compare Layer 2 design patterns (channels, rollups, sidechains)
- Analyze Optimistic vs ZK-Rollups tradeoffs
- Evaluate the impact of Dencun upgrade (EIP-4844)
- Explain Account Abstraction (ERC-4337) and its UX improvements

The Problem: How do we scale without sacrificing security?

The Challenge
Ethereum can only process 15 transactions per second, while Visa handles 65,000 TPS. Traditional scaling approaches (increasing block size, reducing block time) sacrifice decentralization or security.

Why It Matters

- High gas fees (∼$50-200 during peak) exclude everyday users
- Bitcoin Lightning Network launched in 2018, but adoption remains low
- Ethereum's Dencun upgrade (March 2024) reduced L2 fees by 90% via EIP-4844

What We Need

- Understanding design constraints
- Mechanisms that inherit L1 security while increasing throughput 10-1000x
- Solutions that don't require users to trust new validator sets

The Cryptoeconomics Question
How do we optimize for scalability without breaking decentralization or security?

Today's lesson: How Layer 2 Scaling addresses this challenge

The Blockchain Scalability Trilemma

The Trilemma:
Can only optimize 2 of 3 properties:

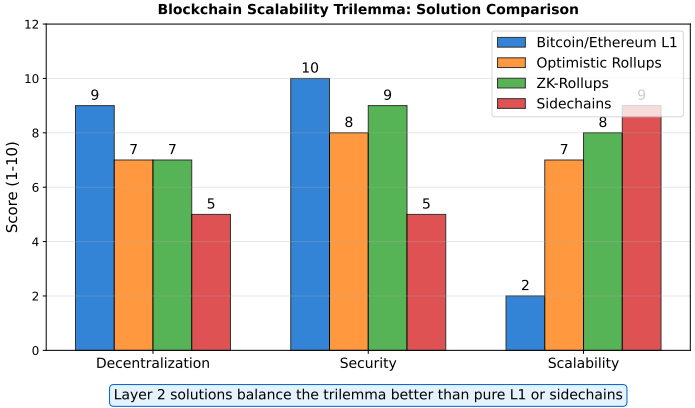
- **Decentralization**: Independent validators
- **Security**: Cost to attack network
- **Scalability**: TPS throughput

Current TPS:

- Bitcoin: $\sim$7 TPS
- Ethereum: $\sim$15 TPS
- Visa: $\sim$65,000 TPS

Solution: Layer 2 moves transactions off-chain while inheriting L1 security

Trilemma Comparison by Solution



Rollups achieve better balance than L1 alone or sidechains

What is Layer 2?

Layer 1 (L1)

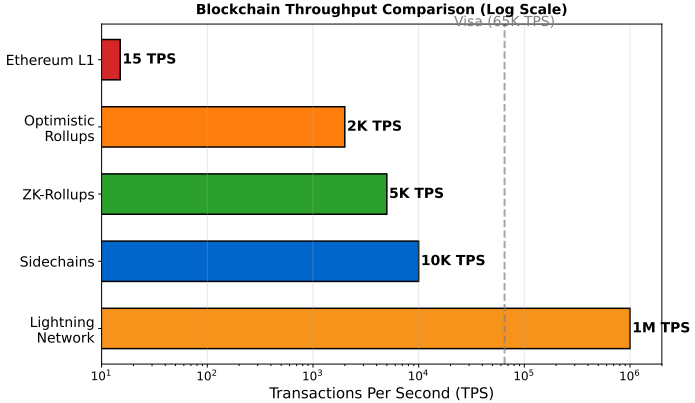
- Base blockchain protocol
- Full consensus for every transaction
- High security, low throughput
- Examples: Bitcoin, Ethereum

Layer 2 (L2)

- Built on top of L1
- Process transactions off-chain
- Settle final state on L1
- Inherit L1 security guarantees

Key Insight: Trade immediate finality for higher throughput

Throughput Comparison



L2s can match or exceed traditional payment networks like Visa

Layer 2 Design Patterns

State Channels:

- P2P direct channels
- Ex: Lightning Network

Sidechains:

- Independent chain
- Two-way peg to L1

Rollups:

- Batch off-chain
- Post data on-chain

Optimistic: Fraud proofs
ZK: Validity proofs

Plasma:

- Child chains
- Merkle commits

Validium:

- Off-chain DA
- Validity proofs

Lightning Network: Bitcoin's Layer 2

Problem: Bitcoin's 7 TPS cannot support global payments
Solution: Bidirectional payment channels
Mechanism:

1. Open channel (on-chain funding)
2. Transact off-chain (update state)
3. Close channel (broadcast to L1)

Network Topology:
Channels form payment routing graph

Capacity:

- Millions of TPS possible
- Sub-second finality
- Minimal on-chain footprint

Rollups: Ethereum's Scaling Strategy

Core Idea:
Execute off-chain, post compressed data on-chain
Architecture:

- **Data Availability**: TX data on L1
- **Computation**: Off-chain sequencer
- **State Roots**: Merkle root to L1

Benefits:

- 100-1000x throughput gain
- Inherit L1 security
- Lower transaction costs

Two Variants:
Optimistic vs ZK (differ in validity proof)

Optimistic Rollups

Mechanism

- Assume transactions valid by default
- Anyone can submit fraud proof
- Challenge period: 7 days
- If no challenge, state finalized

Advantages

- EVM compatibility (easy migration)
- Lower gas costs than L1

Fraud Proof System

- Verifier claims state is invalid
- Interactive bisection game on L1
- Dishonest party loses stake

Disadvantages

- Long withdrawal delay (7 days)
- Honest verifier assumption

(c) Joerg Osterrieder 2025

ZK-Rollups (Zero-Knowledge Rollups)

Mechanism:

- Cryptographic validity proofs per batch
- SNARK/STARK: Prove without revealing
- L1 verifies proof (constant cost)
- Finality: $\sim$10-30 min after proof

Advantages:

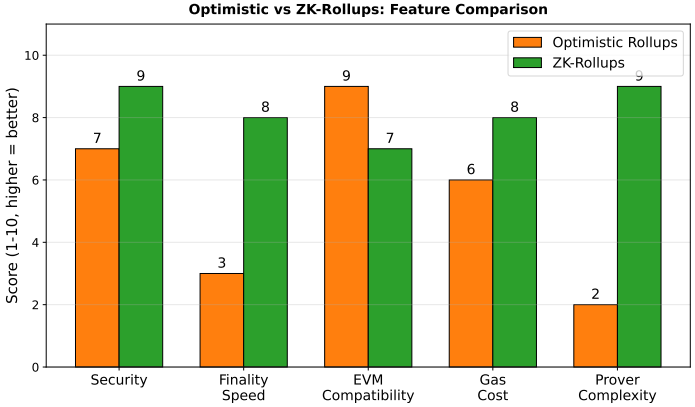
- Fast withdrawals (no challenge)
- Stronger security guarantees

Disadvantages:

- Complex crypto, higher prover costs
- EVM compatibility (improving)

(c) Joerg Osterrieder 2025

Optimistic vs ZK-Rollups



ZK-Rollups excel in security and finality; Optimistic wins on EVM compatibility

Sidechains

Definition

- Independent blockchain with own consensus
- Two-way peg to main chain
- Assets locked on L1, minted on sidechain

Examples

- Polygon PoS (Ethereum)
- Liquid Network (Bitcoin)

Advantages

- Custom consensus rules
- High throughput, low fees

Disadvantages

- **Weaker security**: Does NOT inherit L1 security
- Trust in sidechain validators
- Bridge attack surface

(c) Joerg Osterrieder 2025

Bridges: Connecting Chains

Purpose: Transfer assets between L1/L2 or across chains
Lock-and-Mint Pattern:

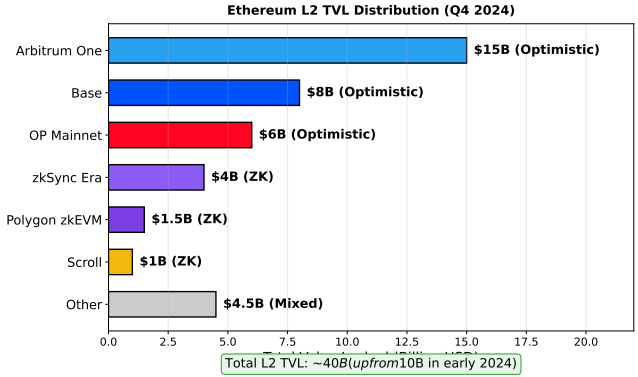
1. Lock assets on source chain
2. Mint wrapped tokens on dest
3. Burn to unlock original

Bridge Types:

- **Trusted**: Centralized (fast)
- **Federated**: Multi-sig ops
- **ZK-Verified**: Highest security

Risk: Major attack targets
($2B+ stolen 2022-2023)

L2 TVL Distribution



Arbitrum leads by TVL; optimistic rollups currently dominate

2024: The Year of Layer 2 Explosion

Dencun Upgrade (March 2024):

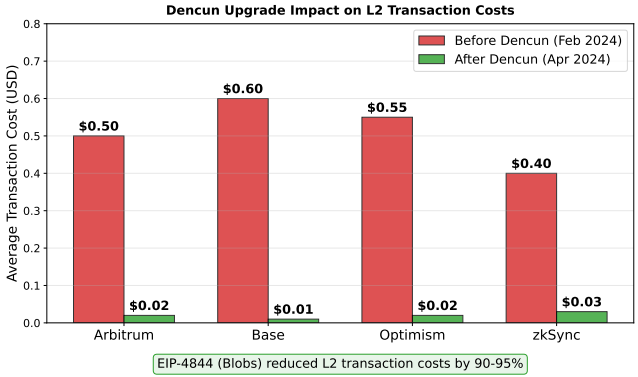
- EIP-4844 blob transactions
- L2 fees reduced by 90%+
- \$0.50-2.00 $\rightarrow$ \$0.01-0.05
- User migration accelerated

Key Trends:

- TVL: \$54B (205% YoY)
- L2 TX ¿ L1 daily volume
- App chains for specific use
- ZK maturity (zkSync, Scroll)

(c) Joerg Osterrieder 2025

Dencun Impact on L2 Fees



EIP-4844 blob transactions were the most significant scaling upgrade since the Merge

Security Comparison

Solution	Inherits L1 Security	Trust Model	Finality
Optimistic Rollup	Yes	1-of-N honest	7 days
ZK-Rollup	Yes	Cryptographic	10-30 min
State Channel	Yes	Counterparty online	Instant
Sidechain	No	Validator set	Chain-dependent

Key Takeaway: Rollups inherit L1 security; sidechains do not

(c) Joerg Osterrieder 2025

Future Directions

Scaling:

- **Full Danksharding**: 100K+ TPS
- **zkEVM**: Full EVM equivalence
- **Layer 3**: App-specific rollups

Infrastructure:

- **Interoperability**: Cross-rollup comms
- **Sequencer Decentralization**: Remove SPOF
- **Shared Sequencing**: Multi-rollup infra

Account Abstraction: The UX Revolution

EOA Problems:

- Must hold ETH for gas
- Single key = single point of failure
- No batching (2 TX for approve+swap)
- Lost key = lost funds forever

ERC-4337 Solution:

- Programmable smart wallets
- Custom validation (multi-sig, recovery)
- Sponsored transactions
- Bundled ops (1 click)

No protocol changes required – works on existing Ethereum

ERC-4337 Architecture

Key Components

- **UserOperation**: Pseudo-transaction struct
- **Bundler**: Collects and submits UserOps
- **EntryPoint**: On-chain singleton contract
- **Smart Account**: User's wallet contract
- **Paymaster**: Pays gas on user's behalf

Transaction Flow

1. User signs UserOperation
2. Bundler collects UserOps
3. Bundler submits batch to EntryPoint
4. EntryPoint validates and executes
5. Paymaster (optional) covers gas

ERC-4337 achieves account abstraction without modifying Ethereum protocol

Account Abstraction Use Cases

1. **Gasless Transactions:**
   - DApp sponsors gas for users
   - Pay gas in USDC/DAI
2. **Social Recovery:**
   - Guardians can recover wallet
   - No seed phrase SPOF
3. **Session Keys:**
   - Limited time permissions
   - Gaming: no constant signing
4. **Batch Transactions:**
   - Approve+swap+stake in 1 click
   - Better UX, lower gas

(c) Joerg Osterrieder 2025

Account Abstraction Adoption (2024-2025)

Milestones:

- Mar 2023: ERC-4337 mainnet
- 2024: Major wallet integration
- Late 2024: 10M+ smart accounts
- 2025: Default on L2s

Leading Implementations:

- **Safe**: Multi-sig + modular
- **Coinbase**: Passkey-based
- **ZeroDev**: Developer SDK
- **Alchemy**: Bundler infra

Account abstraction is key to achieving Web2-like UX in crypto

Problem Solved? Layer 2 Scaling

The Original Problem

How do we scale without sacrificing security?

How Layer 2 Scaling Solves It

- **Optimistic Rollups**: Assume validity by default, use fraud proofs for disputes (7-day challenge period)
- **ZK-Rollups**: Prove correct execution cryptographically via SNARKs/STARKs (10-30 min finality)
- **State Channels**: Move repeated interactions off-chain, settle final state on L1 (Lightning Network)

Remaining Limitations

- **Bridge Risk**: $2B+ stolen from cross-chain bridges (2022-2023)
- **Sequencer Centralization**: Most rollups use single sequencer (SPOF)
- **Withdrawal Delays**: Optimistic rollups require 7-day wait for L1 finality

Open Questions

- Will rollups become the dominant scaling paradigm, or will app-specific chains (L3s) fragment liquidity?
- Risk: Over-optimization for TPS at the expense of decentralization (sequencer monopolies)

Layer 2 Scaling solves throughput bottleneck but introduces new trust assumptions and operational complexity

(c) Joerg Osterrieder 2025

Summary

L2 Solutions:

- **State Channels**: P2P, instant (Lightning)
- **Optimistic**: Fraud proofs, 7-day wait
- **ZK-Rollups**: Validity proofs, fast

Key Developments:

- **EIP-4844**: L2 fees ↓90%
- **ERC-4337**: Smart wallets UX
- **Future**: L3s, danksharding

L2 solutions scale blockchains while preserving decentralization and security

Questions for Reflection

1. Why do optimistic rollups have a 7-day withdrawal delay?
2. What makes ZK-rollups more secure than optimistic rollups?
3. Why don't sidechains inherit Layer 1 security?
4. How did EIP-4844 reduce L2 transaction costs so dramatically?
5. How does ERC-4337 solve the onboarding problem for new crypto users?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the blockchain scalability trilemma?
A) Trade-off between speed, cost, and privacy
B) Trade-off between decentralization, security, and scalability
C) Trade-off between throughput, latency, and data availability
D) Trade-off between validators, miners, and users
Answer: B – The trilemma states you can only optimize 2 of 3 properties: decentralization, security, and scalability.

Q2. What is the approximate transaction throughput of Ethereum Layer 1?
A) 7 TPS B) 15 TPS C) 65 TPS D) 1000 TPS
Answer: B – Ethereum L1 processes around 15 transactions per second, while Bitcoin does 7 TPS.

Q3. What is the primary purpose of Layer 2 solutions?
A) Replace Layer 1 blockchains entirely
B) Process transactions off-chain while inheriting L1 security
C) Create new cryptocurrencies
D) Increase the block size of Layer 1
Answer: B – L2s move computation off-chain but settle final state on L1, inheriting its security.

Q4. Which Layer 2 pattern is used by Bitcoin's Lightning Network?
A) Rollups B) Sidechains C) State Channels D) Plasma
Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q5. What is the key difference between Layer 2 rollups and sidechains?
A) Rollups are faster than sidechains
B) Sidechains are cheaper than rollups
C) Rollups inherit L1 security; sidechains do not
D) Sidechains use proof-of-stake; rollups use proof-of-work
Answer: C – Rollups post data to L1 and inherit its security, while sidechains have independent consensus.

Quiz Questions (6–10)

Q6. How do optimistic rollups verify transaction validity?
A) Every transaction is verified immediately on L1
B) Transactions are assumed valid unless challenged with a fraud proof
C) Cryptographic proofs are generated for every batch
D) A trusted third party validates all transactions
Answer: B – Optimistic rollups assume validity by default and allow anyone to submit fraud proofs during a challenge period.

Q7. What is the typical withdrawal delay for optimistic rollups?
A) Instant B) 10-30 minutes C) 7 days D) 30 days
Answer: C – The 7-day challenge period allows time for fraud proofs before finalizing state.

Q8. What type of cryptographic proofs do ZK-Rollups use?
A) Proof-of-Work B) Fraud proofs C) SNARK/STARK proofs D) Merkle proofs
Answer: C – ZK-Rollups use SNARK or STARK zero-knowledge proofs to verify correct execution.

Q9. What is the main advantage of ZK-Rollups over optimistic rollups?
A) Lower transaction costs
B) Better EVM compatibility
C) Fast finality without challenge period (10-30 min)
D) Simpler technology
Answer: C – ZK-Rollups achieve finality after proof verification (10-30 min), avoiding the 7-day wait.

Q10. Which Ethereum upgrade significantly reduced L2 transaction fees in March 2024?
A) The Merge B) Shanghai upgrade C) Dencun upgrade (EIP-4844) D) Shapella
Answer: C – Dencun introduced blob transactions (EIP-4844), reducing L2 fees by 90%+.

Quiz Questions (11–15)

Q11. What was the approximate fee reduction after EIP-4844 implementation?
A) 10-20% reduction B) 50% reduction C) 90%+ reduction D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q12. Which L2 solution currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Polygon zkEVM
Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q13. What is the primary security risk associated with cross-chain bridges?
A) High gas fees
B) Slow transaction speed
C) Major attack target ($2B+ stolen in 2022-2023)
D) Incompatibility with smart contracts
Answer: C – Bridges are vulnerable to attacks, with over $2B stolen in recent years.

Q14. What is the "lock-and-mint" pattern used for?
A) Creating new cryptocurrencies
B) Transferring assets between chains via bridges
C) Mining new blocks
D) Validating transactions
Answer: B – Assets are locked on source chain, wrapped tokens minted on destination, then burned to unlock.

Q15. Which trust model provides the highest security for bridges?
A) Trusted (centralized custodian)
B) Federated (multi-sig operators)
C) ZK-Verified (cryptographic proofs)
D) All are equally secure
Answer: C – ZK-verified bridges use cryptographic proofs for the highest security level.

Quiz Questions (16–20)

Q16. What is the combined Layer 2 TVL as of late 2024?
A) $15B B) $30B C) $54B D) $100B
Answer: C – Combined L2 TVL reached $54B by Dec 2024 (205% YoY growth).

Q17. What is a Layer 3 (L3) solution?
A) A faster version of Layer 1
B) Application-specific rollups built on top of Layer 2
C) A replacement for Layer 2
D) A sidechain for Layer 1
Answer: B – L3s are specialized rollups built on L2s for specific applications.

Q18. What does "sequencer decentralization" aim to address?
A) High transaction fees
B) Slow transaction speed
C) Single point of failure in L2 architecture
D) EVM compatibility issues
Answer: C – Decentralizing sequencers removes the centralized bottleneck in current L2 designs.

Q19. What is the primary advantage of state channels like Lightning Network?
A) Highest security
B) Instant finality with millions of TPS
C) Best for smart contracts
D) Lowest setup cost
Answer: B – State channels enable instant finality and can handle millions of TPS for payments.

Q20. What future upgrade promises 100,000+ TPS through massive data availability?
A) EIP-4844 B) Full Danksharding C) The Merge D) zkEVM
Answer: B – Full Danksharding will dramatically increase data availability, enabling 100,000+ TPS.

Quiz Questions (21–24) – Account Abstraction

Q21. What standard defines Account Abstraction on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-4337 D) EIP-1559
Answer: C – ERC-4337 enables smart contract wallets without protocol changes.

Q22. What component in ERC-4337 allows third parties to pay gas for users?
A) Bundler B) EntryPoint C) Paymaster D) UserOperation
Answer: C – Paymasters sponsor gas fees, enabling gasless transactions for users.

Q23. Which is NOT a benefit of Account Abstraction?
A) Social recovery of wallets
B) Gasless transactions
C) Faster block times on L1
D) Batch transactions in single click
Answer: C – Account abstraction improves wallet UX, not L1 block production speed.

Q24. What role does the Bundler play in ERC-4337?
A) Validates smart contracts
B) Collects UserOperations and submits them to EntryPoint
C) Stores user private keys
D) Processes fraud proofs
Answer: B – Bundlers aggregate UserOps and submit batches to the EntryPoint contract.

L41: Layer 2 Scaling Solutions

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Why Should We Care About Layer 2 Scaling?

- Gas fees during NFT mints can exceed $200—users rage-quit to centralized exchanges
- The scalability trilemma forces impossible choices: speed, security, or decentralization—pick two

[COMIC: Frustrated user watching gas fees spike during mainnet congestion. Speech bubble: "$150 to send $20?!" Background shows Ethereum network traffic jam with transactions queued up]

[PLACEHOLDER] — When Ethereum gets congested, everyone pays the price—literally

Learning Objectives

- Describe the blockchain scalability trilemma
- Compare Layer 2 design patterns (channels, rollups, sidechains)
- Analyze Optimistic vs ZK-Rollups tradeoffs
- Evaluate the impact of Dencun upgrade (EIP-4844)
- Explain Account Abstraction (ERC-4337) and its UX improvements

Building on L40: Lab: Testnet Lending

The Problem: How do we scale without sacrificing security?

The Challenge
Ethereum can only process 15 transactions per second, while Visa handles 65,000 TPS (transactions per second). Traditional scaling approaches (increasing block size, reducing block time) sacrifice decentralization or security.

Why It Matters

- High gas fees (∼$50-200 during peak) exclude everyday users
- Bitcoin Lightning Network launched in 2018, but adoption remains low
- Ethereum's Dencun upgrade (March 2024) reduced L2 fees by 90% via EIP-4844

What We Need

- Understanding design constraints
- Mechanisms that inherit L1 security while increasing throughput 10-1000x
- Solutions that don't require users to trust new validator sets

The Cryptoeconomics Question
How do we optimize for scalability without breaking decentralization or security?

Today's lesson: How Layer 2 Scaling addresses this challenge

Why Can't Blockchains Have It All?

The Trilemma:
Can only optimize 2 of 3 properties:

- **Decentralization**: Independent validators
- **Security**: Cost to attack network
- **Scalability**: TPS throughput

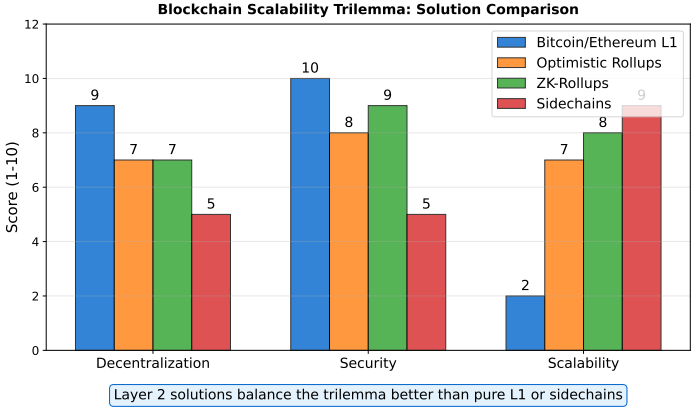
Current TPS:

- Bitcoin: ∼7 TPS
- Ethereum: ∼15 TPS
- Visa: ∼65,000 TPS

Solution: Layer 2 moves transactions off-chain while inheriting L1 security

→ *Problem: How do we scale without sacrificing... — The Blockchain Scalability Trilemma shows we cannot have decentralization, security, AND scalability simultaneously—L2 solutions choose which to optimize*

How Do Different Solutions Navigate the Trilemma?



Rollups achieve better balance than L1 alone or sidechains

How Does Layer 2 Make Ethereum Faster?

Layer 1 (L1)

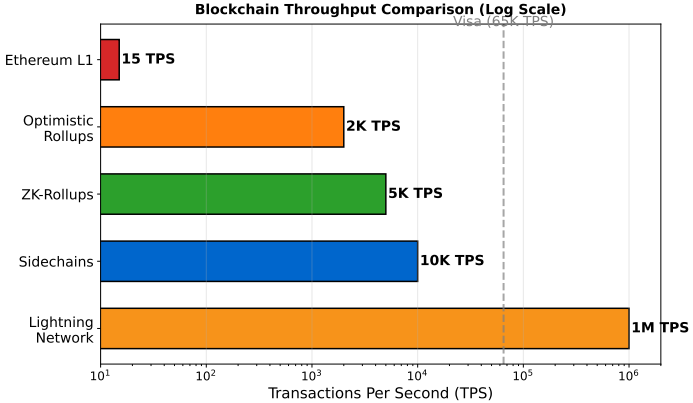
- Base blockchain protocol
- Full consensus for every transaction
- High security, low throughput
- Examples: Bitcoin, Ethereum

Layer 2 (L2)

- Built on top of L1
- Process transactions off-chain
- Settle final state on L1
- Inherit L1 security guarantees

Key Insight: Trade immediate finality for higher throughput

How Much Faster Are Layer 2 Solutions?



L2s can match or exceed traditional payment networks like Visa

What Are the Different Layer 2 Approaches?

State Channels:

- P2P direct channels
- Ex: Lightning Network

Sidechains:

- Independent chain
- Two-way peg to L1

Rollups:

(batch transactions off-chain, post summaries to L1)

- Batch off-chain
- Post data on-chain

Optimistic: Fraud proofs
ZK: Validity proofs

Plasma:

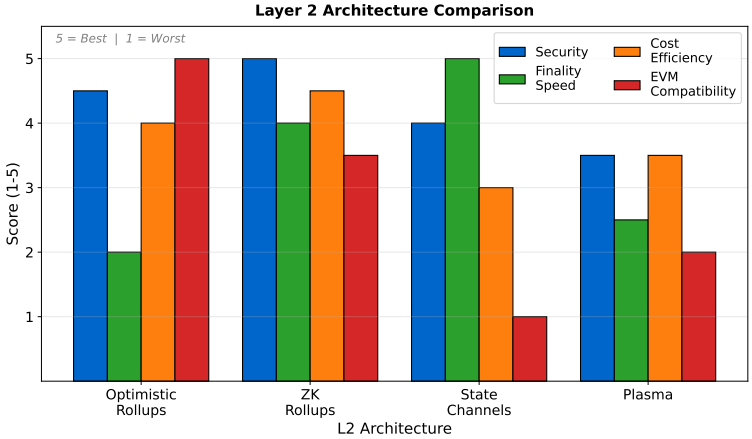
- Child chains
- Merkle commits

Validium:

- Off-chain DA
- Validity proofs

(c) Joerg Osterrieder 2025

How Do Layer 2 Architectures Compare?



ZK-Rollups excel in security; State Channels offer instant finality; Optimistic Rollups lead in EVM compatibility

How Does Lightning Network Scale Bitcoin?

Problem: Bitcoin's 7 TPS cannot support global payments
Solution: Bidirectional payment channels
Mechanism:

1. Open channel (on-chain funding)
2. Transact off-chain (update state)
3. Close channel (broadcast to L1)

Network Topology:
Channels form payment routing graph

Capacity:

- Millions of TPS possible
- Sub-second finality
- Minimal on-chain footprint

→ *Problem: How do we scale without sacrificing... — Lightning Network: Bitcoin's Layer 2 demonstrates moving transactions off-chain solves throughput but requires trust in channel counterparties staying online*

Why Are Rollups Ethereum's Best Bet?

Core Idea:
Execute off-chain, post compressed data on-chain
Architecture:

- **Data Availability (DA)**: TX data on L1 (ensuring data is accessible for verification)
- **Computation**: Off-chain sequencer (operator that orders transactions for a rollup)
- **State Roots**: Merkle root to L1

Benefits:

- 100-1000x throughput gain
- Inherit L1 security
- Lower transaction costs

Two Variants:
Optimistic vs ZK (differ in validity proof)

How Do Optimistic Rollups Work?

Mechanism

- Assume transactions valid by default
- Anyone can submit fraud proof (evidence proving a transaction was invalid)
- Challenge period: 7 days
- If no challenge, state finalized

Advantages

- EVM compatibility (easy migration)
- Lower gas costs than L1

Fraud Proof System

- Verifier claims state is invalid
- Interactive bisection game on L1
- Dishonest party loses stake

Disadvantages

- Long withdrawal delay (7 days)
- Honest verifier assumption

What Makes ZK-Rollups More Secure?

Mechanism:

- Cryptographic validity proofs per batch
- SNARK/STARK: Prove without revealing
- L1 verifies proof (constant cost)
- Finality: $\sim$10-30 min after proof

Advantages:

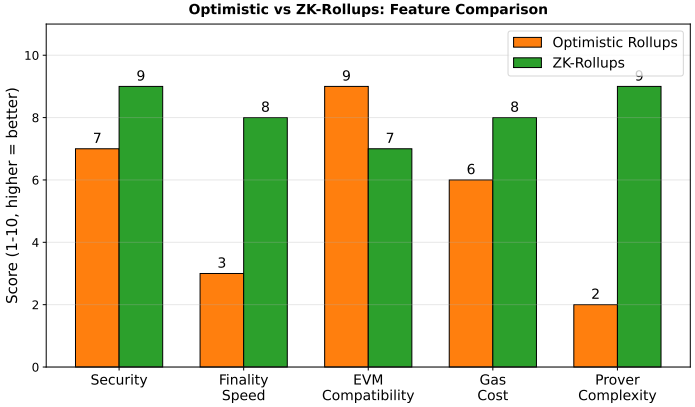
- Fast withdrawals (no challenge)
- Stronger security guarantees

Disadvantages:

- Complex crypto, higher prover costs
- EVM compatibility (improving)

(c) Joerg Osterrieder 2025

What's the Difference Between Optimistic and ZK-Rollups?



ZK-Rollups excel in security and finality; Optimistic wins on EVM compatibility

Problem Check-In: Layer 2 Scaling

Recall Our Problem

How do we scale without sacrificing security?

What We've Learned So Far

- The scalability trilemma forces trade-offs: you cannot maximize decentralization, security, AND throughput
- L2 solutions (rollups, channels, sidechains) move computation off-chain while settling on L1
- These patterns let us scale 100-1000x while choosing which security properties to preserve

Still to Address

- How specific rollup types (Optimistic vs ZK) differ in their security/speed trade-offs
- Do rollups truly inherit L1 security, or do sequencer centralization and bridge risks undermine this?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we scale without sacrificing..."?

(c) Joerg Osterrieder 2025

Why Don't Sidechains Inherit L1 Security?

Definition

- Independent blockchain with own consensus
- Two-way peg to main chain
- Assets locked on L1, minted on sidechain

Examples

- Polygon PoS (Ethereum)
- Liquid Network (Bitcoin)

Advantages

- Custom consensus rules
- High throughput, low fees

Disadvantages

- **Weaker security**: Does NOT inherit L1 security
- Trust in sidechain validators
- Bridge attack surface

→ *Problem: How do we scale without sacrificing... — Sidechains reveals sidechains sacrifice L1 security inheritance—faster but riskier than rollups*

How Do Bridges Connect Different Chains?

Purpose: Transfer assets between L1/L2 or across chains
Lock-and-Mint Pattern:

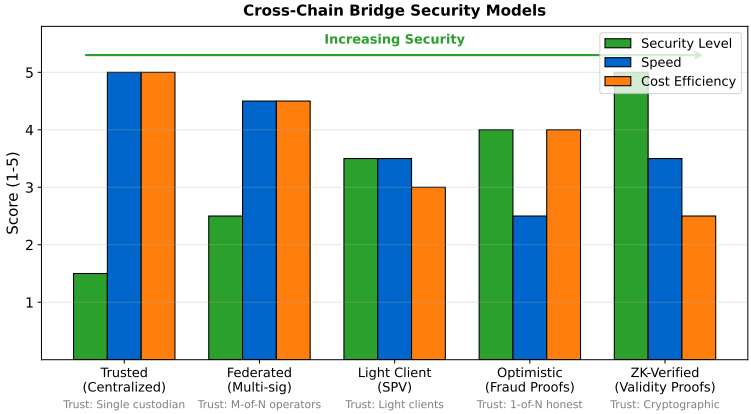
1. Lock assets on source chain
2. Mint wrapped tokens on dest
3. Burn to unlock original

Bridge Types:

- **Trusted**: Centralized (fast)
- **Federated**: Multi-sig ops
- **ZK-Verified**: Highest security

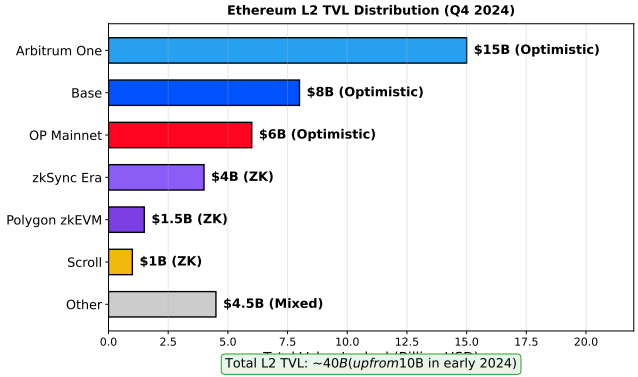
Risk: Major attack targets
($2B+ stolen 2022-2023)

How Do Bridge Security Models Compare?



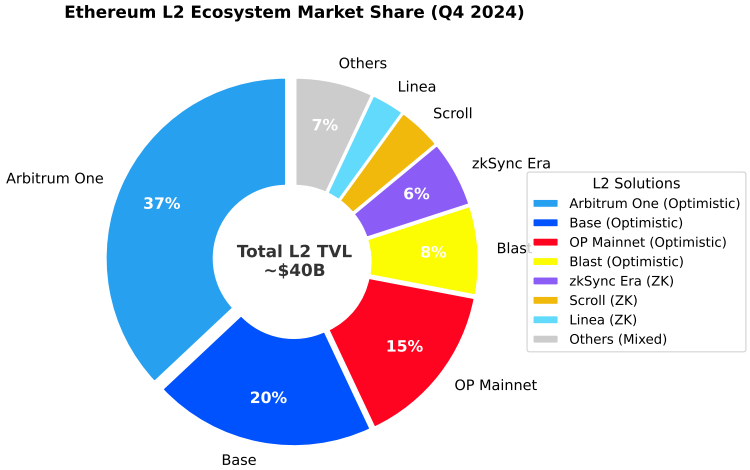
ZK-verified bridges offer the highest security; trusted bridges are fastest but riskiest

Where Is Layer 2 Value Locked?



Arbitrum leads by TVL; optimistic rollups currently dominate

Who Leads the Layer 2 Ecosystem?



Optimistic rollups (Arbitrum, Base, OP) hold 72% market share; ZK rollups growing rapidly

Why Did Layer 2 Explode in 2024?

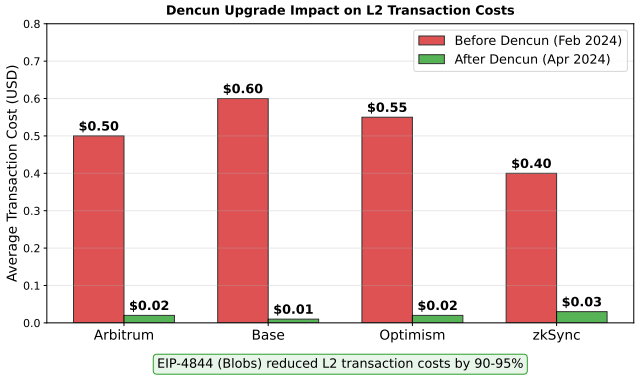
Dencun Upgrade (March 2024):

- EIP-4844 blob transactions
- L2 fees reduced by 90%+
- \$0.50-2.00 $\rightarrow$ \$0.01-0.05
- User migration accelerated

Key Trends:

- TVL: \$54B (205% YoY)
- L2 TX ¿ L1 daily volume
- App chains for specific use
- ZK maturity (zkSync, Scroll)

How Much Did Dencun Reduce Layer 2 Fees?



EIP-4844 blob transactions were the most significant scaling upgrade since the Merge

How Do Security Models Compare?

Solution	Inherits L1 Security	Trust Model	Finality
Optimistic Rollup	Yes	1-of-N honest	7 days
ZK-Rollup	Yes	Cryptographic	10-30 min
State Channel	Yes	Counterparty online	Instant
Sidechain	No	Validator set	Chain-dependent

Key Takeaway: Rollups inherit L1 security; sidechains do not

→ Problem: How do we scale without sacrificing... — Security Comparison confirms rollups inherit L1 security while sidechains require trusting a new validator set—the core scaling trade-off

What's Next for Layer 2 Scaling?

Scaling:

- **Full Danksharding**: 100K+ TPS
- **zkEVM**: Full EVM equivalence
- **Layer 3**: App-specific rollups

Infrastructure:

- **Interoperability**: Cross-rollup comms
- **Sequencer Decentralization**: Remove SPOF
- **Shared Sequencing**: Multi-rollup infra

How Does Account Abstraction Fix Wallet UX?

EOA Problems:

- Must hold ETH for gas
- Single key = single point of failure
- No batching (2 TX for approve+swap)
- Lost key = lost funds forever

ERC-4337 Solution:

- Programmable smart wallets
- Custom validation (multi-sig, recovery)
- Sponsored transactions
- Bundled ops (1 click)

No protocol changes required – works on existing Ethereum

How Does ERC-4337 Work?

Key Components

- **UserOperation**: Pseudo-transaction struct
- **Bundler**: Collects and submits UserOps
- **EntryPoint**: On-chain singleton contract
- **Smart Account**: User's wallet contract
- **Paymaster**: Pays gas on user's behalf

Transaction Flow

1. User signs UserOperation
2. Bundler collects UserOps
3. Bundler submits batch to EntryPoint
4. EntryPoint validates and executes
5. Paymaster (optional) covers gas

ERC-4337 achieves account abstraction without modifying Ethereum protocol

What Can You Do with Smart Wallets?

1. **Gasless Transactions:**
   - DApp sponsors gas for users
   - Pay gas in USDC/DAI
2. **Social Recovery:**
   - Guardians can recover wallet
   - No seed phrase SPOF
3. **Session Keys:**
   - Limited time permissions
   - Gaming: no constant signing
4. **Batch Transactions:**
   - Approve+swap+stake in 1 click
   - Better UX, lower gas

How Widely Adopted Is Account Abstraction?

Milestones:

- Mar 2023: ERC-4337 mainnet
- 2024: Major wallet integration
- Late 2024: 10M+ smart accounts
- 2025: Default on L2s

Leading Implementations:

- **Safe**: Multi-sig + modular
- **Coinbase**: Passkey-based
- **ZeroDev**: Developer SDK
- **Alchemy**: Bundler infra

Account abstraction is key to achieving Web2-like UX in crypto

Problem Solved? Layer 2 Scaling

The Original Problem

How do we scale without sacrificing security?

How Layer 2 Scaling Solves It

- **Optimistic Rollups**: Assume validity by default, use fraud proofs for disputes (7-day challenge period)
- **ZK-Rollups**: Prove correct execution cryptographically via SNARKs/STARKs (10-30 min finality)
- **State Channels**: Move repeated interactions off-chain, settle final state on L1 (Lightning Network)

Remaining Limitations

- **Bridge Risk**: $2B+ stolen from cross-chain bridges (2022-2023)
- **Sequencer Centralization**: Most rollups use single sequencer (SPOF)
- **Withdrawal Delays**: Optimistic rollups require 7-day wait for L1 finality

Open Questions

- Will rollups become the dominant scaling paradigm, or will app-specific chains (L3s) fragment liquidity?
- Risk: Over-optimization for TPS at the expense of decentralization (sequencer monopolies)

Layer 2 Scaling solves throughput bottleneck but introduces new trust assumptions and operational complexity

(c) Joerg Osterrieder 2025

The Economics of Layer 2 Scaling

Incentive Structure

- **Core Problem:** Optimizing multiple competing goals
- **Why act honestly?** Choose based on use case requirements
- **Value Flow:** Gain in one dimension, sacrifice in another

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Gain in one dimension, sacrifice in another

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Layer 2 Scaling

Alternatives Considered

1. **Chosen Design:** Different points on trade-off frontier
2. **Alternative:** Layer 2 solutions, hybrid approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Layer 2 Scaling

Critical Failure Mode

- **What breaks:** Over-optimization for single metric
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

What Are the Real Risks of Layer 2?

- Bridges are the weakest link: $2B+ stolen from cross-chain exploits (2022-2023)
- Moving assets between L1 and L2 requires trust in bridge security—a new attack surface

[COMIC: User nervously crossing a rickety bridge labeled "L1 to L2" while hackers saw at the ropes below. Warning sign reads: "Bridge Exploits Ahead!" User's assets shown as bags of money on the swaying bridge]

[PLACEHOLDER] — Layer 2 solves scalability but bridges introduce new risks—always verify bridge security models

Summary

L2 Solutions:

- **State Channels**: P2P, instant (Lightning)
- **Optimistic**: Fraud proofs, 7-day wait
- **ZK-Rollups**: Validity proofs, fast

Next Lesson: L42 – Flash Loans

Key Developments:

- **EIP-4844**: L2 fees ↓90%
- **ERC-4337**: Smart wallets UX
- **Future**: L3s, danksharding

L2 solutions scale blockchains while preserving decentralization and security

Questions for Reflection

1. Why do optimistic rollups have a 7-day withdrawal delay?
2. What makes ZK-rollups more secure than optimistic rollups?
3. Why don't sidechains inherit Layer 1 security?
4. How did EIP-4844 reduce L2 transaction costs so dramatically?
5. How does ERC-4337 solve the onboarding problem for new crypto users?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the blockchain scalability trilemma?
A) Trade-off between speed, cost, and privacy
B) Trade-off between decentralization, security, and scalability
C) Trade-off between throughput, latency, and data availability
D) Trade-off between validators, miners, and users
Answer: B – The trilemma states you can only optimize 2 of 3 properties: decentralization, security, and scalability.

Q2. What is the approximate transaction throughput of Ethereum Layer 1?
A) 7 TPS B) 15 TPS C) 65 TPS D) 1000 TPS
Answer: B – Ethereum L1 processes around 15 transactions per second, while Bitcoin does 7 TPS.

Q3. What is the primary purpose of Layer 2 solutions?
A) Replace Layer 1 blockchains entirely
B) Process transactions off-chain while inheriting L1 security
C) Create new cryptocurrencies
D) Increase the block size of Layer 1
Answer: B – L2s move computation off-chain but settle final state on L1, inheriting its security.

Q4. Which Layer 2 pattern is used by Bitcoin's Lightning Network?
A) Rollups B) Sidechains C) State Channels D) Plasma
Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q5. What is the key difference between Layer 2 rollups and sidechains?
A) Rollups are faster than sidechains
B) Sidechains are cheaper than rollups
C) Rollups inherit L1 security; sidechains do not
D) Sidechains use proof-of-stake; rollups use proof-of-work
Answer: C – Rollups post data to L1 and inherit its security, while sidechains have independent consensus.

Quiz Questions (6–10)

Q6. How do optimistic rollups verify transaction validity?
A) Every transaction is verified immediately on L1
B) Transactions are assumed valid unless challenged with a fraud proof
C) Cryptographic proofs are generated for every batch
D) A trusted third party validates all transactions
Answer: B – Optimistic rollups assume validity by default and allow anyone to submit fraud proofs during a challenge period.

Q7. What is the typical withdrawal delay for optimistic rollups?
A) Instant B) 10-30 minutes C) 7 days D) 30 days
Answer: C – The 7-day challenge period allows time for fraud proofs before finalizing state.

Q8. What type of cryptographic proofs do ZK-Rollups use?
A) Proof-of-Work B) Fraud proofs C) SNARK/STARK proofs D) Merkle proofs
Answer: C – ZK-Rollups use SNARK or STARK zero-knowledge proofs to verify correct execution.

Q9. What is the main advantage of ZK-Rollups over optimistic rollups?
A) Lower transaction costs
B) Better EVM compatibility
C) Fast finality without challenge period (10-30 min)
D) Simpler technology
Answer: C – ZK-Rollups achieve finality after proof verification (10-30 min), avoiding the 7-day wait.

Q10. Which Ethereum upgrade significantly reduced L2 transaction fees in March 2024?
A) The Merge B) Shanghai upgrade C) Dencun upgrade (EIP-4844) D) Shapella
Answer: C – Dencun introduced blob transactions (EIP-4844), reducing L2 fees by 90%+.

Quiz Questions (11–15)

Q11. What was the approximate fee reduction after EIP-4844 implementation?
A) 10-20% reduction B) 50% reduction C) 90%+ reduction D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q12. Which L2 solution currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Polygon zkEVM
Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q13. What is the primary security risk associated with cross-chain bridges?
A) High gas fees
B) Slow transaction speed
C) Major attack target ($2B+ stolen in 2022-2023)
D) Incompatibility with smart contracts
Answer: C – Bridges are vulnerable to attacks, with over $2B stolen in recent years.

Q14. What is the "lock-and-mint" pattern used for?
A) Creating new cryptocurrencies
B) Transferring assets between chains via bridges
C) Mining new blocks
D) Validating transactions
Answer: B – Assets are locked on source chain, wrapped tokens minted on destination, then burned to unlock.

Q15. Which trust model provides the highest security for bridges?
A) Trusted (centralized custodian)
B) Federated (multi-sig operators)
C) ZK-Verified (cryptographic proofs)
D) All are equally secure
Answer: C – ZK-verified bridges use cryptographic proofs for the highest security level.

Quiz Questions (16–20)

Q16. What is the combined Layer 2 TVL as of late 2024?
A) $15B B) $30B C) $54B D) $100B
Answer: C – Combined L2 TVL reached $54B by Dec 2024 (205% YoY growth).

Q17. What is a Layer 3 (L3) solution?
A) A faster version of Layer 1
B) Application-specific rollups built on top of Layer 2
C) A replacement for Layer 2
D) A sidechain for Layer 1
Answer: B – L3s are specialized rollups built on L2s for specific applications.

Q18. What does "sequencer decentralization" aim to address?
A) High transaction fees
B) Slow transaction speed
C) Single point of failure in L2 architecture
D) EVM compatibility issues
Answer: C – Decentralizing sequencers removes the centralized bottleneck in current L2 designs.

Q19. What is the primary advantage of state channels like Lightning Network?
A) Highest security
B) Instant finality with millions of TPS
C) Best for smart contracts
D) Lowest setup cost
Answer: B – State channels enable instant finality and can handle millions of TPS for payments.

Q20. What future upgrade promises 100,000+ TPS through massive data availability?
A) EIP-4844 B) Full Danksharding C) The Merge D) zkEVM
Answer: B – Full Danksharding will dramatically increase data availability, enabling 100,000+ TPS.

Quiz Questions (21–24) – Account Abstraction

Q21. What standard defines Account Abstraction on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-4337 D) EIP-1559
Answer: C – ERC-4337 enables smart contract wallets without protocol changes.

Q22. What component in ERC-4337 allows third parties to pay gas for users?
A) Bundler B) EntryPoint C) Paymaster D) UserOperation
Answer: C – Paymasters sponsor gas fees, enabling gasless transactions for users.

Q23. Which is NOT a benefit of Account Abstraction?
A) Social recovery of wallets
B) Gasless transactions
C) Faster block times on L1
D) Batch transactions in single click
Answer: C – Account abstraction improves wallet UX, not L1 block production speed.

Q24. What role does the Bundler play in ERC-4337?
A) Validates smart contracts
B) Collects UserOperations and submits them to EntryPoint
C) Stores user private keys
D) Processes fraud proofs
Answer: B – Bundlers aggregate UserOps and submit batches to the EntryPoint contract.

L41: Layer 2 Scaling Solutions

Mini-Lecture – Module F: Advanced Topics

Blockchain & Cryptocurrency Course

January 2026

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Describe the blockchain scalability trilemma
- Compare Layer 2 design patterns (channels, rollups, sidechains)
- Analyze Optimistic vs ZK-Rollups tradeoffs
- Evaluate the impact of Dencun upgrade (EIP-4844)

Scalability Trilemma

charts/01_scalability_trilemma/chart.pdf

What is Layer 2?

Layer 1 (L1):

- Base blockchain (Bitcoin, Ethereum)
- Full consensus for every tx; high security, low throughput
- Bitcoin: 7 TPS, Ethereum: 15 TPS

Layer 2 (L2):

- Built on top of L1; process tx off-chain
- Settle final state on L1; inherit L1 security
- Throughput: 100-1000x improvement

Key Trade-off: Immediate finality for higher throughput.

L2 Throughput Comparison

charts/02_l2_throughput_comparison/chart.pdf

Layer 2 Design Patterns

1. **State Channels:** Direct peer-to-peer (Lightning Network)
2. **Sidechains:** Independent blockchain with two-way peg
3. **Rollups:** Batch tx, compute off-chain, post data on-chain
   - **Optimistic:** Assume valid, allow fraud proofs (7-day delay)
   - **ZK-Rollups:** Cryptographic validity proofs (instant finality)
4. **Plasma:** Hierarchical child chains
5. **Validium:** Off-chain data + validity proofs

(c) Joerg Osterrieder 2025

Optimistic vs ZK-Rollups

charts/03_rollup_types/chart.pdf

Major Layer 2 Networks

Optimistic Rollups:

- **Arbitrum:** Largest TVL ($12B); Nitro upgrade
- **Optimism:** OP Stack framework; Base uses it
- **Base:** Coinbase L2; fastest growing (43% L2 share)

ZK-Rollups:

- **zkSync Era:** EVM-compatible ZK
- **StarkNet:** Cairo language; account abstraction native
- **Polygon zkEVM:** ZK + full EVM equivalence

L2 TVL Growth

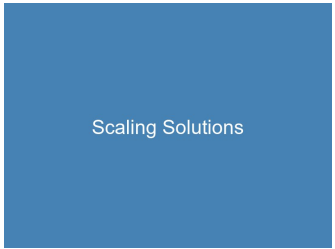
charts/04_l2_tvl/chart.pdf

Key Takeaways

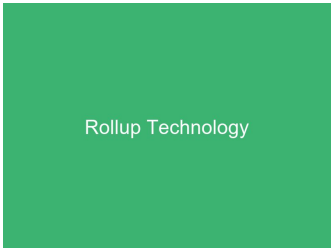
1. **Trilemma:** Optimize 2 of 3: decentralization, security, scalability
2. **L2 Purpose:** Off-chain compute, L1 data availability, inherit security
3. **Optimistic Rollups:** EVM compatible, 7-day withdrawal delay
4. **ZK-Rollups:** Instant finality, complex cryptography
5. **Base Leads:** 43% L2 market share (Dec 2025)

Next: L42 – Flash Loans

Layer 2 in Practice



Scaling Solutions



Rollup Tech

Network Growth

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) Three blockchains B) Cannot optimize all 3 properties C) Three layers D) Three tokens

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) Three blockchains B) Cannot optimize all 3 properties C) Three layers D) Three tokens
Answer: B – Decentralization, security, scalability: pick 2.

Q2. Ethereum L1 TPS?
A) 7 B) 15 C) 100 D) 1000

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) Three blockchains B) Cannot optimize all 3 properties C) Three layers D) Three tokens
Answer: B – Decentralization, security, scalability: pick 2.

Q2. Ethereum L1 TPS?
A) 7 B) 15 C) 100 D) 1000
Answer: B – Ethereum 15 TPS; Bitcoin 7 TPS.

Q3. What do rollups do?
A) Store all data off-chain B) Execute off-chain, post data on-chain C) Replace L1 D) Mine faster

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) Three blockchains B) Cannot optimize all 3 properties C) Three layers D) Three tokens
Answer: B – Decentralization, security, scalability: pick 2.

Q2. Ethereum L1 TPS?
A) 7 B) 15 C) 100 D) 1000
Answer: B – Ethereum 15 TPS; Bitcoin 7 TPS.

Q3. What do rollups do?
A) Store all data off-chain B) Execute off-chain, post data on-chain C) Replace L1 D) Mine faster
Answer: B – Compute off-chain, data on L1.

Q4. Optimistic rollup withdrawal delay?
A) Instant B) 1 hour C) 7 days D) 30 days

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) Three blockchains B) Cannot optimize all 3 properties C) Three layers D) Three tokens
Answer: B – Decentralization, security, scalability: pick 2.

Q2. Ethereum L1 TPS?
A) 7 B) 15 C) 100 D) 1000
Answer: B – Ethereum 15 TPS; Bitcoin 7 TPS.

Q3. What do rollups do?
A) Store all data off-chain B) Execute off-chain, post data on-chain C) Replace L1 D) Mine faster
Answer: B – Compute off-chain, data on L1.

Q4. Optimistic rollup withdrawal delay?
A) Instant B) 1 hour C) 7 days D) 30 days
Answer: C – Challenge period for fraud proofs.

Q5. ZK-Rollup advantage over Optimistic?
A) Lower cost B) Faster finality C) Better EVM compatibility D) Simpler code

Quiz (1/2)

Q1. What is the blockchain scalability trilemma?
A) Three blockchains B) Cannot optimize all 3 properties C) Three layers D) Three tokens
Answer: B – Decentralization, security, scalability: pick 2.

Q2. Ethereum L1 TPS?
A) 7 B) 15 C) 100 D) 1000
Answer: B – Ethereum 15 TPS; Bitcoin 7 TPS.

Q3. What do rollups do?
A) Store all data off-chain B) Execute off-chain, post data on-chain C) Replace L1 D) Mine faster
Answer: B – Compute off-chain, data on L1.

Q4. Optimistic rollup withdrawal delay?
A) Instant B) 1 hour C) 7 days D) 30 days
Answer: C – Challenge period for fraud proofs.

Q5. ZK-Rollup advantage over Optimistic?
A) Lower cost B) Faster finality C) Better EVM compatibility D) Simpler code
Answer: B – Instant finality after proof verification.

Quiz (2/2)

Q6. What is Lightning Network?
A) Ethereum L2 B) Bitcoin payment channels C) ZK-Rollup D) Sidechain

Quiz (2/2)

Q6. What is Lightning Network?
A) Ethereum L2 B) Bitcoin payment channels C) ZK-Rollup D) Sidechain
Answer: B – State channels for Bitcoin payments.

Q7. Which L2 has largest market share (Dec 2025)?
A) Arbitrum B) Optimism C) Base D) zkSync

Quiz (2/2)

Q6. What is Lightning Network?
A) Ethereum L2 B) Bitcoin payment channels C) ZK-Rollup D) Sidechain
Answer: B – State channels for Bitcoin payments.

Q7. Which L2 has largest market share (Dec 2025)?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads with 43% share.

Q8. What is a sidechain's security model?
A) Inherits L1 security B) Has own consensus C) No security D) Uses oracles

Quiz (2/2)

Q6. What is Lightning Network?
A) Ethereum L2 B) Bitcoin payment channels C) ZK-Rollup D) Sidechain
Answer: B – State channels for Bitcoin payments.

Q7. Which L2 has largest market share (Dec 2025)?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads with 43% share.

Q8. What is a sidechain's security model?
A) Inherits L1 security B) Has own consensus C) No security D) Uses oracles
Answer: B – Independent consensus; does NOT inherit L1 security.

Q9. What upgrade reduced L2 fees by 10x?
A) The Merge B) Shanghai C) Dencun (EIP-4844) D) Cancun

Quiz (2/2)

Q6. What is Lightning Network?
A) Ethereum L2 B) Bitcoin payment channels C) ZK-Rollup D) Sidechain
Answer: B – State channels for Bitcoin payments.

Q7. Which L2 has largest market share (Dec 2025)?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads with 43% share.

Q8. What is a sidechain's security model?
A) Inherits L1 security B) Has own consensus C) No security D) Uses oracles
Answer: B – Independent consensus; does NOT inherit L1 security.

Q9. What upgrade reduced L2 fees by 10x?
A) The Merge B) Shanghai C) Dencun (EIP-4844) D) Cancun
Answer: C – Dencun introduced blob data for cheaper L2 posting.

Q10. Optimistic rollup disadvantage?
A) Complex math B) Long withdrawal delay C) Low throughput D) High fees

Quiz (2/2)

Q6. What is Lightning Network?
A) Ethereum L2 B) Bitcoin payment channels C) ZK-Rollup D) Sidechain
Answer: B – State channels for Bitcoin payments.

Q7. Which L2 has largest market share (Dec 2025)?
A) Arbitrum B) Optimism C) Base D) zkSync
Answer: C – Base leads with 43% share.

Q8. What is a sidechain's security model?
A) Inherits L1 security B) Has own consensus C) No security D) Uses oracles
Answer: B – Independent consensus; does NOT inherit L1 security.

Q9. What upgrade reduced L2 fees by 10x?
A) The Merge B) Shanghai C) Dencun (EIP-4844) D) Cancun
Answer: C – Dencun introduced blob data for cheaper L2 posting.

Q10. Optimistic rollup disadvantage?
A) Complex math B) Long withdrawal delay C) Low throughput D) High fees
Answer: B – 7-day challenge period.

Thank you

Questions?

Next: L42 – Flash Loans

Quiz: Layer2 Scaling

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) Speed, cost, privacy B) Decentralization, security, scalability C) Throughput, latency, data D) Validators, miners, users

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) Speed, cost, privacy B) Decentralization, security, scalability C) Throughput, latency, data D) Validators, miners, users
Answer: B – Can only optimize 2 of 3: decentralization, security, and scalability.

Q2. Which Layer 2 pattern does Bitcoin's Lightning Network use?
A) Rollups B) Sidechains C) State Channels D) Plasma

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) Speed, cost, privacy B) Decentralization, security, scalability C) Throughput, latency, data D) Validators, miners, users
Answer: B – Can only optimize 2 of 3: decentralization, security, and scalability.

Q2. Which Layer 2 pattern does Bitcoin's Lightning Network use?
A) Rollups B) Sidechains C) State Channels D) Plasma
Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q3. What is the key difference between rollups and sidechains?
A) Rollups are faster B) Sidechains are cheaper C) Rollups inherit L1 security; sidechains do not D) Sidechains use PoS

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) Speed, cost, privacy B) Decentralization, security, scalability C) Throughput, latency, data D) Validators, miners, users
Answer: B – Can only optimize 2 of 3: decentralization, security, and scalability.

Q2. Which Layer 2 pattern does Bitcoin's Lightning Network use?
A) Rollups B) Sidechains C) State Channels D) Plasma
Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q3. What is the key difference between rollups and sidechains?
A) Rollups are faster B) Sidechains are cheaper C) Rollups inherit L1 security; sidechains do not D) Sidechains use PoS
Answer: C – Rollups post data to L1 and inherit its security; sidechains have independent consensus.

Q4. What is the typical withdrawal delay for optimistic rollups?
A) Instant B) 10-30 minutes C) 7 days D) 30 days

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) Speed, cost, privacy B) Decentralization, security, scalability C) Throughput, latency, data D) Validators, miners, users
Answer: B – Can only optimize 2 of 3: decentralization, security, and scalability.

Q2. Which Layer 2 pattern does Bitcoin's Lightning Network use?
A) Rollups B) Sidechains C) State Channels D) Plasma
Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q3. What is the key difference between rollups and sidechains?
A) Rollups are faster B) Sidechains are cheaper C) Rollups inherit L1 security; sidechains do not D) Sidechains use PoS
Answer: C – Rollups post data to L1 and inherit its security; sidechains have independent consensus.

Q4. What is the typical withdrawal delay for optimistic rollups?
A) Instant B) 10-30 minutes C) 7 days D) 30 days
Answer: C – The 7-day challenge period allows time for fraud proofs.

Q5. Which cryptographic proofs do ZK-Rollups use?
A) Proof-of-Work B) Fraud proofs C) SNARK/STARK proofs D) Merkle proofs

Quiz (1–5)

Q1. What is the blockchain scalability trilemma?
A) Speed, cost, privacy B) Decentralization, security, scalability C) Throughput, latency, data D) Validators, miners, users
Answer: B – Can only optimize 2 of 3: decentralization, security, and scalability.

Q2. Which Layer 2 pattern does Bitcoin's Lightning Network use?
A) Rollups B) Sidechains C) State Channels D) Plasma
Answer: C – Lightning uses bidirectional payment channels for peer-to-peer transactions.

Q3. What is the key difference between rollups and sidechains?
A) Rollups are faster B) Sidechains are cheaper C) Rollups inherit L1 security; sidechains do not D) Sidechains use PoS
Answer: C – Rollups post data to L1 and inherit its security; sidechains have independent consensus.

Q4. What is the typical withdrawal delay for optimistic rollups?
A) Instant B) 10-30 minutes C) 7 days D) 30 days
Answer: C – The 7-day challenge period allows time for fraud proofs.

Q5. Which cryptographic proofs do ZK-Rollups use?
A) Proof-of-Work B) Fraud proofs C) SNARK/STARK proofs D) Merkle proofs
Answer: C – ZK-Rollups use SNARK or STARK zero-knowledge proofs.

Quiz (6–10)

Q6. What was the approximate fee reduction after EIP-4844 (Dencun)?
A) 10-20% B) 50% C) 90%+ D) No change

Quiz (6–10)

Q6. What was the approximate fee reduction after EIP-4844 (Dencun)?
A) 10-20% B) 50% C) 90%+ D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q7. Which Ethereum L2 currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Base

Quiz (6–10)

Q6. What was the approximate fee reduction after EIP-4844 (Dencun)?
A) 10-20% B) 50% C) 90%+ D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q7. Which Ethereum L2 currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Base
Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q8. What is the main advantage of ZK-Rollups over optimistic rollups?
A) Lower cost B) Better EVM compatibility C) Fast finality (10-30 min) D) Simpler technology

Quiz (6–10)

Q6. What was the approximate fee reduction after EIP-4844 (Dencun)?
A) 10-20% B) 50% C) 90%+ D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q7. Which Ethereum L2 currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Base
Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q8. What is the main advantage of ZK-Rollups over optimistic rollups?
A) Lower cost B) Better EVM compatibility C) Fast finality (10-30 min) D) Simpler technology
Answer: C – ZK-Rollups achieve finality after proof verification, avoiding the 7-day wait.

Q9. Why are cross-chain bridges considered high-risk?
A) High gas fees B) Slow speed C) Major attack target ($2B+ stolen 2022-2023) D) Incompatibility

Quiz (6–10)

Q6. What was the approximate fee reduction after EIP-4844 (Dencun)?
A) 10-20% B) 50% C) 90%+ D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q7. Which Ethereum L2 currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Base
Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q8. What is the main advantage of ZK-Rollups over optimistic rollups?
A) Lower cost B) Better EVM compatibility C) Fast finality (10-30 min) D) Simpler technology
Answer: C – ZK-Rollups achieve finality after proof verification, avoiding the 7-day wait.

Q9. Why are cross-chain bridges considered high-risk?
A) High gas fees B) Slow speed C) Major attack target ($2B+ stolen 2022-2023) D) Incompatibility
Answer: C – Bridges are vulnerable attack targets with over $2B stolen in recent years.

Q10. What future upgrade promises 100,000+ TPS through massive data availability?
A) EIP-4844 B) Full Danksharding C) The Merge D) zkEVM

Quiz (6–10)

Q6. What was the approximate fee reduction after EIP-4844 (Dencun)?
A) 10-20% B) 50% C) 90%+ D) No change
Answer: C – L2 fees dropped from $0.50-2.00 to $0.01-0.05, a 90%+ reduction.

Q7. Which Ethereum L2 currently leads by Total Value Locked (TVL)?
A) Optimism B) Arbitrum C) zkSync D) Base
Answer: B – Arbitrum has the highest TVL among Ethereum Layer 2 solutions.

Q8. What is the main advantage of ZK-Rollups over optimistic rollups?
A) Lower cost B) Better EVM compatibility C) Fast finality (10-30 min) D) Simpler technology
Answer: C – ZK-Rollups achieve finality after proof verification, avoiding the 7-day wait.

Q9. Why are cross-chain bridges considered high-risk?
A) High gas fees B) Slow speed C) Major attack target ($2B+ stolen 2022-2023) D) Incompatibility
Answer: C – Bridges are vulnerable attack targets with over $2B stolen in recent years.

Q10. What future upgrade promises 100,000+ TPS through massive data availability?
A) EIP-4844 B) Full Danksharding C) The Merge D) zkEVM
Answer: B – Full Danksharding will dramatically increase data availability.

L42: Flash Loans and Composability

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand flash loan mechanics and atomicity
- Analyze legitimate flash loan use cases
- Examine flash loan attack vectors and notable exploits
- Explore DeFi composability ("money legos")
- Understand MEV and its relationship to flash loans

The Problem: What new attacks does DeFi enable?

The Challenge
DeFi's composability allows any smart contract to interact with any other protocol within a single atomic transaction. This enables powerful arbitrage and refinancing strategies, but also creates a new attack surface: adversaries can borrow unlimited capital, manipulate protocol state, extract profits, and repay loans—all within one block, with zero upfront capital.

Why It Matters

- Flash loans eliminate capital requirements for large-scale attacks
- Historical examples: bZx attacks ($950K, Feb 2020), Harvest Finance ($34M, Oct 2020), Euler Finance ($197M, Mar 2023)

What We Need

- Risk management and mitigation
- Understanding atomic transaction risks and oracle manipulation vectors

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Flash Loans addresses this challenge

What is a Flash Loan?

Definition:
Uncollateralized loan borrowed and repaid within single transaction

Key Properties:

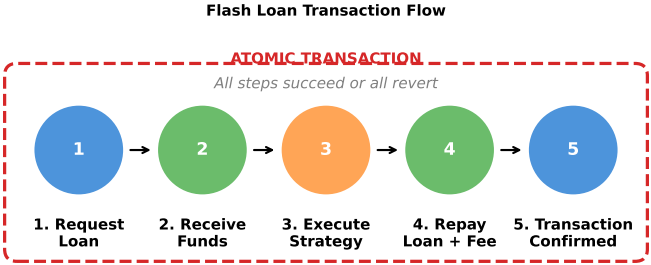
- *Atomicity*: All-or-nothing
- If repayment fails: TX reverts
- No collateral required

Characteristics:

- **Size**: Unlimited (pool limit)
- **Duration**: One block
- **Risk to lender**: Zero

Unique to DeFi:
Impossible in traditional finance

Flash Loan Transaction Flow



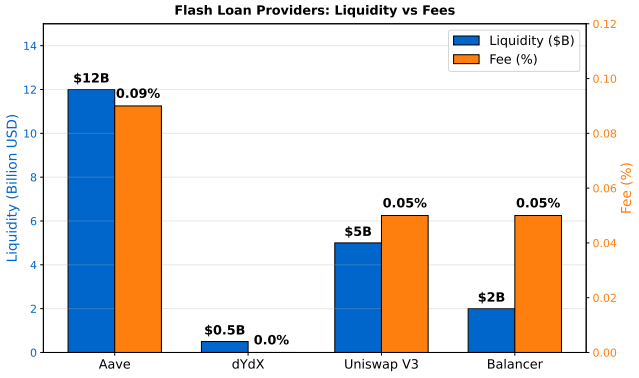
If any step fails, the entire transaction reverts – zero risk to lender

Traditional Loans vs Flash Loans

Property	Traditional Loan	Flash Loan
Collateral	Required (often ¿100%)	None
Duration	Days/months/years	Single transaction
Creditworthiness	Required (KYC)	Not required
Repayment Guarantee	Legal contracts	Smart contract atomicity
Risk to Lender	Default risk	Zero (reverts)

Paradigm Shift: Code execution guarantees replace legal enforcement

Flash Loan Providers



Aave is largest provider; dYdX offers free flash loans

DeFi Composability

“Money Legos”:

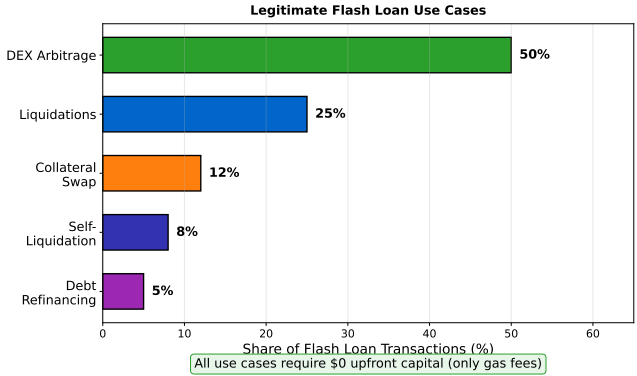
- Permissionless integration
- Any contract calls any contract
- Atomic multi-protocol TX

Risk:
Cascading failures, expanded attack surface

Composability Examples:

1. Uniswap → Aave → Borrow
2. Flash → Liquidate → Swap → Repay
3. Compound → Curve yield

Legitimate Use Cases



All use cases democratize capital-intensive strategies to anyone

Flash Loan Use Case: Arbitrage

Scenario:
ETH: $2000 (Uniswap) vs $2020 (SushiSwap)
Steps:

1. Borrow 1000 ETH (flash loan)
2. Buy on Uniswap ($2M)
3. Sell on SushiSwap ($2.02M)
4. Repay + fee ($2.001M)

Result:

- Profit: $19,000 in one TX
- Capital needed: Gas only ($50-200)

Democratization:
Anyone can arbitrage, not just whales

Flash Loan Use Case: Collateral Swap

Problem:
User has debt with Asset A collateral, wants Asset B
Steps:

1. Flash borrow Asset A
2. Repay existing debt
3. Withdraw collateral A
4. Deposit collateral B
5. Re-borrow Asset A
6. Repay flash loan

Result:

- Collateral swapped atomically
- Zero liquidation risk
- Fee: 0.05-0.09% only

Key Benefit:
Atomicity ensures no risk during swap

Flash Loan Attacks: Overview

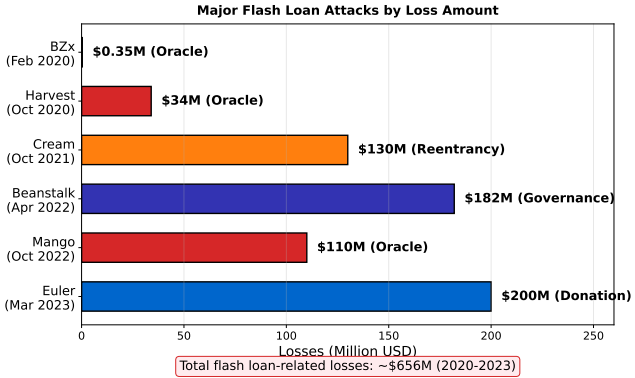
Dark Side:
Enable large-scale attacks with zero capital
Attack Pattern:

1. Flash borrow massive amount
2. Manipulate state (oracle/gov)
3. Exploit for profit
4. Repay flash loan

Impact:
$500M+ stolen (2020-2023)

Key Insight:
Flash loans *amplify* existing vulnerabilities — they are not the root cause

Major Flash Loan Attacks



Oracle manipulation is most common attack vector

Attack Example: Oracle Manipulation

Vulnerability:
Protocol uses single DEX as oracle
Attack Steps:

1. Flash borrow 10K ETH
2. Buy all TOKEN (10x pump)
3. Oracle reads inflated price
4. Borrow stables at fake price
5. Sell TOKEN (price normalizes)
6. Repay flash loan

Real Example:
Harvest Finance: $34M stolen

Mitigation:

- Use TWAP (time-weighted)
- Use Chainlink oracles
- Multiple price sources

Defense Mechanisms

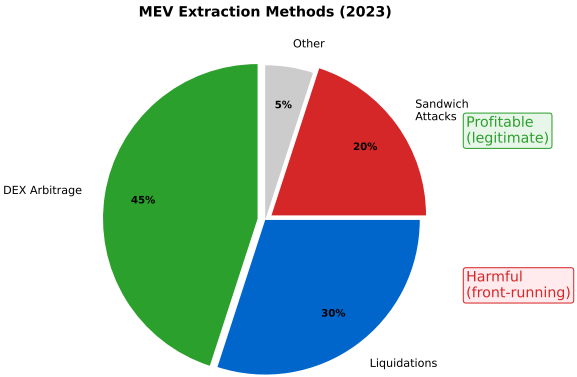
Oracle Protection:

- Decentralized oracles (Chainlink)
- TWAP: Average over blocks
- Multiple price sources

Protocol Protection:

- Reentrancy guards
- Governance timelocks
- Vote locking periods
- Circuit breakers

MEV and Flash Loans



Flash loans amplify both legitimate arbitrage and harmful MEV extraction

MEV Extraction Techniques

MEV: Maximal Extractable Value
Profit from transaction ordering
Techniques:

- **Front-running**: TX before victim
- **Back-running**: TX after victim
- **Sandwich**: Front + back-run

Flash Loans + MEV:
Amplify arbitrage and liquidation profits
Scale:

- $600M+ extracted (2023)
- Flashbots: Democratize MEV
- Reduces gas wars

Economic Impact

Positive Effects

- Democratize arbitrage
- Increase market efficiency
- Enable capital-efficient refinancing
- Liquidation bots improve protocol health

Negative Effects

- Enable zero-capital attacks
- Amplify protocol vulnerabilities
- MEV extraction harms users
- Governance manipulation risk

Net Assessment: Powerful tool that magnifies both good and bad protocol design

(c) Joerg Osterrieder 2025

Flash Loans and Regulation

Legal Gray Area:
No clear regulatory framework
Key Questions:

- Theft or code exploitation?
- Protocol or attacker liable?
- Code is law vs legal?

Precedent:
Mango Markets attacker arrested (Dec 2022)

- Charged: market manipulation
- Not: flash loan use itself

Protocol Responsibility:
Bug bounties, audits, insurance

Problem Solved? Flash Loans

The Original Problem

What new attacks does DeFi enable?

How Flash Loans Solves It

- Atomic transactions enable instant arbitrage and liquidations, democratizing capital-intensive strategies
- All-or-nothing execution ensures zero risk to lenders via transaction reversion
- Composability allows permissionless integration across protocols

Remaining Limitations

- Oracle manipulation: Single-block price feeds can be distorted to exploit lending protocols
- Governance attacks: Flash-borrowed tokens enable malicious proposal execution without long-term commitment

Open Questions

- How do we design flash-loan-resistant protocols without sacrificing composability?
- Risk: Black swan events, cascading failures

Flash Loans partially solves "What new attacks does DeFi enable" but introduces new trade-offs

Summary

Flash Loans:

- Uncollateralized, atomic
- Zero lender risk (reverts)
- Use: Arbitrage, collateral swap
- Composability: “Money legos”

Security:

- Attacks: $500M+ stolen
- Amplify vulnerabilities
- Defenses: TWAP, Chainlink
- Circuit breakers, timelocks

Flash loans are a powerful tool that magnifies both good and bad protocol design

Questions for Reflection

1. Why can flash loans exist in DeFi but not in traditional finance?
2. How do flash loans democratize arbitrage opportunities?
3. What makes oracle manipulation the most common attack vector?
4. Should flash loan attackers be prosecuted if they exploit code bugs?
5. How can protocols defend against flash loan governance attacks?

Quiz Questions (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. In the arbitrage example, ETH is $2000 on Uniswap and $2020 on SushiSwap. What is the profit from a 1000 ETH flash loan arbitrage (before fees)?
A) $10,000 B) $19,000 C) $20,000 D) $2,000
Answer: C – Buy for $2M, sell for $2.02M = $20,000 profit.

Q5. What does DeFi composability refer to?
A) Combining multiple cryptocurrencies B) Permissionless integration like "money legos"
C) Creating new tokens D) Merging blockchain networks
Answer: B – Composability allows atomic transactions across multiple protocols.

Quiz Questions (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) $50M+ B) $100M+ C) $500M+ D) $1B+
Answer: C – Over $500M stolen during this period.

Q9. In the Harvest Finance attack, what was the primary vulnerability exploited?
A) Reentrancy bug B) Single DEX price oracle C) Governance takeover D) Smart contract bug
Answer: B – Single DEX oracle allowed price manipulation.

Q10. What is TWAP and how does it defend against flash loan attacks?
A) Total Weighted Asset Pool B) Time-Weighted Average Price
C) Token Withdrawal Attack Prevention D) Trusted Wallet Authentication
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

Quiz Questions (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value
C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles
Answer: C – Vote locking prevents flash loan governance attacks.

Q14. What was the approximate MEV volume extracted in 2023?
A) $60M+ B) $200M+ C) $600M+ D) $2B+
Answer: C – Over $600M extracted via MEV in 2023.

Q15. In a sandwich attack, what does the attacker do?
A) Front-run and back-run a victim's transaction B) Split transaction into parts
C) Surround smart contract with malicious code D) Execute trades on multiple DEXs
Answer: A – Sandwich attacks place transaction before and after victim's transaction.

Quiz Questions (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API
C) Chainlink decentralized oracles D) On-chain voting
Answer: C – Chainlink aggregates prices from multiple sources, preventing manipulation.

Q19. What is the primary reason flash loans amplify protocol vulnerabilities?
A) They are free to execute B) They provide unlimited capital for exploitation
C) They bypass security checks D) They cannot be traced
Answer: B – Flash loans allow borrowing unlimited amounts to exploit vulnerabilities at scale.

Q20. In a collateral swap using flash loans, what is the main benefit?
A) Lower interest rates B) Zero liquidation risk during swap
C) No transaction fees D) Increased borrowing capacity
Answer: B – Atomicity ensures instant swap with zero liquidation risk.

L42: Flash Loans and Composability

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Why Can You Borrow Millions Without Collateral?

- Borrow $100 million with zero collateral—if you can repay it in the same transaction
- DeFi's atomic execution creates opportunities impossible in traditional finance

[COMIC: Wide-eyed developer realizing they can borrow millions for free. Speech bubble: "Wait... I can borrow $100M with ZERO collateral?!" Calculator showing astronomical numbers]

[PLACEHOLDER] — The power to borrow unlimited capital—if you can use and return it in 12 seconds

Learning Objectives

- Understand flash loan (loan borrowed and repaid in same transaction) mechanics and atomicity (all-or-nothing execution)
- Analyze legitimate flash loan use cases
- Examine flash loan attack vectors and notable exploits
- Explore DeFi composability ("money legos")
- Understand MEV—Maximal Extractable Value (profit from reordering transactions) and its relationship to flash loans

Building on L41: Layer 2 Scaling

The Problem: What new attacks does DeFi enable?

The Challenge
DeFi's composability allows any smart contract to interact with any other protocol within a single atomic transaction. This enables powerful arbitrage and refinancing strategies, but also creates a new attack surface: adversaries can borrow unlimited capital, manipulate protocol state, extract profits, and repay loans—all within one block, with zero upfront capital.

Why It Matters

- Flash loans eliminate capital requirements for large-scale attacks
- Historical examples: bZx attacks ($950K, Feb 2020), Harvest Finance ($34M, Oct 2020), Euler Finance ($197M, Mar 2023)
- Enables both arbitrage (profiting from price differences across markets) and exploits

What We Need

- Risk management and mitigation
- Understanding atomic transaction risks and oracle (external price data feed for smart contracts) manipulation vectors

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Flash Loans addresses this challenge

How Can You Borrow Millions Without Collateral?

Definition:
Uncollateralized loan borrowed and repaid within single transaction

Key Properties:

- *Atomicity*: All-or-nothing
- If repayment fails: TX reverts
- No collateral required

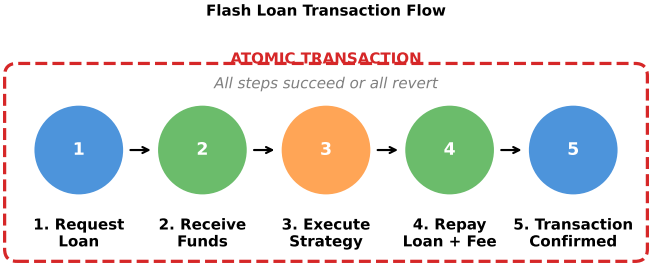
Characteristics:

- **Size**: Unlimited (pool limit)
- **Duration**: One block
- **Risk to lender**: Zero

Unique to DeFi:
Impossible in traditional finance

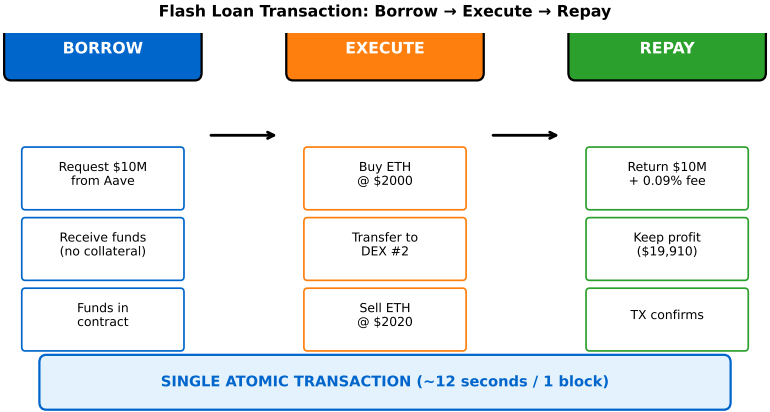
→ *Problem: What new attacks does DeFi enable? — What is a Flash Loan? shows DeFi enables borrowing unlimited capital with zero collateral—impossible in traditional finance, enabling new attack vectors*

How Does a Flash Loan Transaction Work?



If any step fails, the entire transaction reverts – zero risk to lender

What Happens in Each Phase of a Flash Loan?



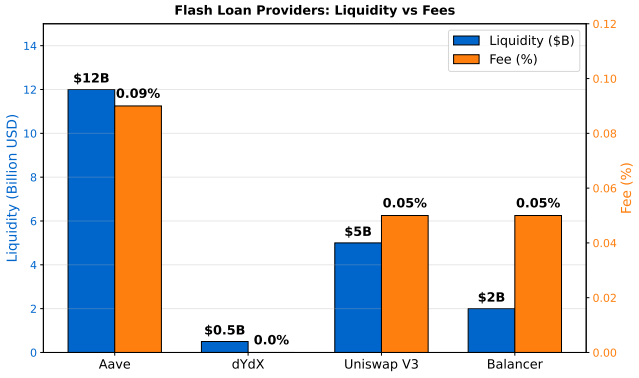
All three phases must complete within one block (∼12 seconds on Ethereum)

How Do Flash Loans Differ from Traditional Loans?

Property	Traditional Loan	Flash Loan
Collateral	Required (often ¿100%)	None
Duration	Days/months/years	Single transaction
Creditworthiness	Required (KYC)	Not required
Repayment Guarantee	Legal contracts	Smart contract atomicity
Risk to Lender	Default risk	Zero (reverts)

Paradigm Shift: Code execution guarantees replace legal enforcement

Which Platforms Offer Flash Loans?



Aave is largest provider; dYdX offers free flash loans

Why Is DeFi Called "Money Legos"?

"Money Legos":

- Permissionless integration
- Any contract calls any contract
- Atomic multi-protocol TX

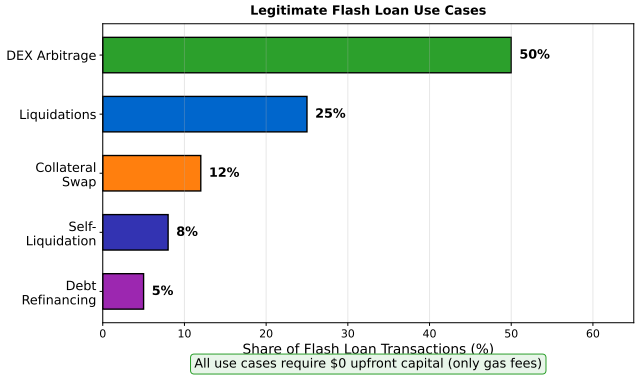
Risk:
Cascading failures, expanded attack surface

Composability Examples:

1. Uniswap → Aave → Borrow
2. Flash → Liquidate → Swap → Repay
3. Compound → Curve yield

→ *Problem: What new attacks does DeFi enable? — DeFi Composability reveals composability creates cascading risk: one protocol's weakness can be exploited via another protocol's flash loan*

What Can Flash Loans Be Used For?



All use cases democratize capital-intensive strategies to anyone

How Do Flash Loans Enable Zero-Capital Arbitrage?

Scenario:
ETH: $2000 (Uniswap) vs $2020 (SushiSwap)
Steps:

1. Borrow 1000 ETH (flash loan)
2. Buy on Uniswap ($2M)
3. Sell on SushiSwap ($2.02M)
4. Repay + fee ($2.001M)

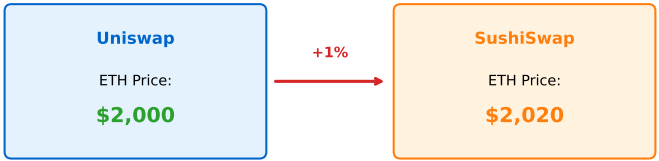
Result:

- Profit: $19,000 in one TX
- Capital needed: Gas only ($50-200)

Democratization:
Anyone can arbitrage, not just whales

How Does Flash Loan Arbitrage Work in Practice?

Flash Loan Arbitrage: $18,200 Profit with Zero Capital



PROFIT CALCULATION

```
Flash borrow: 1,000 ETH (from Aave)
Buy on Uniswap: 1,000 ETH × 2,000 = 2,000,000
Sell on SushiSwap: 1,000 ETH × 2,020 = 2,020,000
Repay + Fee (0.09%): $2,000,000 + $1,800 = $2,001,800
NET PROFIT: $2,020,000 - $2,001,800 = $18,200
```

Capital Required: Only gas fees (~$50-200)

Flash loans democratize arbitrage: profit without capital, paying only gas fees

How Do Flash Loans Enable Collateral Swaps?

Problem:
User has debt with Asset A collateral, wants Asset B
Steps:

1. Flash borrow Asset A
2. Repay existing debt
3. Withdraw collateral A
4. Deposit collateral B
5. Re-borrow Asset A
6. Repay flash loan

Result:

- Collateral swapped atomically
- Zero liquidation risk
- Fee: 0.05-0.09% only

Key Benefit:
Atomicity ensures no risk during swap

Problem Check-In: Flash Loans

Recall Our Problem

What new attacks does DeFi enable?

What We've Learned So Far

- Flash loans are uncollateralized loans repaid within one transaction—if repayment fails, everything reverts
- DeFi composability lets any smart contract call any other protocol atomically ("money legos")
- Together these enable zero-capital attacks: borrow millions, exploit vulnerability, profit, repay—all in one block

Still to Address

- Specific attack patterns (oracle manipulation, governance attacks) and defense mechanisms
- Can protocols be designed to be flash-loan-resistant without sacrificing the composability that makes DeFi powerful?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "What new attacks does DeFi enable?"?

What Makes Flash Loans Dangerous?

Dark Side:
Enable large-scale attacks with zero capital
Attack Pattern:

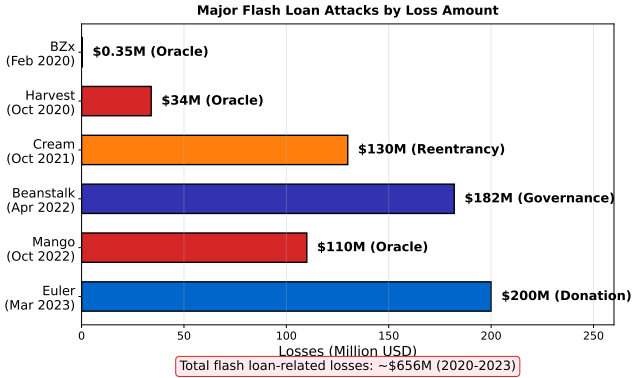
1. Flash borrow massive amount
2. Manipulate state (oracle/gov)
3. Exploit for profit
4. Repay flash loan

Impact:
$500M+ stolen (2020-2023)

Key Insight:
Flash loans *amplify* existing vulnerabilities — they are not the root cause

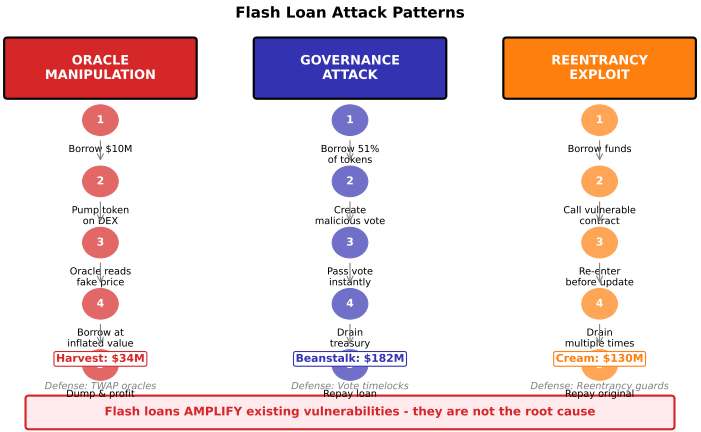
→ *Problem: What new attacks does DeFi enable? — Flash Loan Attacks: Overview demonstrates flash loans amplify existing vulnerabilities: attackers need only gas fees to execute million-dollar exploits*

What Were the Major Flash Loan Attacks?



Oracle manipulation is most common attack vector

What Are the Common Flash Loan Attack Patterns?



Each attack exploits a different vulnerability; defenses exist but trade-offs apply

How Do Attackers Manipulate Price Oracles?

Vulnerability:
Protocol uses single DEX (Decentralized Exchange) as oracle

Attack Steps:

1. Flash borrow 10K ETH
2. Buy all TOKEN (10x pump)
3. Oracle reads inflated price
4. Borrow stables at fake price
5. Sell TOKEN (price normalizes)
6. Repay flash loan

Real Example:
Harvest Finance: $34M stolen

Mitigation:

- Use TWAP (time-weighted)
- Use Chainlink oracles
- Multiple price sources

How Can Protocols Defend Against Flash Loan Attacks?

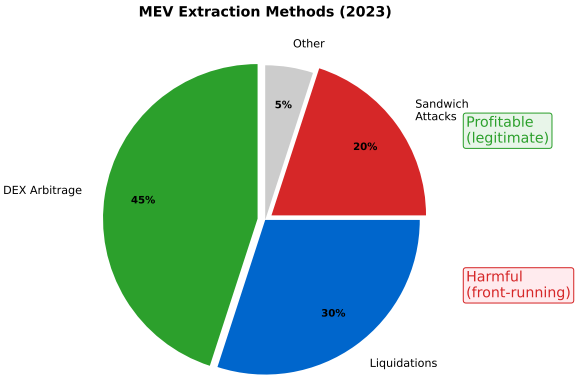
Oracle Protection:

- Decentralized oracles (Chainlink)
- TWAP: Average over blocks
- Multiple price sources

Protocol Protection:

- Reentrancy guards
- Governance timelocks
- Vote locking periods
- Circuit breakers

How Do Flash Loans Enable MEV Extraction?



Flash loans amplify both legitimate arbitrage and harmful MEV extraction | → Problem: What new attacks does DeFi enable? — MEV and Flash Loans shows MEV extractors use flash loans to profit from transaction ordering, harming regular users via front-running

How Do Bots Extract MEV from Flash Loans?

MEV: Maximal Extractable Value
Profit from transaction ordering
Techniques:

- **Front-running (placing your transaction ahead of someone else's to profit)**: TX before victim
- **Back-running**: TX after victim
- **Sandwich**: Front + back-run

Flash Loans + MEV:
Amplify arbitrage and liquidation profits
Scale:

- $600M+ extracted (2023)
- Flashbots: Democratize MEV
- Reduces gas wars

What Is the Economic Impact of Flash Loans?

Positive Effects

- Democratize arbitrage
- Increase market efficiency
- Enable capital-efficient refinancing
- Liquidation bots improve protocol health

Negative Effects

- Enable zero-capital attacks
- Amplify protocol vulnerabilities
- MEV extraction harms users
- Governance manipulation risk

Net Assessment: Powerful tool that magnifies both good and bad protocol design

(c) Joerg Osterrieder 2025

Are Flash Loan Exploits Legal or Illegal?

Legal Gray Area:
No clear regulatory framework
Key Questions:

- Theft or code exploitation?
- Protocol or attacker liable?
- Code is law vs legal?

Precedent:
Mango Markets attacker arrested (Dec 2022)

- Charged: market manipulation
- Not: flash loan use itself

Protocol Responsibility:
Bug bounties, audits, insurance

(c) Joerg Osterrieder 2025

Problem Solved? Flash Loans

The Original Problem

What new attacks does DeFi enable?

How Flash Loans Solves It

- Atomic transactions enable instant arbitrage and liquidations, democratizing capital-intensive strategies
- All-or-nothing execution ensures zero risk to lenders via transaction reversion
- Composability allows permissionless integration across protocols

Remaining Limitations

- Oracle manipulation: Single-block price feeds can be distorted to exploit lending protocols
- Governance attacks: Flash-borrowed tokens enable malicious proposal execution without long-term commitment

Open Questions

- How do we design flash-loan-resistant protocols without sacrificing composability?
- Risk: Black swan events, cascading failures

Flash Loans partially solves "What new attacks does DeFi enable" but introduces new trade-offs

The Economics of Flash Loans

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Flash Loans

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Flash Loans

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

What Does Flash Loan Arbitrage Really Look Like?

- Profitable arbitrage requires finding price discrepancies, writing exploit code, and competing with MEV bots—all in milliseconds
- The gap between "borrow millions for free" and "profitable arbitrage" is filled with failed transactions and gas costs

[COMIC: Developer surrounded by multiple monitors showing complex arbitrage calculations, failed transactions, and MEV bot competition. Speech bubble: "The arbitrage looked so simple in the tutorial..." Red "TX FAILED" messages scattered around]

[PLACEHOLDER] — Flash loans democratize capital access but not the expertise needed to profit from it

Summary

Flash Loans:

- Uncollateralized, atomic
- Zero lender risk (reverts)
- Use: Arbitrage, collateral swap
- Composability: "Money legos"

Next Lesson: L43 – Smart Contract Security

Security:

- Attacks: $500M+ stolen
- Amplify vulnerabilities
- Defenses: TWAP, Chainlink
- Circuit breakers, timelocks

Flash loans are a powerful tool that magnifies both good and bad protocol design

Questions for Reflection

1. Why can flash loans exist in DeFi but not in traditional finance?
2. How do flash loans democratize arbitrage opportunities?
3. What makes oracle manipulation the most common attack vector?
4. Should flash loan attackers be prosecuted if they exploit code bugs?
5. How can protocols defend against flash loan governance attacks?

Quiz Questions (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. In the arbitrage example, ETH is $2000 on Uniswap and $2020 on SushiSwap. What is the profit from a 1000 ETH flash loan arbitrage (before fees)?
A) $10,000 B) $19,000 C) $20,000 D) $2,000
Answer: C – Buy for $2M, sell for $2.02M = $20,000 profit.

Q5. What does DeFi composability refer to?
A) Combining multiple cryptocurrencies B) Permissionless integration like "money legos"
C) Creating new tokens D) Merging blockchain networks
Answer: B – Composability allows atomic transactions across multiple protocols.

Quiz Questions (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) $50M+ B) $100M+ C) $500M+ D) $1B+
Answer: C – Over $500M stolen during this period.

Q9. In the Harvest Finance attack, what was the primary vulnerability exploited?
A) Reentrancy bug B) Single DEX price oracle C) Governance takeover D) Smart contract bug
Answer: B – Single DEX oracle allowed price manipulation.

Q10. What is TWAP and how does it defend against flash loan attacks?
A) Total Weighted Asset Pool B) Time-Weighted Average Price
C) Token Withdrawal Attack Prevention D) Trusted Wallet Authentication
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

Quiz Questions (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value
C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles
Answer: C – Vote locking prevents flash loan governance attacks.

Q14. What was the approximate MEV volume extracted in 2023?
A) $60M+ B) $200M+ C) $600M+ D) $2B+
Answer: C – Over $600M extracted via MEV in 2023.

Q15. In a sandwich attack, what does the attacker do?
A) Front-run and back-run a victim's transaction B) Split transaction into parts
C) Surround smart contract with malicious code D) Execute trades on multiple DEXs
Answer: A – Sandwich attacks place transaction before and after victim's transaction.

Quiz Questions (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API
C) Chainlink decentralized oracles D) On-chain voting
Answer: C – Chainlink aggregates prices from multiple sources, preventing manipulation.

Q19. What is the primary reason flash loans amplify protocol vulnerabilities?
A) They are free to execute B) They provide unlimited capital for exploitation
C) They bypass security checks D) They cannot be traced
Answer: B – Flash loans allow borrowing unlimited amounts to exploit vulnerabilities at scale.

Q20. In a collateral swap using flash loans, what is the main benefit?
A) Lower interest rates B) Zero liquidation risk during swap
C) No transaction fees D) Increased borrowing capacity
Answer: B – Atomicity ensures instant swap with zero liquidation risk.

L42: Flash Loans and Composability

Mini-Lecture — Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand flash loan mechanics and atomicity
- Analyze legitimate use cases: arbitrage, collateral swaps
- Examine attack vectors and notable exploits
- Explore DeFi composability ("money legos")

Flash loans are unique to DeFi – impossible in traditional finance

What is a Flash Loan?

- **Definition**: Uncollateralized loan borrowed and repaid within single transaction
- **Key Property**: *Atomicity* – loan and repayment are all-or-nothing
- **If repayment fails**: Entire transaction reverts, lender loses nothing
- **Loan Size**: Unlimited (constrained only by liquidity pool)
- **Duration**: Fraction of a second (one block)

Smart contract execution model enables zero-collateral lending

Traditional Loans vs Flash Loans

Property	Traditional Loan	Flash Loan
Collateral	Required (often ¿100%)	None
Duration	Days/months/years	Single transaction
Creditworthiness	Required (KYC)	Not required
Repayment Guarantee	Legal contracts	Smart contract atomicity
Risk to Lender	Default risk	Zero (reverts)

Paradigm Shift: Code execution guarantees replace legal enforcement

Flash Loan Providers

Provider	Fee	Notes
Aave	0.09%	Largest provider by volume
dYdX	0%	Free flash loans
Balancer	0%	Flash loans from liquidity pools
Uniswap V3	Swap fee only	Flash swaps (different mechanism)

Aave is the largest provider; dYdX offers free flash loans

Legitimate Use Cases

1. **Arbitrage**
   - ETH at $2000 on Uniswap, $2020 on SushiSwap
   - Borrow 1000 ETH → Buy on Uniswap → Sell on SushiSwap → Repay
   - Profit: $20,000 minus fees; Capital required: only gas fees
2. **Collateral Swap**
   - Swap collateral atomically without liquidation risk
   - Borrow → Repay debt → Withdraw → Deposit new → Reborrow → Repay flash loan
3. **Self-Liquidation**
   - Close underwater positions without external liquidator fees

Flash loans democratize capital-intensive strategies

DeFi Composability: Money Legos

- **Composability**: DeFi protocols are interoperable building blocks
- **Permissionless**: Any contract can call any other contract
- **Atomic**: Multiple protocol interactions in one transaction

Example Chain:

1. Flash loan from Aave
2. Swap on Uniswap
3. Deposit into Curve
4. Borrow from Compound
5. Repay flash loan

Risk: Cascading failures and expanded attack surface

(c) Joerg Osterrieder 2025

Flash Loan Attacks

Attack Pattern:

1. Borrow massive amount via flash loan
2. Manipulate protocol state (price oracle, governance)
3. Exploit manipulation for profit
4. Repay flash loan

Major Attacks:

- bZx (Feb 2020): $350K – First major flash loan attack
- Harvest Finance (Oct 2020): $34M – Oracle manipulation
- Cream Finance (Oct 2021): $130M – Price oracle exploit
- Mango Markets (Oct 2022): $114M – Market manipulation

Impact: $500M+ stolen via flash loan attacks (2020–2023)

Defense Mechanisms

1. **Decentralized Oracles**: Use Chainlink (not single DEX price)
2. **TWAP**: Time-Weighted Average Price over multiple blocks
3. **Reentrancy Guards**: Prevent recursive contract calls
4. **Governance Delays**: Timelock on parameter changes
5. **Vote Locking**: Require tokens locked before voting
6. **Circuit Breakers**: Pause if anomalous activity detected

Flash loans amplify existing vulnerabilities – fix the root cause

MEV and Flash Loans

- **MEV (Maximal Extractable Value)**: Profit from transaction ordering
- **Flash Loans + MEV**: Amplify arbitrage and liquidation profits

MEV Techniques:

- **Front-running**: Place transaction before victim's
- **Back-running**: Place transaction after victim's
- **Sandwich Attacks**: Front-run + back-run

Flashbots: Democratize MEV extraction, reduce gas wars
MEV Volume: $600M+ extracted in 2023

Visual Concepts

Flash: Instant execution

Speed: Single block

Loans: Zero collateral

Images: Unsplash (CC0 license)

Quiz Questions (1–5)

Q1. What key property enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q5. What does DeFi composability refer to?
A) Combining cryptocurrencies B) Permissionless integration like "money legos"
C) Creating new tokens D) Merging blockchain networks
Answer: B – Composability allows atomic transactions across multiple protocols.

Quiz Questions (6–10)

Q6. Which is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q7. How much was stolen via flash loan attacks between 2020-2023?
A) $50M+ B) $100M+ C) $500M+ D) $1B+
Answer: C – Over $500M stolen during this period.

Q8. What defense mechanism averages prices over multiple blocks?
A) Chainlink oracles B) TWAP (Time-Weighted Average Price)
C) Reentrancy guards D) Circuit breakers
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

Q9. What is MEV?
A) Maximum Extractable Value B) Miner Extractable Value
C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q10. In a sandwich attack, what does the attacker do?
A) Front-run and back-run a victim's transaction B) Split transaction into parts
C) Surround contract with malicious code D) Execute trades on multiple DEXs
Answer: A – Sandwich attacks place transactions before and after victim's transaction.

Flash Loans and Composability

Mini-Lecture Version

Blockchain & Cryptocurrency Course

Module F: Advanced Topics

December 2025

Learning Objectives: Flash loan mechanics — Legitimate use cases — Attack vectors — DeFi composability — MEV relationship

What is a Flash Loan?

Formal Definition

An uncollateralized loan borrowed and repaid within a single atomic transaction.

Key Properties:

- **Atomicity**: Loan and repayment are all-or-nothing (reverts if unpaid)
- **Zero Collateral**: Enabled by smart contract execution model
- **Unlimited Size**: Constrained only by pool liquidity (Aave: $10B+)
- **Instant Duration**: Single block (fraction of a second)

Unique to DeFi – impossible in traditional finance due to atomic transaction model

(c) Joerg Osterrieder 2025

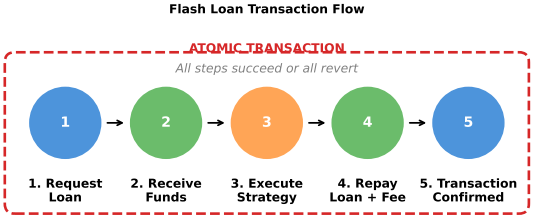
Flash Loan Transaction Flow

Execution Sequence:

1. Borrow from pool
2. Execute strategy
3. Repay loan + fee

If Repayment Fails:

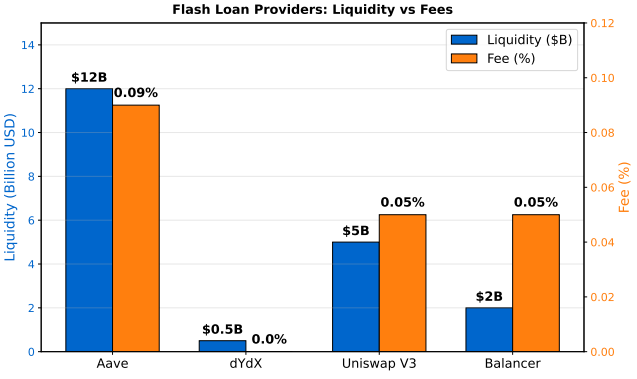
- Entire tx reverts
- Lender loses nothing
- Borrower pays only gas



Code execution guarantees replace legal enforcement

(c) Joerg Osterrieder 2025

Flash Loan Providers and Fees



Key Differences:

- Aave: 0.09% fee, largest pool
- dYdX: 0% fee (free!)
- Uniswap: 0.3% via swaps

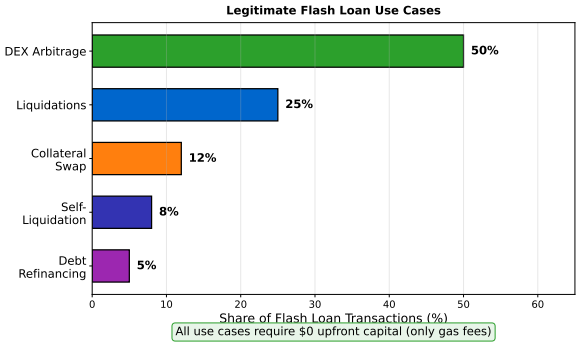
Choosing Provider:

- Large arb: minimize fee
- Multi-asset: pool diversity
- Complex: composability

dYdX offers free flash loans; Aave dominates by liquidity depth

(c) Joerg Osterrieder 2025

Legitimate Flash Loan Use Cases



Arbitrage Example:

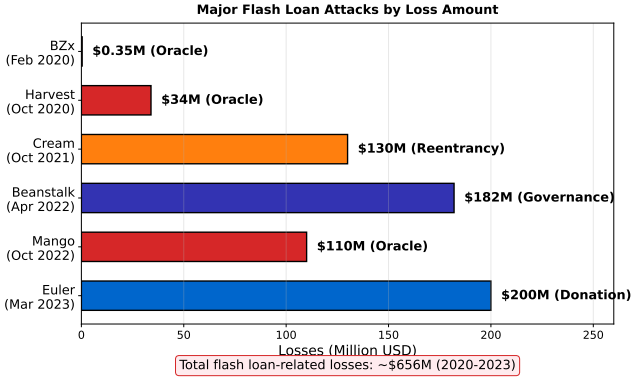
- ETH: $2000 (Uni) vs $2020 (Sushi)
- Borrow 1000 ETH, buy/sell
- Profit: $20K minus fees
- Capital needed: only gas ($50)

Collateral Swap:

- Swap collateral atomically
- Zero liquidation risk
- Fee: 0.05-0.09%

(c) Joerg Osterrieder 2025

Flash Loan Attacks: The Dark Side



Attack Pattern:

1. Borrow massive amount
2. Manipulate state
3. Exploit for profit
4. Repay flash loan

Notable Attacks:

- Harvest: $34M (oracle)
- bZx: $8M (2020)
- Total: $500M+ stolen

Flash loans amplify existing vulnerabilities – they are not the root cause

MEV Extraction and Defenses

MEV + Flash Loans:

- Front-running: tx before victim
- Back-running: tx after victim
- Sandwich: both combined
- 2023 MEV: $600M+ extracted

Flashbots: Democratize MEV

Defense Mechanisms:

- Chainlink oracles (not DEX)
- TWAP: average over blocks
- Vote locking: tokens locked
- Circuit breakers: pause on anomaly

TWAP = Time-Weighted Average Price prevents single-block manipulation

(c) Joerg Osterrieder 2025

Key Takeaways

1. **Flash loans** are uncollateralized loans repaid atomically in one transaction
2. **Zero lender risk**: Transaction reverts if repayment fails
3. **Democratization**: Anyone can arbitrage with only gas fees ($50-200)
4. **Double-edged**: Enables both market efficiency and $500M+ in attacks

Bottom Line: Flash loans are a powerful DeFi primitive that amplifies both good protocol design and vulnerabilities – use decentralized oracles and vote locking as defense.

(c) Joerg Osterrieder 2025

Concrete Examples: Making It Real

Aave Flash Loan (Dec 2025)

- Pool liquidity: $14B+
- Fee: 0.09% ($9K per $10M)
- Max loan: entire pool
- Duration: 12 seconds (1 block)

Arbitrage Math

- Price diff: 1% spread
- Loan size: $1M
- Gross profit: $10,000
- Fee (0.09%): $900
- Gas: $100
- Net: $9,000

Major Attack Examples

- Harvest (Oct 2020): $34M
- Pancake Bunny: $45M
- Cream Finance: $130M
- Euler (Mar 2023): $197M

Provider Comparison

- Aave: 0.09% ($14B TVL)
- dYdX: 0% (free loans)
- Balancer: 0.01% (low fee)
- Uniswap V3: via swaps

Data verified Dec 2025 — Sources: DefiLlama, Aave docs, rekt.news

(c) Joerg Osterrieder 2025

DeFi Composability: Money Legos

Composability Defined:

- Protocols as interoperable building blocks
- Permissionless: any contract calls any other
- Atomic: multi-protocol txs in one block

Composability Chain Example:

1. Flash loan from Aave
2. Swap on Uniswap
3. Deposit into Curve
4. Borrow from Compound
5. Repay flash loan

Benefits:

- Capital efficiency
- Innovation speed
- User choice

Risks:

- Cascading failures
- Expanded attack surface
- Complexity bugs

Composability is DeFi's greatest strength and greatest vulnerability

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity

Quiz Questions (1–5)

Q1. What enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity
Answer: B – Atomicity ensures loan and repayment occur in one transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of second) D) 1 week

Quiz Questions (1–5)

Q1. What enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity
Answer: B – Atomicity ensures loan and repayment occur in one transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which provider offers 0% fee flash loans?
A) Aave B) Balancer C) dYdX D) Uniswap

Quiz Questions (1–5)

Q1. What enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity
Answer: B – Atomicity ensures loan and repayment occur in one transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which provider offers 0% fee flash loans?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers free flash loans; Aave charges 0.09%.

Q4. What happens if a flash loan cannot be repaid?
A) Borrower penalized B) Entire tx reverts C) Lender loses funds D) Loan extended

Quiz Questions (1–5)

Q1. What enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity
Answer: B – Atomicity ensures loan and repayment occur in one transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which provider offers 0% fee flash loans?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers free flash loans; Aave charges 0.09%.

Q4. What happens if a flash loan cannot be repaid?
A) Borrower penalized B) Entire tx reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q5. What does DeFi composability mean?
A) Combining cryptocurrencies B) Permissionless protocol integration C) Creating tokens D) Merging chains

Quiz Questions (1–5)

Q1. What enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity
Answer: B – Atomicity ensures loan and repayment occur in one transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which provider offers 0% fee flash loans?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers free flash loans; Aave charges 0.09%.

Q4. What happens if a flash loan cannot be repaid?
A) Borrower penalized B) Entire tx reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q5. What does DeFi composability mean?
A) Combining cryptocurrencies B) Permissionless protocol integration C) Creating tokens D) Merging chains
Answer: B – Composability = protocols as interoperable "money legos."

Quiz Questions (6–10)

Q6. How much was stolen via flash loan attacks (2020-2023)?
A) $50M+ B) $100M+ C) $500M+ D) $1B+

Quiz Questions (6–10)

Q6. How much was stolen via flash loan attacks (2020-2023)?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q7. What is the most common flash loan attack vector?
A) Reentrancy B) Oracle manipulation C) Governance takeover D) Gas griefing

Quiz Questions (6–10)

Q6. How much was stolen via flash loan attacks (2020-2023)?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q7. What is the most common flash loan attack vector?
A) Reentrancy B) Oracle manipulation C) Governance takeover D) Gas griefing
Answer: B – Single DEX oracle price manipulation is most common.

Q8. What does TWAP defend against?
A) Reentrancy attacks B) Single-block price manipulation C) Gas wars D) Front-running

Quiz Questions (6–10)

Q6. How much was stolen via flash loan attacks (2020-2023)?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q7. What is the most common flash loan attack vector?
A) Reentrancy B) Oracle manipulation C) Governance takeover D) Gas griefing
Answer: B – Single DEX oracle price manipulation is most common.

Q8. What does TWAP defend against?
A) Reentrancy attacks B) Single-block price manipulation C) Gas wars D) Front-running
Answer: B – TWAP averages prices over blocks, preventing single-tx manipulation.

Q9. What capital is needed for flash loan arbitrage?
A) \$1M minimum B) 10% collateral C) Only gas fees D) No capital

Quiz Questions (6–10)

Q6. How much was stolen via flash loan attacks (2020-2023)?
A) $50M+ B) $100M+ C) $500M+ D) $1B+
Answer: C – Over $500M stolen during this period.

Q7. What is the most common flash loan attack vector?
A) Reentrancy B) Oracle manipulation C) Governance takeover D) Gas griefing
Answer: B – Single DEX oracle price manipulation is most common.

Q8. What does TWAP defend against?
A) Reentrancy attacks B) Single-block price manipulation C) Gas wars D) Front-running
Answer: B – TWAP averages prices over blocks, preventing single-tx manipulation.

Q9. What capital is needed for flash loan arbitrage?
A) $1M minimum B) 10% collateral C) Only gas fees D) No capital
Answer: C – Flash loans democratize arbitrage; only gas fees ($50-200) needed.

Q10. What is MEV?
A) Maximum Ether Value B) Miner Extracted Volume C) Maximal Extractable Value D) Market Efficiency

Quiz Questions (6–10)

Q6. How much was stolen via flash loan attacks (2020-2023)?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q7. What is the most common flash loan attack vector?
A) Reentrancy B) Oracle manipulation C) Governance takeover D) Gas griefing
Answer: B – Single DEX oracle price manipulation is most common.

Q8. What does TWAP defend against?
A) Reentrancy attacks B) Single-block price manipulation C) Gas wars D) Front-running
Answer: B – TWAP averages prices over blocks, preventing single-tx manipulation.

Q9. What capital is needed for flash loan arbitrage?
A) \$1M minimum B) 10% collateral C) Only gas fees D) No capital
Answer: C – Flash loans democratize arbitrage; only gas fees (\$50-200) needed.

Q10. What is MEV?
A) Maximum Ether Value B) Miner Extracted Volume C) Maximal Extractable Value D) Market Efficiency
Answer: C – MEV = profit from transaction ordering (\$600M+ in 2023).

Quiz: Flash Loans

Instructions: 23 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools

Quiz (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week

Quiz (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap

Quiz (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. In the arbitrage example, ETH is $2000 on Uniswap and $2020 on SushiSwap. What is the profit from a 1000 ETH flash loan arbitrage (before fees)?
A) $10,000 B) $19,000 C) $20,000 D) $2,000

Quiz (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. In the arbitrage example, ETH is $2000 on Uniswap and $2020 on SushiSwap. What is the profit from a 1000 ETH flash loan arbitrage (before fees)?
A) $10,000 B) $19,000 C) $20,000 D) $2,000
Answer: C – Buy for $2M, sell for $2.02M = $20,000 profit.

Q5. What does DeFi composability refer to?
A) Combining multiple cryptocurrencies B) Permissionless integration like "money legos" C) Creating new tokens
D) Merging blockchain networks

Quiz (1–5)

Q1. What is the key property that enables flash loans to be uncollateralized?
A) Smart contract code B) Atomic transaction execution C) Low gas fees D) High liquidity pools
Answer: B – Atomicity ensures loan and repayment occur in a single transaction.

Q2. What is the typical duration of a flash loan?
A) 1 hour B) 1 day C) 1 block (fraction of a second) D) 1 week
Answer: C – Flash loans are borrowed and repaid within one block.

Q3. Which flash loan provider offers free flash loans (0% fee)?
A) Aave B) Balancer C) dYdX D) Uniswap
Answer: C – dYdX offers 0% fee; Aave charges 0.09%.

Q4. In the arbitrage example, ETH is $2000 on Uniswap and $2020 on SushiSwap. What is the profit from a 1000 ETH flash loan arbitrage (before fees)?
A) $10,000 B) $19,000 C) $20,000 D) $2,000
Answer: C – Buy for $2M, sell for $2.02M = $20,000 profit.

Q5. What does DeFi composability refer to?
A) Combining multiple cryptocurrencies B) Permissionless integration like "money legos" C) Creating new tokens
D) Merging blockchain networks
Answer: B – Composability allows atomic transactions across multiple protocols.

Quiz (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended

Quiz (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation

Quiz (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+

Quiz (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q9. In the Harvest Finance attack, what was the primary vulnerability exploited?
A) Reentrancy bug B) Single DEX price oracle C) Governance takeover D) Smart contract bug

Quiz (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q9. In the Harvest Finance attack, what was the primary vulnerability exploited?
A) Reentrancy bug B) Single DEX price oracle C) Governance takeover D) Smart contract bug
Answer: B – Single DEX oracle allowed price manipulation.

Q10. What is TWAP and how does it defend against flash loan attacks?
A) Total Weighted Asset Pool B) Time-Weighted Average Price C) Token Withdrawal Attack Prevention
D) Trusted Wallet Authentication

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What happens if a flash loan cannot be repaid within the transaction?
A) Borrower charged penalty B) Entire transaction reverts C) Lender loses funds D) Loan extended
Answer: B – Atomicity ensures transaction reverts, protecting the lender.

Q7. Which of the following is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q8. How much was stolen via flash loan attacks between 2020-2023?
A) \$50M+ B) \$100M+ C) \$500M+ D) \$1B+
Answer: C – Over \$500M stolen during this period.

Q9. In the Harvest Finance attack, what was the primary vulnerability exploited?
A) Reentrancy bug B) Single DEX price oracle C) Governance takeover D) Smart contract bug
Answer: B – Single DEX oracle allowed price manipulation.

Q10. What is TWAP and how does it defend against flash loan attacks?
A) Total Weighted Asset Pool B) Time-Weighted Average Price C) Token Withdrawal Attack Prevention
D) Trusted Wallet Authentication
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital

Quiz (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value

Quiz (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles

Quiz (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles
Answer: C – Vote locking prevents flash loan governance attacks.

Q14. What was the approximate MEV volume extracted in 2023?
A) $60M+ B) $200M+ C) $600M+ D) $2B+

Quiz (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles
Answer: C – Vote locking prevents flash loan governance attacks.

Q14. What was the approximate MEV volume extracted in 2023?
A) $60M+ B) $200M+ C) $600M+ D) $2B+
Answer: C – Over $600M extracted via MEV in 2023.

Q15. In a sandwich attack, what does the attacker do?
A) Front-run and back-run a victim's transaction B) Split transaction into parts C) Surround smart contract with malicious code D) Execute trades on multiple DEXs

Quiz (11–15)

Q11. What is the typical capital requirement to execute a flash loan arbitrage?
A) $1 million minimum B) 10% collateral C) Only gas fees ($50-$200) D) No capital
Answer: C – Flash loans democratize arbitrage by requiring only gas fees.

Q12. What does MEV stand for?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

Q13. Which defense mechanism requires tokens to be locked before voting?
A) Circuit breakers B) Reentrancy guards C) Vote locking D) TWAP oracles
Answer: C – Vote locking prevents flash loan governance attacks.

Q14. What was the approximate MEV volume extracted in 2023?
A) $60M+ B) $200M+ C) $600M+ D) $2B+
Answer: C – Over $600M extracted via MEV in 2023.

Q15. In a sandwich attack, what does the attacker do?
A) Front-run and back-run a victim's transaction B) Split transaction into parts C) Surround smart contract with malicious code D) Execute trades on multiple DEXs
Answer: A – Sandwich attacks place transaction before and after victim's transaction.

Quiz (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys

Quiz (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering

Quiz (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API C) Chainlink decentralized oracles D) On-chain voting

Quiz (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API C) Chainlink decentralized oracles D) On-chain voting
Answer: C – Chainlink aggregates prices from multiple sources, preventing manipulation.

Q19. What is the primary reason flash loans amplify protocol vulnerabilities?
A) They are free to execute B) They provide unlimited capital for exploitation C) They bypass security checks
D) They cannot be traced

Quiz (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API C) Chainlink decentralized oracles D) On-chain voting
Answer: C – Chainlink aggregates prices from multiple sources, preventing manipulation.

Q19. What is the primary reason flash loans amplify protocol vulnerabilities?
A) They are free to execute B) They provide unlimited capital for exploitation C) They bypass security checks
D) They cannot be traced
Answer: B – Flash loans allow borrowing unlimited amounts to exploit vulnerabilities at scale.

Q20. In a collateral swap using flash loans, what is the main benefit?
A) Lower interest rates B) Zero liquidation risk during swap C) No transaction fees D) Increased borrowing capacity

Quiz (16–20)

Q16. What organization helps democratize MEV extraction and reduce gas wars?
A) Chainlink B) Flashbots C) OpenZeppelin D) ConsenSys
Answer: B – Flashbots democratizes MEV extraction and reduces network congestion.

Q17. What was the charge against the Mango Markets attacker in December 2022?
A) Flash loan abuse B) Market manipulation C) Smart contract hacking D) Money laundering
Answer: B – Charged with market manipulation, not specifically flash loan use.

Q18. Which oracle solution is recommended to prevent flash loan price manipulation?
A) Single DEX price feed B) Centralized price API C) Chainlink decentralized oracles D) On-chain voting
Answer: C – Chainlink aggregates prices from multiple sources, preventing manipulation.

Q19. What is the primary reason flash loans amplify protocol vulnerabilities?
A) They are free to execute B) They provide unlimited capital for exploitation C) They bypass security checks
D) They cannot be traced
Answer: B – Flash loans allow borrowing unlimited amounts to exploit vulnerabilities at scale.

Q20. In a collateral swap using flash loans, what is the main benefit?
A) Lower interest rates B) Zero liquidation risk during swap C) No transaction fees D) Increased borrowing capacity
Answer: B – Atomicity ensures instant swap with zero liquidation risk.

Quiz (21–23)

Q21. Which is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation

Quiz (21–23)

Q21. Which is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q22. What defense mechanism averages prices over multiple blocks?
A) Chainlink oracles B) TWAP (Time-Weighted Average Price) C) Reentrancy guards D) Circuit breakers

Quiz (21–23)

Q21. Which is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q22. What defense mechanism averages prices over multiple blocks?
A) Chainlink oracles B) TWAP (Time-Weighted Average Price) C) Reentrancy guards D) Circuit breakers
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

Q23. What is MEV?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value

Quiz (21–23)

Q21. Which is NOT a legitimate flash loan use case?
A) Arbitrage between DEXs B) Collateral swapping C) Oracle price manipulation D) Self-liquidation
Answer: C – Oracle manipulation is an attack vector, not legitimate use.

Q22. What defense mechanism averages prices over multiple blocks?
A) Chainlink oracles B) TWAP (Time-Weighted Average Price) C) Reentrancy guards D) Circuit breakers
Answer: B – TWAP averages prices over blocks, preventing single-transaction manipulation.

Q23. What is MEV?
A) Maximum Extractable Value B) Miner Extractable Value C) Maximal Extractable Value D) Market Efficiency Value
Answer: C – MEV is Maximal Extractable Value, profit from transaction ordering.

L43: Smart Contract Security

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand the stakes of smart contract security
- Identify top vulnerability types (reentrancy, access control, oracle manipulation)
- Analyze real-world exploits (The DAO, Parity, bridge hacks)
- Apply security tools (Slither, Mythril, formal verification)
- Implement defense in depth strategies

The Problem: How do we prevent billion-dollar bugs?

The Challenge
Smart contracts are immutable code controlling billions in assets. A single bug cannot be patched post-deployment and can drain entire protocols. How do we write code that is secure enough to hold irreversible value?

Why It Matters

- $10B+ stolen cumulatively (2016–2024); $2.2B in 2024 alone
- Historical disasters: The DAO ($60M), Parity ($150M), Ronin bridge ($625M), Wormhole ($320M)

What We Need

- Risk management and mitigation
- Secure development practices and formal verification

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Smart Contract Security addresses this challenge

The Stakes of Smart Contract Security

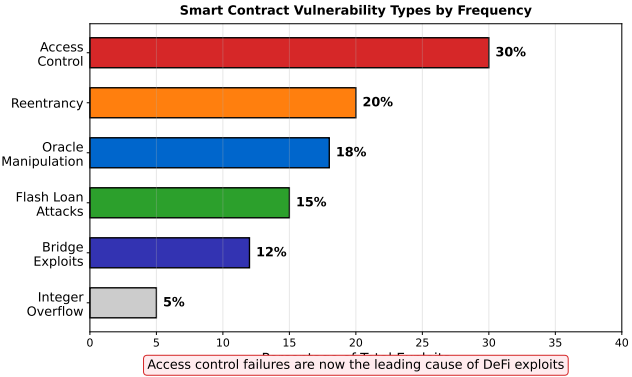
Why It Matters:

- **Code is Law**: Immutable, self-executing
- **High-Value**: Billions in DeFi TVL
- **Irreversible**: No patching w/o upgrades

Risk Scale:

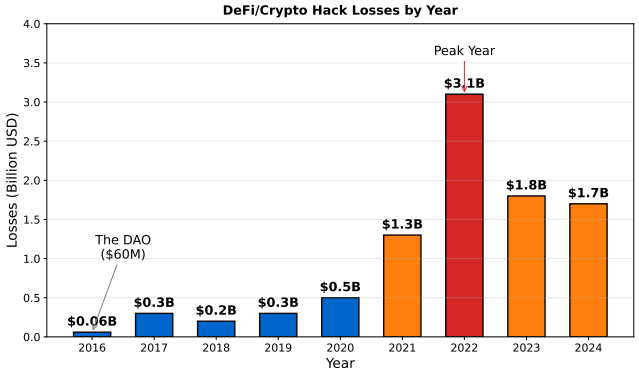
- $10B+ stolen (2016-2024)
- 2024 alone: $2.2B
- One bug = entire protocol
- Cascading composability risk

Top Vulnerability Types



Access control failures have become the leading cause of DeFi exploits

Historical Losses



*2022 was peak year (**$**3.8B per Chainalysis); 2024: **$**2.2B across 303 incidents*

Reentrancy: The DAO Hack (2016)

Context:
The DAO: $150M raised
Vulnerability:
External call before state update
Attack:

1. Deposit 1 ETH
2. Call withdraw(1)
3. Fallback calls withdraw() again
4. Balance not updated yet
5. Loop until drained

Result:

- $60M drained
- Ethereum hard fork
- ETH vs ETC split

Root Cause:
State updated AFTER external call

Reentrancy: Defense

Checks-Effects-Interactions:

1. **Check**: Verify conditions
2. **Effect**: Update state FIRST
3. **Interaction**: External calls LAST

Key Rule: Always update state before external calls

Reentrancy Guard:

- Lock flag prevents recursion
- OpenZeppelin ReentrancyGuard
- Industry standard solution

Access Control Vulnerabilities

Common Mistakes

- Missing onlyOwner modifier
- Default function visibility (public)
- Unprotected selfdestruct
- Constructor typo (pre-0.5.0)

Parity Wallet Hack (2017)

- initWallet() unprotected
- Attacker became owner
- Called selfdestruct
- $150M+ frozen forever

Best Practices

- Use OpenZeppelin Ownable
- Explicit visibility modifiers
- Role-based access control
- Multi-sig for critical functions

2024 Hacks

- DMM Bitcoin: $305M (key theft)
- WazirX: $230M (exchange)
- Private key compromises: 44%

Oracle Manipulation

Problem:
DeFi relies on external price data
Vulnerable Pattern:
Single DEX price as oracle
Attack:

1. Flash loan massive funds
2. Manipulate DEX price (10x)
3. Protocol reads fake price
4. Exploit at wrong price
5. Restore, repay, profit

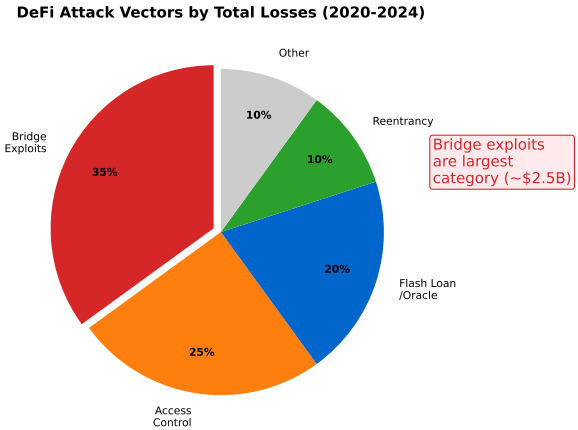
Real Examples:

- Harvest Finance: $34M
- Cream Finance: $130M

Defense:

- Chainlink oracles
- TWAP (time-weighted)
- Multiple price sources

Attack Vectors by Loss Amount



Bridge exploits account for largest share of total losses

Bridge Exploits: The New Frontier

Why Bridges?
Cross-chain = lock-and-mint
Notable Exploits:

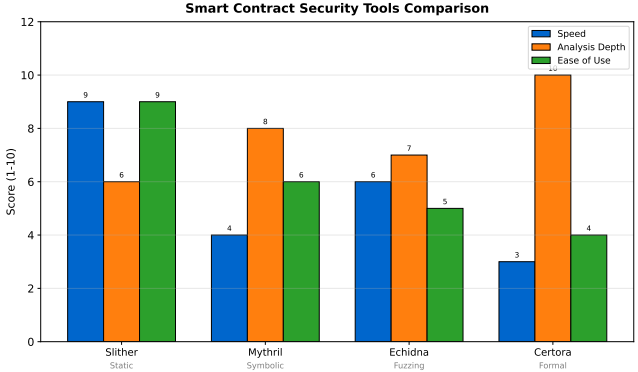
- Ronin (2022): $625M - key theft
- Wormhole: $320M - sig bug
- Nomad: $190M - init vuln

Attack Surface:

- Validators, contracts, keys
- Centralized validator sets
- Complex multi-chain logic
- $10B+ locked in bridges

Trend: Bridge security is 2024-2025 priority

Security Tools Comparison



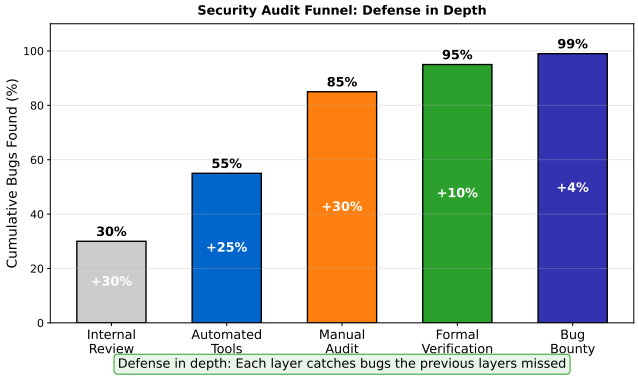
Combine fast tools (Slither) with deep analysis (Mythril, Certora)

Security Tools Overview

Tool	Type	Detects
Slither	Static analyzer	Reentrancy, overflow, access
Mythril	Symbolic execution	Integer bugs, unchecked calls
Echidna	Fuzzer	Invariant violations
Certora	Formal verifier	Specification violations

- **Slither**: Fast, easy CI/CD integration
- **Mythril**: Deep analysis, finds complex bugs
- **Echidna**: Property-based testing
- **Certora**: Mathematical proofs

Defense in Depth



Each security layer catches bugs that previous layers missed

Audit Process

Pre-Launch:

1. Internal review, peer review
2. Automated: Slither, Mythril
3. Manual audit ($50k-500k)
4. Formal verification (Certora)

Firms: Trail of Bits, OpenZeppelin

Post-Launch:

- Bug bounty (Immunefi)
- Monitoring (Forta, Defender)
- Insurance (Nexus Mutual)

Bug Bounty Programs

Overview:

- Incentivize white-hat hackers
- Platforms: Immunefi, Code4rena
- Payouts: $1k to $10M+
- Record: Wormhole $10M (2022)

Notable Programs:

- MakerDAO: Up to $10M
- ETH Foundation: $250k
- Compound: $500k

ROI: $1 bounty = $100+ saved

Best practice: Continuous bounty, not just pre-launch

Upgradeable Contracts

Problem:
Immutable contracts cannot be patched
Solution: Proxy Pattern

- Separate storage and logic
- Transparent: Proxy holds storage
- UUPS: Upgrade in implementation

Risk:
Admin key $\rightarrow$ malicious upgrade
Mitigation:

- Multi-sig governance
- Timelock delays
- Immutable after maturity

(c) Joerg Osterrieder 2025

Security Best Practices

Code:

- Solidity 0.8.0+
- Checks-Effects-Interactions
- Reentrancy guards
- Explicit visibility

Design:

- Chainlink oracles
- Pull over push
- No unbounded loops

Process:

- Slither + Mythril CI/CD
- Professional audit
- Bug bounty
- Forta monitoring

(c) Joerg Osterrieder 2025

Problem Solved? Smart Contract Security

The Original Problem

How do we prevent billion-dollar bugs?

How Smart Contract Security Solves It

- Reentrancy guards and checks-effects-interactions pattern prevent recursive draining
- Formal verification (Certora), audits, and bug bounties catch vulnerabilities before deployment
- Defense in depth: automated tools (Slither, Mythril), professional audits, continuous monitoring (Forta)

Remaining Limitations

- Audits miss bugs: 2024 saw $2.2B stolen despite many audited protocols
- Formal verification has limits: cannot model all real-world attack vectors
- Human error in key management: 44% of 2024 losses from private key theft

Open Questions

- Can we make smart contracts provably secure against all attack vectors?
- Risk: Black swan events, cascading failures across composable protocols

Smart Contract Security reduces but cannot eliminate risks; composability introduces systemic vulnerabilities

Summary

Landscape:

- \$10B+ cumulative losses
- 2024: \$2.2B across 303 hacks
- Top: Access control (44%)
- DAO hack $\rightarrow$ ETH hard fork

Defense:

- Tools: Slither, Mythril, Certora
- Audits + bounties + monitoring
- Upgradeable: Enables patches
- Trend: CEXs now targeted more

Defense in depth is essential: No single tool catches all vulnerabilities

Questions for Reflection

1. Why is the Checks-Effects-Interactions pattern important?
2. How do oracle manipulation attacks exploit DeFi protocols?
3. What makes bridge security particularly challenging?
4. Should audited protocols still have bug bounties?
5. What are the trade-offs of upgradeable contracts?

Sources & References

Hack Statistics:

- Chainalysis 2024 Report: $2.2B stolen (303 incidents); $3.8B in 2022
- chainalysis.com/blog/crypto-hacking-stolen-funds-2025

Major Incidents (verified):

- The DAO (June 2016): $60M – Wikipedia: The_DAO
- Parity Wallet (Nov 2017): $150M+ – TechCrunch, CNBC reports
- Ronin Bridge (Mar 2022): $625M – CoinDesk, Halborn analysis
- Wormhole (Feb 2022): $320M – Chainalysis incident report
- DMM Bitcoin (May 2024): $305M – TechCrunch, FBI attribution
- WazirX (July 2024): $230M – Crystal Intelligence analysis

All figures verified via Chainalysis, Elliptic, and primary news sources

Quiz Questions (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment
B) Code is immutable and self-executing with high-value assets at stake
C) Blockchain networks prevent all security vulnerabilities
D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently
B) $60M drained, leading to Ethereum hard fork (ETH/ETC split)
C) Only $10M was stolen and later recovered
D) No significant impact on Ethereum
Answer: B – $60M was drained via reentrancy, leading to controversial hard fork creating ETH and ETC.

Q5. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users
B) Verify conditions, update state FIRST, then make external calls LAST
C) Check balances, calculate effects, interact with DEXs
D) Validate inputs, log events, send transactions
Answer: B – This pattern prevents reentrancy by updating state before external calls.

Quiz Questions (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated
B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds
D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price
C) Stealing API keys D) DDoS attacks on oracle networks
Answer: B – Flash loan manipulates DEX pool price used as oracle.

Q10. What is the best defense against oracle manipulation?
A) Single DEX price B) Decentralized oracles (Chainlink), TWAP, multiple sources
C) Disable price updates D) Manual price entry
Answer: B – Multiple decentralized sources and TWAP prevent manipulation.

Quiz Questions (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions
B) Complex multi-chain logic, centralized validators, high-value targets
C) They lack smart contract functionality
D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier.

Q15. What does Echidna do?
A) Static code analysis B) Symbolic execution C) Property-based fuzzing D) Runtime monitoring
Answer: C – Echidna fuzzes to find invariant violations.

Quiz Questions (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain
B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation
C) Contracts are deleted and redeployed
D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher
B) Admin key compromise allows malicious upgrade
C) Storage is lost during upgrade
D) They cannot be used with ERC-20 tokens
Answer: B – If admin key is compromised, attacker can upgrade to malicious implementation.

Q20. What does "defense in depth" mean for smart contract security?
A) Using only one security tool thoroughly
B) Layered approach: automated tools + audits + formal verification + bounties + monitoring
C) Focusing only on the most common vulnerability
D) Relying solely on audits
Answer: B – Multiple security layers catch bugs that previous layers missed; no single tool is sufficient.

L43: Smart Contract Security

Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Smart Contract Security in a Nutshell

- "It's been audited" provides false confidence—audited protocols still lose billions
- Immutable code means bugs live forever; one exploit drains everything

[COMIC: Confident developer pointing to audit certificate while hacker lurks behind server. Developer speech bubble: "Relax! It's been audited by three firms!" Audit badge glowing while reentrancy attack code scrolls in background]

[PLACEHOLDER] — An audit is a snapshot in time—attackers have forever to find what auditors missed

Learning Objectives

- Understand the stakes of smart contract security
- Identify top vulnerability types (reentrancy (bug where attacker repeatedly calls a function before it finishes), access control (rules about who can call which functions), oracle manipulation)
- Analyze real-world exploits (The DAO, Parity, bridge hacks)
- Apply security tools (Slither (automated vulnerability scanner for Solidity), Mythril (deep analysis tool exploring all execution paths), formal verification)
- Implement defense in depth strategies

Building on L42: Flash Loans

The Problem: How do we prevent billion-dollar bugs?

The Challenge
Smart contracts are immutable code controlling billions in assets. A single bug cannot be patched post-deployment and can drain entire protocols. How do we write code that is secure enough to hold irreversible value?

Why It Matters

- $10B+ stolen cumulatively (2016–2024); $2.2B in 2024 alone
- Historical disasters: The DAO ($60M), Parity ($150M), Ronin bridge ($625M), Wormhole ($320M)

What We Need

- Risk management and mitigation
- Secure development practices and formal verification

The Cryptoeconomics Question
Managing systemic and idiosyncratic risks

Today's lesson: How Smart Contract Security addresses this challenge

Why Do Smart Contracts Get Hacked?

Why It Matters:

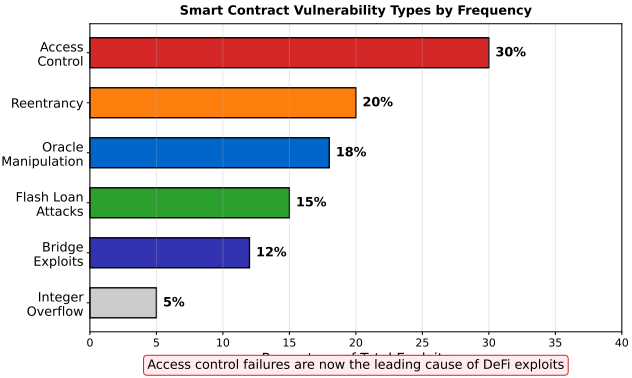
- **Code is Law**: Immutable, self-executing
- **High-Value**: Billions in DeFi TVL
- **Irreversible**: No patching w/o upgrades

Risk Scale:

- $10B+ stolen (2016-2024)
- 2024 alone: $2.2B
- One bug = entire protocol
- Cascading composability risk

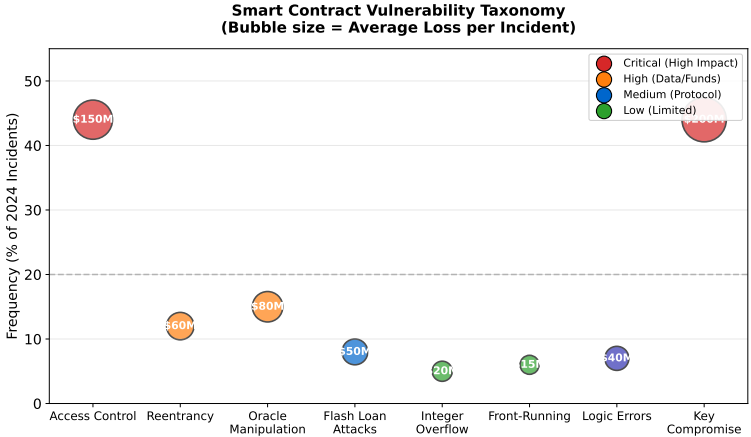
→ *Problem: How do we prevent billion-dollar bugs? — The Stakes of Smart Contract Security shows immutable code + high-value assets = catastrophic consequences for any bug—no patches possible after deployment*

What Are the Most Common Smart Contract Vulnerabilities?



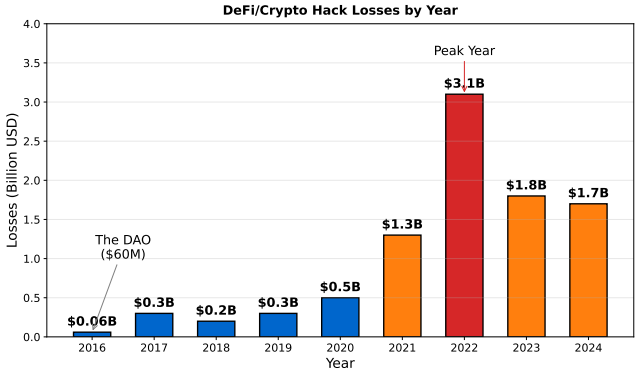
Access control failures have become the leading cause of DeFi exploits

How Do Different Vulnerabilities Compare by Impact?



Bubble size indicates average loss per incident; Access control and key compromise dominate losses

How Have Smart Contract Losses Changed Over Time?



*2022 was peak year (**$**3.8B per Chainalysis); 2024: **$**2.2B across 303 incidents*

How Does a Reentrancy Attack Work?

Context:
The DAO: $150M raised
Vulnerability:
External call before state update
Attack:

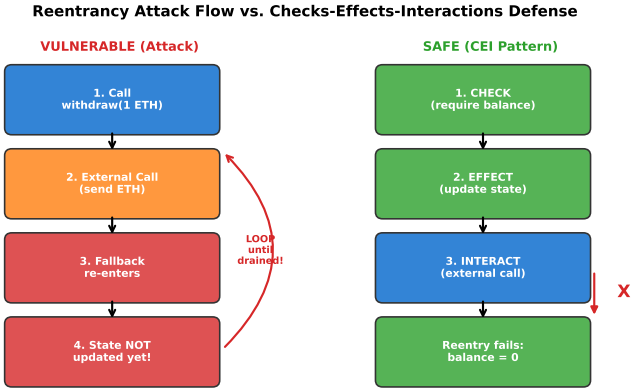
1. Deposit 1 ETH
2. Call withdraw(1)
3. Fallback calls withdraw() again
4. Balance not updated yet
5. Loop until drained

Result:

- $60M drained
- Ethereum hard fork
- ETH vs ETC split

Root Cause:
State updated AFTER external call

What Does a Reentrancy Attack Look Like?



Key Insight: Update state BEFORE external calls to prevent recursive exploitation

Checks-Effects-Interactions (CEI) pattern: verify conditions, update state, then call externally

How Can You Prevent Reentrancy Attacks?

Checks-Effects-Interactions (pattern: verify, update state, then call external):

1. **Check**: Verify conditions
2. **Effect**: Update state FIRST
3. **Interaction**: External calls LAST

Key Rule: Always update state before external calls

Reentrancy Guard:

- Lock flag prevents recursion
- OpenZeppelin ReentrancyGuard
- Industry standard solution

→ *Problem: How do we prevent billion-dollar bugs? — Reentrancy: Defense provides a concrete defense pattern: update state BEFORE external calls to prevent recursive draining attacks*

What Happens When Functions Aren't Protected?

Common Mistakes

- Missing onlyOwner modifier
- Default function visibility (public)
- Unprotected selfdestruct
- Constructor typo (pre-0.5.0)

Parity Wallet Hack (2017)

- initWallet() unprotected
- Attacker became owner
- Called selfdestruct
- $150M+ frozen forever

Best Practices

- Use OpenZeppelin Ownable
- Explicit visibility modifiers
- Role-based access control
- Multi-sig for critical functions

2024 Hacks

- DMM Bitcoin: $305M (key theft)
- WazirX: $230M (exchange)
- Private key compromises: 44%

Why Can't You Trust a Single Price Source?

Problem:
DeFi relies on external price data
Vulnerable Pattern:
Single DEX price as oracle
Attack:

1. Flash loan massive funds
2. Manipulate DEX price (10x)
3. Protocol reads fake price
4. Exploit at wrong price
5. Restore, repay, profit

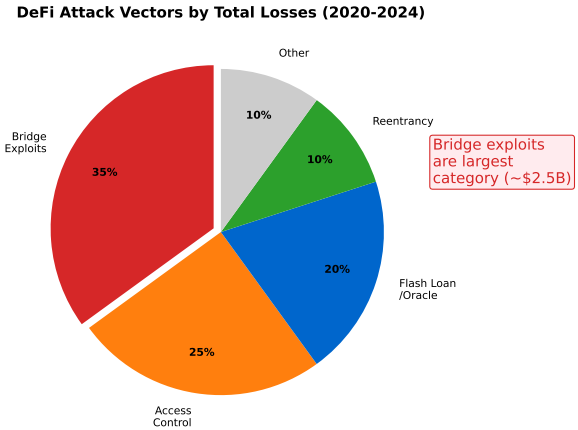
Real Examples:

- Harvest Finance: $34M
- Cream Finance: $130M

Defense:

- Chainlink oracles
- TWAP (time-weighted)
- Multiple price sources

Which Attack Vectors Cause the Biggest Losses?



Bridge exploits account for largest share of total losses

Problem Check-In: Smart Contract Security

Recall Our Problem

How do we prevent billion-dollar bugs?

What We've Learned So Far

- Reentrancy attacks exploit external calls that re-enter the contract before state is updated (The DAO lost $60M)
- Access control failures now cause 44% of losses—unprotected functions let attackers take ownership
- These bugs are preventable with patterns (Checks-Effects-Interactions) and tools (Slither, Mythril)

Still to Address

- Bridge security, formal verification, and the full security toolchain (audits, bounties, monitoring)
- Can we ever achieve provably secure smart contracts, or will attackers always find new vectors?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How do we prevent billion-dollar bugs?"?

Why Are Bridges So Vulnerable to Attacks?

Why Bridges?
Cross-chain = lock-and-mint
Notable Exploits:

- Ronin (2022): $625M - key theft
- Wormhole: $320M - sig bug
- Nomad: $190M - init vuln

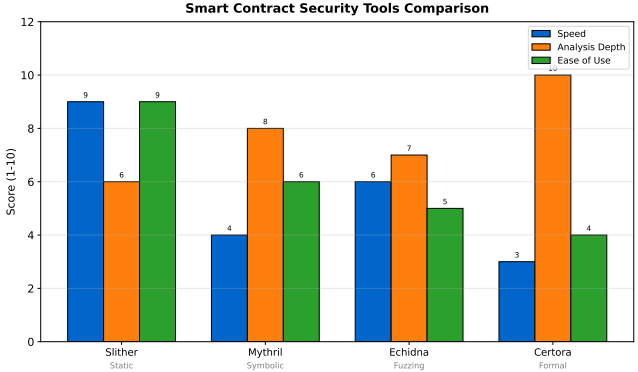
Attack Surface:

- Validators, contracts, keys
- Centralized validator sets
- Complex multi-chain logic
- $10B+ locked in bridges

Trend: Bridge security is 2024-2025 priority

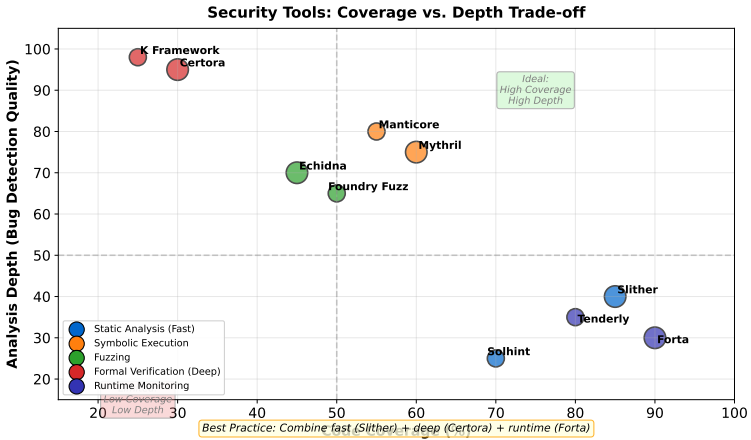
→ *Problem: How do we prevent billion-dollar bugs? — Bridge Exploits: The New Frontier reveals bridges are the new attack frontier: $2B+ stolen from cross-chain bridges due to complex multi-chain logic*

How Do Different Security Tools Compare?



Combine fast tools (Slither) with deep analysis (Mythril, Certora)

What Are the Trade-Offs Between Security Tools?



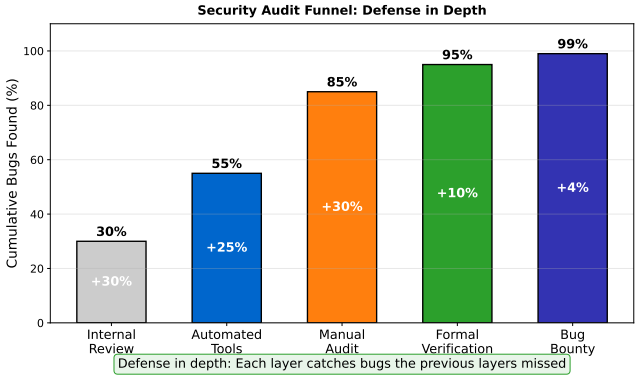
Trade-off: Static analysis offers speed and coverage; formal verification provides depth but limited coverage

Which Security Tools Should You Use?

Tool	Type	Detects
Slither	Static analyzer	Reentrancy, overflow, access
Mythril	Symbolic execution	Integer bugs, unchecked calls
Echidna	Fuzzer (tool throwing random inputs to find failures)	Invariant violations
Certora	Formal verifier	Specification violations

- **Slither**: Fast, easy CI/CD integration
- **Mythril**: Deep analysis, finds complex bugs
- **Echidna**: Property-based testing
- **Certora**: Mathematical proofs

Why Do You Need Multiple Security Layers?



Each security layer catches bugs that previous layers missed

What Does a Security Audit Actually Cover?

Pre-Launch:

1. Internal review, peer review
2. Automated: Slither, Mythril
3. Manual audit ($50k-500k)
4. Formal verification (Certora)

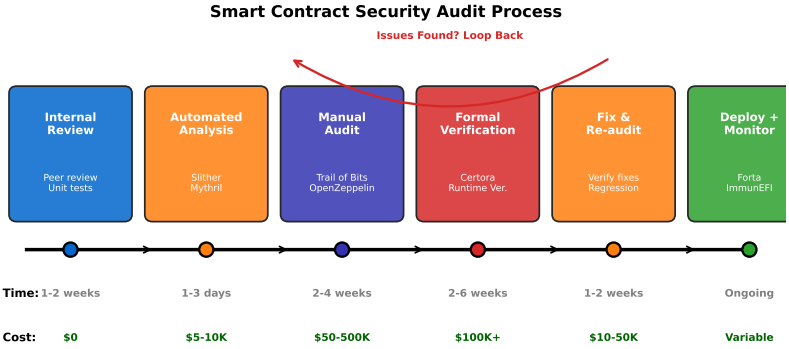
Firms: Trail of Bits, OpenZeppelin

Post-Launch:

- Bug bounty (Immunefi)
- Monitoring (Forta, Defender)
- Insurance (Nexus Mutual)

→ *Problem: How do we prevent billion-dollar bugs? — Audit Process shows defense-in-depth is essential: no single tool catches all bugs, so we layer automated analysis + audits + bounties*

How Does a Security Audit Work?



Typical Total: 6-12 weeks | Cost: $100K – 1M+ for comprehensive audit

Comprehensive audits take 6-12 weeks and cost $100K-$1M+; issues loop back for re-audit

How Much Are Vulnerabilities Worth?

Overview:

- Incentivize white-hat hackers
- Platforms: Immunefi, Code4rena
- Payouts: $1k to $10M+
- Record: Wormhole $10M (2022)

Notable Programs:

- MakerDAO: Up to $10M
- ETH Foundation: $250k
- Compound: $500k

ROI: $1 bounty = $100+ saved

Best practice: Continuous bounty, not just pre-launch

Can You Fix Bugs in Immutable Contracts?

Problem:
Immutable contracts cannot be patched
Solution: Proxy Pattern (separating storage from logic for upgrades)

- Separate storage and logic
- Transparent: Proxy holds storage
- UUPS: Upgrade in implementation

Risk:
Admin key $\rightarrow$ malicious upgrade
Mitigation:

- Multi-sig governance
- Timelock delays
- Immutable after maturity

What Are the Essential Security Best Practices?

Code:

- Solidity 0.8.0+
- Checks-Effects-Interactions
- Reentrancy guards
- Explicit visibility

Design:

- Chainlink oracles
- Pull over push
- No unbounded loops

Process:

- Slither + Mythril CI/CD
- Professional audit
- Bug bounty
- Forta monitoring

Problem Solved? Smart Contract Security

The Original Problem

How do we prevent billion-dollar bugs?

How Smart Contract Security Solves It

- Reentrancy guards and checks-effects-interactions pattern prevent recursive draining
- Formal verification (Certora), audits, and bug bounties catch vulnerabilities before deployment
- Defense in depth: automated tools (Slither, Mythril), professional audits, continuous monitoring (Forta)

Remaining Limitations

- Audits miss bugs: 2024 saw $2.2B stolen despite many audited protocols
- Formal verification has limits: cannot model all real-world attack vectors
- Human error in key management: 44% of 2024 losses from private key theft

Open Questions

- Can we make smart contracts provably secure against all attack vectors?
- Risk: Black swan events, cascading failures across composable protocols

Smart Contract Security reduces but cannot eliminate risks; composability introduces systemic vulnerabilities

The Economics of Smart Contract Security

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Smart Contract Security

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Smart Contract Security

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Smart Contract Security Reality Check

- The reentrancy attack pattern: external call triggers fallback, re-enters withdraw before balance updates
- Understanding attack flows is essential—every DeFi developer must know how these exploits work

[COMIC: Diagram showing reentrancy attack flow as a loop. Attacker contract calling withdraw() repeatedly while victim contract's balance check shows stale data. Arrows forming infinite loop with "Balance: 10 ETH" stuck while funds drain]

[PLACEHOLDER] — One line of code in the wrong order can cost millions—Checks-Effects-Interactions saves lives

Summary

Landscape:

- $10B+ cumulative losses
- 2024: $2.2B across 303 hacks
- Top: Access control (44%)
- DAO hack → ETH hard fork

Next Lesson: L44 – Lab: Security Audit

Defense:

- Tools: Slither, Mythril, Certora
- Audits + bounties + monitoring
- Upgradeable: Enables patches
- Trend: CEXs now targeted more

Defense in depth is essential: No single tool catches all vulnerabilities

Questions for Reflection

1. Why is the Checks-Effects-Interactions pattern important?
2. How do oracle manipulation attacks exploit DeFi protocols?
3. What makes bridge security particularly challenging?
4. Should audited protocols still have bug bounties?
5. What are the trade-offs of upgradeable contracts?

Sources & References

Hack Statistics:

- Chainalysis 2024 Report: $2.2B stolen (303 incidents); $3.8B in 2022
- chainalysis.com/blog/crypto-hacking-stolen-funds-2025

Major Incidents (verified):

- The DAO (June 2016): $60M – Wikipedia: The_DAO
- Parity Wallet (Nov 2017): $150M+ – TechCrunch, CNBC reports
- Ronin Bridge (Mar 2022): $625M – CoinDesk, Halborn analysis
- Wormhole (Feb 2022): $320M – Chainalysis incident report
- DMM Bitcoin (May 2024): $305M – TechCrunch, FBI attribution
- WazirX (July 2024): $230M – Crystal Intelligence analysis

All figures verified via Chainalysis, Elliptic, and primary news sources

Quiz Questions (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment
B) Code is immutable and self-executing with high-value assets at stake
C) Blockchain networks prevent all security vulnerabilities
D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently
B) $60M drained, leading to Ethereum hard fork (ETH/ETC split)
C) Only $10M was stolen and later recovered
D) No significant impact on Ethereum
Answer: B – $60M was drained via reentrancy, leading to controversial hard fork creating ETH and ETC.

Q5. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users
B) Verify conditions, update state FIRST, then make external calls LAST
C) Check balances, calculate effects, interact with DEXs
D) Validate inputs, log events, send transactions
Answer: B – This pattern prevents reentrancy by updating state before external calls.

Quiz Questions (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated
B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds
D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price
C) Stealing API keys D) DDoS attacks on oracle networks
Answer: B – Flash loan manipulates DEX pool price used as oracle.

Q10. What is the best defense against oracle manipulation?
A) Single DEX price B) Decentralized oracles (Chainlink), TWAP, multiple sources
C) Disable price updates D) Manual price entry
Answer: B – Multiple decentralized sources and TWAP prevent manipulation.

Quiz Questions (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions
B) Complex multi-chain logic, centralized validators, high-value targets
C) They lack smart contract functionality
D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier.

Q15. What does Echidna do?
A) Static code analysis B) Symbolic execution C) Property-based fuzzing D) Runtime monitoring
Answer: C – Echidna fuzzes to find invariant violations.

Quiz Questions (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain
B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation
C) Contracts are deleted and redeployed
D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher
B) Admin key compromise allows malicious upgrade
C) Storage is lost during upgrade
D) They cannot be used with ERC-20 tokens
Answer: B – If admin key is compromised, attacker can upgrade to malicious implementation.

Q20. What does "defense in depth" mean for smart contract security?
A) Using only one security tool thoroughly
B) Layered approach: automated tools + audits + formal verification + bounties + monitoring
C) Focusing only on the most common vulnerability
D) Relying solely on audits
Answer: B – Multiple security layers catch bugs that previous layers missed; no single tool is sufficient.

L43: Smart Contract Security

Mini-Lecture — Module F: Advanced Topics

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand why smart contract security is critical
- Identify top vulnerability types: reentrancy, access control, oracle manipulation
- Analyze real-world exploits: The DAO, Parity, bridge hacks
- Apply defense in depth strategies

After this mini-lecture, you will understand the most common attack vectors and defenses.

The Stakes of Smart Contract Security

Why Security Matters:

- **Code is Law**: Immutable and self-executing
- **High-Value Targets**: Billions in DeFi assets
- **Irreversibility**: No patches without upgrades
- **Composability Risk**: Bugs cascade across protocols

Losses to Date:

- Cumulative: $10B+ stolen (2016–2024)
- 2024: $2.2B across 303 incidents
- 2022 peak: $3.8B (Chainalysis)

Photo: FlyD / Unsplash (CC0)

Top Vulnerability Types

Vulnerability	Share of Losses	Example
Access Control	44%	Parity Wallet ($150M)
Reentrancy	15%	The DAO ($60M)
Oracle Manipulation	12%	Harvest Finance ($34M)
Bridge Exploits	18%	Ronin ($625M)
Other	11%	Integer overflow, logic bugs

Key Insight: Access control failures (missing modifiers, unprotected functions) have become the leading cause of DeFi exploits, surpassing reentrancy.

(c) Joerg Osterrieder 2025

Reentrancy: The DAO Hack (2016)

Attack Mechanism:

1. Attacker deposits 1 ETH to The DAO
2. Calls `withdraw(1)` – contract sends 1 ETH
3. Attacker's fallback function recursively calls `withdraw()`
4. Balance not yet updated – contract sends another 1 ETH
5. Loop continues until contract drained

Result: $60M drained, Ethereum hard fork (ETH/ETC split)

Root Cause: State updated *after* external call instead of *before*

Reentrancy Defense: Checks-Effects-Interactions

The Pattern:

1. **Checks**: Verify conditions (require statements)
2. **Effects**: Update state variables FIRST
3. **Interactions**: Make external calls LAST

Additional Protection:

- **Reentrancy Guard**: Lock flag prevents recursive calls
- **OpenZeppelin ReentrancyGuard**: Industry standard implementation
- **Pull over Push**: Let users withdraw instead of pushing funds

Always update state before external calls – this is the single most important pattern.

Access Control Vulnerabilities

Common Mistakes:

- Missing `onlyOwner` modifier
- Default visibility (public)
- Unprotected `selfdestruct`
- Constructor typo (pre-0.5.0)

Parity Wallet (2017):

- `initWallet()` was unprotected
- Attacker became owner
- Called `selfdestruct`
- $150M+ frozen forever

2024 Major Hacks:

- DMM Bitcoin: $305M (key theft)
- WazirX: $230M (exchange)
- Private key compromises: 44%

Best Practices:

- Use OpenZeppelin Ownable
- Explicit visibility modifiers
- Role-based access control (RBAC)
- Multi-sig for critical functions

Oracle Manipulation Attacks

The Problem: DeFi relies on external price data (oracles)

Attack Vector:

1. Flash loan borrow massive funds (no collateral)
2. Manipulate DEX pool price (e.g., 10x increase)
3. Protocol reads manipulated price as "true" price
4. Exploit: borrow, liquidate, or mint at wrong price
5. Restore pool, repay flash loan, keep profit

Real Examples:

- Harvest Finance: $34M (2020)
- Cream Finance: $130M (2021)

Defense: Chainlink oracles, TWAP (time-weighted average), multiple sources

Bridge Exploits: The New Frontier

Why Bridges Are Targets:

- Cross-chain requires lock-and-mint
- Complex multi-chain logic
- Centralized validator sets
- \$10B+ locked in bridges

Notable Exploits:

- Ronin (2022): \$625M – validator keys
- Wormhole (2022): \$320M – signature bug
- Nomad (2022): \$190M – init vulnerability

Photo: Towfiqu barbhuiya / Unsplash (CC0)

Bridge security is a top priority for 2024–2025; largest attack surface in Web3.

Defense in Depth

Layer	Tool/Process	Catches
1. Development	Peer review, unit tests	Logic errors
2. Automated	Slither, Mythril (CI/CD)	Common vulnerabilities
3. Manual Audit	Trail of Bits, OpenZeppelin	Complex bugs
4. Formal Verification	Certora	Specification violations
5. Bug Bounty	Immunefi ($10M+ payouts)	Edge cases
6. Monitoring	Forta, OpenZeppelin Defender	Live exploits
7. Insurance	Nexus Mutual	Financial recovery

Each layer catches bugs that previous layers missed; no single tool is sufficient.

Smart Contract Security in Practice

Access Control
Protect critical functions

Private Keys
44% of 2024 hacks

Code Audits
Multiple review layers

Security is not a product – it is a process. (Bruce Schneier)

Photos: FlyD, Towfiqu barbhuiya / Unsplash (CC0)

Quiz Questions (1–3)

Q1. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users
B) Verify conditions, update state FIRST, make external calls LAST
C) Check balances, calculate effects, interact with DEXs
D) Validate inputs, log events, send transactions
Answer: B – Prevents reentrancy by updating state before external calls.

Q2. What caused the Parity Wallet hack (2017)?
A) Reentrancy attack B) Unprotected `initWallet()` function
C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected init, became owner, called selfdestruct.

Q3. How do oracle manipulation attacks work?
A) Hacking Chainlink nodes
B) Flash loan manipulates DEX price, protocol reads false price
C) Stealing API keys D) DDoS attacks
Answer: B – Flash loans temporarily distort prices that naive protocols trust.

Quiz Questions (4–6)

Q4. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M)
C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin (2022) lost $625M via validator key compromise.

Q5. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier using mathematical specifications.

Q6. What does "defense in depth" mean?
A) Using only one security tool thoroughly
B) Layered approach: automated tools + audits + bounties + monitoring
C) Focusing only on the most common vulnerability
D) Relying solely on professional audits
Answer: B – Multiple layers catch bugs that previous layers missed.

Quiz: Smart Contract Security

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently B) $60M drained, leading to Ethereum hard fork (ETH/ETC split) C) Only $10M was stolen and later recovered D) No significant impact on Ethereum

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently B) $60M drained, leading to Ethereum hard fork (ETH/ETC split) C) Only $10M was stolen and later recovered D) No significant impact on Ethereum
Answer: B – $60M was drained via reentrancy, leading to controversial hard fork creating ETH and ETC.

Q5. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users B) Verify conditions, update state FIRST, then make external calls LAST C) Check balances, calculate effects, interact with DEXs D) Validate inputs, log events, send transactions

Quiz (1–5)

Q1. What is the primary reason smart contract security is critical?
A) Contracts can be easily patched after deployment B) Code is immutable and self-executing with high-value assets at stake C) Blockchain networks prevent all security vulnerabilities D) Smart contracts are not subject to financial risk
Answer: B – Smart contracts are immutable (code is law) and often hold billions in assets, making vulnerabilities catastrophic.

Q2. How much was lost to crypto hacks in 2024?
A) $500M B) $1.1B C) $2.2B D) $3.8B
Answer: C – $2.2B was stolen across 303 incidents in 2024 (per Chainalysis); $3.8B was the 2022 peak.

Q3. What is the leading cause of DeFi exploits?
A) Reentrancy attacks B) Oracle manipulation C) Access control failures D) Integer overflow
Answer: C – Access control failures (44% of losses) have become the leading vulnerability type.

Q4. What was the outcome of The DAO hack in 2016?
A) Ethereum shut down permanently B) $60M drained, leading to Ethereum hard fork (ETH/ETC split) C) Only $10M was stolen and later recovered D) No significant impact on Ethereum
Answer: B – $60M was drained via reentrancy, leading to controversial hard fork creating ETH and ETC.

Q5. What is the Checks-Effects-Interactions pattern?
A) Check oracles, effect prices, interact with users B) Verify conditions, update state FIRST, then make external calls LAST C) Check balances, calculate effects, interact with DEXs D) Validate inputs, log events, send transactions
Answer: B – This pattern prevents reentrancy by updating state before external calls.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price C) Stealing API keys D) DDoS attacks on oracle networks

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price C) Stealing API keys D) DDoS attacks on oracle networks
Answer: B – Flash loan manipulates DEX pool price used as oracle.

Q10. What is the best defense against oracle manipulation?
A) Single DEX price B) Decentralized oracles (Chainlink), TWAP, multiple sources C) Disable price updates D) Manual price entry

Quiz (6–10)

Q6. How does a reentrancy attack work?
A) Attacker calls withdraw() recursively before balance is updated B) Attacker overflows integer variables C) Attacker manipulates oracle price feeds D) Attacker guesses private keys
Answer: A – External call triggers fallback that recursively calls withdraw().

Q7. What caused the Parity Wallet hack (2017)?
A) Reentrancy B) Unprotected initWallet() function C) Oracle manipulation D) Integer overflow
Answer: B – Attacker called unprotected initWallet(), became owner, called selfdestruct.

Q8. What percentage of 2024 hacks involved private key compromises?
A) 10% B) 25% C) 44% D) 75%
Answer: C – 44% of 2024 losses from key theft.

Q9. How do oracle manipulation attacks exploit DeFi protocols?
A) Hacking Chainlink nodes B) Flash loan manipulates DEX price, protocol reads false price C) Stealing API keys D) DDoS attacks on oracle networks
Answer: B – Flash loan manipulates DEX pool price used as oracle.

Q10. What is the best defense against oracle manipulation?
A) Single DEX price B) Decentralized oracles (Chainlink), TWAP, multiple sources C) Disable price updates D) Manual price entry
Answer: B – Multiple decentralized sources and TWAP prevent manipulation.

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier.

Q15. What does Echidna do?
A) Static code analysis B) Symbolic execution C) Property-based fuzzing D) Runtime monitoring

Quiz (11–15)

Q11. What was the largest bridge exploit?
A) Wormhole ($320M) B) Nomad ($190M) C) Ronin Bridge ($625M) D) Poly Network ($600M)
Answer: C – Ronin Bridge (2022) lost $625M via validator key compromise.

Q12. Why are bridges particularly vulnerable?
A) They use outdated Solidity versions B) Complex multi-chain logic, centralized validators, high-value targets C) They lack smart contract functionality D) Bridges are not vulnerable
Answer: B – Large attack surface and billions in locked assets.

Q13. What type of analysis does Slither perform?
A) Formal verification B) Fuzzing C) Static analysis D) Runtime monitoring
Answer: C – Slither is a fast static analyzer.

Q14. Which tool provides mathematical proofs of contract correctness?
A) Slither B) Mythril C) Echidna D) Certora
Answer: D – Certora is a formal verifier.

Q15. What does Echidna do?
A) Static code analysis B) Symbolic execution C) Property-based fuzzing D) Runtime monitoring
Answer: C – Echidna fuzzes to find invariant violations.

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher B) Admin key compromise allows malicious upgrade C) Storage is lost during upgrade D) They cannot be used with ERC-20 tokens

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher B) Admin key compromise allows malicious upgrade C) Storage is lost during upgrade D) They cannot be used with ERC-20 tokens
Answer: B – If admin key is compromised, attacker can upgrade to malicious implementation.

Q20. What does "defense in depth" mean for smart contract security?
A) Using only one security tool thoroughly B) Layered approach: automated tools + audits + formal verification + bounties + monitoring C) Focusing only on the most common vulnerability D) Relying solely on audits

Quiz (16–20)

Q16. What is the typical cost range for a professional smart contract audit?
A) $1k–$5k B) $10k–$25k C) $50k–$500k D) $1M+
Answer: C – Manual audits by firms like Trail of Bits or OpenZeppelin cost $50k–$500k for 2-4 weeks.

Q17. What was the record bug bounty payout?
A) $1M B) $5M C) $10M D) $25M
Answer: C – Wormhole paid $10M bounty in 2022 (highest on record).

Q18. How do upgradeable contracts work?
A) Code is rewritten on-chain B) Proxy pattern: proxy holds storage, delegates to upgradeable implementation C) Contracts are deleted and redeployed D) Upgrades happen automatically via AI
Answer: B – Proxy separates storage (in proxy) from logic (in implementation), allowing logic upgrades.

Q19. What is the main risk of upgradeable contracts?
A) Gas costs are higher B) Admin key compromise allows malicious upgrade C) Storage is lost during upgrade D) They cannot be used with ERC-20 tokens
Answer: B – If admin key is compromised, attacker can upgrade to malicious implementation.

Q20. What does "defense in depth" mean for smart contract security?
A) Using only one security tool thoroughly B) Layered approach: automated tools + audits + formal verification + bounties + monitoring C) Focusing only on the most common vulnerability D) Relying solely on audits
Answer: B – Multiple security layers catch bugs that previous layers missed; no single tool is sufficient.

Lab Session: Security Audit

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module F: Advanced Topics

(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this lab session, you will be able to:

- Perform manual security code review
- Use automated tools (Slither, Mythril)
- Write exploit contracts demonstrating vulnerabilities
- Implement secure fixes using best practices
- Create professional audit reports

The Problem: Smart Contract Security Vulnerabilities

The Challenge
Every deployed smart contract is permanently exposed on-chain. A single vulnerability can lead to millions in losses. How do we systematically identify and fix security flaws before attackers exploit them?

Why It Matters

- $3.8 billion lost to DeFi hacks in 2022 alone
- Ronin Bridge exploit: $625M stolen via access control flaw

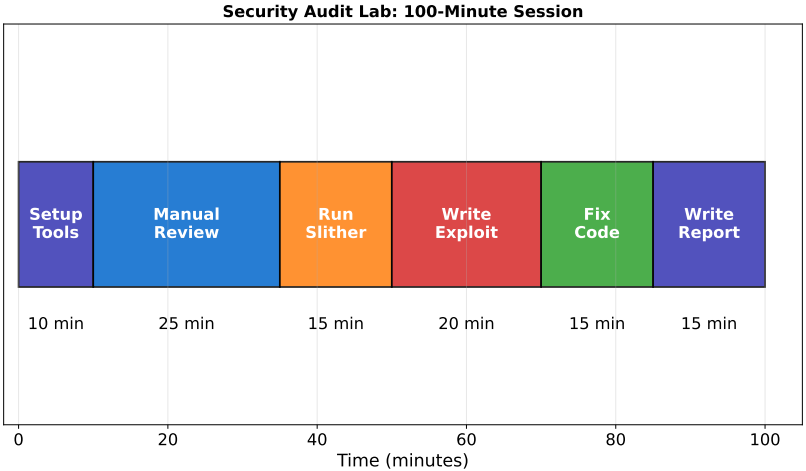
What You'll Explore

- Vulnerability identification through code review
- Automated security tools (Slither, Mythril)
- Attack vector analysis and exploit writing

The Cryptoeconomics Question
Security flaws create economic opportunities for attackers. How do we align incentives to reward discovery before exploitation?

Today's lesson: Hands-on security audit workflow from detection to remediation

Lab Session Structure



Complete security audit workflow from review to report

Lab Overview

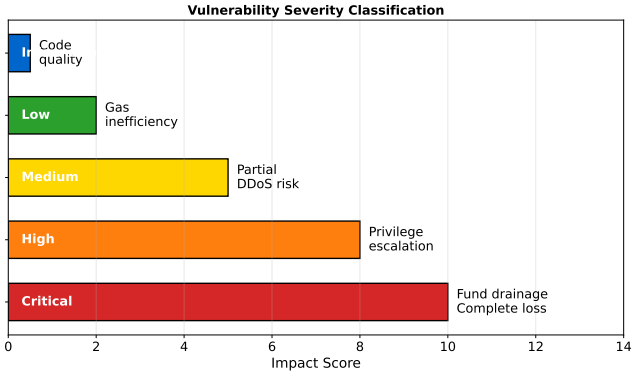
Contracts to Audit:

1. **VulnerableBank**: Reentrancy vulnerability
2. **InsecureToken**: Integer overflow, access control
3. **BadOracle**: Oracle manipulation

Deliverables:

- Audit report with severity classifications
- Exploit contracts demonstrating vulnerabilities
- Secure implementations with fixes

Vulnerability Severity Classification



Critical and High severity issues require immediate fixes

Exercise 1: VulnerableBank (Reentrancy)

Manual Review Tasks:

1. Read the withdraw function carefully
2. Identify external call before state update
3. Classify as Critical severity

Fix with Checks-Effects-Interactions:

- Update balance BEFORE external call
- Or use OpenZeppelin ReentrancyGuard

Exercise 2: InsecureToken (Multiple Issues)

Vulnerabilities to Find:

- Integer overflow (Solidity ¡ 0.8)
- Missing access control on mint
- Unprotected selfdestruct

Fix:

- Upgrade to Solidity 0.8.0+
- Add onlyOwner modifier
- Initialize owner in constructor

Exercise 3: BadOracle (Price Manipulation)

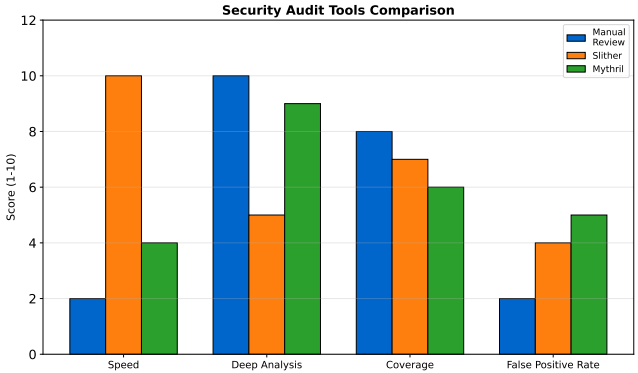
Vulnerability:

- Instant spot price from Uniswap
- Manipulable via flash loans

Secure Alternatives:

- Uniswap V2 TWAP oracle (time-weighted)
- Chainlink price feeds (decentralized oracle)
- Hybrid approach with multiple sources

Audit Tools Comparison



Combine manual review with automated tools for best coverage

Automated Analysis

Slither (Static Analysis):

- Fast pattern-based detection
- Run: `slither contracts/VulnerableBank.sol`

Mythril (Symbolic Execution):

- Deep path analysis
- Run: `myth analyze contracts/VulnerableBank.sol`

Key Detectors:

- SWC-107: Reentrancy
- SWC-101: Integer overflow
- SWC-105: Unprotected withdrawal

Audit Report Template

For Each Finding:

1. **Title**: Descriptive vulnerability name
2. **Severity**: Critical / High / Medium / Low
3. **Location**: Contract, function, line numbers
4. **Description**: What is the vulnerability
5. **Impact**: What can attacker achieve
6. **Recommendation**: How to fix

(c) Joerg Osterrieder 2025

Lab Deliverables

Submit:

1. **Audit Report (PDF):**
   - Findings for all three contracts
   - Severity classifications
   - Fix recommendations with code
2. **Code Submissions:**
   - Exploit contracts (AttackBank.sol, etc.)
   - Secure implementations
   - Test suite proving fixes work

Problem Solved? Security Audit Effectiveness

The Original Problem

How do we systematically identify and prevent smart contract vulnerabilities before deployment?

How Security Audits Solve It

- Manual review catches logic flaws automated tools miss
- Combined tooling (Slither + Mythril) provides comprehensive coverage
- Bug bounties reward white-hat discovery over exploitation

Remaining Limitations

- Audits are snapshots - code changes post-audit reintroduce risk
- Zero-day vulnerabilities unknown to auditors and tools

The Economic Model

- **Cost:** Time investment ($50k-$300k per audit), requires deep expertise
- **Reward:** Prevents exploits worth millions, preserves protocol reputation
- **Risk:** False sense of security, missing subtle bugs, post-audit modifications

Security audits reduce but don't eliminate risk - ongoing monitoring and bug bounties essential

Key Takeaways

- Security audit combines manual review and automated tools
- Reentrancy is critical - use Checks-Effects-Interactions
- Solidity 0.8.0+ provides built-in overflow protection
- Never trust spot prices - use TWAP or Chainlink
- Exploit writing proves vulnerability severity
- Professional reports follow structured template

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control issues
Answer: B – Update state (Effects) before external calls (Interactions) to prevent reentrant calls from exploiting stale state.

Q2. In the VulnerableBank example, what makes the withdraw function vulnerable?
A) Missing require check B) External call before balance update C) No access modifier D) Integer overflow
Answer: B – The contract sends ETH before updating the user's balance, allowing reentrancy.

Q3. Which Solidity version introduced built-in overflow/underflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow/underflow without SafeMath.

Q4. What severity classification should be assigned to a reentrancy vulnerability allowing fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Vulnerabilities enabling direct fund theft are classified as Critical severity.

Q5. Which tool uses symbolic execution for deep path analysis in smart contract audits?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril performs symbolic execution, while Slither uses fast static analysis.

Quiz Questions (6–10)

Q6. What is the main vulnerability when using Uniswap spot prices directly in smart contracts?
A) High gas costs B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction using flash loans.

Q7. What does TWAP stand for in the context of oracle security?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Trustless Web API Protocol D) Two-Way Authentication Process
Answer: A – TWAP averages prices over time, making manipulation more expensive.

Q8. Which OpenZeppelin contract should be used to prevent reentrancy attacks?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier to prevent reentrant calls.

Q9. In the InsecureToken example, what is the issue with the mint function?
A) Integer overflow B) Missing access control C) Gas inefficiency D) Wrong data type
Answer: B – Anyone can call mint without onlyOwner modifier, allowing unlimited token creation.

Q10. What is SWC-107 in the Smart Contract Weakness Classification registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Quiz Questions (11–15)

Q11. Which of the following is NOT a required section in a professional audit report?
A) Severity classification B) Contract source code C) Impact description D) Fix recommendation
Answer: B – Reports reference code locations but don't include full source (available separately).

Q12. What is the primary advantage of Slither over Mythril in security audits?
A) More accurate results B) Faster execution C) Better documentation D) Lower cost
Answer: B – Slither's static analysis is much faster than Mythril's symbolic execution.

Q13. Why should selfdestruct functions be protected with access control?
A) High gas cost B) Irreversible contract destruction C) Network congestion D) Compiler warnings
Answer: B – Selfdestruct permanently removes contract code and sends funds; unrestricted access is critical.

Q14. What is the correct order in the Checks-Effects-Interactions pattern?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects
Answer: C – Validate inputs (Checks), update state (Effects), then make external calls (Interactions).

Q15. Which oracle solution provides decentralized, off-chain data feeds?
A) Uniswap TWAP B) Chainlink C) Balancer D) Aave
Answer: B – Chainlink aggregates data from multiple independent node operators.

Quiz Questions (16–20)

Q16. What is the purpose of writing exploit contracts during security audits?
A) Increase audit fees B) Prove vulnerability severity C) Test compiler D) Generate documentation
Answer: B – Exploit contracts demonstrate real attack scenarios, validating findings.

Q17. Which vulnerability does Solidity 0.8.0+ NOT automatically prevent?
A) Integer overflow B) Integer underflow C) Reentrancy D) Both A and B
Answer: C – Solidity 0.8.0+ checks arithmetic but doesn't prevent reentrancy (use ReentrancyGuard).

Q18. What is the first step in the security audit workflow?
A) Automated scanning B) Writing exploits C) Manual code review D) Report generation
Answer: C – Manual review identifies architecture issues and logic flaws automated tools miss.

Q19. In the BadOracle example, which fix provides the most robust price security?
A) Higher gas limit B) TWAP + Chainlink hybrid C) Faster transactions D) More tokens
Answer: B – Combining on-chain TWAP with off-chain Chainlink reduces single point of failure.

Q20. What severity level is typically assigned to missing access control on critical functions?
A) Low B) Medium C) High D) Informational
Answer: C – Unprotected critical functions (mint, destroy) are High severity, potentially Critical if exploitable.

Lab Session: Security Audit

BSc Blockchain, Crypto Economy & NFTs

Course Instructor

Module F: Advanced Topics

(c) Joerg Osterrieder 2025

Security Audit Lab in a Nutshell

- A checklist approach catches common vulnerabilities before they become headlines
- Systematic auditing combines manual review with automated tools for defense in depth

[COMIC: Security auditor with magnifying glass examining code, checklist in hand. Checklist shows: "Reentrancy? Access control? Oracle manipulation?" Red warning flags appear next to vulnerable code sections]

[PLACEHOLDER] — Before deployment: check twice, deploy once—there are no take-backs on mainnet

Learning Objectives

By the end of this lab session, you will be able to:

- Perform manual security code review
- Use automated tools (Slither, Mythril)
- Write exploit contracts demonstrating vulnerabilities
- Implement secure fixes using best practices
- Create professional audit reports

Building on L43: Smart Contract Security

The Problem: Smart Contract Security Vulnerabilities

The Challenge
Every deployed smart contract is permanently exposed on-chain. A single vulnerability can lead to millions in losses. How do we systematically identify and fix security flaws before attackers exploit them?

Why It Matters

- $3.8 billion lost to DeFi hacks in 2022 alone
- Ronin Bridge exploit: $625M stolen via access control flaw

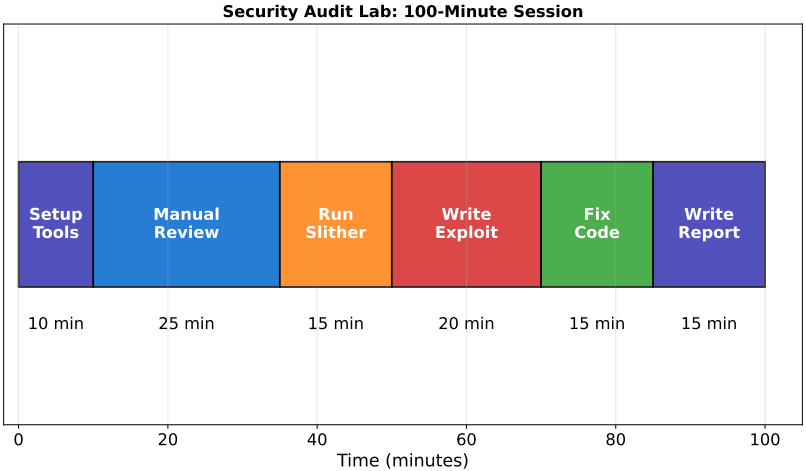
What You'll Explore

- Vulnerability identification through code review
- Automated security tools (Slither, Mythril)
- Attack vector analysis and exploit writing

The Cryptoeconomics Question
Security flaws create economic opportunities for attackers. How do we align incentives to reward discovery before exploitation?

Today's lesson: Hands-on security audit workflow from detection to remediation

How Does a Security Audit Work?



Complete security audit workflow from review to report

What Will You Audit Today?

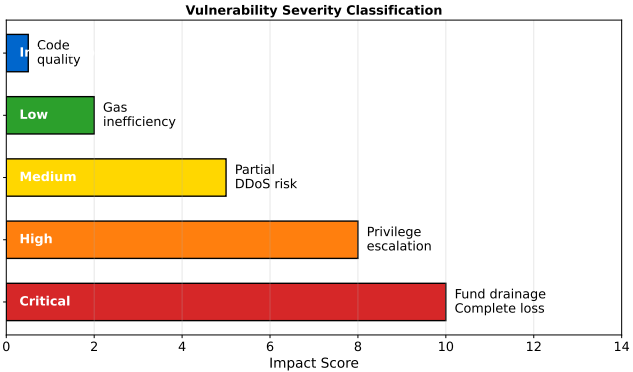
Contracts to Audit:

1. **VulnerableBank**: Reentrancy vulnerability
2. **InsecureToken**: Integer overflow, access control
3. **BadOracle**: Oracle manipulation

Deliverables:

- Audit report with severity classifications
- Exploit contracts demonstrating vulnerabilities
- Secure implementations with fixes

How Do You Classify Vulnerability Severity?



Critical and High severity issues require immediate fixes

Can You Spot the Reentrancy Bug?

Manual Review Tasks:

1. Read the withdraw function carefully
2. Identify external call before state update
3. Classify as Critical severity

Fix with Checks-Effects-Interactions:

- Update balance BEFORE external call
- Or use OpenZeppelin ReentrancyGuard

What's Wrong with This Token Contract?

Vulnerabilities to Find:

- Integer overflow (Solidity ¡ 0.8)
- Missing access control on mint
- Unprotected selfdestruct

Fix:

- Upgrade to Solidity 0.8.0+
- Add onlyOwner modifier
- Initialize owner in constructor

How Would You Exploit This Oracle?

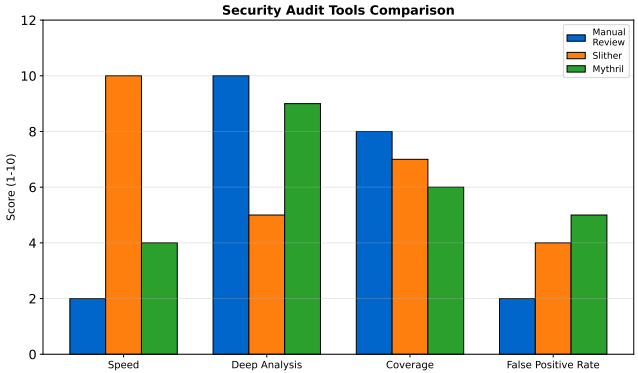
Vulnerability:

- Instant spot price from Uniswap
- Manipulable via flash loans

Secure Alternatives:

- Uniswap V2 TWAP oracle (time-weighted)
- Chainlink price feeds (decentralized oracle)
- Hybrid approach with multiple sources

How Do Audit Tools Compare?



Combine manual review with automated tools for best coverage

Which Tool Should You Use First?

Slither (Static Analysis):

- Fast pattern-based detection
- Run: `slither contracts/VulnerableBank.sol`

Mythril (Symbolic Execution):

- Deep path analysis
- Run: `myth analyze contracts/VulnerableBank.sol`

Key Detectors:

- SWC-107: Reentrancy
- SWC-101: Integer overflow
- SWC-105: Unprotected withdrawal

What Goes in an Audit Report?

For Each Finding:

1. **Title**: Descriptive vulnerability name
2. **Severity**: Critical / High / Medium / Low
3. **Location**: Contract, function, line numbers
4. **Description**: What is the vulnerability
5. **Impact**: What can attacker achieve
6. **Recommendation**: How to fix

What Should You Submit for This Lab?

Submit:

1. **Audit Report (PDF):**
   - Findings for all three contracts
   - Severity classifications
   - Fix recommendations with code
2. **Code Submissions:**
   - Exploit contracts (AttackBank.sol, etc.)
   - Secure implementations
   - Test suite proving fixes work

Problem Solved? Security Audit Effectiveness

The Original Problem

How do we systematically identify and prevent smart contract vulnerabilities before deployment?

How Security Audits Solve It

- Manual review catches logic flaws automated tools miss
- Combined tooling (Slither + Mythril) provides comprehensive coverage
- Bug bounties reward white-hat discovery over exploitation

Remaining Limitations

- Audits are snapshots - code changes post-audit reintroduce risk
- Zero-day vulnerabilities unknown to auditors and tools

The Economic Model

- **Cost:** Time investment ($50k-$300k per audit), requires deep expertise
- **Reward:** Prevents exploits worth millions, preserves protocol reputation
- **Risk:** False sense of security, missing subtle bugs, post-audit modifications

Security audits reduce but don't eliminate risk - ongoing monitoring and bug bounties essential

The Economics of Security Audit

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Security Audit

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Security Audit

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

How Do You Ensure Audit Effectiveness?

- Trust but verify: automated tools catch patterns, but manual review finds logic flaws
- Defense in depth means layering Slither + Mythril + manual audit + bug bounties + monitoring

[COMIC: Security auditor at desk with multiple layers of defense illustrated as shields. Motto banner reads: "Trust but Verify." Each shield labeled: Slither, Mythril, Manual Review, Bug Bounty, Forta Monitoring]

[PLACEHOLDER] — No single tool catches everything—security requires continuous vigilance, not one-time audits

Key Takeaways

- Security audit combines manual review and automated tools
- Reentrancy is critical - use Checks-Effects-Interactions
- Solidity 0.8.0+ provides built-in overflow protection
- Never trust spot prices - use TWAP or Chainlink
- Exploit writing proves vulnerability severity
- Professional reports follow structured template

Next Lesson: L45 – Global Regulation

Quiz Questions (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control issues
Answer: B – Update state (Effects) before external calls (Interactions) to prevent reentrant calls from exploiting stale state.

Q2. In the VulnerableBank example, what makes the withdraw function vulnerable?
A) Missing require check B) External call before balance update C) No access modifier D) Integer overflow
Answer: B – The contract sends ETH before updating the user's balance, allowing reentrancy.

Q3. Which Solidity version introduced built-in overflow/underflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow/underflow without SafeMath.

Q4. What severity classification should be assigned to a reentrancy vulnerability allowing fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Vulnerabilities enabling direct fund theft are classified as Critical severity.

Q5. Which tool uses symbolic execution for deep path analysis in smart contract audits?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril performs symbolic execution, while Slither uses fast static analysis.

Quiz Questions (6–10)

Q6. What is the main vulnerability when using Uniswap spot prices directly in smart contracts?
A) High gas costs B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction using flash loans.

Q7. What does TWAP stand for in the context of oracle security?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Trustless Web API Protocol D) Two-Way Authentication Process
Answer: A – TWAP averages prices over time, making manipulation more expensive.

Q8. Which OpenZeppelin contract should be used to prevent reentrancy attacks?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier to prevent reentrant calls.

Q9. In the InsecureToken example, what is the issue with the mint function?
A) Integer overflow B) Missing access control C) Gas inefficiency D) Wrong data type
Answer: B – Anyone can call mint without onlyOwner modifier, allowing unlimited token creation.

Q10. What is SWC-107 in the Smart Contract Weakness Classification registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Quiz Questions (11–15)

Q11. Which of the following is NOT a required section in a professional audit report?
A) Severity classification B) Contract source code C) Impact description D) Fix recommendation
Answer: B – Reports reference code locations but don't include full source (available separately).

Q12. What is the primary advantage of Slither over Mythril in security audits?
A) More accurate results B) Faster execution C) Better documentation D) Lower cost
Answer: B – Slither's static analysis is much faster than Mythril's symbolic execution.

Q13. Why should selfdestruct functions be protected with access control?
A) High gas cost B) Irreversible contract destruction C) Network congestion D) Compiler warnings
Answer: B – Selfdestruct permanently removes contract code and sends funds; unrestricted access is critical.

Q14. What is the correct order in the Checks-Effects-Interactions pattern?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects
Answer: C – Validate inputs (Checks), update state (Effects), then make external calls (Interactions).

Q15. Which oracle solution provides decentralized, off-chain data feeds?
A) Uniswap TWAP B) Chainlink C) Balancer D) Aave
Answer: B – Chainlink aggregates data from multiple independent node operators.

Quiz Questions (16–20)

Q16. What is the purpose of writing exploit contracts during security audits?
A) Increase audit fees B) Prove vulnerability severity C) Test compiler D) Generate documentation
Answer: B – Exploit contracts demonstrate real attack scenarios, validating findings.

Q17. Which vulnerability does Solidity 0.8.0+ NOT automatically prevent?
A) Integer overflow B) Integer underflow C) Reentrancy D) Both A and B
Answer: C – Solidity 0.8.0+ checks arithmetic but doesn't prevent reentrancy (use ReentrancyGuard).

Q18. What is the first step in the security audit workflow?
A) Automated scanning B) Writing exploits C) Manual code review D) Report generation
Answer: C – Manual review identifies architecture issues and logic flaws automated tools miss.

Q19. In the BadOracle example, which fix provides the most robust price security?
A) Higher gas limit B) TWAP + Chainlink hybrid C) Faster transactions D) More tokens
Answer: B – Combining on-chain TWAP with off-chain Chainlink reduces single point of failure.

Q20. What severity level is typically assigned to missing access control on critical functions?
A) Low B) Medium C) High D) Informational
Answer: C – Unprotected critical functions (mint, destroy) are High severity, potentially Critical if exploitable.

L44: Lab – Security Audit

Mini-Lecture – Module F: Advanced Topics

Blockchain & Cryptocurrency Course

January 2026

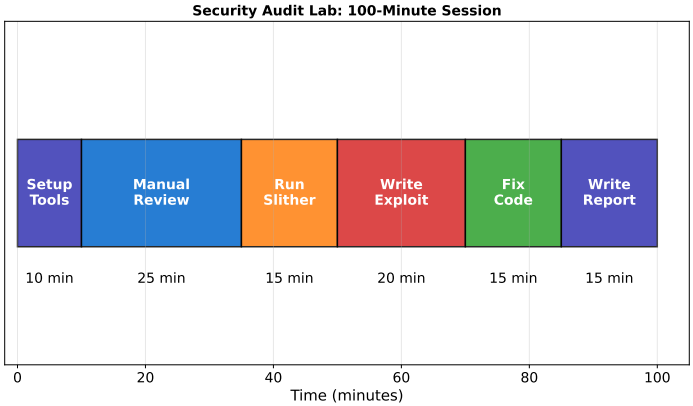
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

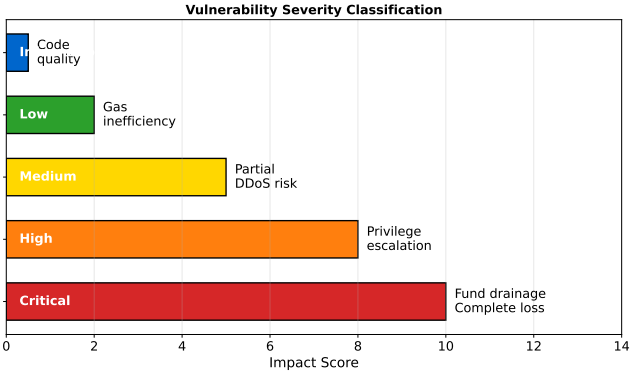
- Perform manual security code review
- Use automated tools (Slither, Mythril)
- Write exploit contracts to demonstrate vulnerabilities
- Create professional audit reports with severity classifications

Security Audit Workflow



Complete workflow: Manual review → Automated scan → Exploit → Fix → Report.

Vulnerability Severity Classification



Critical/High require immediate fixes; **Medium/Low** scheduled remediation.

Lab Exercises: Three Vulnerable Contracts

VulnerableBank (Reentrancy):

- External call before state update
- Fix: Checks-Effects-Interactions pattern

InsecureToken (Multiple Issues):

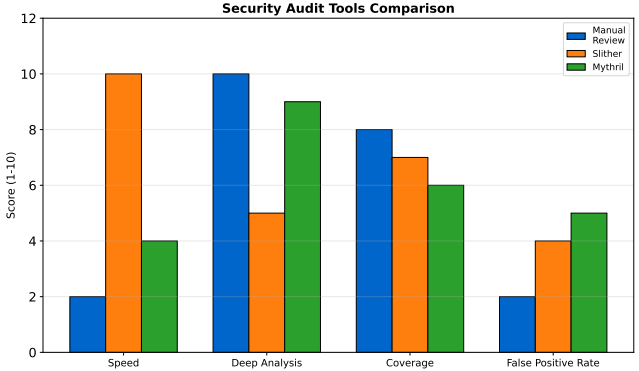
- Integer overflow, missing access control
- Fix: Solidity 0.8.0+, onlyOwner modifier

BadOracle (Price Manipulation):

- Spot price vulnerable to flash loans
- Fix: TWAP or Chainlink price feeds

(c) Joerg Osterrieder 2025

Audit Tools Comparison



Best practice: Combine manual review with multiple automated tools.

Automated Analysis Commands

Slither (Static Analysis):

- Fast pattern-based detection
- `slither contracts/VulnerableBank.sol`

Mythril (Symbolic Execution):

- Deep path analysis, slower but thorough
- `myth analyze contracts/VulnerableBank.sol`

Key SWC IDs: SWC-107 (Reentrancy), SWC-101 (Overflow), SWC-105 (Unprotected withdrawal).

Audit Report Structure

For Each Finding:

1. **Title:** Descriptive vulnerability name
2. **Severity:** Critical / High / Medium / Low
3. **Location:** Contract, function, line numbers
4. **Description:** What is the vulnerability
5. **Impact:** What attacker can achieve
6. **Recommendation:** How to fix with code

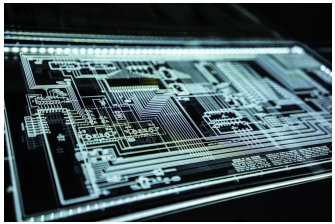
Deliverables: Audit report (PDF) + Exploit contracts + Secure implementations.

Key Takeaways

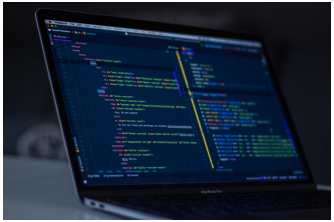
1. **Manual First:** Manual review catches logic flaws automated tools miss
2. **CEI Pattern:** Checks-Effects-Interactions prevents reentrancy
3. **Solidity 0.8.0+:** Built-in overflow protection (no SafeMath needed)
4. **Oracle Security:** Never use spot prices; use TWAP or Chainlink
5. **Exploit Contracts:** Prove severity by demonstrating real attacks

End of Module F. Next: Module G – Regulation & Future

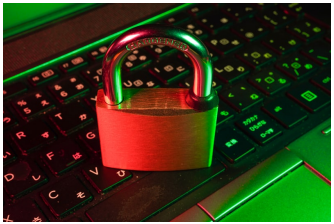
Security Audit in Practice



Security Shield



Code Audit



Protection

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What pattern prevents reentrancy attacks?
A) Factory pattern B) Checks-Effects-Interactions C) Singleton D) Observer

Quiz (1/2)

Q1. What pattern prevents reentrancy attacks?
A) Factory pattern B) Checks-Effects-Interactions C) Singleton D) Observer
Answer: B – Update state before external calls.

Q2. Which Solidity version has built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0+ D) 0.5.0

Quiz (1/2)

Q1. What pattern prevents reentrancy attacks?
A) Factory pattern B) Checks-Effects-Interactions C) Singleton D) Observer
Answer: B – Update state before external calls.

Q2. Which Solidity version has built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0+ D) 0.5.0
Answer: C – Solidity 0.8.0+ automatically reverts on overflow.

Q3. What severity for reentrancy allowing fund theft?
A) Low B) Medium C) High D) Critical

Quiz (1/2)

Q1. What pattern prevents reentrancy attacks?
A) Factory pattern B) Checks-Effects-Interactions C) Singleton D) Observer
Answer: B – Update state before external calls.

Q2. Which Solidity version has built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0+ D) 0.5.0
Answer: C – Solidity 0.8.0+ automatically reverts on overflow.

Q3. What severity for reentrancy allowing fund theft?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft is Critical severity.

Q4. Which tool uses symbolic execution?
A) Slither B) Mythril C) Hardhat D) Truffle

Quiz (1/2)

Q1. What pattern prevents reentrancy attacks?
A) Factory pattern B) Checks-Effects-Interactions C) Singleton D) Observer
Answer: B – Update state before external calls.

Q2. Which Solidity version has built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0+ D) 0.5.0
Answer: C – Solidity 0.8.0+ automatically reverts on overflow.

Q3. What severity for reentrancy allowing fund theft?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft is Critical severity.

Q4. Which tool uses symbolic execution?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril does deep path analysis via symbolic execution.

Q5. What is SWC-107?
A) Integer overflow B) Reentrancy C) Access control D) DoS

Quiz (1/2)

Q1. What pattern prevents reentrancy attacks?
A) Factory pattern B) Checks-Effects-Interactions C) Singleton D) Observer
Answer: B – Update state before external calls.

Q2. Which Solidity version has built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0+ D) 0.5.0
Answer: C – Solidity 0.8.0+ automatically reverts on overflow.

Q3. What severity for reentrancy allowing fund theft?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft is Critical severity.

Q4. Which tool uses symbolic execution?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril does deep path analysis via symbolic execution.

Q5. What is SWC-107?
A) Integer overflow B) Reentrancy C) Access control D) DoS
Answer: B – SWC-107 is the reentrancy weakness classification.

Quiz (2/2)

Q6. Why are spot prices dangerous in smart contracts?
A) High gas B) Flash loan manipulation C) Slow D) Fees

Quiz (2/2)

Q6. Why are spot prices dangerous in smart contracts?
A) High gas B) Flash loan manipulation C) Slow D) Fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. What does TWAP stand for?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Two-Way Auth D) Token Wallet

Quiz (2/2)

Q6. Why are spot prices dangerous in smart contracts?
A) High gas B) Flash loan manipulation C) Slow D) Fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. What does TWAP stand for?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Two-Way Auth D) Token Wallet
Answer: A – TWAP averages prices over time, resisting manipulation.

Q8. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl

Quiz (2/2)

Q6. Why are spot prices dangerous in smart contracts?
A) High gas B) Flash loan manipulation C) Slow D) Fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. What does TWAP stand for?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Two-Way Auth D) Token Wallet
Answer: A – TWAP averages prices over time, resisting manipulation.

Q8. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides nonReentrant modifier.

Q9. First step in security audit workflow?
A) Automated scan B) Exploit writing C) Manual code review D) Report

Quiz (2/2)

Q6. Why are spot prices dangerous in smart contracts?
A) High gas B) Flash loan manipulation C) Slow D) Fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. What does TWAP stand for?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Two-Way Auth D) Token Wallet
Answer: A – TWAP averages prices over time, resisting manipulation.

Q8. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides nonReentrant modifier.

Q9. First step in security audit workflow?
A) Automated scan B) Exploit writing C) Manual code review D) Report
Answer: C – Manual review identifies logic flaws tools miss.

Q10. Why write exploit contracts during audits?
A) Increase fees B) Prove vulnerability severity C) Test compiler D) Generate docs

Quiz (2/2)

Q6. Why are spot prices dangerous in smart contracts?
A) High gas B) Flash loan manipulation C) Slow D) Fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. What does TWAP stand for?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Two-Way Auth D) Token Wallet
Answer: A – TWAP averages prices over time, resisting manipulation.

Q8. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides nonReentrant modifier.

Q9. First step in security audit workflow?
A) Automated scan B) Exploit writing C) Manual code review D) Report
Answer: C – Manual review identifies logic flaws tools miss.

Q10. Why write exploit contracts during audits?
A) Increase fees B) Prove vulnerability severity C) Test compiler D) Generate docs
Answer: B – Exploits demonstrate real attack scenarios.

Thank you

Questions?

Next: Module G – Regulation & Future

Quiz: Lab Security Audit

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft vulnerabilities are Critical severity.

Q4. Which tool uses symbolic execution for deep analysis?
A) Slither B) Mythril C) Hardhat D) Truffle

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft vulnerabilities are Critical severity.

Q4. Which tool uses symbolic execution for deep analysis?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril explores execution paths; Slither uses fast static analysis.

Q5. What does TWAP stand for in oracle security?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Trustless Web API D) Two-Way Auth

Quiz (1–5)

Q1. What is the Checks-Effects-Interactions pattern designed to prevent?
A) Integer overflow B) Reentrancy attacks C) Oracle manipulation D) Access control
Answer: B – Update state before external calls to prevent reentrant exploitation.

Q2. Which Solidity version introduced built-in overflow protection?
A) 0.6.0 B) 0.7.0 C) 0.8.0 D) 0.9.0
Answer: C – Solidity 0.8.0+ automatically reverts on arithmetic overflow.

Q3. What severity is assigned to reentrancy enabling fund drainage?
A) Low B) Medium C) High D) Critical
Answer: D – Direct fund theft vulnerabilities are Critical severity.

Q4. Which tool uses symbolic execution for deep analysis?
A) Slither B) Mythril C) Hardhat D) Truffle
Answer: B – Mythril explores execution paths; Slither uses fast static analysis.

Q5. What does TWAP stand for in oracle security?
A) Time-Weighted Average Price B) Total Weighted Asset Pool C) Trustless Web API D) Two-Way Auth
Answer: A – TWAP averages prices over time to resist manipulation.

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Q9. What is the correct order in Checks-Effects-Interactions?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Q9. What is the correct order in Checks-Effects-Interactions?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects
Answer: C – Validate, update state, then make external calls.

Q10. Why write exploit contracts during audits?
A) Increase fees B) Prove vulnerability severity C) Test compiler D) Generate docs

Quiz (6–10)

Q6. What is the main risk of using Uniswap spot prices?
A) High gas B) Flash loan manipulation C) Slow execution D) Protocol fees
Answer: B – Spot prices can be manipulated within a single transaction.

Q7. Which OpenZeppelin contract prevents reentrancy?
A) Ownable B) Pausable C) ReentrancyGuard D) AccessControl
Answer: C – ReentrancyGuard provides the nonReentrant modifier.

Q8. What is SWC-107 in the weakness registry?
A) Integer overflow B) Reentrancy C) Access control D) Denial of service
Answer: B – SWC-107 specifically identifies reentrancy vulnerabilities.

Q9. What is the correct order in Checks-Effects-Interactions?
A) Effects, Checks, Interactions B) Interactions, Effects, Checks C) Checks, Effects, Interactions D) Checks, Interactions, Effects
Answer: C – Validate, update state, then make external calls.

Q10. Why write exploit contracts during audits?
A) Increase fees B) Prove vulnerability severity C) Test compiler D) Generate docs
Answer: B – Exploit PoCs demonstrate real attack scenarios.

L45: Global Regulatory Landscape

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand why governments regulate cryptocurrencies
- Compare regulatory approaches across major jurisdictions
- Analyze the US fragmented regulatory landscape
- Evaluate EU MiCA as comprehensive framework
- Assess enforcement actions and their impact
- Understand the significance of Bitcoin ETF approval

The Problem: How should governments regulate crypto?

Part 1/4: Global Regulation (Fundamentals)

The Challenge

Without regulation, crypto markets face fraud, money laundering, and systemic risks that erode trust. With regulation, innovation may be stifled by unclear rules and jurisdictional fragmentation. Finding the optimal balance is critical.

Why It Matters

- Regulatory clarity unlocks institutional capital and mainstream adoption
- Fragmentation creates arbitrage opportunities and regulatory evasion
- Overregulation drives innovation offshore; underregulation enables fraud

What We Need

- Risk management and mitigation
- Clear token taxonomies distinguishing securities, commodities, and payment tokens
- Consumer protections without banning permissionless innovation

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How Global Regulation addresses this challenge

Why Regulate Cryptocurrencies?

Regulatory Concerns

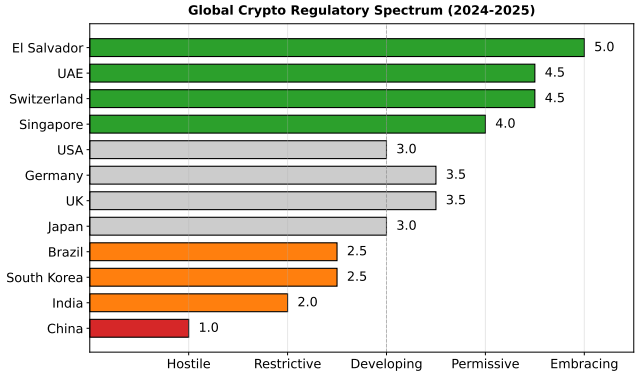
- **Money Laundering**: Anonymous transactions facilitate illicit finance
- **Consumer Protection**: Scams, rug pulls, exchange failures
- **Market Manipulation**: Pump-and-dump, wash trading
- **Tax Evasion**: Unreported capital gains
- **Systemic Risk**: Contagion to traditional finance

Industry Arguments

- **Legitimacy**: Legal certainty attracts institutional capital
- **Innovation**: Clear rules enable compliant products
- **Consumer Trust**: Regulated exchanges reduce fraud
- **Financial Inclusion**: Regulated stablecoins for payments

Core Tension: Innovation vs consumer protection vs financial stability

Global Regulatory Spectrum



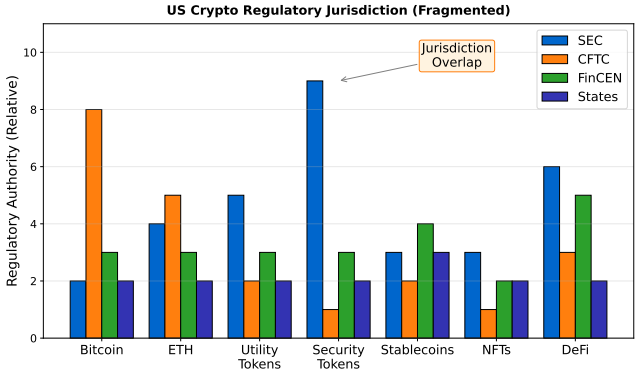
Most jurisdictions moving from restrictive toward regulated permissiveness

The Regulatory Spectrum

Hostile	Restrictive	Permissive
China (2021 ban)	India (30% tax)	Switzerland (clear framework)
Algeria, Bangladesh	South Korea (strict KYC)	Singapore (licensing)
Nepal, Morocco	Brazil (no DeFi clarity)	UAE (crypto-friendly zones)
	Russia (payment ban)	Portugal (tax-friendly)
	Turkey (payment ban)	El Salvador (legal tender)

Trend: Convergence toward licensing regimes with consumer protections

United States: Fragmented Jurisdiction



Multiple agencies with overlapping and unclear jurisdiction

US Regulatory Agencies

- **No Unified Framework**: Multiple agencies with overlapping jurisdiction
- **Key Regulators**:
  - **SEC**: Securities regulation (most tokens per Howey Test)
  - **CFTC**: Commodities (Bitcoin, ETH, derivatives)
  - **FinCEN**: AML/CTF enforcement
  - **OCC**: Banking charters for crypto custody
  - **IRS**: Tax treatment (crypto = property)
  - **State regulators**: Money transmitter licenses (NY BitLicense)
- **Result**: Regulation by enforcement, legal uncertainty

SEC vs CFTC: Jurisdiction Battle

SEC Position

- Most tokens are **securities**
- ICOs = unregistered offerings
- Exchanges must register

Howey Test:

1. Investment of money
2. Common enterprise
3. Expectation of profits
4. From efforts of others

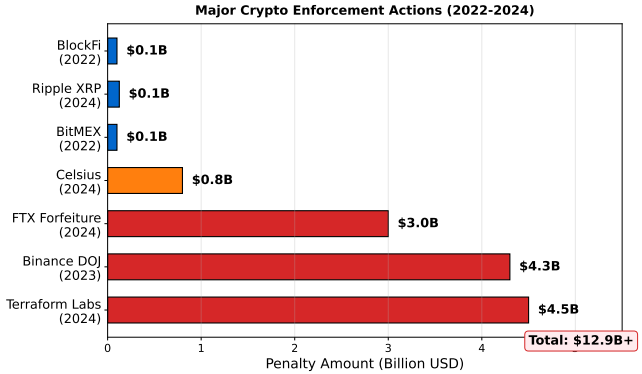
CFTC Position

- BTC and ETH are **commodities**
- Jurisdiction over derivatives
- Lighter regulatory approach

Congressional Debate:

- Multiple bills (FIT21, DCCPA)
- Goal: Clarify jurisdiction
- Status: Stalled until 2025

Major Enforcement Actions



Regulation by enforcement creates legal uncertainty for industry

Notable Enforcement Cases

- **Ripple Labs (2020-2024)**: SEC sued for $1.3B unregistered XRP sales
  - Result: Institutional sales = securities, retail sales = not securities
  - Final penalty: $125M (reduced from $2B SEC request)
- **Binance (2023)**: $4.3B DOJ settlement, CZ resigned and served prison time
- **Terraform Labs (2024)**: $4.5B penalty for UST/LUNA fraud
- **FTX (2022-2024)**: Criminal fraud charges, SBF convicted
- **Pattern**: Enforcement first, rulemaking later

European Union: MiCA Regulation

Overview:

- Comprehensive EU framework
- Approved 2023, full Dec 2024
- 27 EU countries, single regime

Scope:

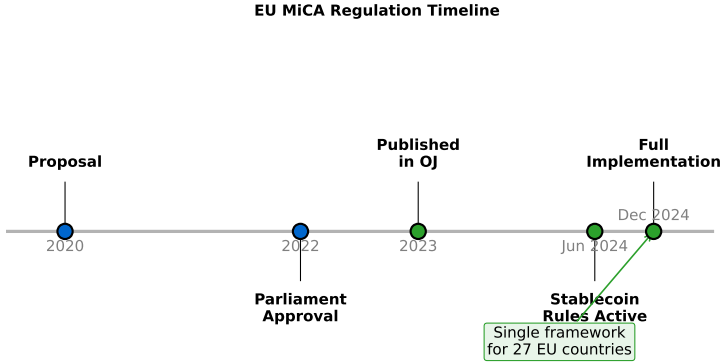
- CASPs (service providers)
- Stablecoin issuers
- NFTs excluded (unless fungible)

Key Requirements:

- CASP authorization + capital
- Market abuse prohibitions
- Consumer protection rules
- Stablecoin reserves

(c) Joerg Osterrieder 2025

MiCA Implementation Timeline

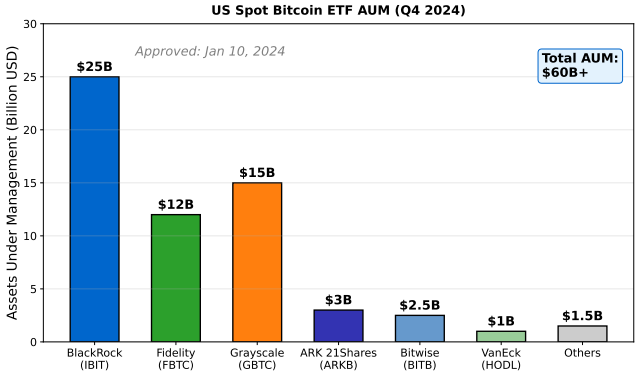


First comprehensive crypto regulation covering entire trading bloc

MiCA: Stablecoin Provisions

- **E-Money Tokens (EMTs)**: Pegged to single fiat (USDC, USDT)
  - Issuers must be credit/e-money institutions
  - 1:1 reserve backing in segregated accounts
  - Redemption at par value anytime
- **Asset-Referenced Tokens (ARTs)**: Basket or non-fiat pegged
  - Stricter capital and governance requirements
- **Significant Tokens**: Enhanced EBA oversight
- **Algorithmic Stablecoins**: Effectively banned (post-Terra)
- **Practical Impact**: USDT delisted by major exchanges (Coinbase, Binance) in EU; Circle (USDC) MiCA-compliant (EMI license July 2024)

2024 Milestone: Bitcoin ETF Approval



SEC approved 11 spot Bitcoin ETFs on January 10, 2024

Bitcoin ETF: Regulatory Significance

- **January 10, 2024**: SEC approves 11 spot Bitcoin ETFs
  - First spot Bitcoin ETFs in US history (after decade of rejections)
  - Issuers: BlackRock (IBIT), Fidelity (FBTC), Grayscale (GBTC)
- **Impact**:
  - $49B total inflows in 2024 (IBIT: $37B, FBTC: $12B)
  - Institutional access via traditional brokerage accounts
  - Bitcoin legitimized as investable asset class
  - BTC reached new ATH ¿$100k (December 2024)
- **July 2024**: SEC approves spot Ethereum ETFs
- **Significance**: Major shift from SEC's hostile stance

Asia-Pacific: Diverse Approaches

- **Singapore (MAS)**:
  - Payment Services Act licensing
  - Strict AML/CFT, retail protections
- **Hong Kong (SFC)**:
  - Mandatory licensing (2023)
  - Positioning as Asian crypto hub post-China ban
- **Japan (FSA)**:
  - Early framework (2017), strict custody standards
- **China**: Complete ban (2021) - transactions, mining, exchanges
  - Rationale: Capital controls, CBDC strategy
  - Result: Mining exodus to US, Kazakhstan, Russia

Switzerland: Crypto Nation

- **Crypto Valley (Zug)**: Global blockchain hub
- **Legal Framework**:
  - DLT Act (2021): Tailored regulation for digital assets
  - Token classification: Payment, Utility, Asset tokens
  - Securities law applies to asset tokens only
- **FINMA Guidance**:
  - Clear licensing categories
  - AML/CFT compliance for exchanges
  - No blanket prohibition on specific activities
- **Advantages**: Regulatory clarity, innovation-friendly, strong rule of law

(c) Joerg Osterrieder 2025

AML/CFT: The Travel Rule

- **FATF Recommendation 16**: Apply to Virtual Asset Service Providers
- **Requirements**:
  - Collect/transmit customer info for transactions ¿$1,000
  - Originator and beneficiary details
- **Implementation**:
  - Centralized exchanges: Implemented (Coinbase, Kraken)
  - Cross-border: Technical solutions (TRP, TRUST, Notabene)
  - Self-hosted wallets: Controversial (EU proposed restrictions)
- **Challenge**: DeFi has no intermediary to enforce rules
- **Tension**: KYC requirements conflict with crypto privacy ethos

DeFi: The Regulatory Challenge

- **Problem**: Traditional regulation assumes intermediaries
- **DeFi Reality**: Smart contracts, no central operator
- **Key Questions**:
  - Who is liable for smart contract exploits?
  - How to enforce AML without custodian?
  - Are DeFi protocols securities or commodities?
- **Enforcement Actions**:
  - Tornado Cash (2022): Treasury sanctioned mixer protocol
  - Uniswap Labs: SEC Wells Notice
  - Ooki DAO (2022): CFTC sued DAO as legal entity
- **Debate**: Code is speech vs code is conduct

2025 US Political Shift

- **2024 Election Impact**:
  - Crypto PACs spent $100M+ on elections
  - Pro-crypto candidates elected to Congress
- **New Administration (2025)**:
  - Promise to make US "crypto capital of the world"
  - SEC Chair Gensler resigned
  - Strategic Bitcoin Reserve proposal discussed
- **Legislative Outlook**:
  - FIT21 (Financial Innovation and Technology Act) revival
  - Stablecoin legislation priority
  - CFTC vs SEC jurisdiction clarity expected
- **Shift**: From enforcement to rulemaking approach

Regulatory Outlook: Future Directions

- **Trend 1: Convergence**: Countries adopting similar frameworks (MiCA template)
- **Trend 2: Stablecoin Focus**: Banking-like regulation for systemic stablecoins
- **Trend 3: DeFi Reckoning**: Regulatory clarity (or crackdown) coming
- **Trend 4: CBDC Competition**: Central banks competing with private stablecoins
- **Trend 5: Global Coordination**: FATF, FSB harmonizing standards
- **Trend 6: Licensing Regimes**: Most jurisdictions requiring VASP licenses

- **Uncertainty Remains**: Technology evolves faster than regulation

Problem Solved? Global Regulation

The Original Problem

How should governments regulate crypto?

How Global Regulation Solves It

- **Regulatory sandboxes**: Allow controlled experimentation (Singapore MAS, UK FCA)
- **Clear taxonomies**: Distinguish security vs utility vs payment tokens (Switzerland DLT Act, MiCA)
- **Risk-based frameworks**: Proportional rules based on systemic significance (MiCA stablecoin tiers)

Remaining Limitations

- **Jurisdictional arbitrage**: Projects relocate to friendly jurisdictions (US to Switzerland/UAE)
- **Enforcement challenges**: DeFi protocols have no legal entity; sanctions bypass (Tornado Cash forks)
- **Regulatory capture risk**: Industry lobbying shapes rules (crypto PACs $100M+ in 2024 elections)

Open Questions

- Will global harmonization emerge, or persist as fragmented patchwork?
- Risk: Black swan events, cascading failures (Terra/Luna, FTX)

Global Regulation partially solves "governments regulate crypto" but introduces new trade-offs

(c) Joerg Osterrieder 2025

Summary

Key Takeaways:

- **Global landscape**: Highly fragmented, evolving rapidly
- **US**: Fragmented (SEC vs CFTC), regulation by enforcement
- **EU**: Comprehensive MiCA framework, December 2024 full implementation
- **Asia**: Diverse (Singapore/HK permissive, China ban, Japan conservative)
- **Switzerland**: Clear framework, crypto-friendly (Crypto Valley)
- **Bitcoin ETF (Jan 2024)**: Major legitimization milestone
- **Enforcement**: $13B+ in penalties (2022-2024)
- **Trend**: Convergence toward licensing with consumer protections

Questions for Reflection

1. How does regulatory fragmentation affect crypto innovation in the US?
2. Why did the EU choose comprehensive legislation (MiCA) vs enforcement?
3. What are the trade-offs of China's complete ban approach?
4. Should DeFi protocols be regulated like traditional financial services?
5. How significant is the Bitcoin ETF approval for mainstream adoption?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code
Answer: C – The Howey Test (investment of money + common enterprise + expectation of profits from others' efforts) determines if a token is a security under SEC jurisdiction.

Q3. Which US regulatory agency has jurisdiction over Bitcoin and Ethereum as commodities?
A) Securities and Exchange Commission (SEC) B) Commodity Futures Trading Commission (CFTC)
C) Financial Crimes Enforcement Network (FinCEN) D) Internal Revenue Service (IRS)
Answer: B – CFTC has jurisdiction over Bitcoin and Ethereum as commodities, while SEC claims most other tokens are securities.

Q4. What was the total penalty amount in the Binance enforcement settlement in 2023?
A) $1.3 billion B) $2.5 billion C) $4.3 billion D) $4.5 billion
Answer: C – Binance paid $4.3B to DOJ in 2023, with CEO CZ resigning and serving prison time.

Q5. When did the SEC approve the first spot Bitcoin ETFs in US history?
A) November 2023 B) January 10, 2024
C) March 2024 D) July 2024
Answer: B – SEC approved 11 spot Bitcoin ETFs on January 10, 2024, ending a decade of rejections.

Quiz Questions (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money
Answer: C – EMTs are stablecoins pegged 1:1 to a single fiat currency (like USDC, USDT), requiring full reserve backing.

Q8. Which stablecoin was delisted by major EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT (Tether) D) BUSD (deprecated)
Answer: C – USDT was delisted by Coinbase and Binance in EU due to MiCA non-compliance; Circle's USDC obtained EMI license in July 2024.

Q9. How much total inflow did Bitcoin ETFs receive in 2024?
A) $25 billion B) $37 billion C) $49 billion D) $62 billion
Answer: C – Bitcoin ETFs received $49B total inflows in 2024 (IBIT: $37B, FBTC: $12B).

Q10. Which country implemented a complete ban on crypto transactions, mining, and exchanges in 2021?
A) India B) Russia C) China D) Turkey
Answer: C – China implemented a complete ban in 2021 to maintain capital controls and support CBDC strategy, causing mining exodus.

Quiz Questions (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities
Answer: A – The court ruled institutional sales were securities (Howey Test met) but retail sales on exchanges were not.

Q13. What was the final penalty amount for Ripple Labs after SEC litigation?
A) $50 million B) $125 million C) $1.3 billion D) $2 billion
Answer: B – Ripple was fined $125M, significantly reduced from the SEC's $2B request.

Q14. Which Swiss city is known as "Crypto Valley" and serves as a global blockchain hub?
A) Zurich B) Geneva C) Zug D) Basel
Answer: C – Zug is known as Crypto Valley, offering clear regulatory framework via DLT Act (2021) and FINMA guidance.

Q15. What regulatory challenge does DeFi pose that traditional finance regulation assumes?
A) Too much transparency B) High transaction fees
C) Existence of intermediaries D) Slow settlement times
Answer: C – Traditional regulation assumes intermediaries; DeFi operates via smart contracts with no central operator to enforce rules.

Quiz Questions (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024
Answer: D – MiCA was approved in 2023 but achieved full implementation in December 2024.

Q18. What is the SEC Chair Gary Gensler's status as of 2025?
A) Reappointed for second term B) Resigned following 2024 election
C) Promoted to Treasury Secretary D) Still serving as SEC Chair
Answer: B – Gensler resigned after the 2024 election, signaling a shift from enforcement to potential rulemaking approach.

Q19. Which regulatory trend involves countries adopting similar frameworks to MiCA?
A) Fragmentation B) Convergence C) Decentralization D) Liberalization
Answer: B – Convergence describes the trend of countries adopting similar comprehensive frameworks, often using MiCA as a template.

Q20. What was the total amount of enforcement penalties levied from 2022-2024?
A) $5 billion B) $8 billion C) $13+ billion D) $20 billion
Answer: C – Over $13B in penalties were levied (2022-2024), including Binance $4.3B, Terraform Labs $4.5B, and others.

L45: Global Regulatory Landscape

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Global Regulation in a Nutshell

- Why do crypto companies incorporate in the Cayman Islands, Dubai, or Switzerland?
- The global race: Some countries compete for blockchain talent while others ban it outright

[COMIC: "Jurisdiction shopping" – A crypto founder stands at a crossroads with signs pointing to different countries: "Cayman Islands: No questions asked", "Switzerland: Clear rules", "USA: Lawyers required", "China: Do not enter". The founder has a suitcase labeled "Token Inc."]

[PLACEHOLDER] — The fragmented regulatory landscape creates incentives for jurisdiction shopping

Learning Objectives

- Understand why governments regulate cryptocurrencies
- Compare regulatory approaches across major jurisdictions
- Analyze the US fragmented regulatory landscape
- Evaluate EU MiCA as comprehensive framework
- Assess enforcement actions and their impact
- Understand the significance of Bitcoin ETF approval

Building on L44: Lab: Security Audit

The Problem: How should governments regulate crypto?

Part 1/4: Global Regulation (Fundamentals)

The Challenge

Without regulation, crypto markets face fraud, money laundering, and systemic risks that erode trust. With regulation, innovation may be stifled by unclear rules and jurisdictional fragmentation. Finding the optimal balance is critical.

Why It Matters

- Regulatory clarity unlocks institutional capital and mainstream adoption
- Fragmentation creates arbitrage opportunities and regulatory evasion
- Overregulation drives innovation offshore; underregulation enables fraud

What We Need

- Risk management and mitigation
- Clear token taxonomies distinguishing securities, commodities, and payment tokens
- Consumer protections without banning permissionless innovation

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How Global Regulation addresses this challenge

Why Do Governments Want to Regulate Cryptocurrencies?

Regulatory Concerns

- **Money Laundering**: Anonymous transactions facilitate illicit finance
- **Consumer Protection**: Scams, rug pulls, exchange failures
- **Market Manipulation**: Pump-and-dump, wash trading
- **Tax Evasion**: Unreported capital gains
- **Systemic Risk**: Contagion to traditional finance

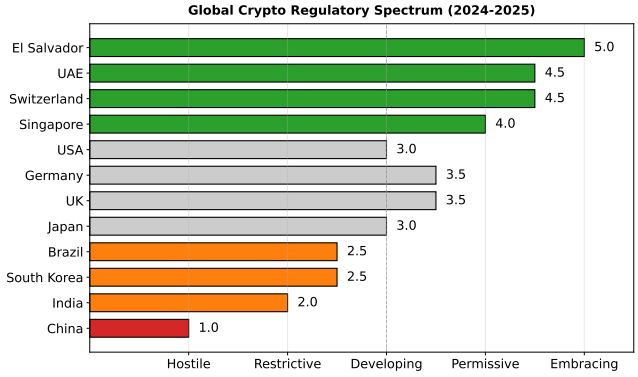
Industry Arguments

- **Legitimacy**: Legal certainty attracts institutional capital
- **Innovation**: Clear rules enable compliant products
- **Consumer Trust**: Regulated exchanges reduce fraud
- **Financial Inclusion**: Regulated stablecoins for payments

Core Tension: Innovation vs consumer protection vs financial stability

→ Problem: How should governments regulate crypto? — Why Regulate Cryptocurrencies? Both concerns and arguments reflect the core tension: unregulated crypto enables crime but also financial innovation

Global Regulatory Spectrum



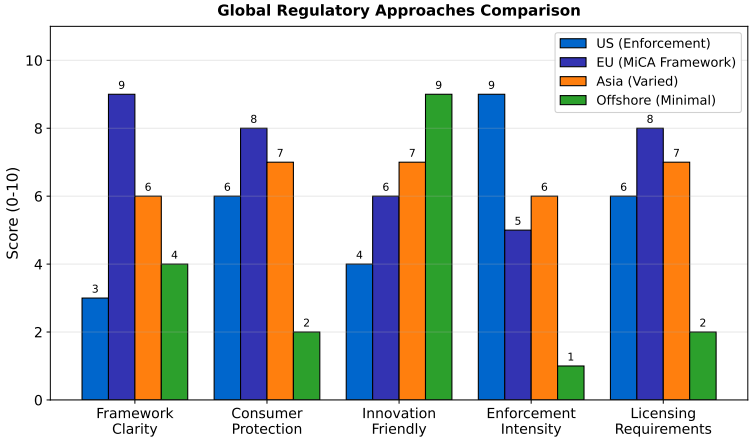
Most jurisdictions moving from restrictive toward regulated permissiveness

How Do Countries Differ in Crypto Regulation?

Hostile	Restrictive	Permissive
China (2021 ban)	India (30% tax)	Switzerland (clear framework)
Algeria, Bangladesh	South Korea (strict KYC)	Singapore (licensing)
Nepal, Morocco	Brazil (no DeFi clarity)	UAE (crypto-friendly zones)
	Russia (payment ban)	Portugal (tax-friendly)
	Turkey (payment ban)	El Salvador (legal tender)

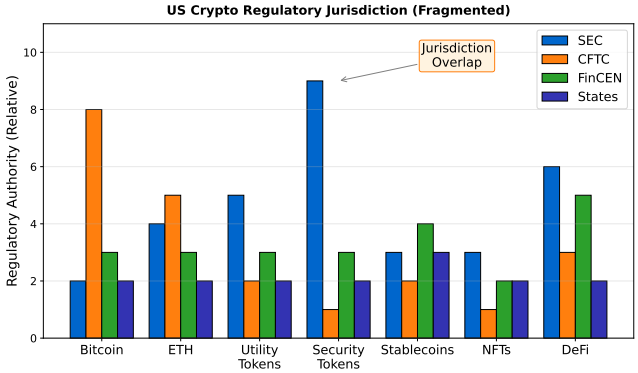
Trend: Convergence toward licensing regimes with consumer protections

Regulatory Approaches by Region



US prioritizes enforcement; EU provides frameworks; Offshore minimizes requirements

United States: Fragmented Jurisdiction



Multiple agencies with overlapping and unclear jurisdiction

Which US Agencies Regulate Crypto?

- **No Unified Framework**: Multiple agencies with overlapping jurisdiction
- **Key Regulators**:
  - **SEC**: Securities regulation (most tokens per Howey Test—a 1946 US Supreme Court test determining if something is a security: investment of money in a common enterprise with expectation of profits from others' efforts)
  - **CFTC**: Commodities (Bitcoin, ETH, derivatives)
  - **FinCEN**: AML/CTF enforcement
  - **OCC**: Banking charters for crypto custody
  - **IRS**: Tax treatment (crypto = property)
  - **State regulators**: Money transmitter licenses (NY BitLicense)
- **Result**: Regulation by enforcement, legal uncertainty

→ *Problem: How should governments regulate crypto? — US Regulatory Agencies Fragmented jurisdiction creates legal uncertainty, driving projects offshore and hindering legitimate innovation*

Who Has Jurisdiction: SEC or CFTC?

SEC Position

- Most tokens are **securities**
- ICOs = unregistered offerings
- Exchanges must register

Howey Test:

1. Investment of money
2. Common enterprise
3. Expectation of profits
4. From efforts of others

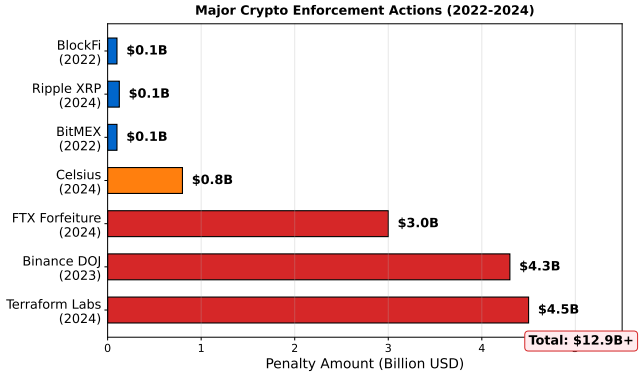
CFTC Position

- BTC and ETH are **commodities**
- Jurisdiction over derivatives
- Lighter regulatory approach

Congressional Debate:

- Multiple bills (FIT21, DCCPA)
- Goal: Clarify jurisdiction
- Status: Stalled until 2025

Major Enforcement Actions



Regulation by enforcement creates legal uncertainty for industry

What Were the Major Enforcement Actions?

- **Ripple Labs (2020-2024)**: SEC sued for $1.3B unregistered XRP sales
  - Result: Institutional sales = securities, retail sales = not securities
  - Final penalty: $125M (reduced from $2B SEC request)
- **Binance (2023)**: $4.3B DOJ settlement, CZ resigned and served prison time
- **Terraform Labs (2024)**: $4.5B penalty for UST/LUNA fraud
- **FTX (2022-2024)**: Criminal fraud charges, SBF convicted
- **Pattern**: Enforcement first, rulemaking later

What is the EU's MiCA Framework?

Overview:

- Comprehensive EU framework
- Approved 2023, full Dec 2024
- 27 EU countries, single regime

Scope:

- CASPs (Crypto Asset Service Providers—exchanges, custodians, and brokers)
- Stablecoin issuers
- NFTs excluded (unless fungible)

Key Requirements:

- CASP authorization + capital
- Market abuse prohibitions
- Consumer protection rules
- Stablecoin reserves

(c) Joerg Osterrieder 2025

Problem Check-In: Global Regulation

Recall Our Problem

How should governments regulate crypto?

What We've Learned So Far

- Regulatory spectrum from hostile (China ban) to permissive (Switzerland), with most jurisdictions converging toward licensing regimes
- US fragmentation: SEC (securities), CFTC (commodities), FinCEN (AML) with overlapping jurisdiction and enforcement-first approach
- No unified framework means companies face regulatory arbitrage incentives and legal uncertainty that stifles compliant innovation

Still to Address

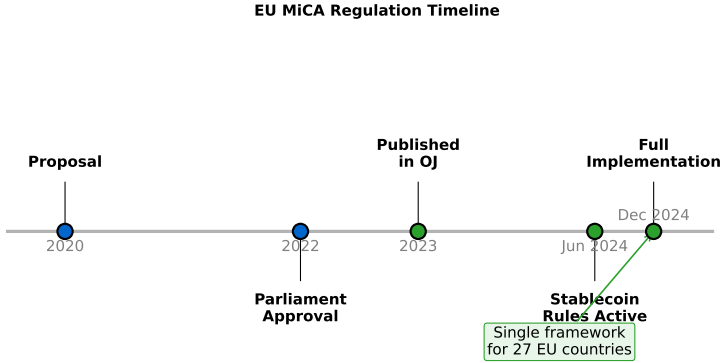
- Bitcoin ETF approval significance, DeFi regulatory challenges, and 2025 US political shift toward pro-crypto policy
- Can enforcement-first regulation transition to clear rulemaking without losing consumer protection?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How should governments regulate crypto?"?

MiCA Implementation Timeline

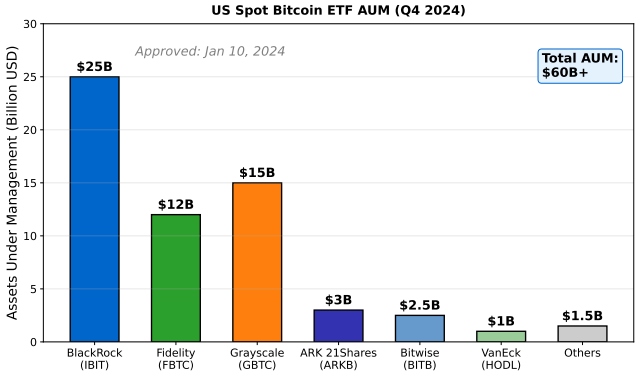


First comprehensive crypto regulation covering entire trading bloc | → Problem: How should governments regulate crypto? — MiCA Implementation Timeline
MiCA provides a template answer: comprehensive ex-ante rules rather than enforcement-first approach

How Does MiCA Regulate Stablecoins?

- **E-Money Tokens (EMTs—stablecoins pegged 1:1 to a single fiat currency)**: Pegged to single fiat (USDC, USDT)
  - Issuers must be credit/e-money institutions
  - 1:1 reserve backing in segregated accounts
  - Redemption at par value anytime
- **Asset-Referenced Tokens (ARTs—stablecoins backed by baskets of assets or commodities)**: Basket or non-fiat pegged
  - Stricter capital and governance requirements
- **Significant Tokens**: Enhanced EBA oversight
- **Algorithmic Stablecoins**: Effectively banned (post-Terra)
- **Practical Impact**: USDT delisted by major exchanges (Coinbase, Binance) in EU; Circle (USDC) MiCA-compliant (EMI license July 2024)

2024 Milestone: Bitcoin ETF Approval



SEC approved 11 spot Bitcoin ETFs on January 10, 2024

Why Was Bitcoin ETF Approval So Important?

- **January 10, 2024**: SEC approves 11 spot Bitcoin ETFs
  - First spot Bitcoin ETFs in US history (after decade of rejections)
  - Issuers: BlackRock (IBIT), Fidelity (FBTC), Grayscale (GBTC)
- **Impact**:
  - $49B total inflows in 2024 (IBIT: $37B, FBTC: $12B)
  - Institutional access via traditional brokerage accounts
  - Bitcoin legitimized as investable asset class
  - BTC reached new ATH ¿$100k (December 2024)
- **July 2024**: SEC approves spot Ethereum ETFs
- **Significance**: Major shift from SEC's hostile stance

How Do Asian Countries Regulate Crypto?

- **Singapore (MAS)**:
  - Payment Services Act licensing
  - Strict AML/CFT, retail protections
- **Hong Kong (SFC)**:
  - Mandatory licensing (2023)
  - Positioning as Asian crypto hub post-China ban
- **Japan (FSA)**:
  - Early framework (2017), strict custody standards
- **China**: Complete ban (2021) - transactions, mining, exchanges
  - Rationale: Capital controls, CBDC strategy
  - Result: Mining exodus to US, Kazakhstan, Russia

What Makes Switzerland Crypto-Friendly?

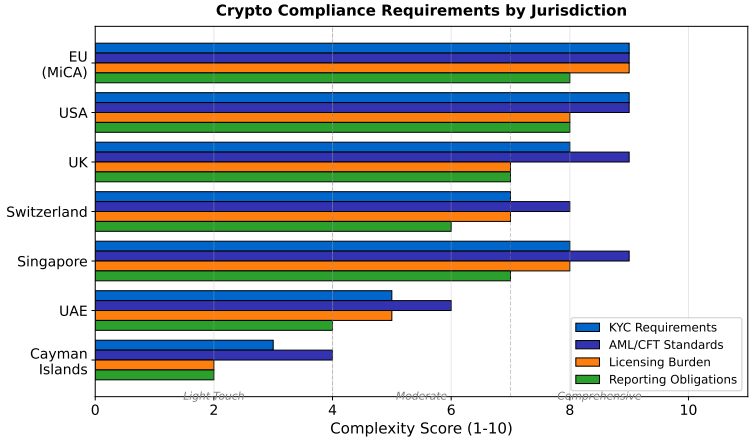
- **Crypto Valley (Zug)**: Global blockchain hub
- **Legal Framework**:
  - DLT Act (2021): Tailored regulation for digital assets
  - Token classification: Payment, Utility, Asset tokens
  - Securities law applies to asset tokens only
- **FINMA Guidance**:
  - Clear licensing categories
  - AML/CFT compliance for exchanges
  - No blanket prohibition on specific activities
- **Advantages**: Regulatory clarity, innovation-friendly, strong rule of law

→ *Problem: How should governments regulate crypto? — Switzerland: Crypto Nation Switzerland demonstrates that clear regulatory frameworks attract innovation rather than driving it offshore*

What is the FATF Travel Rule?

- **FATF (Financial Action Task Force, the global anti-money laundering standard-setter) Recommendation 16**: Apply to Virtual Asset Service Providers
- **Requirements**:
  - Collect/transmit customer info for transactions ¿$1,000
  - Originator and beneficiary details
- **Implementation**:
  - Centralized exchanges: Implemented (Coinbase, Kraken)
  - Cross-border: Technical solutions (TRP, TRUST, Notabene)
  - Self-hosted wallets: Controversial (EU proposed restrictions)
- **Challenge**: DeFi has no intermediary to enforce rules
- **Tension**: KYC requirements conflict with crypto privacy ethos

Compliance Requirements by Jurisdiction



EU/MiCA and US have highest compliance burden; offshore jurisdictions minimal

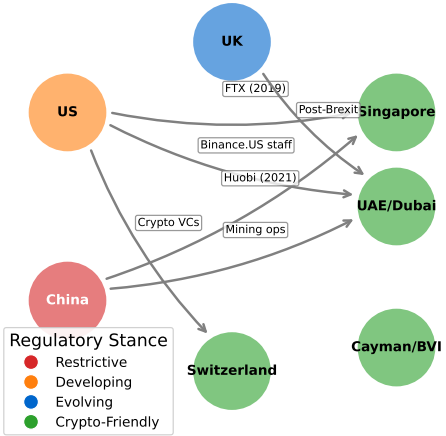
Why is Regulating DeFi So Difficult?

- **Problem**: Traditional regulation assumes intermediaries
- **DeFi Reality**: Smart contracts, no central operator
- **Key Questions**:
  - Who is liable for smart contract exploits?
  - How to enforce AML without custodian?
  - Are DeFi protocols securities or commodities?
- **Enforcement Actions**:
  - Tornado Cash (2022): Treasury sanctioned mixer protocol
  - Uniswap Labs: SEC Wells Notice (formal notification that the SEC staff intends to recommend enforcement action)
  - Ooki DAO (2022): CFTC sued DAO as legal entity
- **Debate**: Code is speech vs code is conduct

How Did the 2024 Election Change Crypto Regulation?

- **2024 Election Impact**:
  - Crypto PACs spent $100M+ on elections
  - Pro-crypto candidates elected to Congress
- **New Administration (2025)**:
  - Promise to make US "crypto capital of the world"
  - SEC Chair Gensler resigned
  - Strategic Bitcoin Reserve proposal discussed
- **Legislative Outlook**:
  - FIT21 (Financial Innovation and Technology Act) revival
  - Stablecoin legislation priority
  - CFTC vs SEC jurisdiction clarity expected
- **Shift**: From enforcement to rulemaking approach

Regulatory Arbitrage: Company Migrations



Restrictive jurisdictions (US, China) lose companies to crypto-friendly hubs (Singapore, UAE, Switzerland)

What Regulatory Trends Will Shape the Future?

- **Trend 1: Convergence**: Countries adopting similar frameworks (MiCA template)
- **Trend 2: Stablecoin Focus**: Banking-like regulation for systemic stablecoins
- **Trend 3: DeFi Reckoning**: Regulatory clarity (or crackdown) coming
- **Trend 4: CBDC Competition**: Central banks competing with private stablecoins
- **Trend 5: Global Coordination**: FATF, FSB harmonizing standards
- **Trend 6: Licensing Regimes**: Most jurisdictions requiring VASP licenses

- **Uncertainty Remains**: Technology evolves faster than regulation

Problem Solved? Global Regulation

The Original Problem

How should governments regulate crypto?

How Global Regulation Solves It

- **Regulatory sandboxes**: Allow controlled experimentation (Singapore MAS, UK FCA)
- **Clear taxonomies**: Distinguish security vs utility vs payment tokens (Switzerland DLT Act, MiCA)
- **Risk-based frameworks**: Proportional rules based on systemic significance (MiCA stablecoin tiers)

Remaining Limitations

- **Jurisdictional arbitrage**: Projects relocate to friendly jurisdictions (US to Switzerland/UAE)
- **Enforcement challenges**: DeFi protocols have no legal entity; sanctions bypass (Tornado Cash forks)
- **Regulatory capture risk**: Industry lobbying shapes rules (crypto PACs $100M+ in 2024 elections)

Open Questions

- Will global harmonization emerge, or persist as fragmented patchwork?
- Risk: Black swan events, cascading failures (Terra/Luna, FTX)

Global Regulation partially solves "governments regulate crypto" but introduces new trade-offs

(c) Joerg Osterrieder 2025

The Economics of Global Regulation

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Global Regulation

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Global Regulation

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

Global Regulation: The Journey

- Companies move headquarters to optimize for regulatory treatment
- The result: A patchwork map of crypto havens and hostile zones

[COMIC: "Regulatory arbitrage map" – A world map shows crypto company headquarters: clusters in Switzerland, Singapore, UAE, Cayman Islands. Arrows show migration patterns from US/EU. Legend: Green = "Welcome!", Yellow = "Papers please", Red = "Banned". A startup on a boat sails between jurisdictions.]

[PLACEHOLDER] — Regulatory arbitrage drives company location decisions until global frameworks converge

Summary

Key Takeaways:

- **Global landscape**: Highly fragmented, evolving rapidly
- **US**: Fragmented (SEC vs CFTC), regulation by enforcement
- **EU**: Comprehensive MiCA framework, December 2024 full implementation
- **Asia**: Diverse (Singapore/HK permissive, China ban, Japan conservative)
- **Switzerland**: Clear framework, crypto-friendly (Crypto Valley)
- **Bitcoin ETF (Jan 2024)**: Major legitimization milestone
- **Enforcement**: $13B+ in penalties (2022-2024)
- **Trend**: Convergence toward licensing with consumer protections

Next Lesson: L46 – Swiss FINMA and EU MiCA

Questions for Reflection

1. How does regulatory fragmentation affect crypto innovation in the US?
2. Why did the EU choose comprehensive legislation (MiCA) vs enforcement?
3. What are the trade-offs of China's complete ban approach?
4. Should DeFi protocols be regulated like traditional financial services?
5. How significant is the Bitcoin ETF approval for mainstream adoption?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code
Answer: C – The Howey Test (investment of money + common enterprise + expectation of profits from others' efforts) determines if a token is a security under SEC jurisdiction.

Q3. Which US regulatory agency has jurisdiction over Bitcoin and Ethereum as commodities?
A) Securities and Exchange Commission (SEC) B) Commodity Futures Trading Commission (CFTC)
C) Financial Crimes Enforcement Network (FinCEN) D) Internal Revenue Service (IRS)
Answer: B – CFTC has jurisdiction over Bitcoin and Ethereum as commodities, while SEC claims most other tokens are securities.

Q4. What was the total penalty amount in the Binance enforcement settlement in 2023?
A) $1.3 billion B) $2.5 billion C) $4.3 billion D) $4.5 billion
Answer: C – Binance paid $4.3B to DOJ in 2023, with CEO CZ resigning and serving prison time.

Q5. When did the SEC approve the first spot Bitcoin ETFs in US history?
A) November 2023 B) January 10, 2024
C) March 2024 D) July 2024
Answer: B – SEC approved 11 spot Bitcoin ETFs on January 10, 2024, ending a decade of rejections.

Quiz Questions (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money
Answer: C – EMTs are stablecoins pegged 1:1 to a single fiat currency (like USDC, USDT), requiring full reserve backing.

Q8. Which stablecoin was delisted by major EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT (Tether) D) BUSD (deprecated)
Answer: C – USDT was delisted by Coinbase and Binance in EU due to MiCA non-compliance; Circle's USDC obtained EMI license in July 2024.

Q9. How much total inflow did Bitcoin ETFs receive in 2024?
A) $25 billion B) $37 billion C) $49 billion D) $62 billion
Answer: C – Bitcoin ETFs received $49B total inflows in 2024 (IBIT: $37B, FBTC: $12B).

Q10. Which country implemented a complete ban on crypto transactions, mining, and exchanges in 2021?
A) India B) Russia C) China D) Turkey
Answer: C – China implemented a complete ban in 2021 to maintain capital controls and support CBDC strategy, causing mining exodus.

Quiz Questions (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities
Answer: A – The court ruled institutional sales were securities (Howey Test met) but retail sales on exchanges were not.

Q13. What was the final penalty amount for Ripple Labs after SEC litigation?
A) $50 million B) $125 million C) $1.3 billion D) $2 billion
Answer: B – Ripple was fined $125M, significantly reduced from the SEC's $2B request.

Q14. Which Swiss city is known as "Crypto Valley" and serves as a global blockchain hub?
A) Zurich B) Geneva C) Zug D) Basel
Answer: C – Zug is known as Crypto Valley, offering clear regulatory framework via DLT Act (2021) and FINMA guidance.

Q15. What regulatory challenge does DeFi pose that traditional finance regulation assumes?
A) Too much transparency B) High transaction fees
C) Existence of intermediaries D) Slow settlement times
Answer: C – Traditional regulation assumes intermediaries; DeFi operates via smart contracts with no central operator to enforce rules.

Quiz Questions (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024
Answer: D – MiCA was approved in 2023 but achieved full implementation in December 2024.

Q18. What is the SEC Chair Gary Gensler's status as of 2025?
A) Reappointed for second term B) Resigned following 2024 election
C) Promoted to Treasury Secretary D) Still serving as SEC Chair
Answer: B – Gensler resigned after the 2024 election, signaling a shift from enforcement to potential rulemaking approach.

Q19. Which regulatory trend involves countries adopting similar frameworks to MiCA?
A) Fragmentation B) Convergence C) Decentralization D) Liberalization
Answer: B – Convergence describes the trend of countries adopting similar comprehensive frameworks, often using MiCA as a template.

Q20. What was the total amount of enforcement penalties levied from 2022-2024?
A) $5 billion B) $8 billion C) $13+ billion D) $20 billion
Answer: C – Over $13B in penalties were levied (2022-2024), including Binance $4.3B, Terraform Labs $4.5B, and others.

L45: Global Regulatory Landscape

Mini-Lecture – Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Compare regulatory approaches across major jurisdictions
- Understand the US fragmented regulatory landscape (SEC vs CFTC)
- Evaluate EU MiCA as comprehensive framework
- Assess enforcement actions and Bitcoin ETF approval significance

Core Tension: Innovation vs consumer protection vs financial stability

(c) Joerg Osterrieder 2025

The Global Regulatory Spectrum

Hostile	Restrictive	Permissive
China (2021 ban)	India (30% tax)	Switzerland (clear framework)
Algeria, Bangladesh	South Korea (strict KYC)	Singapore (licensing)
Nepal, Morocco	Russia (payment ban)	UAE (crypto-friendly zones)
	Turkey (payment ban)	El Salvador (legal tender)

Trend: Convergence toward licensing regimes with consumer protections

Most jurisdictions moving from restrictive toward regulated permissiveness

United States: Fragmented Jurisdiction

Key Regulators

- **SEC**: Securities (Howey Test)
- **CFTC**: Commodities (BTC, ETH)
- **FinCEN**: AML/CTF enforcement
- **IRS**: Crypto = property (tax)
- **States**: Money transmitter licenses

Howey Test (Securities)

1. Investment of money
2. Common enterprise
3. Expectation of profits
4. From efforts of others

Result: Regulation by enforcement

Multiple agencies with overlapping and unclear jurisdiction

Major Enforcement Actions (2022–2024)

- **Binance (2023)**: $4.3B DOJ settlement, CEO resigned
- **Terraform Labs (2024)**: $4.5B penalty for UST/LUNA fraud
- **FTX (2022-2024)**: Criminal fraud, SBF convicted
- **Ripple Labs**: $125M (reduced from $2B SEC request)
  - Institutional sales = securities, retail = not securities

Total Penalties (2022–2024): Over $13 billion

Pattern: Enforcement first, rulemaking later

2024 Milestone: Bitcoin ETF Approval

January 10, 2024: SEC approves 11 spot Bitcoin ETFs

- First spot Bitcoin ETFs in US history
- Issuers: BlackRock (IBIT), Fidelity (FBTC), Grayscale
- **$49B** total inflows in 2024
- BTC reached new ATH ¿$100k (Dec 2024)

July 2024: Spot Ethereum ETFs approved

Ended a decade of spot ETF rejections

Significance

- Institutional access via brokerages
- Bitcoin legitimized as asset class
- Major shift from SEC hostile stance

European Union: MiCA Regulation

MiCA (Markets in Crypto-Assets): First comprehensive framework

- **Timeline**: Approved 2023, full implementation December 2024
- **Scope**: CASPs, stablecoin issuers (EMTs, ARTs), excludes most NFTs

Key Requirements

- Authorization for CASPs
- Market abuse prohibitions
- Consumer protection (disclosure)
- Stablecoin reserve requirements

Stablecoin Impact

- **USDT**: Delisted by major EU exchanges
- **USDC**: MiCA-compliant (July 2024)
- Algorithmic stablecoins: Banned

Single framework across 27 EU countries

Asia-Pacific: Diverse Approaches

Permissive

- **Singapore (MAS)**: Payment Services Act licensing, strict AML
- **Hong Kong (SFC)**: Mandatory licensing (2023), Asian hub ambitions
- **Japan (FSA)**: Early framework (2017), strict custody standards

Restrictive/Hostile

- **China**: Complete ban (2021) – transactions, mining, exchanges
  - Rationale: Capital controls, CBDC
  - Result: Mining exodus to US, Kazakhstan

Switzerland: Crypto Valley (Zug), DLT Act 2021, clear token classification

DeFi: The Regulatory Challenge

Problem: Traditional regulation assumes intermediaries exist

- DeFi operates via smart contracts with no central operator
- Key questions: Liability? AML enforcement? Securities or commodities?

Enforcement Actions

- **Tornado Cash (2022)**: Treasury sanctioned mixer protocol
- **Uniswap Labs**: SEC Wells Notice issued
- **Ooki DAO (2022)**: CFTC sued DAO as legal entity

Central Debate: Is code speech or conduct?

FATF Travel Rule requires VASPs to collect/transmit info for transactions ¿$1,000

2025 US Political Shift

2024 Election Impact

- Crypto PACs spent $100M+ on elections
- Pro-crypto candidates elected
- SEC Chair Gensler resigned

Legislative Outlook

- FIT21 bill revival expected
- Stablecoin legislation priority
- CFTC vs SEC clarity coming
- Strategic Bitcoin Reserve discussed

Shift: From enforcement-first to rulemaking approach

Promise to make US "crypto capital of the world"

Summary: Key Takeaways

- **Global landscape**: Highly fragmented, evolving rapidly toward convergence
- **US**: Fragmented (SEC vs CFTC), $13B+ in enforcement penalties
- **EU**: Comprehensive MiCA framework (December 2024)
- **Asia**: Diverse (Singapore/HK permissive, China ban, Japan conservative)
- **Bitcoin ETF (Jan 2024)**: $49B inflows, major legitimization
- **DeFi**: Regulatory challenge – no intermediaries to regulate
- **Trend**: Licensing regimes with consumer protections

Image Attributions

Law/Gavel
GR Stocks (Unsplash)
CC0 License

US Capitol
Andy Feliciotti (Unsplash)
CC0 License

Regulation Sign
Martin Sanchez (Unsplash)
CC0 License

All images sourced from Unsplash under the Unsplash License (free for commercial and non-commercial use).

Quiz Questions (1–5)

Q1. Which US test determines if a token is a security?
A) Commodity Test B) Howey Test C) FATF Test D) BitLicense Test
Answer: B – Investment + common enterprise + profit expectation from others' efforts.

Q2. Which agency has jurisdiction over Bitcoin as a commodity?
A) SEC B) CFTC C) FinCEN D) IRS
Answer: B – CFTC regulates Bitcoin and Ethereum as commodities.

Q3. What was the total Binance DOJ settlement in 2023?
A) $1.3B B) $2.5B C) $4.3B D) $4.5B
Answer: C – Binance paid $4.3B; CEO CZ resigned and served prison time.

Q4. When did SEC approve spot Bitcoin ETFs?
A) Nov 2023 B) Jan 10, 2024 C) Mar 2024 D) Jul 2024
Answer: B – 11 spot Bitcoin ETFs approved January 10, 2024.

Q5. What does MiCA stand for?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Monetary Integration of Crypto D) Multi-jurisdictional Investment in Crypto
Answer: B – Markets in Crypto-Assets Regulation (EU).

Quiz Questions (6–10)

Q6. How much did Bitcoin ETFs receive in total inflows in 2024?
A) $25B B) $37B C) $49B D) $62B
Answer: C – $49B total (IBIT $37B, FBTC $12B).

Q7. Which stablecoin was delisted by EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT D) BUSD
Answer: C – USDT (Tether) was delisted; Circle's USDC obtained EMI license.

Q8. Which country implemented a complete crypto ban in 2021?
A) India B) Russia C) China D) Turkey
Answer: C – China banned transactions, mining, and exchanges in 2021.

Q9. Which DeFi protocol was sanctioned by US Treasury in 2022?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned as a mixer facilitating money laundering.

Q10. Which Swiss city is known as "Crypto Valley"?
A) Zurich B) Geneva C) Zug D) Basel
Answer: C – Zug offers clear regulatory framework via DLT Act (2021).

Quiz: Global Regulation

Instructions: Multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains

Quiz (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code

Quiz (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code
Answer: C – The Howey Test (investment of money + common enterprise + expectation of profits from others' efforts) determines if a token is a security under SEC jurisdiction.

Q3. Which US regulatory agency has jurisdiction over Bitcoin and Ethereum as commodities?
A) Securities and Exchange Commission (SEC) B) Commodity Futures Trading Commission (CFTC)
C) Financial Crimes Enforcement Network (FinCEN) D) Internal Revenue Service (IRS)

Quiz (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code
Answer: C – The Howey Test (investment of money + common enterprise + expectation of profits from others' efforts) determines if a token is a security under SEC jurisdiction.

Q3. Which US regulatory agency has jurisdiction over Bitcoin and Ethereum as commodities?
A) Securities and Exchange Commission (SEC) B) Commodity Futures Trading Commission (CFTC)
C) Financial Crimes Enforcement Network (FinCEN) D) Internal Revenue Service (IRS)
Answer: B – CFTC has jurisdiction over Bitcoin and Ethereum as commodities, while SEC claims most other tokens are securities.

Q4. What was the total penalty amount in the Binance enforcement settlement in 2023?
A) $1.3 billion B) $2.5 billion C) $4.3 billion D) $4.5 billion

Quiz (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code
Answer: C – The Howey Test (investment of money + common enterprise + expectation of profits from others' efforts) determines if a token is a security under SEC jurisdiction.

Q3. Which US regulatory agency has jurisdiction over Bitcoin and Ethereum as commodities?
A) Securities and Exchange Commission (SEC) B) Commodity Futures Trading Commission (CFTC)
C) Financial Crimes Enforcement Network (FinCEN) D) Internal Revenue Service (IRS)
Answer: B – CFTC has jurisdiction over Bitcoin and Ethereum as commodities, while SEC claims most other tokens are securities.

Q4. What was the total penalty amount in the Binance enforcement settlement in 2023?
A) $1.3 billion B) $2.5 billion C) $4.3 billion D) $4.5 billion
Answer: C – Binance paid $4.3B to DOJ in 2023, with CEO CZ resigning and serving prison time.

Q5. When did the SEC approve the first spot Bitcoin ETFs in US history?
A) November 2023 B) January 10, 2024
C) March 2024 D) July 2024

Quiz (1–5)

Q1. Which of the following is NOT a primary regulatory concern for cryptocurrencies?
A) Money laundering and illicit finance B) Consumer protection from fraud
C) Decentralization of governance D) Tax evasion and unreported gains
Answer: C – Decentralization is a feature, not a regulatory concern; regulators focus on AML, consumer protection, and tax compliance.

Q2. What is the Howey Test used for in US cryptocurrency regulation?
A) Determining if Bitcoin is a commodity B) Testing exchange security
C) Determining if a token is a security D) Evaluating smart contract code
Answer: C – The Howey Test (investment of money + common enterprise + expectation of profits from others' efforts) determines if a token is a security under SEC jurisdiction.

Q3. Which US regulatory agency has jurisdiction over Bitcoin and Ethereum as commodities?
A) Securities and Exchange Commission (SEC) B) Commodity Futures Trading Commission (CFTC)
C) Financial Crimes Enforcement Network (FinCEN) D) Internal Revenue Service (IRS)
Answer: B – CFTC has jurisdiction over Bitcoin and Ethereum as commodities, while SEC claims most other tokens are securities.

Q4. What was the total penalty amount in the Binance enforcement settlement in 2023?
A) $1.3 billion B) $2.5 billion C) $4.3 billion D) $4.5 billion
Answer: C – Binance paid $4.3B to DOJ in 2023, with CEO CZ resigning and serving prison time.

Q5. When did the SEC approve the first spot Bitcoin ETFs in US history?
A) November 2023 B) January 10, 2024
C) March 2024 D) July 2024

Quiz (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets

Quiz (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money

Quiz (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money
Answer: C – EMTs are stablecoins pegged 1:1 to a single fiat currency (like USDC, USDT), requiring full reserve backing.

Q8. Which stablecoin was delisted by major EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT (Tether) D) BUSD

Quiz (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money
Answer: C – EMTs are stablecoins pegged 1:1 to a single fiat currency (like USDC, USDT), requiring full reserve backing.

Q8. Which stablecoin was delisted by major EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT (Tether) D) BUSD
Answer: C – USDT was delisted by Coinbase and Binance in EU due to MiCA non-compliance; Circle's USDC obtained EMI license in July 2024.

Q9. How much total inflow did Bitcoin ETFs receive in 2024?
A) $25 billion B) $37 billion C) $49 billion D) $62 billion

Quiz (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money
Answer: C – EMTs are stablecoins pegged 1:1 to a single fiat currency (like USDC, USDT), requiring full reserve backing.

Q8. Which stablecoin was delisted by major EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT (Tether) D) BUSD
Answer: C – USDT was delisted by Coinbase and Binance in EU due to MiCA non-compliance; Circle's USDC obtained EMI license in July 2024.

Q9. How much total inflow did Bitcoin ETFs receive in 2024?
A) $25 billion B) $37 billion C) $49 billion D) $62 billion
Answer: C – Bitcoin ETFs received $49B total inflows in 2024 (IBIT: $37B, FBTC: $12B).

Q10. Which country implemented a complete ban on crypto transactions, mining, and exchanges in 2021?
A) India B) Russia C) China D) Turkey

Quiz (6–10)

Q6. What does MiCA stand for in the European Union regulatory framework?
A) Market Infrastructure for Crypto Assets B) Markets in Crypto-Assets
C) Multi-jurisdictional Investment in Crypto Administration D) Monetary Integration of Crypto Assets
Answer: B – MiCA is "Markets in Crypto-Assets Regulation," the EU's comprehensive framework implemented December 2024.

Q7. Under MiCA, what are E-Money Tokens (EMTs)?
A) Tokens pegged to baskets of currencies B) Algorithmic stablecoins
C) Tokens pegged to a single fiat currency D) NFTs representing digital money
Answer: C – EMTs are stablecoins pegged 1:1 to a single fiat currency (like USDC, USDT), requiring full reserve backing.

Q8. Which stablecoin was delisted by major EU exchanges due to MiCA non-compliance?
A) USDC B) DAI C) USDT (Tether) D) BUSD
Answer: C – USDT was delisted by Coinbase and Binance in EU due to MiCA non-compliance; Circle's USDC obtained EMI license in July 2024.

Q9. How much total inflow did Bitcoin ETFs receive in 2024?
A) $25 billion B) $37 billion C) $49 billion D) $62 billion
Answer: C – Bitcoin ETFs received $49B total inflows in 2024 (IBIT: $37B, FBTC: $12B).

Q10. Which country implemented a complete ban on crypto transactions, mining, and exchanges in 2021?
A) India B) Russia C) China D) Turkey
Answer: C – China implemented a complete ban in 2021 to maintain capital controls and support CBDC strategy, causing mining exodus.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries

Quiz (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities

Quiz (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities
Answer: A – The court ruled institutional sales were securities (Howey Test met) but retail sales on exchanges were not.

Q13. What was the final penalty amount for Ripple Labs after SEC litigation?
A) $50 million B) $125 million C) $1.3 billion D) $2 billion

Quiz (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities
Answer: A – The court ruled institutional sales were securities (Howey Test met) but retail sales on exchanges were not.

Q13. What was the final penalty amount for Ripple Labs after SEC litigation?
A) $50 million B) $125 million C) $1.3 billion D) $2 billion
Answer: B – Ripple was fined $125M, significantly reduced from the SEC's $2B request.

Q14. Which Swiss city is known as "Crypto Valley" and serves as a global blockchain hub?
A) Zurich B) Geneva C) Zug D) Basel

Quiz (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities
Answer: A – The court ruled institutional sales were securities (Howey Test met) but retail sales on exchanges were not.

Q13. What was the final penalty amount for Ripple Labs after SEC litigation?
A) $50 million B) $125 million C) $1.3 billion D) $2 billion
Answer: B – Ripple was fined $125M, significantly reduced from the SEC's $2B request.

Q14. Which Swiss city is known as "Crypto Valley" and serves as a global blockchain hub?
A) Zurich B) Geneva C) Zug D) Basel
Answer: C – Zug is known as Crypto Valley, offering clear regulatory framework via DLT Act (2021) and FINMA guidance.

Q15. What regulatory challenge does DeFi pose that traditional finance regulation assumes?
A) Too much transparency B) High transaction fees
C) Existence of intermediaries D) Slow settlement times

Quiz (11–15)

Q11. What is the FATF Travel Rule requirement for Virtual Asset Service Providers?
A) Verify customer identities for all transactions B) Collect/transmit customer info for transactions over $1,000
C) Report all transactions to government authorities D) Block transactions from sanctioned countries
Answer: B – FATF Recommendation 16 requires VASPs to collect and transmit originator/beneficiary details for transactions ¿$1,000.

Q12. In the Ripple Labs case, how did the court distinguish institutional vs retail XRP sales?
A) Institutional sales were securities, retail sales were not B) Both were securities
C) Neither were securities D) Only ICO sales were securities
Answer: A – The court ruled institutional sales were securities (Howey Test met) but retail sales on exchanges were not.

Q13. What was the final penalty amount for Ripple Labs after SEC litigation?
A) $50 million B) $125 million C) $1.3 billion D) $2 billion
Answer: B – Ripple was fined $125M, significantly reduced from the SEC's $2B request.

Q14. Which Swiss city is known as "Crypto Valley" and serves as a global blockchain hub?
A) Zurich B) Geneva C) Zug D) Basel
Answer: C – Zug is known as Crypto Valley, offering clear regulatory framework via DLT Act (2021) and FINMA guidance.

Q15. What regulatory challenge does DeFi pose that traditional finance regulation assumes?
A) Too much transparency B) High transaction fees
C) Existence of intermediaries D) Slow settlement times
Answer: C – Traditional regulation assumes intermediaries; DeFi operates via smart contracts with no central operator to enforce rules.

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound

Quiz (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024

Quiz (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024
Answer: D – MiCA was approved in 2023 but achieved full implementation in December 2024.

Q18. What is the SEC Chair Gary Gensler's status as of 2025?
A) Reappointed for second term B) Resigned following 2024 election
C) Promoted to Treasury Secretary D) Still serving as SEC Chair

Quiz (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024
Answer: D – MiCA was approved in 2023 but achieved full implementation in December 2024.

Q18. What is the SEC Chair Gary Gensler's status as of 2025?
A) Reappointed for second term B) Resigned following 2024 election
C) Promoted to Treasury Secretary D) Still serving as SEC Chair
Answer: B – Gensler resigned after the 2024 election, signaling a shift from enforcement to potential rulemaking approach.

Q19. Which regulatory trend involves countries adopting similar frameworks to MiCA?
A) Fragmentation B) Convergence C) Decentralization D) Liberalization

Quiz (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024
Answer: D – MiCA was approved in 2023 but achieved full implementation in December 2024.

Q18. What is the SEC Chair Gary Gensler's status as of 2025?
A) Reappointed for second term B) Resigned following 2024 election
C) Promoted to Treasury Secretary D) Still serving as SEC Chair
Answer: B – Gensler resigned after the 2024 election, signaling a shift from enforcement to potential rulemaking approach.

Q19. Which regulatory trend involves countries adopting similar frameworks to MiCA?
A) Fragmentation B) Convergence C) Decentralization D) Liberalization
Answer: B – Convergence describes the trend of countries adopting similar comprehensive frameworks, often using MiCA as a template.

Q20. What was the total amount of enforcement penalties levied from 2022-2024?
A) $5 billion B) $8 billion C) $13+ billion D) $20 billion

Quiz (16–20)

Q16. Which DeFi protocol was sanctioned by the US Treasury in 2022 as a mixer?
A) Uniswap B) Aave C) Tornado Cash D) Compound
Answer: C – Tornado Cash was sanctioned in 2022 for facilitating money laundering, raising debate about code as speech vs conduct.

Q17. When did MiCA achieve full implementation across the EU?
A) June 2023 B) December 2023
C) June 2024 D) December 2024
Answer: D – MiCA was approved in 2023 but achieved full implementation in December 2024.

Q18. What is the SEC Chair Gary Gensler's status as of 2025?
A) Reappointed for second term B) Resigned following 2024 election
C) Promoted to Treasury Secretary D) Still serving as SEC Chair
Answer: B – Gensler resigned after the 2024 election, signaling a shift from enforcement to potential rulemaking approach.

Q19. Which regulatory trend involves countries adopting similar frameworks to MiCA?
A) Fragmentation B) Convergence C) Decentralization D) Liberalization
Answer: B – Convergence describes the trend of countries adopting similar comprehensive frameworks, often using MiCA as a template.

Q20. What was the total amount of enforcement penalties levied from 2022-2024?
A) $5 billion B) $8 billion C) $13+ billion D) $20 billion
Answer: C – Over $13B in penalties were levied (2022-2024), including Binance $4.3B, Terraform Labs $4.5B, and others.

L46: Swiss FINMA and EU MiCA

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand Swiss FINMA's principles-based approach to crypto regulation
- Analyze token classification frameworks (FINMA vs MiCA)
- Evaluate EU MiCA as comprehensive crypto-asset regulation
- Compare stablecoin requirements between frameworks
- Assess CASP licensing and compliance requirements
- Understand real-world implementation challenges (2024-2025)

The Problem: How should governments regulate crypto?

Part 2/4: Swiss FINMA & EU MiCA

The Challenge

Switzerland and the EU have developed contrasting approaches to crypto regulation. Switzerland uses a principles-based framework (FINMA) focused on flexibility, while the EU uses a rules-based system (MiCA) with detailed prescriptive requirements. How can regulators balance innovation with investor protection?

Why It Matters

- Without clear regulation, exchanges and issuers face legal uncertainty
- These frameworks (Swiss Crypto Valley, MiCA) serve as global regulatory templates

What We Need

- Risk management and mitigation
- Token classification systems that map crypto assets to existing regulatory categories
- Cross-border clarity and market access for crypto service providers

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How Swiss FINMA & EU MiCA addresses this challenge

Why Focus on Switzerland and EU?

Switzerland

- Crypto Valley (Zug): 1,000+ blockchain companies
- Clear legal framework since 2019
- Home to Ethereum, Cardano, Tezos foundations
- Principles-based, flexible approach

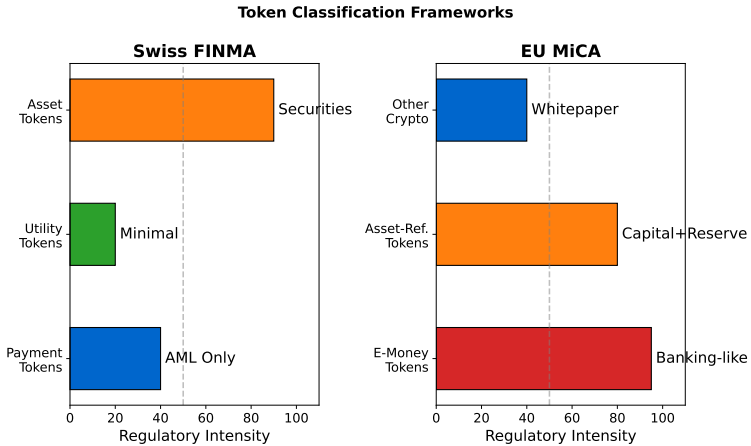
EU MiCA

- First comprehensive crypto framework
- 27 member states (450M people)
- Template for other jurisdictions
- Rules-based, detailed requirements

Key Contrast: Principles-based (Switzerland) vs rules-based (EU)

(c) Joerg Osterrieder 2025

Token Classification Comparison



Economic function determines regulatory treatment, not technology

FINMA Token Classification

Payment Tokens:

- Means of payment
- Ex: BTC, LTC
- AML only

Utility Tokens:

- Access to service
- Ex: FIL, Golem
- Minimal regulation

Asset Tokens:

- Claims/equity
- Ex: tokenized securities
- Securities law

Note: Categories not mutually exclusive; hybrid tokens possible

DLT Act (2021): Swiss Blockchain Legislation

DLT Securities:

- Tokenized securities
- Blockchain registry
- Same legal status

DLT Trading:

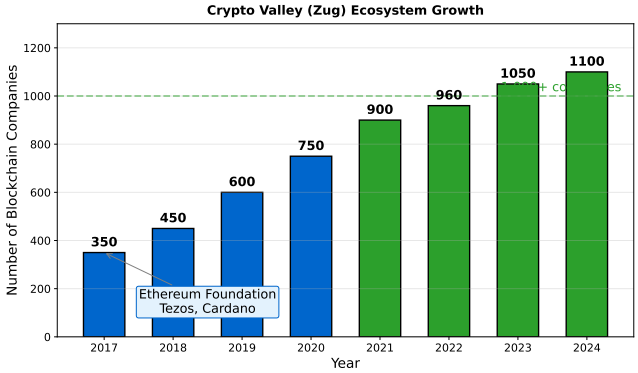
- New license type
- Lower barriers
- CHF 500K capital

Bankruptcy:

- Asset segregation
- Customer protected
- Institutional custody

DLT Act provides legal certainty for tokenization in Switzerland

Swiss Crypto Valley Growth



Regulatory clarity attracted global blockchain companies to Switzerland

MiCA: Overview

Timeline:

- Proposed: Sept 2020
- Approved: April 2023
- Full: Dec 30, 2024

Scope:
Crypto-assets, issuers, CASPs
Exclusions: NFTs, CBDCs

Objectives:

- Legal certainty
- Consumer protection
- Financial stability
- Innovation support

MiCA: First comprehensive crypto framework for 27 EU member states

MiCA: Crypto-Asset Definitions

E-Money Tokens:

- Single fiat peg
- Ex: USDC, USDT
- Strictest rules

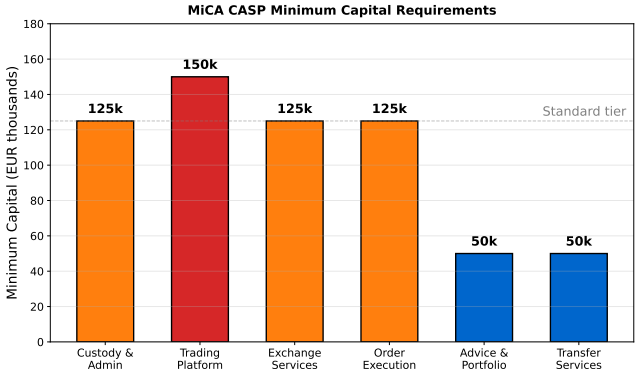
Asset-Referenced:

- Basket/commodity peg
- Capital, reserves
- Governance rules

Other Crypto:

- BTC, ETH, utility
- White paper only
- Lightest rules

MiCA CASP Capital Requirements



Single authorization valid across all 27 EU member states (passporting)

MiCA: CASP Services

Authorized Services:

- Custody and administration
- Trading platform operation
- Exchange (fiat/crypto)
- Order execution

Additional Services:

- Crypto placement
- Advisory services
- Portfolio management
- Transfer services

Passporting: Single auth valid EU-wide — **Transition:** 18-month grandfathering

MiCA: E-Money Token Requirements

Issuer Authorization:

- Credit/e-money institution
- CASP license insufficient

Reserve Requirements:

- 1:1 HQLA backing
- Segregated assets
- Daily reconciliation

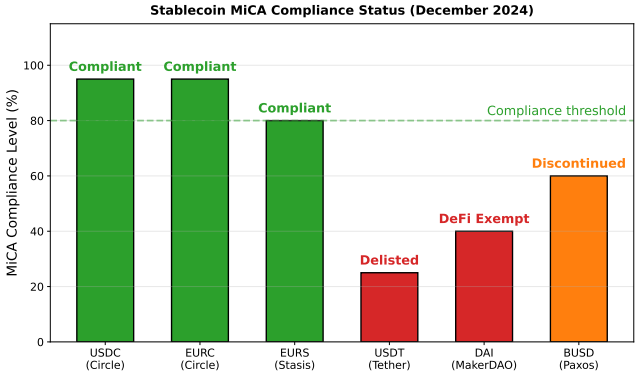
Redemption Rights:

- Par value anytime
- No redemption fees

Restrictions:

- No interest payments
- EBA supervises large EMTs

Stablecoin MiCA Compliance (2024)



USDT delisted from EU exchanges; USDC positioned as MiCA-compliant

Stablecoin Compliance Reality

Circle (USDC):

- France license Jul 2024
- First MiCA-compliant
- USDC + EURC OK

Tether (USDT):

- No EU license
- Delisted Dec 2024
- Coinbase EU removed

Market Impact:

- USDC gains share
- Euro coins emerging
- Compliance = edge

MiCA: Market Abuse Provisions

Prohibited Conduct:

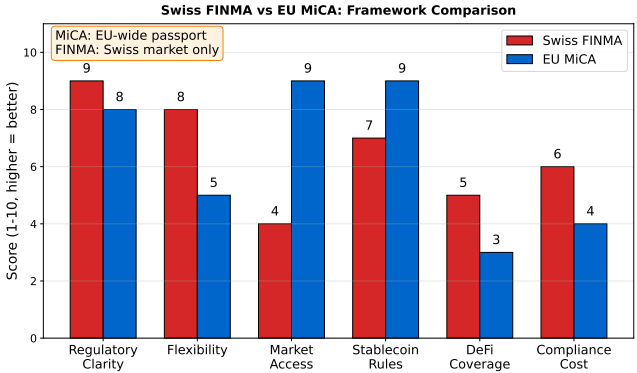
- **Insider Dealing:** MNPI trading
- **Manipulation:** wash trading, spoofing, pump-and-dump
- **Unlawful Disclosure**

Enforcement:

- National authorities
- Criminal penalties
- CASPs must monitor
- Mandatory reporting

Same market abuse rules as traditional securities now apply to crypto

Framework Comparison



Both frameworks provide regulatory clarity; MiCA offers broader market access

Swiss vs EU: Key Differences

Aspect	Switzerland	EU MiCA
Approach	Principles-based	Rules-based
Token Classification	Flexible (3 types)	Rigid (3 types)
Stablecoin Rules	Case-by-case	Banking-like
Market Access	Swiss only	27 EU countries
DeFi Treatment	Unclear	Excluded (for now)
Compliance Cost	Moderate	Higher

Strategy: Swiss firms seeking EU presence for MiCA passport

CASP Authorization Progress (2024-2025)

Major Exchanges:

- Binance: multi-jurisdiction
- Kraken: Germany, Ireland
- Coinbase: Irish e-money
- Bitstamp: Luxembourg

Bottlenecks:

- Regulators overwhelmed
- Varying interpretations
- Standards still finalizing

Preferred:
Ireland, France, Germany

MiCA 2.0: What's Next

EC Review (2025):

- DeFi regulation
- NFT fractionalization
- Staking and lending

Transfer of Funds:

- Travel Rule for crypto
- Wallet verification

Technical Standards:

- Custody specifications
- Sustainability disclosures
- PoW energy reporting

Global Influence:
Template for UK, Japan, Singapore

(c) Joerg Osterrieder 2025

Problem Solved? Swiss FINMA & EU MiCA

The Original Problem

How should governments regulate crypto?

How Swiss FINMA & EU MiCA Solves It

- FINMA's principles-based approach provides flexibility while ensuring payment tokens comply with AML and asset tokens follow securities law
- MiCA's comprehensive framework classifies EMTs, ARTs, and other crypto-assets with clear CASP licensing requirements and EU-wide passporting
- Both create legal certainty through token classification (FINMA: 3 types, MiCA: 3 types), enabling innovation within regulated boundaries

Remaining Limitations

- High compliance costs for smaller firms (MiCA capital requirements: EUR 125K-750K)
- Regulatory arbitrage risk: firms may forum-shop between jurisdictions (Swiss vs EU)
- DeFi protocols remain largely unregulated (excluded from MiCA 1.0)

Open Questions

- Will the Swiss principles-based model or EU rules-based model become the global standard?
- Risk: Black swan events, cascading failures across interconnected DeFi protocols

Swiss FINMA & EU MiCA partially solve "how to regulate crypto" but introduce new trade-offs between flexibility and clarity

Summary

Switzerland:

- Principles-based, flexible
- Payment/Utility/Asset tokens
- DLT Act innovation
- 1,100+ Crypto Valley firms

EU MiCA:

- Rules-based, 27 countries
- EMTs, ARTs, Other crypto
- Full Dec 2024 implementation
- USDC compliant, USDT delisted

Future: MiCA 2.0 (DeFi, NFTs)

Questions for Reflection

1. What are the trade-offs between principles-based vs rules-based regulation?
2. Why did Circle succeed in obtaining MiCA compliance while Tether did not?
3. How does the EU passport benefit crypto firms compared to Swiss-only?
4. Should DeFi protocols be included in MiCA 2.0?
5. What makes Crypto Valley attractive despite lacking EU market access?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and fall under securities regulation.

Q3. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025
Answer: C – MiCA was proposed in 2020, approved in 2023, fully implemented December 30, 2024.

Q4. What is the minimum capital requirement for CASP custody services under MiCA?
A) EUR 50,000 B) EUR 125,000 C) EUR 250,000 D) EUR 750,000
Answer: B – Custody services require EUR 125,000 minimum capital.

Q5. Which stablecoin obtained MiCA e-money license in France (July 2024)?
A) Tether (USDT) B) Circle (USDC) C) BUSD (deprecated 2023) D) DAI
Answer: B – Circle obtained the first global stablecoin e-money license for USDC and EURC.

Quiz Questions (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license category with CHF 500,000 minimum capital.

Q8. Which of the following is excluded from MiCA's scope?
A) E-money tokens (EMTs) B) Asset-referenced tokens (ARTs) C) CBDCs D) CASPs
Answer: C – CBDCs and non-fractionalized NFTs are excluded from MiCA.

Q9. How many blockchain companies are located in Swiss Crypto Valley (Zug)?
A) 250+ B) 500+ C) 1,000+ D) 2,000+
Answer: C – Over 1,000 blockchain companies (1,100+ as of 2024), including Ethereum, Cardano, Tezos.

Q10. Under MiCA, what is required for E-Money Token (EMT) redemption?
A) 2-day settlement B) Up to 5% fee C) Redeem at par anytime, no fees D) 30-day holding
Answer: C – EMTs must be redeemable at par value at any time with no redemption fees.

Quiz Questions (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens
Answer: C – Utility tokens have minimal regulation compared to payment (AML) and asset (securities law).

Q13. What is the key benefit of MiCA passporting?
A) Lower capital B) Exemption from AML C) Single authorization across 27 EU countries D) No reporting
Answer: C – Passporting allows CASPs to operate EU-wide with one authorization.

Q14. Under the DLT Act, how are customer crypto assets treated in bankruptcy?
A) Part of general estate B) Segregated from bankruptcy estate C) Distributed to creditors D) Frozen
Answer: B – Customer crypto assets are segregated and protected from the bankruptcy estate.

Q15. Which market abuse practice is prohibited under MiCA?
A) Staking rewards B) Wash trading and spoofing C) Yield farming D) Liquidity provision
Answer: B – MiCA prohibits wash trading, spoofing, layering, and pump-and-dump schemes.

Quiz Questions (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation
Answer: D – The lesson mentions Ethereum, Cardano, and Tezos foundations as examples.

Q18. What is expected in MiCA 2.0 review?
A) Removal of stablecoin rules B) DeFi regulation C) Complete deregulation D) Merger with Swiss
Answer: B – MiCA 2.0 is expected to address DeFi (currently excluded), NFT fractionalization, and staking/lending.

Q19. How long is the MiCA grandfathering period for existing providers?
A) 6 months B) 12 months C) 18 months D) 24 months
Answer: C – Existing crypto service providers have an 18-month transition period to obtain CASP authorization.

Q20. Which jurisdictions are preferred for CASP licenses?
A) Spain, Portugal, Greece B) Ireland, France, Germany C) Poland, Hungary, Romania D) Malta, Cyprus
Answer: B – Ireland, France, and Germany are preferred due to established regulatory infrastructure.

L46: Swiss FINMA and EU MiCA

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

What Are the Key Regulatory Frameworks?

- "We want to be the most innovative place for blockchain!" - Every regulator's pitch
- The promise: Clear rules that enable innovation while protecting consumers

[COMIC: "Innovation sandbox" promise – A regulator holds open a sandbox labeled "Regulatory Sandbox" with a red carpet leading in. Inside, happy blockchain startups build sandcastles. Sign reads: "Build anything! (Terms and conditions apply)"]

[PLACEHOLDER] — Both Switzerland and EU promise innovation-friendly regulation, but with different approaches

Learning Objectives

- Understand Swiss FINMA's principles-based approach to crypto regulation
- Analyze token classification frameworks (FINMA vs MiCA)
- Evaluate EU MiCA as comprehensive crypto-asset regulation
- Compare stablecoin requirements between frameworks
- Assess CASP licensing and compliance requirements
- Understand real-world implementation challenges (2024-2025)

Building on L45: Global Regulation

The Problem: How should governments regulate crypto?

Part 2/4: Swiss FINMA & EU MiCA

The Challenge

Switzerland and the EU have developed contrasting approaches to crypto regulation. Switzerland uses a principles-based framework (FINMA) focused on flexibility, while the EU uses a rules-based system (MiCA) with detailed prescriptive requirements. How can regulators balance innovation with investor protection?

Why It Matters

- Without clear regulation, exchanges and issuers face legal uncertainty
- These frameworks (Swiss Crypto Valley, MiCA) serve as global regulatory templates

What We Need

- Risk management and mitigation
- Token classification systems that map crypto assets to existing regulatory categories
- Cross-border clarity and market access for crypto service providers

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How Swiss FINMA & EU MiCA addresses this challenge

Why Are Switzerland and EU Leading Crypto Regulation?

Switzerland

- Crypto Valley (Zug): 1,000+ blockchain companies
- Clear legal framework since 2019
- Home to Ethereum, Cardano, Tezos foundations
- Principles-based, flexible approach

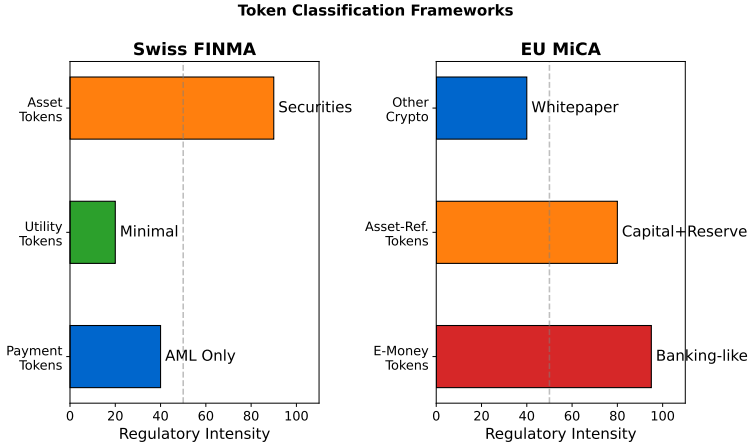
EU MiCA

- First comprehensive crypto framework
- 27 member states (450M people)
- Template for other jurisdictions
- Rules-based, detailed requirements

Key Contrast: Principles-based (Switzerland) vs rules-based (EU)

→ *Problem: How should governments regulate crypto? — Why Focus on Switzerland and EU? These two frameworks represent competing regulatory philosophies: flexibility (Switzerland) vs. comprehensiveness (EU)*

How Do Token Classification Systems Compare?



Economic function determines regulatory treatment, not technology

How Does FINMA Classify Tokens?

Payment Tokens:

- Means of payment
- Ex: BTC, LTC
- AML only

Utility Tokens:

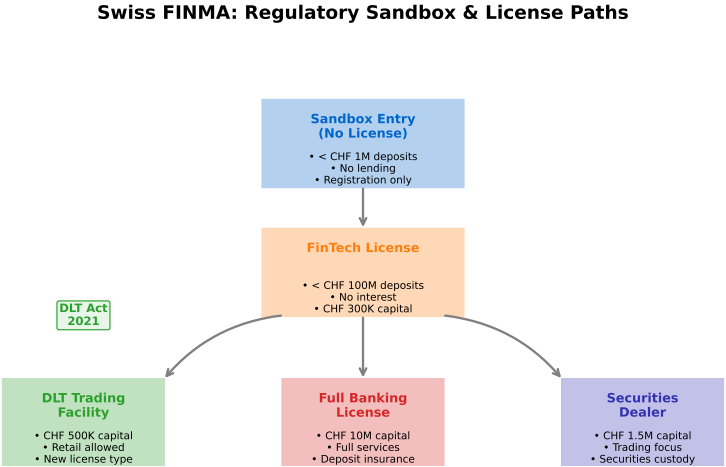
- Access to service
- Ex: FIL, Golem
- Minimal regulation

Asset Tokens:

- Claims/equity
- Ex: tokenized securities
- Securities law

Note: Categories not mutually exclusive; hybrid tokens possible

How Does FINMA's Regulatory Sandbox Work?



Progressive licensing structure enables startups to scale from sandbox to full banking license

What Does the DLT Act Enable in Switzerland?

DLT Securities:

- Tokenized securities
- Blockchain registry
- Same legal status

DLT Trading:

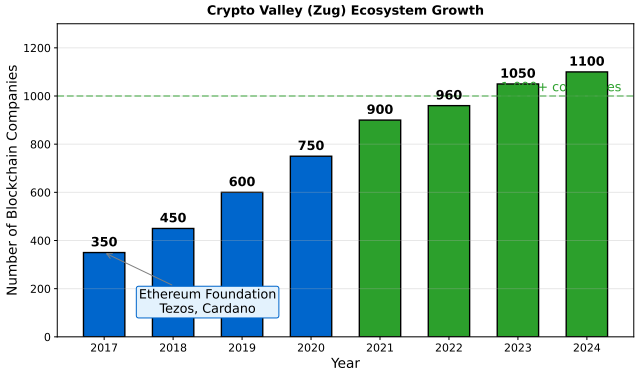
- New license type
- Lower barriers
- CHF 500K capital

Bankruptcy:

- Asset segregation
- Customer protected
- Institutional custody

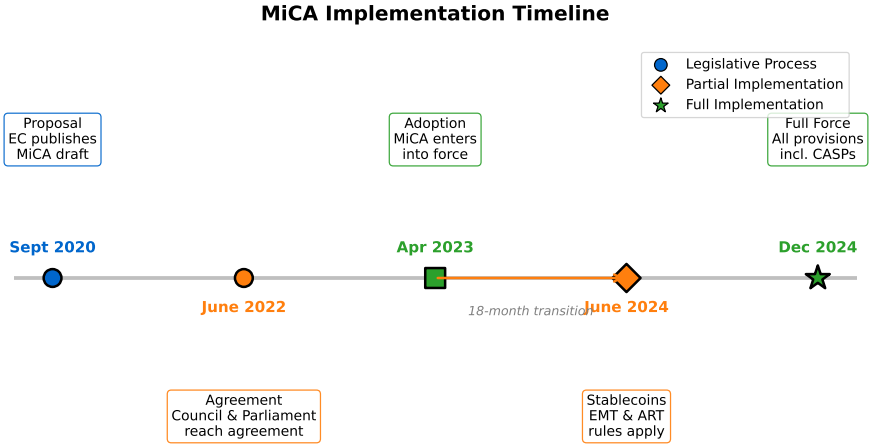
DLT Act provides legal certainty for tokenization in Switzerland

How Has Swiss Crypto Valley Grown?



Regulatory clarity attracted global blockchain companies to Switzerland | → Problem: How should governments regulate crypto? — Swiss Crypto Valley Growth: Regulatory clarity directly correlates with innovation attraction—1,100+ blockchain firms prove the model works

When Was MiCA Implemented?



MiCA: From proposal (2020) to full implementation (Dec 2024) with 18-month transition period

What Are MiCA's Key Design Principles?

Timeline:

- Proposed: Sept 2020
- Approved: April 2023
- Full: Dec 30, 2024

Scope:
Crypto-assets, issuers, CASPs
Exclusions: NFTs, CBDCs

Objectives:

- Legal certainty
- Consumer protection
- Financial stability
- Innovation support

MiCA: First comprehensive crypto framework for 27 EU member states

How Does MiCA Define Crypto-Assets?

E-Money Tokens:

- Single fiat peg
- Ex: USDC, USDT
- Strictest rules

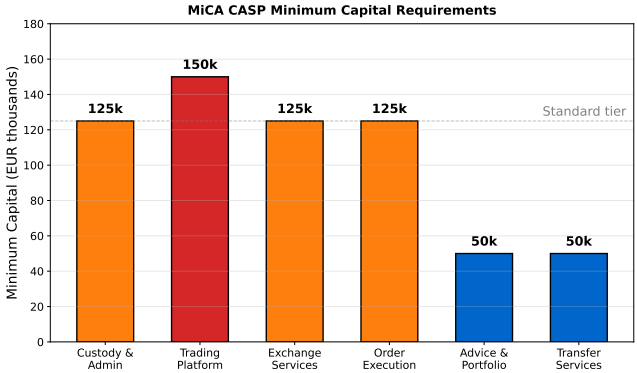
Asset-Referenced:

- Basket/commodity peg
- Capital, reserves
- Governance rules

Other Crypto:

- BTC, ETH, utility
- White paper only
- Lightest rules

What Capital Do CASPs Need Under MiCA?



Single authorization valid across all 27 EU member states (passporting—a single authorization valid across all 27 EU member states)

What Services Require CASP Authorization?

Authorized Services:

- Custody and administration
- Trading platform operation
- Exchange (fiat/crypto)
- Order execution

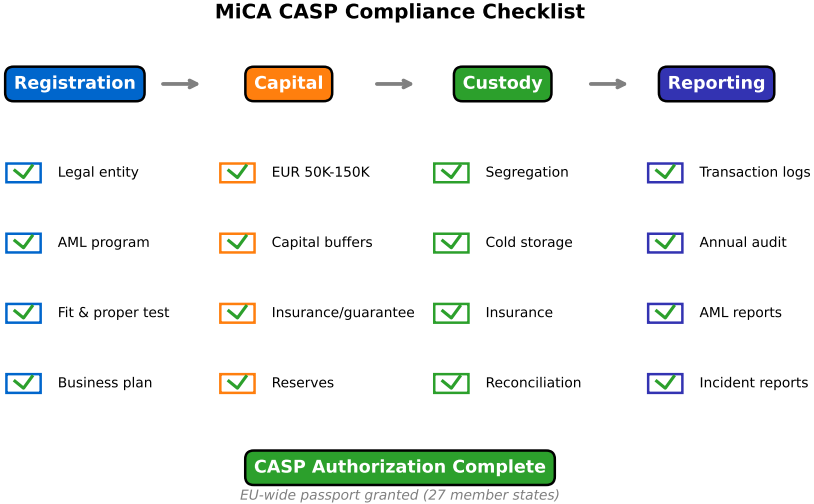
Additional Services:

- Crypto placement
- Advisory services
- Portfolio management
- Transfer services

Passporting: Single auth valid EU-wide — **Transition:** 18-month grandfathering period (allowing existing providers to continue operating while obtaining full CASP licenses)

→ Problem: How should governments regulate crypto? — MiCA: CASP Services: EU passporting solves the fragmentation problem: one license for 27 countries vs. 50+ US state licenses

What Steps Achieve CASP Compliance?



Complete all four phases to obtain MiCA CASP authorization with EU-wide passporting

Problem Check-In: Swiss FINMA & EU MiCA

Recall Our Problem

How should governments regulate crypto?

What We've Learned So Far

- FINMA's principles-based token classification: Payment (AML only), Utility (minimal), Asset (securities law)
- MiCA's comprehensive framework: EMTs, ARTs, and CASP licensing with EU-wide passporting
- Both create legal certainty but trade off flexibility (Swiss) against broader market access (EU)

Still to Address

- Stablecoin compliance reality (USDC compliant, USDT delisted), market abuse provisions, and MiCA 2.0 roadmap
- Will the Swiss or EU model become the global template for crypto regulation?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How should governments regulate crypto?"?

What Are the Requirements for E-Money Tokens?

Issuer Authorization:

- Credit/e-money institution
- CASP license insufficient

Reserve Requirements:

- 1:1 HQLA (High-Quality Liquid Assets such as government bonds and cash) backing
- Segregated assets
- Daily reconciliation

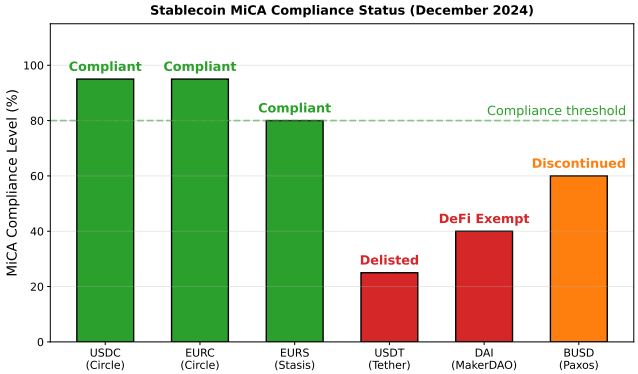
Redemption Rights:

- Par value anytime
- No redemption fees

Restrictions:

- No interest payments
- EBA supervises large EMTs

Which Stablecoins Comply with MiCA?



USDT delisted from EU exchanges; USDC positioned as MiCA-compliant

Which Stablecoins Are MiCA-Compliant?

Circle (USDC):

- France license Jul 2024
- First MiCA-compliant
- USDC + EURC OK

Tether (USDT):

- No EU license
- Delisted Dec 2024
- Coinbase EU removed

Market Impact:

- USDC gains share
- Euro coins emerging
- Compliance = edge

How Does MiCA Combat Market Manipulation?

Prohibited Conduct:

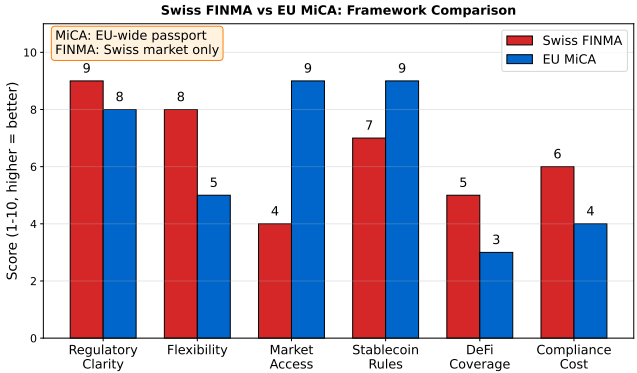
- **Insider Dealing:** MNPI (Material Non-Public Information) trading
- **Manipulation:** wash trading, spoofing, pump-and-dump
- **Unlawful Disclosure**

Enforcement:

- National authorities
- Criminal penalties
- CASPs must monitor
- Mandatory reporting

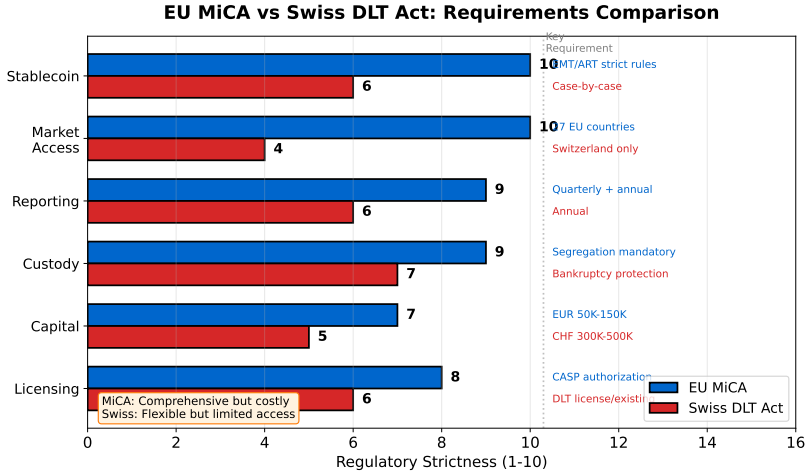
Same market abuse rules as traditional securities now apply to crypto | → Problem: How should governments regulate crypto? — MiCA: Market Abuse Provisions: Traditional market abuse rules now apply to crypto—closing the regulatory gap that enabled manipulation

How Do the Frameworks Compare?



Both frameworks provide regulatory clarity; MiCA offers broader market access

How Do Requirements Differ Between MiCA and Swiss DLT Act?



MiCA: Stricter requirements but EU-wide access; Swiss: Flexible but limited market

How Do Swiss and EU Approaches Differ?

Aspect	Switzerland	EU MiCA
Approach	Principles-based	Rules-based
Token Classification	Flexible (3 types)	Rigid (3 types)
Stablecoin Rules	Case-by-case	Banking-like
Market Access	Swiss only	27 EU countries
DeFi Treatment	Unclear	Excluded (for now)
Compliance Cost	Moderate	Higher

Strategy: Swiss firms seeking EU presence for MiCA passport

Which Exchanges Have Obtained CASP Licenses?

Major Exchanges:

- Binance: multi-jurisdiction
- Kraken: Germany, Ireland
- Coinbase: Irish e-money
- Bitstamp: Luxembourg

Bottlenecks:

- Regulators overwhelmed
- Varying interpretations
- Standards still finalizing

Preferred:
Ireland, France, Germany

What Will MiCA 2.0 Address?

EC Review (2025):

- DeFi regulation
- NFT fractionalization
- Staking and lending

Transfer of Funds:

- Travel Rule for crypto
- Wallet verification

Technical Standards:

- Custody specifications
- Sustainability disclosures
- PoW energy reporting

Global Influence:
Template for UK, Japan, Singapore

(c) Joerg Osterrieder 2025

Problem Solved? Swiss FINMA & EU MiCA

The Original Problem

How should governments regulate crypto?

How Swiss FINMA & EU MiCA Solves It

- FINMA's principles-based approach provides flexibility while ensuring payment tokens comply with AML and asset tokens follow securities law
- MiCA's comprehensive framework classifies EMTs, ARTs, and other crypto-assets with clear CASP licensing requirements and EU-wide passporting
- Both create legal certainty through token classification (FINMA: 3 types, MiCA: 3 types), enabling innovation within regulated boundaries

Remaining Limitations

- High compliance costs for smaller firms (MiCA capital requirements: EUR 125K-750K)
- Regulatory arbitrage risk: firms may forum-shop between jurisdictions (Swiss vs EU)
- DeFi protocols remain largely unregulated (excluded from MiCA 1.0)

Open Questions

- Will the Swiss principles-based model or EU rules-based model become the global standard?
- Risk: Black swan events, cascading failures across interconnected DeFi protocols

Swiss FINMA & EU MiCA partially solve "how to regulate crypto" but introduce new trade-offs between flexibility and clarity

The Economics of Swiss FINMA & EU MiCA

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Swiss FINMA & EU MiCA

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Swiss FINMA & EU MiCA

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

What Does Regulatory Compliance Really Cost?

- The sandbox was free; the full license costs EUR 125K-750K capital plus lawyers
- Small startups: "We just wanted to build cool DeFi..."

[COMIC: "Compliance cost reality" – A startup founder sits at a desk buried in paperwork: "MiCA Application", "CASP License", "AML Policy", "Capital Requirements". Bills labeled "Legal: EUR 500K", "Compliance Officer: EUR 150K/yr" pile up. The founder's coffee mug reads "I just wanted to code."]

[PLACEHOLDER] — Regulatory clarity comes with compliance costs that favor larger, well-funded players

Summary

Switzerland:

- Principles-based, flexible
- Payment/Utility/Asset tokens
- DLT Act innovation
- 1,100+ Crypto Valley firms

EU MiCA:

- Rules-based, 27 countries
- EMTs, ARTs, Other crypto
- Full Dec 2024 implementation
- USDC compliant, USDT delisted

Future: MiCA 2.0 (DeFi, NFTs)

Next Lesson: L47 – CBDCs and Future Trends

Questions for Reflection

1. What are the trade-offs between principles-based vs rules-based regulation?
2. Why did Circle succeed in obtaining MiCA compliance while Tether did not?
3. How does the EU passport benefit crypto firms compared to Swiss-only?
4. Should DeFi protocols be included in MiCA 2.0?
5. What makes Crypto Valley attractive despite lacking EU market access?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and fall under securities regulation.

Q3. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025
Answer: C – MiCA was proposed in 2020, approved in 2023, fully implemented December 30, 2024.

Q4. What is the minimum capital requirement for CASP custody services under MiCA?
A) EUR 50,000 B) EUR 125,000 C) EUR 250,000 D) EUR 750,000
Answer: B – Custody services require EUR 125,000 minimum capital.

Q5. Which stablecoin obtained MiCA e-money license in France (July 2024)?
A) Tether (USDT) B) Circle (USDC) C) BUSD (deprecated 2023) D) DAI
Answer: B – Circle obtained the first global stablecoin e-money license for USDC and EURC.

Quiz Questions (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license category with CHF 500,000 minimum capital.

Q8. Which of the following is excluded from MiCA's scope?
A) E-money tokens (EMTs) B) Asset-referenced tokens (ARTs) C) CBDCs D) CASPs
Answer: C – CBDCs and non-fractionalized NFTs are excluded from MiCA.

Q9. How many blockchain companies are located in Swiss Crypto Valley (Zug)?
A) 250+ B) 500+ C) 1,000+ D) 2,000+
Answer: C – Over 1,000 blockchain companies (1,100+ as of 2024), including Ethereum, Cardano, Tezos.

Q10. Under MiCA, what is required for E-Money Token (EMT) redemption?
A) 2-day settlement B) Up to 5% fee C) Redeem at par anytime, no fees D) 30-day holding
Answer: C – EMTs must be redeemable at par value at any time with no redemption fees.

Quiz Questions (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens
Answer: C – Utility tokens have minimal regulation compared to payment (AML) and asset (securities law).

Q13. What is the key benefit of MiCA passporting?
A) Lower capital B) Exemption from AML C) Single authorization across 27 EU countries D) No reporting
Answer: C – Passporting allows CASPs to operate EU-wide with one authorization.

Q14. Under the DLT Act, how are customer crypto assets treated in bankruptcy?
A) Part of general estate B) Segregated from bankruptcy estate C) Distributed to creditors D) Frozen
Answer: B – Customer crypto assets are segregated and protected from the bankruptcy estate.

Q15. Which market abuse practice is prohibited under MiCA?
A) Staking rewards B) Wash trading and spoofing C) Yield farming D) Liquidity provision
Answer: B – MiCA prohibits wash trading, spoofing, layering, and pump-and-dump schemes.

Quiz Questions (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation
Answer: D – The lesson mentions Ethereum, Cardano, and Tezos foundations as examples.

Q18. What is expected in MiCA 2.0 review?
A) Removal of stablecoin rules B) DeFi regulation C) Complete deregulation D) Merger with Swiss
Answer: B – MiCA 2.0 is expected to address DeFi (currently excluded), NFT fractionalization, and staking/lending.

Q19. How long is the MiCA grandfathering period for existing providers?
A) 6 months B) 12 months C) 18 months D) 24 months
Answer: C – Existing crypto service providers have an 18-month transition period to obtain CASP authorization.

Q20. Which jurisdictions are preferred for CASP licenses?
A) Spain, Portugal, Greece B) Ireland, France, Germany C) Poland, Hungary, Romania D) Malta, Cyprus
Answer: B – Ireland, France, and Germany are preferred due to established regulatory infrastructure.

L46: Swiss FINMA and EU MiCA

Condensed Mini-Lecture (10 min)

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand Swiss FINMA's principles-based approach to crypto regulation
- Analyze token classification frameworks (FINMA vs MiCA)
- Evaluate EU MiCA as comprehensive crypto-asset regulation
- Compare stablecoin requirements between frameworks

Focus: Two leading regulatory frameworks shaping global crypto policy

Why Focus on Switzerland and EU?

Switzerland (Crypto Valley)

- 1,100+ blockchain companies in Zug
- Principles-based, flexible approach
- Home to Ethereum, Cardano, Tezos
- DLT Act (2021) provides legal clarity

EU MiCA

- First comprehensive crypto framework
- 27 member states (450M people)
- Rules-based, detailed requirements
- Full implementation: Dec 30, 2024

Key Contrast: Principles-based (Switzerland) vs rules-based (EU)

(c) Joerg Osterrieder 2025

FINMA Token Classification

Three Token Categories (can overlap as hybrid tokens):

1. **Payment Tokens**: Means of payment (Bitcoin, Litecoin)
   - Regulation: AML only (not securities law)
2. **Utility Tokens**: Access to application/service (Filecoin)
   - Regulation: Minimal if truly utility
3. **Asset Tokens**: Represent claims or equity
   - Regulation: Securities law (prospectus, licensing)

Economic function determines regulatory treatment, not technology

Swiss DLT Act (2021)

Key Innovations:

- **DLT Securities**: Legal recognition of tokenized securities on blockchain
- **DLT Trading Facilities**: New license (CHF 500,000 minimum capital)
- **Crypto Asset Segregation**: Customer assets protected in bankruptcy

Impact: Legal certainty attracted 1,100+ blockchain companies to Crypto Valley (Zug), including major foundations (Ethereum, Cardano, Tezos).

Switzerland: Adapt existing law to new technology vs creating new rules

MiCA: Markets in Crypto-Assets Regulation

Timeline: Proposed 2020, Approved April 2023, Full effect December 30, 2024

Three Asset Categories:

1. **E-Money Tokens (EMTs)**: Stable value referencing single fiat (USDC, USDT)
   - Strictest regulation: banking-like requirements
2. **Asset-Referenced Tokens (ARTs)**: Basket/commodity-backed stablecoins
3. **Other Crypto-Assets**: All other tokens (BTC, ETH, utility tokens)
   - Disclosure requirements (white paper)

Scope: Crypto-assets, issuers, CASPs; Excluded: NFTs (non-fractionalized), CBDCs

MiCA: CASP Authorization

Crypto-Asset Service Providers (CASPs) require authorization for:

- Custody and administration of crypto-assets
- Operation of trading platforms
- Exchange services (crypto-fiat, crypto-crypto)
- Advice and portfolio management

Capital Requirements:

- Custody services: EUR 125,000
- Trading platforms: EUR 150,000
- Exchanges: EUR 150,000

Key Benefit: Single authorization valid across all 27 EU member states (passporting)

Stablecoin Compliance Reality (2024)

Circle (USDC)

- E-money license in France (July 2024)
- First global stablecoin MiCA-compliant
- USDC and EURC fully authorized

Tether (USDT)

- Did NOT obtain EU e-money license
- Delisted from EU exchanges (Dec 2024)
- Coinbase Europe, Crypto.com removed

EMT Requirements: 1:1 backing in high-quality liquid assets, redemption at par anytime with no fees, no interest payments allowed

Compliance as competitive advantage: USDC gaining EU market share

Swiss vs EU: Key Differences

Aspect	Switzerland	EU MiCA
Approach	Principles-based	Rules-based
Token Classification	Flexible (3 types)	Rigid (3 types)
Stablecoin Rules	Case-by-case	Banking-like
Market Access	Swiss only	27 EU countries
DeFi Treatment	Unclear	Excluded (for now)
Compliance Cost	Moderate	Higher

Strategy: Swiss firms seeking EU presence for MiCA passport; Irish, French, German licenses preferred for CASP authorization

Summary

Key Takeaways:

- **Swiss FINMA**: Principles-based, DLT Act, Crypto Valley (1,100+ companies)
- **FINMA tokens**: Payment (AML), Utility (minimal), Asset (securities)
- **EU MiCA**: Rules-based, 27 countries, full effect Dec 2024
- **MiCA tokens**: EMTs (banking-like), ARTs, Other crypto-assets
- **USDC vs USDT**: Circle MiCA-compliant; Tether delisted from EU
- **CASP passporting**: Single authorization valid EU-wide
- **Future**: MiCA 2.0 to address DeFi, NFTs, staking/lending

(c) Joerg Osterrieder 2025

Image Credits

Switzerland (Unsplash CC0)

Europe (Unsplash CC0)

Regulation (Unsplash CC0)

All images from Unsplash.com under CC0 license (free for commercial use, no attribution required).

Quiz Questions (1–3)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU
Answer: C – FINMA uses principles-based regulation focusing on economic function.

Q2. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025
Answer: C – MiCA: proposed 2020, approved 2023, fully implemented Dec 30, 2024.

Q3. Which stablecoin obtained MiCA e-money license in France (July 2024)?
A) Tether (USDT) B) Circle (USDC) C) Binance USD D) DAI
Answer: B – Circle obtained the first global stablecoin e-money license for USDC/EURC.

Quiz Questions (4–5)

Q4. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges
C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU license and was delisted from exchanges.

Q5. What is the key benefit of MiCA passporting?
A) Lower capital requirements B) Exemption from AML
C) Single authorization across 27 EU countries D) No reporting obligations
Answer: C – Passporting allows CASPs to operate EU-wide with one authorization.

Bonus: What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license with CHF 500,000 minimum capital.

Quiz: Swiss FINMA EU MiCA

Instructions: 21 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA

Quiz (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally

Quiz (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and fall under securities regulation.

Q3. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and fall under securities regulation.

Q3. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025
Answer: C – MiCA was proposed in 2020, approved in 2023, fully implemented December 30, 2024.

Q4. What is the minimum capital requirement for CASP custody services under MiCA?
A) EUR 50,000 B) EUR 125,000 C) EUR 250,000 D) EUR 750,000

Quiz (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and fall under securities regulation.

Q3. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025
Answer: C – MiCA was proposed in 2020, approved in 2023, fully implemented December 30, 2024.

Q4. What is the minimum capital requirement for CASP custody services under MiCA?
A) EUR 50,000 B) EUR 125,000 C) EUR 250,000 D) EUR 750,000
Answer: B – Custody services require EUR 125,000 minimum capital.

Q5. Which stablecoin obtained MiCA e-money license in France (July 2024)?
A) Tether (USDT) B) Circle (USD C) C) Binance USD (BUS D) D) DAI

Quiz (1–5)

Q1. What is the primary regulatory approach of Swiss FINMA?
A) Rules-based B) Technology-based C) Principles-based D) Identical to EU MiCA
Answer: C – FINMA uses a principles-based approach focusing on economic function.

Q2. Under FINMA's token classification, which tokens are subject to securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and fall under securities regulation.

Q3. When was MiCA fully implemented across the EU?
A) September 2020 B) April 2023 C) December 30, 2024 D) Expected 2025
Answer: C – MiCA was proposed in 2020, approved in 2023, fully implemented December 30, 2024.

Q4. What is the minimum capital requirement for CASP custody services under MiCA?
A) EUR 50,000 B) EUR 125,000 C) EUR 250,000 D) EUR 750,000
Answer: B – Custody services require EUR 125,000 minimum capital.

Q5. Which stablecoin obtained MiCA e-money license in France (July 2024)?
A) Tether (USDT) B) Circle (USD C) C) Binance USD (BUS D) D) DAI
Answer: B – Circle obtained the first global stablecoin e-money license for USDC and EURC.

Quiz (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant

Quiz (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license category with CHF 500,000 minimum capital.

Q8. Which of the following is excluded from MiCA's scope?
A) E-money tokens (EMTs) B) Asset-referenced tokens (ARTs) C) CBDCs D) CASPs

Quiz (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license category with CHF 500,000 minimum capital.

Q8. Which of the following is excluded from MiCA's scope?
A) E-money tokens (EMTs) B) Asset-referenced tokens (ARTs) C) CBDCs D) CASPs
Answer: C – CBDCs and non-fractionalized NFTs are excluded from MiCA.

Q9. How many blockchain companies are located in Swiss Crypto Valley (Zug)?
A) 250+ B) 500+ C) 1,000+ D) 2,000+

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license category with CHF 500,000 minimum capital.

Q8. Which of the following is excluded from MiCA's scope?
A) E-money tokens (EMTs) B) Asset-referenced tokens (ARTs) C) CBDCs D) CASPs
Answer: C – CBDCs and non-fractionalized NFTs are excluded from MiCA.

Q9. How many blockchain companies are located in Swiss Crypto Valley (Zug)?
A) 250+ B) 500+ C) 1,000+ D) 2,000+
Answer: C – Over 1,000 blockchain companies (1,100+ as of 2024), including Ethereum, Cardano, Tezos.

Q10. Under MiCA, what is required for E-Money Token (EMT) redemption?
A) 2-day settlement B) Up to 5% fee C) Redeem at par anytime, no fees D) 30-day holding

Quiz (6–10)

Q6. What happened to USDT in the EU following MiCA implementation?
A) Granted e-money license B) Delisted from EU exchanges C) Automatically grandfathered D) Became dominant
Answer: B – Tether did NOT obtain an EU e-money license and was delisted from exchanges.

Q7. What is the minimum capital for a Swiss DLT Trading Facility?
A) CHF 100,000 B) CHF 250,000 C) CHF 500,000 D) CHF 1,000,000
Answer: C – The DLT Act introduced this license category with CHF 500,000 minimum capital.

Q8. Which of the following is excluded from MiCA's scope?
A) E-money tokens (EMTs) B) Asset-referenced tokens (ARTs) C) CBDCs D) CASPs
Answer: C – CBDCs and non-fractionalized NFTs are excluded from MiCA.

Q9. How many blockchain companies are located in Swiss Crypto Valley (Zug)?
A) 250+ B) 500+ C) 1,000+ D) 2,000+
Answer: C – Over 1,000 blockchain companies (1,100+ as of 2024), including Ethereum, Cardano, Tezos.

Q10. Under MiCA, what is required for E-Money Token (EMT) redemption?
A) 2-day settlement B) Up to 5% fee C) Redeem at par anytime, no fees D) 30-day holding
Answer: C – EMTs must be redeemable at par value at any time with no redemption fees.

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights

Quiz (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens

Quiz (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens
Answer: C – Utility tokens have minimal regulation compared to payment (AML) and asset (securities law).

Q13. What is the key benefit of MiCA passporting?
A) Lower capital B) Exemption from AML C) Single authorization across 27 EU countries D) No reporting

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens
Answer: C – Utility tokens have minimal regulation compared to payment (AML) and asset (securities law).

Q13. What is the key benefit of MiCA passporting?
A) Lower capital B) Exemption from AML C) Single authorization across 27 EU countries D) No reporting
Answer: C – Passporting allows CASPs to operate EU-wide with one authorization.

Q14. Under the DLT Act, how are customer crypto assets treated in bankruptcy?
A) Part of general estate B) Segregated from bankruptcy estate C) Distributed to creditors D) Frozen

Quiz (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens
Answer: C – Utility tokens have minimal regulation compared to payment (AML) and asset (securities law).

Q13. What is the key benefit of MiCA passporting?
A) Lower capital B) Exemption from AML C) Single authorization across 27 EU countries D) No reporting
Answer: C – Passporting allows CASPs to operate EU-wide with one authorization.

Q14. Under the DLT Act, how are customer crypto assets treated in bankruptcy?
A) Part of general estate B) Segregated from bankruptcy estate C) Distributed to creditors D) Frozen
Answer: B – Customer crypto assets are segregated and protected from the bankruptcy estate.

Q15. Which market abuse practice is prohibited under MiCA?
A) Staking rewards B) Wash trading and spoofing C) Yield farming D) Liquidity provision

Quiz (11–15)

Q11. What is prohibited for stablecoins under MiCA?
A) Cross-border transfers B) Interest payments C) Fiat currency backing D) Redemption rights
Answer: B – MiCA explicitly prohibits interest payments on stablecoins to prevent bank-like activities.

Q12. Which FINMA token type is subject to the LEAST regulation?
A) Payment tokens B) Asset tokens C) Utility tokens D) Hybrid tokens
Answer: C – Utility tokens have minimal regulation compared to payment (AML) and asset (securities law).

Q13. What is the key benefit of MiCA passporting?
A) Lower capital B) Exemption from AML C) Single authorization across 27 EU countries D) No reporting
Answer: C – Passporting allows CASPs to operate EU-wide with one authorization.

Q14. Under the DLT Act, how are customer crypto assets treated in bankruptcy?
A) Part of general estate B) Segregated from bankruptcy estate C) Distributed to creditors D) Frozen
Answer: B – Customer crypto assets are segregated and protected from the bankruptcy estate.

Q15. Which market abuse practice is prohibited under MiCA?
A) Staking rewards B) Wash trading and spoofing C) Yield farming D) Liquidity provision
Answer: B – MiCA prohibits wash trading, spoofing, layering, and pump-and-dump schemes.

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement

Quiz (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation

Quiz (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation
Answer: D – The lesson mentions Ethereum, Cardano, and Tezos foundations as examples.

Q18. What is expected in MiCA 2.0 review?
A) Removal of stablecoin rules B) DeFi regulation C) Complete deregulation D) Merger with Swiss

Quiz (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation
Answer: D – The lesson mentions Ethereum, Cardano, and Tezos foundations as examples.

Q18. What is expected in MiCA 2.0 review?
A) Removal of stablecoin rules B) DeFi regulation C) Complete deregulation D) Merger with Swiss
Answer: B – MiCA 2.0 is expected to address DeFi (currently excluded), NFT fractionalization, and staking/lending.

Q19. How long is the MiCA grandfathering period for existing providers?
A) 6 months B) 12 months C) 18 months D) 24 months

Quiz (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation
Answer: D – The lesson mentions Ethereum, Cardano, and Tezos foundations as examples.

Q18. What is expected in MiCA 2.0 review?
A) Removal of stablecoin rules B) DeFi regulation C) Complete deregulation D) Merger with Swiss
Answer: B – MiCA 2.0 is expected to address DeFi (currently excluded), NFT fractionalization, and staking/lending.

Q19. How long is the MiCA grandfathering period for existing providers?
A) 6 months B) 12 months C) 18 months D) 24 months
Answer: C – Existing crypto service providers have an 18-month transition period to obtain CASP authorization.

Q20. Which jurisdictions are preferred for CASP licenses?
A) Spain, Portugal, Greece B) Ireland, France, Germany C) Poland, Hungary, Romania D) Malta, Cyprus

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What must EMT issuers maintain as reserve backing?
A) 50% fiat, 50% crypto B) 1:1 backing in high-quality liquid assets C) Fractional (30%) D) No requirement
Answer: B – EMT issuers must maintain 1:1 backing in high-quality liquid assets, segregated, with daily reconciliation.

Q17. Which organization founded in Switzerland is NOT mentioned in the lesson?
A) Ethereum Foundation B) Cardano Foundation C) Tezos Foundation D) Bitcoin Foundation
Answer: D – The lesson mentions Ethereum, Cardano, and Tezos foundations as examples.

Q18. What is expected in MiCA 2.0 review?
A) Removal of stablecoin rules B) DeFi regulation C) Complete deregulation D) Merger with Swiss
Answer: B – MiCA 2.0 is expected to address DeFi (currently excluded), NFT fractionalization, and staking/lending.

Q19. How long is the MiCA grandfathering period for existing providers?
A) 6 months B) 12 months C) 18 months D) 24 months
Answer: C – Existing crypto service providers have an 18-month transition period to obtain CASP authorization.

Q20. Which jurisdictions are preferred for CASP licenses?
A) Spain, Portugal, Greece B) Ireland, France, Germany C) Poland, Hungary, Romania D) Malta, Cyprus
Answer: B – Ireland, France, and Germany are preferred due to established regulatory infrastructure.

(c) Joerg Osterrieder 2025

Q21. Under FINMA, which tokens fall under securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally

Quiz (21–21)

Q21. Under FINMA, which tokens fall under securities law?
A) Payment tokens B) Utility tokens C) Asset tokens D) All tokens equally
Answer: C – Asset tokens represent claims/equity and require securities regulation.

L47: CBDCs and Future Trends

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand Central Bank Digital Currencies (CBDCs)
- Compare retail vs wholesale CBDC designs
- Analyze privacy vs surveillance tradeoffs
- Evaluate China e-CNY and Digital Euro progress
- Identify key future trends in blockchain technology
- Assess career opportunities in the blockchain space

The Problem: How should governments regulate crypto?

Part 3/4: CBDCs & Future

The Challenge

As cryptocurrencies threaten monetary sovereignty and stablecoins gain adoption, central banks face a critical question: Should governments create their own digital currencies, and how can they balance innovation with control?

Why It Matters

- Without CBDCs, private stablecoins could displace national currencies
- China's e-CNY already has 260M+ wallets, potentially challenging USD dominance

What We Need

- Risk management and mitigation
- Understanding CBDC design choices and fundamental trade-offs (privacy vs. control)

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How CBDCs address monetary sovereignty while introducing new privacy and surveillance challenges

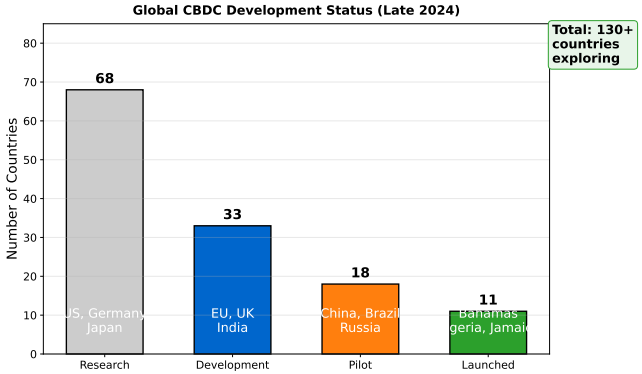
What is a CBDC?

Definition: Digital central bank money
Key Characteristics:

- Legal tender status
- Central bank liability
- Electronic/digital form
- May use DLT (not required)

Not Cryptocurrency:
Centrally issued and controlled
Motivation:
Cash decline, stablecoins, inclusion
Status:
130+ countries (90% global GDP)

Global CBDC Development Status



130+ countries exploring CBDCs, representing 90% of global GDP

Retail vs Wholesale CBDCs

Aspect	Retail CBDC	Wholesale CBDC
Users	General public	Financial institutions
Use Case	Payments, store of value	Interbank settlement
Access	Widely accessible	Restricted to banks
Technology	Various (may use DLT)	Likely DLT (efficiency)
Privacy	Balance privacy vs AML	Less concern
Examples	e-CNY, Digital Euro	mBridge, Project Jasper

Focus: Retail CBDCs have greater societal impact and complexity

Privacy vs Surveillance Tradeoff

Privacy Concerns

- Central bank sees all transactions
- Government surveillance potential
- Social credit system risks
- No cash-like anonymity

Privacy Technologies

- Zero-knowledge proofs
- Tiered privacy (small anonymous, large KYC)

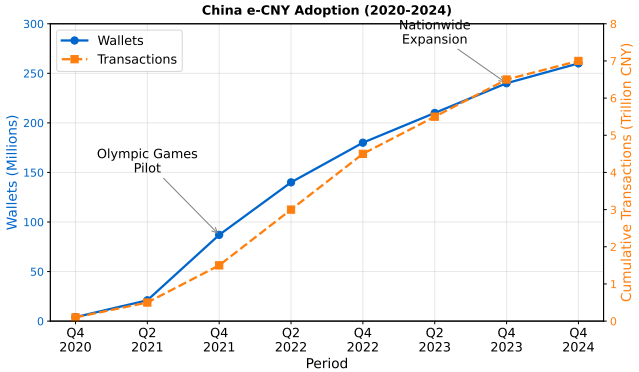
AML/CFT Requirements

- Full anonymity enables illicit finance
- Regulatory pressure (FATF)
- Tax enforcement needs

Design Spectrum

- **Full Surveillance**: China e-CNY
- **Balanced**: Digital Euro
- **Privacy-First**: Unlikely in practice

China e-CNY Adoption



Largest CBDC pilot globally, 260M+ wallets by late 2024

Case Study: China's e-CNY

Architecture:

- Two-tier: PBOC + banks
- Centralized database
- Largest pilot (2020-present)

Features:

- Dual offline payment
- Programmable (smart contracts)
- "Controllable anonymity"

2024 Stats:

- 260M+ wallets
- 7T+ yuan transactions

Implications:

- Challenge USD dominance
- Surveillance concerns
- Competes with Alipay/WeChat

Case Study: Digital Euro

Status: Prep phase (2024-2026)
Design Principles:

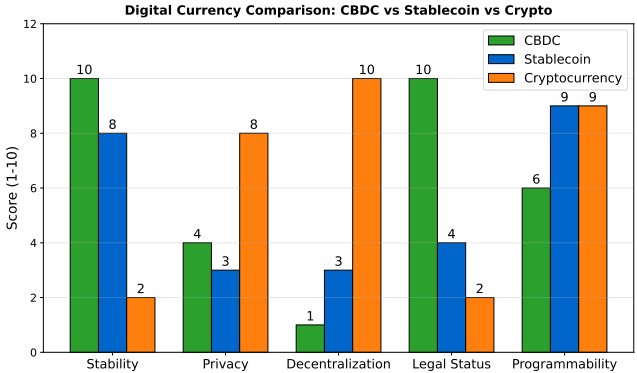
- Privacy-focused (¿ e-CNY)
- Offline capability
- Free for basic use
- Banks distribute

Privacy Model:

- Small tx: cash-like privacy
- Large tx: full AML compliance

Timeline:
Decision late 2025, rollout 2027-2028
Motivation:
Monetary sovereignty, counter stablecoins

Digital Currency Comparison



CBDCs may crowd out stablecoins but not cryptocurrencies (different use cases)

Cross-Border CBDC: mBridge

mBridge: Multi-CBDC platform
Participants:
China, HK, Thailand, UAE, Saudi
Benefits vs SWIFT:

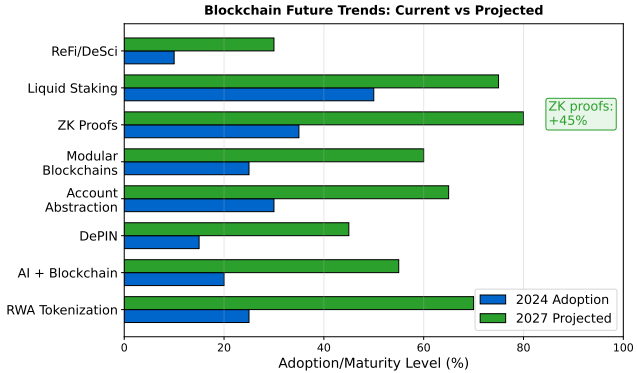
- Instant (vs 2-5 days)
- Lower costs
- 24/7 operation

Technology:
Permissioned blockchain
Status:
MVP June 2024, live transactions
Geopolitics:

- Bypass USD/SWIFT
- BRICS alternative system

(c) Joerg Osterrieder 2025

Future Trends: Current vs Projected



ZK proofs, liquid staking, and RWA tokenization showing strongest growth

Trend 1: Institutional Adoption Acceleration

2024 Drivers:

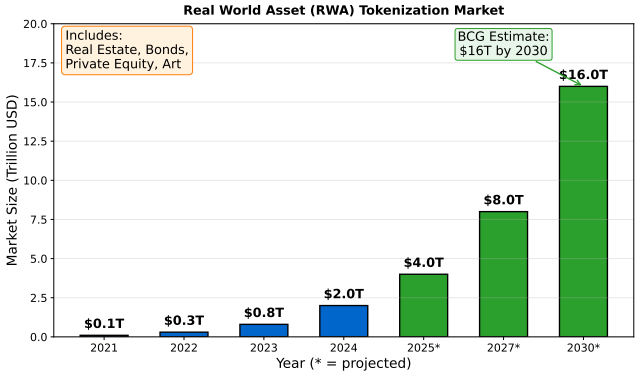
- Bitcoin ETFs (Jan 2024)
- Ethereum ETFs (Jul 2024)
- MiCA, Swiss frameworks
- Custody: Coinbase, Fidelity

Products:

- Tokenized securities
- Crypto lending/prime brokerage
- CME futures, options

Impact:
$1T+ institutional capital by 2030

RWA Tokenization Market Growth



Real world asset tokenization projected to reach $16T by 2030 (BCG estimate)

Trend 2: RWA Tokenization

Definition:
Representing real assets on blockchain
Asset Classes:

- Real estate (fractional)
- Private equity, VC
- Bonds (govt, corporate)
- Commodities, carbon credits

Advantages:

- Fractional ownership
- 24/7 trading
- Programmable compliance

Leaders:
Centrifuge, Ondo, Securitize, tZERO

BCG projects $16T RWA tokenization by 2030

Trend 3: AI + Blockchain Convergence

AI for Blockchain:

- Smart contract auditing
- MEV optimization
- DeFi risk modeling
- On-chain analytics

Blockchain for AI:

- Decentralized AI training
- Verifiable AI models
- AI agent payments
- Data marketplaces

Projects:
Fetch.ai, SingularityNET, Render, Bittensor

Two-way synergy: AI improves blockchain, blockchain decentralizes AI

(c) Joerg Osterrieder 2025

Trend 4: Zero-Knowledge Proofs Everywhere

ZK Maturation:
From research to production
Applications:

- ZK-Rollups: StarkNet, zkSync
- Privacy: Aztec, Railgun
- Identity: prove age w/o birthdate
- Compliance: private proofs

Technology:

- ZK ASICs (faster proofs)
- Polygon zkEVM, Scroll
- SNARKs vs STARKs tradeoffs

Impact:
Privacy + scalability without compromise

ZK technology enables proving statements without revealing underlying data

Emerging Risks and Challenges

Quantum Computing:

- ECDSA vulnerable (10-20 yr)
- Post-quantum migration needed

Regulatory Fragmentation:

- Conflicting national rules
- Compliance complexity

Centralization Creep:

- Lido: 30%+ staked ETH
- MEV/Flashbots dominance

Systemic DeFi Risk:

- Composability = cascading failures
- Protocol interdependencies

All risks require proactive mitigation strategies from the ecosystem

(c) Joerg Osterrieder 2025

Career Paths in Blockchain (2025+)

Technical Roles

- Smart contract developer
- Blockchain protocol engineer
- Security auditor
- ZK cryptographer

Finance/Economics

- DeFi analyst
- Tokenomics designer
- Crypto trader/quant

Legal/Compliance

- Crypto regulatory specialist
- AML/CFT compliance officer
- Web3 lawyer

Business/Product

- Web3 product manager
- DAO operations
- Community manager

Demand: 50,000+ open blockchain jobs, growing 30%+ annually

Problem Solved? CBDCs & Future

The Original Problem

How should governments regulate crypto?

How CBDCs Address It

- **Retail CBDCs**: Provide digital cash alternative (e-CNY, Digital Euro) competing with private stablecoins
- **Wholesale CBDCs**: Enable efficient cross-border settlement (mBridge) with programmable policy tools
- **Design flexibility**: Tiered privacy models balance AML compliance with cash-like anonymity for small transactions

Remaining Limitations

- **Privacy vs surveillance**: "Controllable anonymity" enables government tracking of all transactions (China model)
- **Bank disintermediation**: CBDCs could reduce role of commercial banks in monetary system

Open Questions

- Will CBDCs coexist with or displace cryptocurrencies and stablecoins?
- Risk: Quantum computing threatens ECDSA signatures (10-20 year horizon)

CBDCs provide government control over digital money but sacrifice privacy and may disrupt banking systems

Summary

CBDCs:

- 130+ countries (90% GDP)
- Privacy vs surveillance tradeoff
- e-CNY: 260M+ wallets
- Digital Euro: decision late 2025
- mBridge: cross-border MVP 2024

Future Trends:

- RWA tokenization: $16T by 2030
- ZK proofs: privacy + scalability
- AI + Blockchain synergies
- 50,000+ blockchain jobs

CBDCs and emerging trends will reshape global finance

Questions for Reflection

1. What are the key differences between retail and wholesale CBDCs?
2. How should CBDCs balance privacy and AML compliance?
3. Why might e-CNY adoption remain limited despite government push?
4. Which future trend (RWA, ZK, AI+Blockchain) has most potential?
5. How might mBridge affect the global financial system?

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q4. What is China's CBDC called?
A) Digital Yuan B) e-CNY C) China Coin D) PBOC Token
Answer: B – China's CBDC is officially called e-CNY (electronic Chinese Yuan).

Q5. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets by late 2024, the largest CBDC pilot globally.

Quiz Questions (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – The Digital Euro decision is expected late 2025, with rollout planned for 2027-2028.

Q9. How does the Digital Euro handle privacy for small transactions?
A) Full KYC required B) Cash-like privacy C) No privacy D) Blockchain transparency
Answer: B – Small transactions get cash-like privacy; large transactions require full AML compliance.

Q10. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Quiz Questions (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q14. Which is NOT an advantage of RWA tokenization?
A) Fractional ownership B) 24/7 trading C) Guaranteed profits D) Programmable compliance
Answer: C – Tokenization offers fractional ownership, 24/7 trading, and programmable compliance, but not guaranteed profits.

Q15. What percentage of staked ETH does Lido control, raising centralization concerns?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating validator concentration concerns.

Quiz Questions (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%
Answer: B – There are 50,000+ open blockchain jobs with 30%+ annual growth.

Q19. Which is NOT mentioned as an AI + Blockchain convergence use case?
A) Smart contract auditing B) Decentralized AI training C) Physical robot control D) AI agent payments
Answer: C – The lesson covers smart contract auditing, decentralized AI training, and AI agent payments, but not physical robot control.

Q20. What feature does e-CNY support that does NOT require internet connection?
A) International transfers B) Dual offline payment C) Smart contract execution D) Real-time auditing
Answer: B – e-CNY supports dual offline payment capability, allowing transactions without internet connection.

(c) Joerg Osterrieder 2025

L47: CBDCs and Future Trends

Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

CBDCs in a Nutshell

- "We created Bitcoin to escape central bank control." – Satoshi's vision
- "We'll create our own cryptocurrency." – Central banks worldwide

[COMIC: "Government cryptocurrency" irony – A central banker proudly presents "Our Decentralized Digital Currency" on a screen. The code shows: "if (government.says.freeze) { freeze(wallet); }". Satoshi's ghost facepalms in the corner.]

[PLACEHOLDER] — CBDCs represent governments entering the digital currency space they once dismissed

Learning Objectives

- Understand Central Bank Digital Currencies (CBDCs)
- Compare retail vs wholesale CBDC designs
- Analyze privacy vs surveillance tradeoffs
- Evaluate China e-CNY and Digital Euro progress
- Identify key future trends in blockchain technology
- Assess career opportunities in the blockchain space

Building on L46: Swiss FINMA and EU MiCA

The Problem: How should governments regulate crypto?

Part 3/4: CBDCs & Future

The Challenge

As cryptocurrencies threaten monetary sovereignty and stablecoins gain adoption, central banks face a critical question: Should governments create their own digital currencies, and how can they balance innovation with control?

Why It Matters

- Without CBDCs, private stablecoins could displace national currencies
- China's e-CNY already has 260M+ wallets, potentially challenging USD dominance

What We Need

- Risk management and mitigation
- Understanding CBDC design choices and fundamental trade-offs (privacy vs. control)

The Cryptoeconomics Question

Managing systemic and idiosyncratic risks

Today's lesson: How CBDCs address monetary sovereignty while introducing new privacy and surveillance challenges

What Are Central Bank Digital Currencies?

Definition: CBDC (Central Bank Digital Currency)—digital money issued directly by a nation's central bank

Key Characteristics:

- Legal tender status
- Central bank liability
- Electronic/digital form
- May use DLT (not required)

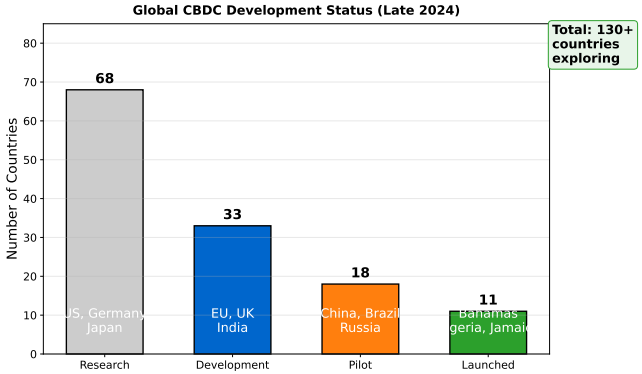
Not Cryptocurrency:
Centrally issued and controlled

Motivation:
Cash decline, stablecoins, inclusion

Status:
130+ countries (90% global GDP)

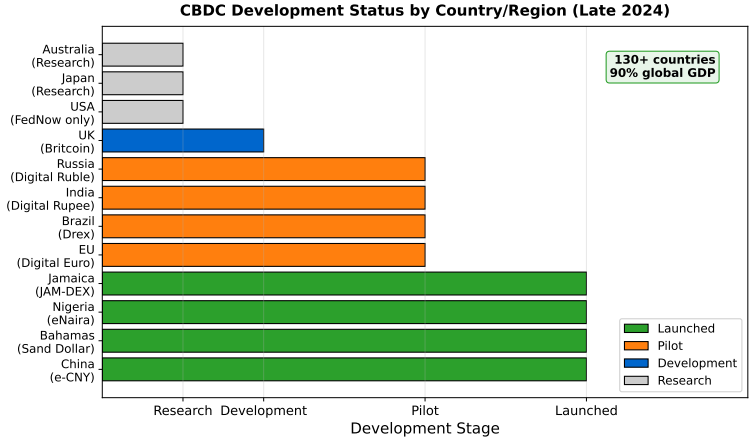
→ *Problem: How should governments regulate crypto? — What is a CBDC? CBDCs represent governments entering the digital currency space—regulate by competing rather than just restricting*

Which Countries Are Developing CBDCs?



130+ countries exploring CBDCs, representing 90% of global GDP

CBDC Development by Country



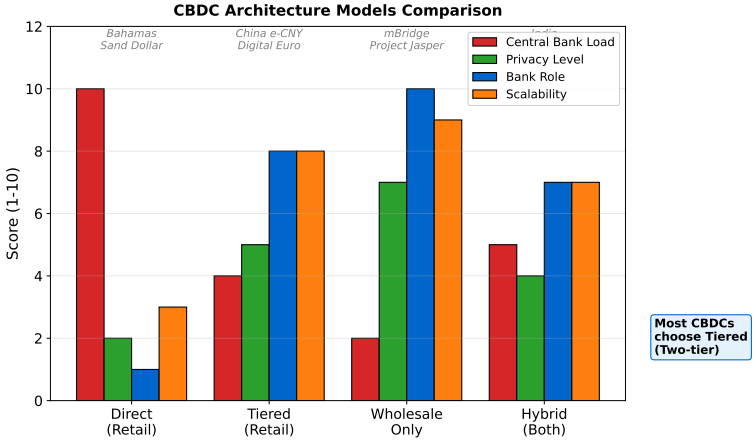
China leads with launched e-CNY; EU and India in pilot phase; US limited to FedNow (not a CBDC)

What's the Difference Between Retail and Wholesale CBDCs?

Aspect	Retail CBDC	Wholesale CBDC
Users	General public	Financial institutions
Use Case	Payments, store of value	Interbank settlement
Access	Widely accessible	Restricted to banks
Technology	Various (may use DLT)	Likely DLT (efficiency)
Privacy	Balance privacy vs AML	Less concern
Examples	e-CNY, Digital Euro	mBridge, Project Jasper

Focus: Retail CBDCs have greater societal impact and complexity

How Are CBDCs Architecturally Structured?



Most CBDCs use two-tier (tiered) architecture: central bank wholesale, commercial banks retail

How Do CBDCs Balance Privacy and Surveillance?

Privacy Concerns

- Central bank sees all transactions
- Government surveillance potential
- Social credit system risks
- No cash-like anonymity

Privacy Technologies

- Zero-knowledge proofs (cryptographic methods that prove a statement is true without revealing the underlying data)
- Tiered privacy (small anonymous, large KYC)

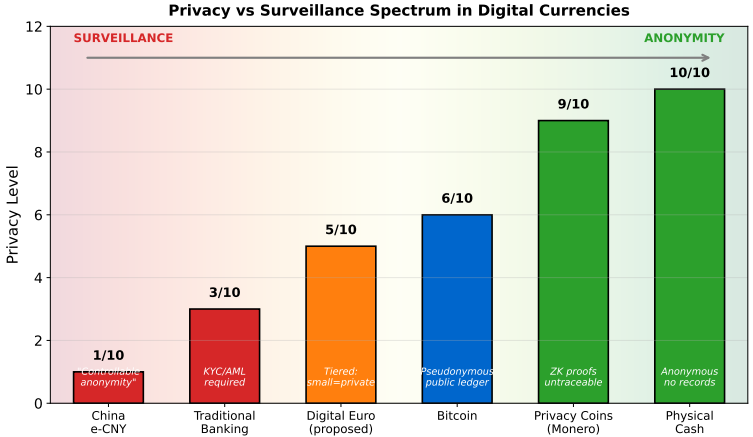
AML/CFT Requirements

- Full anonymity enables illicit finance
- Regulatory pressure (FATF)
- Tax enforcement needs

Design Spectrum

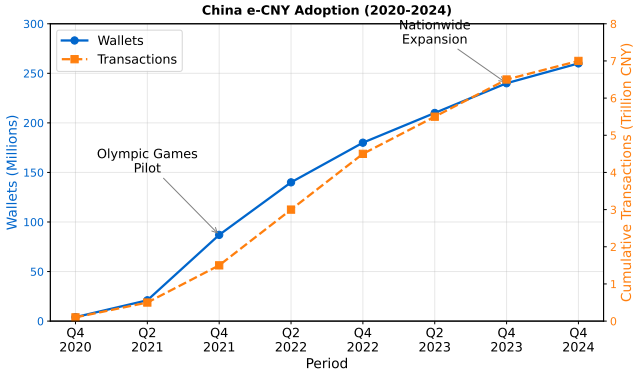
- **Full Surveillance**: China e-CNY
- **Balanced**: Digital Euro
- **Privacy-First**: Unlikely in practice

Privacy Spectrum: CBDCs vs Alternatives



CBDCs offer less privacy than cash or crypto; Digital Euro aims for tiered model with privacy for small transactions

China e-CNY Adoption



Largest CBDC pilot globally, 260M+ wallets by late 2024 | → Problem: How should governments regulate crypto? — China e-CNY Adoption China's "controllable anonymity" shows one answer: full government visibility with programmable policy tools

How Does China's e-CNY Work?

Architecture:

- Two-tier: PBOC (People's Bank of China, the central bank) + commercial banks
- Centralized database
- Largest pilot (2020-present)

Features:

- Dual offline payment
- Programmable (smart contracts)
- "Controllable anonymity"

2024 Stats:

- 260M+ wallets
- 7T+ yuan transactions

Implications:

- Challenge USD dominance
- Surveillance concerns
- Competes with Alipay/WeChat

What is the Digital Euro's Design?

Status: Prep phase (2024-2026)
Design Principles:

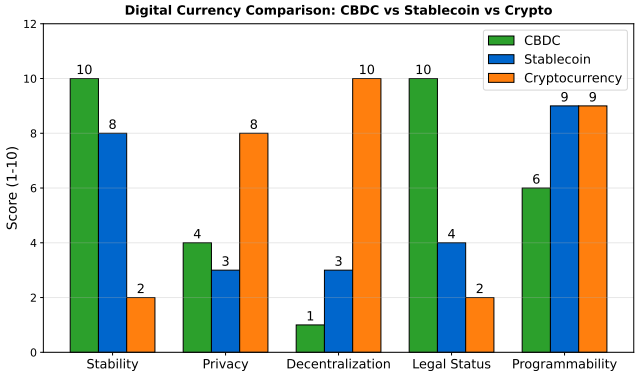
- Privacy-focused (¿ e-CNY)
- Offline capability
- Free for basic use
- Banks distribute

Privacy Model:

- Small tx: cash-like privacy
- Large tx: full AML compliance

Timeline:
Decision late 2025, rollout 2027-2028
Motivation:
Monetary sovereignty, counter stablecoins

Digital Currency Comparison



CBDCs may crowd out stablecoins but not cryptocurrencies (different use cases)

How Does mBridge Enable Cross-Border Payments?

mBridge: Multi-CBDC platform (a cross-border payment system allowing direct central bank digital currency exchanges between participating countries)
Participants:
China, HK, Thailand, UAE, Saudi
Benefits vs SWIFT:

- Instant (vs 2-5 days)
- Lower costs
- 24/7 operation

Technology:
Permissioned blockchain
Status:
MVP June 2024, live transactions
Geopolitics:

- Bypass USD/SWIFT
- BRICS alternative system

→ *Problem: How should governments regulate crypto? — Cross-Border CBDC: mBridge mBridge enables cross-border settlement outside SWIFT—a geopolitical dimension to the regulatory question*

Problem Check-In: CBDCs & Future

Recall Our Problem

How should governments regulate crypto?

What We've Learned So Far

- CBDCs are central bank-issued digital money—not crypto, but competing with private stablecoins for digital payment dominance
- Privacy vs. surveillance tradeoff: China (full visibility) vs. Digital Euro (tiered privacy for small transactions)
- CBDCs offer an alternative approach: governments create compliant digital money rather than regulating private alternatives

Still to Address

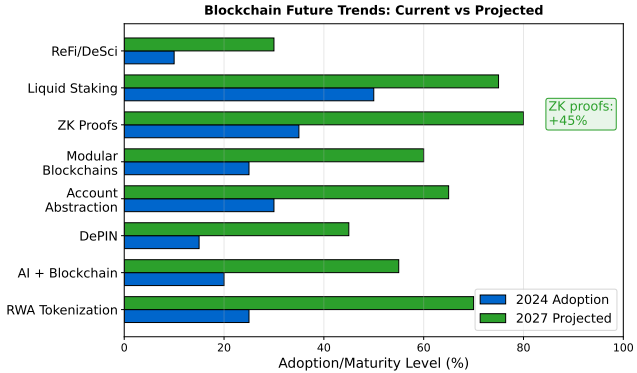
- Future trends: RWA tokenization ($16T by 2030), ZK proofs enabling privacy + compliance, AI + blockchain convergence
- Will CBDCs coexist with crypto, or will governments use them to crowd out private digital currencies?

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How should governments regulate crypto?"?

Future Trends: Current vs Projected



ZK proofs, liquid staking, and RWA tokenization showing strongest growth

Why Are Institutions Entering Crypto Now?

2024 Drivers:

- Bitcoin ETFs (Jan 2024)
- Ethereum ETFs (Jul 2024)
- MiCA, Swiss frameworks
- Custody: Coinbase, Fidelity

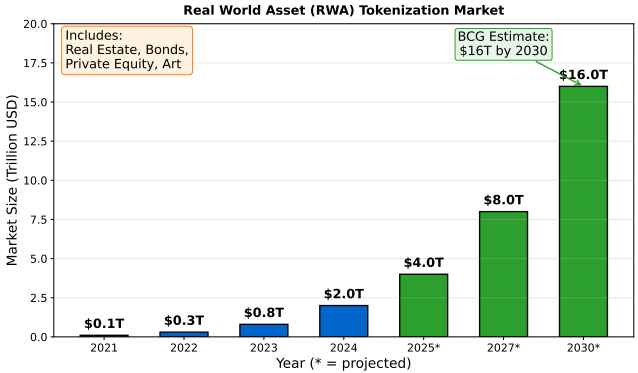
Products:

- Tokenized securities
- Crypto lending/prime brokerage
- CME futures, options

Impact:
$1T+ institutional capital by 2030

(c) Joerg Osterrieder 2025

RWA Tokenization Market Growth



Real world asset tokenization projected to reach $16T by 2030 (BCG estimate)

What is Real-World Asset Tokenization?

Definition:
RWA tokenization means representing real-world assets (real estate, bonds, commodities) as blockchain tokens

Asset Classes:

- Real estate (fractional)
- Private equity, VC
- Bonds (govt, corporate)
- Commodities, carbon credits

Advantages:

- Fractional ownership
- 24/7 trading
- Programmable compliance

Leaders:
Centrifuge, Ondo, Securitize, tZERO

BCG projects $16T RWA tokenization by 2030 | → Problem: How should governments regulate crypto? — Trend 2: RWA Tokenization RWA tokenization creates regulated securities on blockchain—bridging TradFi and DeFi under existing frameworks

How Are AI and Blockchain Converging?

AI for Blockchain:

- Smart contract auditing
- MEV optimization
- DeFi risk modeling
- On-chain analytics

Blockchain for AI:

- Decentralized AI training
- Verifiable AI models
- AI agent payments
- Data marketplaces

Projects:
Fetch.ai, SingularityNET, Render, Bittensor

Two-way synergy: AI improves blockchain, blockchain decentralizes AI

Why Are Zero-Knowledge Proofs Important?

ZK Maturation:
From research to production
Applications:

- ZK-Rollups (Layer 2 scaling solutions using zero-knowledge proofs to batch transactions): StarkNet, zkSync
- Privacy: Aztec, Railgun
- Identity: prove age w/o birthdate
- Compliance: private proofs

Technology:

- ZK ASICs (faster proofs)
- Polygon zkEVM, Scroll
- SNARKs vs STARKs tradeoffs

Impact:
Privacy + scalability without compromise

ZK technology enables proving statements without revealing underlying data

What Are the Emerging Risks for Crypto?

Quantum Computing:

- ECDSA (Elliptic Curve Digital Signature Algorithm, the cryptographic method securing most blockchain wallets) vulnerable (10-20 yr)
- Post-quantum migration needed

Regulatory Fragmentation:

- Conflicting national rules
- Compliance complexity

Centralization Creep:

- Lido: 30%+ staked ETH
- MEV/Flashbots dominance

Systemic DeFi Risk:

- Composability = cascading failures
- Protocol interdependencies

All risks require proactive mitigation strategies from the ecosystem

What Career Opportunities Exist in Blockchain?

Technical Roles

- Smart contract developer
- Blockchain protocol engineer
- Security auditor
- ZK cryptographer

Finance/Economics

- DeFi analyst
- Tokenomics designer
- Crypto trader/quant

Legal/Compliance

- Crypto regulatory specialist
- AML/CFT compliance officer
- Web3 lawyer

Business/Product

- Web3 product manager
- DAO operations
- Community manager

Demand: 50,000+ open blockchain jobs, growing 30%+ annually

Problem Solved? CBDCs & Future

The Original Problem

How should governments regulate crypto?

How CBDCs Address It

- **Retail CBDCs**: Provide digital cash alternative (e-CNY, Digital Euro) competing with private stablecoins
- **Wholesale CBDCs**: Enable efficient cross-border settlement (mBridge) with programmable policy tools
- **Design flexibility**: Tiered privacy models balance AML compliance with cash-like anonymity for small transactions

Remaining Limitations

- **Privacy vs surveillance**: "Controllable anonymity" enables government tracking of all transactions (China model)
- **Bank disintermediation**: CBDCs could reduce role of commercial banks in monetary system

Open Questions

- Will CBDCs coexist with or displace cryptocurrencies and stablecoins?
- Risk: Quantum computing threatens ECDSA signatures (10-20 year horizon)

CBDCs provide government control over digital money but sacrifice privacy and may disrupt banking systems

The Economics of CBDCs & Future

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: CBDCs & Future

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: CBDCs & Future

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

(c) Joerg Osterrieder 2025

CBDCs: The Tradeoff

- CBDCs offer convenience: instant payments, programmable money, financial inclusion
- The cost: Every transaction visible to the government

[COMIC: "Privacy vs surveillance tension" – Split panel. Left: "Cash" – Person buys coffee, no one watching. Right: "CBDC" – Same purchase, but a government eye watches from the receipt: "Coffee, 9:03 AM, Location: Main St, Social Credit: -0.1 (excessive caffeine)"]

[PLACEHOLDER] — The fundamental CBDC tradeoff: convenience and policy tools vs. financial privacy

Summary

CBDCs:

- 130+ countries (90% GDP)
- Privacy vs surveillance tradeoff
- e-CNY: 260M+ wallets
- Digital Euro: decision late 2025
- mBridge: cross-border MVP 2024

Next Lesson: L48 – Course Synthesis

Future Trends:

- RWA tokenization: $16T by 2030
- ZK proofs: privacy + scalability
- AI + Blockchain synergies
- 50,000+ blockchain jobs

CBDCs and emerging trends will reshape global finance

Questions for Reflection

1. What are the key differences between retail and wholesale CBDCs?
2. How should CBDCs balance privacy and AML compliance?
3. Why might e-CNY adoption remain limited despite government push?
4. Which future trend (RWA, ZK, AI+Blockchain) has most potential?
5. How might mBridge affect the global financial system?

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q4. What is China's CBDC called?
A) Digital Yuan B) e-CNY C) China Coin D) PBOC Token
Answer: B – China's CBDC is officially called e-CNY (electronic Chinese Yuan).

Q5. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets by late 2024, the largest CBDC pilot globally.

Quiz Questions (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – The Digital Euro decision is expected late 2025, with rollout planned for 2027-2028.

Q9. How does the Digital Euro handle privacy for small transactions?
A) Full KYC required B) Cash-like privacy C) No privacy D) Blockchain transparency
Answer: B – Small transactions get cash-like privacy; large transactions require full AML compliance.

Q10. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Quiz Questions (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q14. Which is NOT an advantage of RWA tokenization?
A) Fractional ownership B) 24/7 trading C) Guaranteed profits D) Programmable compliance
Answer: C – Tokenization offers fractional ownership, 24/7 trading, and programmable compliance, but not guaranteed profits.

Q15. What percentage of staked ETH does Lido control, raising centralization concerns?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating validator concentration concerns.

Quiz Questions (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%
Answer: B – There are 50,000+ open blockchain jobs with 30%+ annual growth.

Q19. Which is NOT mentioned as an AI + Blockchain convergence use case?
A) Smart contract auditing B) Decentralized AI training C) Physical robot control D) AI agent payments
Answer: C – The lesson covers smart contract auditing, decentralized AI training, and AI agent payments, but not physical robot control.

Q20. What feature does e-CNY support that does NOT require internet connection?
A) International transfers B) Dual offline payment C) Smart contract execution D) Real-time auditing
Answer: B – e-CNY supports dual offline payment capability, allowing transactions without internet connection.

(c) Joerg Osterrieder 2025

L47: CBDCs and Future Trends

Mini-Lecture — Module G: Regulation & Future

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Learning Objectives

- Understand Central Bank Digital Currencies (CBDCs)
- Compare retail vs wholesale CBDC designs
- Analyze privacy vs surveillance tradeoffs
- Evaluate e-CNY and Digital Euro progress
- Identify key future trends in blockchain

Focus: CBDCs fundamentals and future blockchain trajectory

What is a CBDC?

Definition: Digital form of central bank money (fiat currency)

Key Characteristics:

- Legal tender status – government-backed
- Liability of central bank (not commercial bank)
- Electronic/digital form (not physical cash)
- May use DLT (but not required)

Status: 130+ countries exploring CBDCs (90% of global GDP)

Not cryptocurrency: CBDCs are centrally issued and controlled

Retail vs Wholesale CBDCs

Aspect	Retail CBDC	Wholesale CBDC
Users	General public	Financial institutions
Use Case	Payments, store of value	Interbank settlement
Access	Widely accessible	Restricted to banks
Privacy	Balance privacy vs AML	Less concern
Examples	e-CNY, Digital Euro	mBridge, Project Jasper

Key Insight: Retail CBDCs have greater societal impact and complexity

Retail = consumer-facing; Wholesale = bank-to-bank

Privacy vs Surveillance Tradeoff

Privacy Concerns

- Central bank visibility
- Government surveillance potential
- No cash-like anonymity

Privacy Solutions

- Zero-knowledge proofs
- Tiered privacy (small = anonymous)

AML/CFT Requirements

- Full anonymity enables crime
- FATF regulatory pressure
- Tax enforcement needs

Design Spectrum

- **Full Surveillance**: e-CNY
- **Balanced**: Digital Euro

Core CBDC design challenge: balancing privacy with compliance

Case Study: China's e-CNY

Status: Largest CBDC pilot globally (2020–present)

Key Features:

- Two-tier architecture (PBOC wholesale, banks retail)
- Dual offline payment (no internet required)
- "Controllable anonymity" (PBOC sees all transactions)

2024 Stats: 260M+ wallets, 7T+ yuan cumulative transactions

Geopolitical Angle: Potential challenge to USD dominance

Concerns: surveillance capability, limited daily usage vs Alipay/WeChat

Case Study: Digital Euro

Status: Preparation phase (2024–2026)

Design Principles:

- Privacy-focused (stronger than e-CNY)
- Offline capability (like cash)
- Free for basic use
- Intermediated model (banks distribute)

Privacy Model:

- Small transactions: Cash-like privacy
- Large transactions: Full AML compliance

Timeline: Decision expected late 2025, rollout 2027–2028

Motivation: preserve monetary sovereignty, counter private stablecoins

Cross-Border CBDC: mBridge

Project mBridge: Multi-CBDC platform for cross-border payments

Participants: China, Hong Kong, Thailand, UAE, Saudi Arabia

Goals vs SWIFT:

- Instant settlement (vs 2–5 days)
- Lower costs (no correspondent banking fees)
- 24/7 operation

Status: MVP launched June 2024, live transactions completed
Geopolitical Implication: Potential bypass of USD-dominated SWIFT

BRICS interest: alternative payment system for member nations

Key Future Trends

1. **RWA Tokenization**: Real assets on blockchain
   - Real estate, bonds, commodities
   - Projected $16T by 2030 (BCG estimate)
2. **Zero-Knowledge Proofs**: Privacy + scalability
   - ZK-rollups: StarkNet, zkSync, Polygon zkEVM
   - Private identity verification
3. **AI + Blockchain Convergence**:
   - Smart contract auditing, decentralized AI training
   - AI agent payments, verifiable AI models

Institutional adoption accelerating: Bitcoin/Ethereum ETFs approved 2024

Summary: Key Takeaways

- **CBDCs**: 130+ countries exploring, 90% of global GDP
- **Retail vs Wholesale**: Different users, use cases, privacy needs
- **Privacy vs Surveillance**: Core design tradeoff
- **e-CNY**: 260M+ wallets, "controllable anonymity"
- **Digital Euro**: Privacy-focused, decision late 2025
- **mBridge**: Cross-border CBDC, potential SWIFT alternative
- **Future**: RWA tokenization, ZK proofs, AI+blockchain

CBDCs represent the intersection of monetary policy and technology

Visual Context: CBDCs & Future

Central Bank Architecture

Digital Currency Concept

Future Technology

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP.

Q2. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Consumers
Answer: B – Wholesale CBDCs are for interbank settlement.

Q3. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets.

Q4. What privacy model does the Digital Euro propose for small transactions?
A) Full KYC B) Cash-like privacy C) No privacy D) Blockchain transparency
Answer: B – Small transactions get cash-like privacy.

Q5. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet
Answer: B – mBridge MVP launched June 2024.

Quiz Questions (6–10)

Q6. What is projected market size for RWA tokenization by 2030?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates $16 trillion by 2030.

Q7. What technology enables both privacy and scalability in blockchain?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – ZK proofs enable privacy + scalability.

Q8. Which is NOT a mBridge participant?
A) China B) Thailand C) USA D) UAE
Answer: C – USA is not a mBridge participant.

Q9. What feature does e-CNY support without internet?
A) International transfers B) Dual offline payment C) Smart contracts D) Auditing
Answer: B – e-CNY supports dual offline payment.

Q10. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – Decision expected late 2025, rollout 2027–2028.

CBDCs and Future Trends

Learning Objectives: Understand CBDCs and retail vs wholesale designs — Analyze privacy vs surveillance tradeoffs — Evaluate e-CNY and Digital Euro progress — Identify future blockchain trends

11:35
Today
11:30 AM
Markets
Market Cap
All
BTC
Bitcoin
ETH
Ethereum
USDT
TetherUS
ADA
Cardano
BNB
BNB

What is a CBDC?

Formal Definition

A Central Bank Digital Currency (CBDC) is digital fiat money issued directly by a central bank as legal tender.

Key Characteristics:

- Legal tender status – liability of central bank (not commercial bank)
- Digital/electronic form (no physical cash)
- May use DLT but not required (technology agnostic)
- **Not cryptocurrency** – centrally issued and controlled

Status: 130+ countries exploring CBDCs (90% of global GDP)

CBDCs respond to cash decline, private stablecoins, and financial inclusion needs

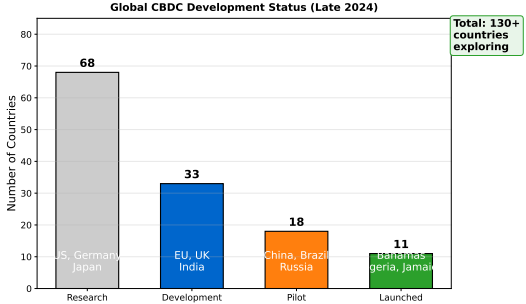
Retail vs Wholesale CBDCs

Retail CBDC:

- Users: General public
- Use case: Payments, store of value
- Privacy: Balance privacy vs AML
- Examples: e-CNY, Digital Euro

Wholesale CBDC:

- Users: Financial institutions only
- Use case: Interbank settlement
- Technology: Likely DLT for efficiency
- Examples: mBridge, Project Jasper



Retail CBDCs have greater societal impact; wholesale CBDCs focus on settlement efficiency

Privacy vs Surveillance Tradeoff

Privacy Concerns

- Central bank sees all transactions
- Government surveillance potential
- Social credit system risks
- No cash-like anonymity

Privacy tech: ZK proofs, tiered privacy (small anonymous, large KYC)

AML/CFT Requirements

- Full anonymity enables illicit finance
- FATF regulatory pressure
- Tax enforcement needs

Design Spectrum:

- Full Surveillance: e-CNY
- Balanced: Digital Euro
- Privacy-First: Unlikely in practice

Key design tradeoff: user privacy vs regulatory compliance

(c) Joerg Osterrieder 2025

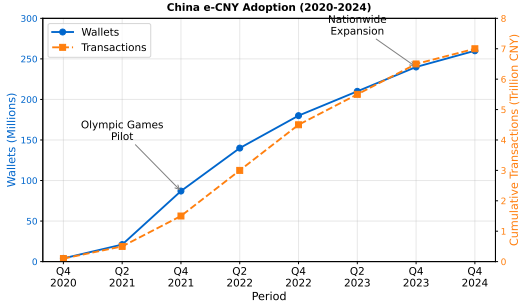
Case Studies: e-CNY vs Digital Euro

China e-CNY (2020-present)

- 260M+ wallets, 7T+ yuan transactions
- Two-tier: PBOC wholesale, banks retail
- "Controllable anonymity" (PBOC sees all)
- Dual offline payment capability

Digital Euro (Decision late 2025)

- Privacy-focused (stronger than e-CNY)
- Small tx: Cash-like privacy
- Rollout planned 2027-2028



e-CNY is largest CBDC pilot globally; Digital Euro prioritizes privacy

Cross-Border CBDC: Project mBridge

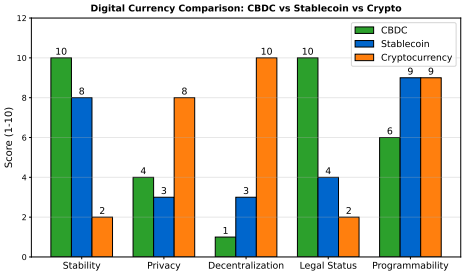
What is mBridge?

- Multi-CBDC platform for cross-border payments
- Participants: China, Hong Kong, Thailand, UAE, Saudi Arabia
- Goal: Replace SWIFT for settlements

Advantages:

- Instant settlement (vs 2-5 days)
- Lower costs (no correspondent banking fees)
- 24/7 operation

Status: MVP launched June 2024, live transactions completed



Geopolitical implications: mBridge may bypass USD-dominated SWIFT system

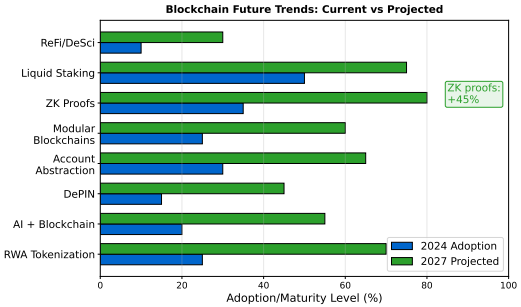
Future Trends in Blockchain

Key Growth Areas:

- **RWA Tokenization**: Real assets on-chain ($16T by 2030)
- **ZK Proofs**: Privacy + scalability (StarkNet, zkSync)
- **AI + Blockchain**: Smart contract auditing, decentralized training
- **Institutional Adoption**: Bitcoin/ETH ETFs, custody solutions

Emerging Risks:

- Quantum computing threat (10-20 year timeline)
- Regulatory fragmentation
- Centralization creep (Lido 30%+ of staked ETH)



ZK proofs, liquid staking, and RWA tokenization showing strongest growth

(c) Joerg Osterrieder 2025

RWA Tokenization: The Next Frontier

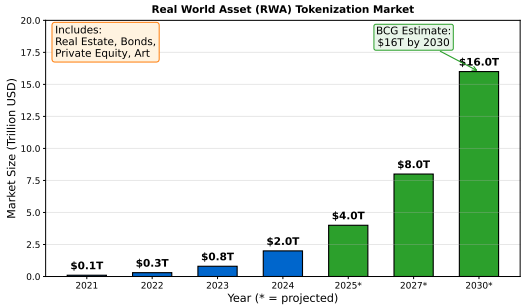
Asset Classes Being Tokenized:

- Real estate (fractional ownership)
- Private equity and venture capital
- Bonds (government, corporate)
- Commodities (gold, carbon credits)

Key Advantages:

- Lower investment barriers
- 24/7 trading (no market hours)
- Programmable compliance

Leaders: Centrifuge, Ondo Finance, Securitize, tZERO



BCG projects RWA tokenization to reach $16 trillion by 2030

(c) Joerg Osterrieder 2025

Key Takeaways

1. **CBDCs are coming**: 130+ countries exploring, 90% of global GDP represented
2. **Design matters**: Privacy vs surveillance is the key tradeoff (e-CNY full surveillance, Digital Euro balanced)
3. **Cross-border revolution**: mBridge may challenge SWIFT dominance (instant, low-cost settlement)
4. **Future growth**: RWA tokenization ($16T by 2030), ZK proofs, AI+Blockchain convergence

Bottom Line: CBDCs will reshape monetary systems while blockchain continues evolving toward institutional adoption and real-world asset integration.

(c) Joerg Osterrieder 2025

Concrete Examples: Making It Real

CBDC Examples (Dec 2025)

- e-CNY: 260M+ wallets, 7T+ yuan tx
- Digital Euro: Decision late 2025
- mBridge: 5 countries, MVP June 2024
- Sand Dollar (Bahamas): First live retail CBDC

Institutional Adoption

- Bitcoin ETFs: Approved Jan 2024 (US)
- Ethereum ETFs: July 2024
- BlackRock BUIDL: $2.9B tokenized fund

RWA Tokenization Leaders

- Centrifuge: Real-world lending
- Ondo Finance: Tokenized treasuries
- Securitize: Security tokens
- Franklin Templeton: On-chain funds

ZK Technology

- StarkNet: ZK-STARK rollup
- zkSync: ZK-SNARK rollup
- Polygon zkEVM: EVM compatible
- Aztec: Private transactions

Data verified Dec 2025 — Sources: Atlantic Council CBDC Tracker, DefiLlama, CoinGecko

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Consumers

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q3. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q3. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets, the largest CBDC pilot globally.

Q4. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge D) Transparency

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q3. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets, the largest CBDC pilot globally.

Q4. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge D) Transparency
Answer: B – e-CNY uses "controllable anonymity" where PBOC can see all transactions.

Q5. When is the Digital Euro rollout planned?
A) 2024 B) 2025 C) 2027-2028 D) 2030

Quiz Questions (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q3. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets, the largest CBDC pilot globally.

Q4. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge D) Transparency
Answer: B – e-CNY uses "controllable anonymity" where PBOC can see all transactions.

Q5. When is the Digital Euro rollout planned?
A) 2024 B) 2025 C) 2027-2028 D) 2030
Answer: C – Digital Euro decision expected late 2025, rollout planned for 2027-2028.

Quiz Questions (6–10)

Q6. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading

Quiz Questions (6–10)

Q6. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Q7. What is the projected market size for RWA tokenization by 2030 (BCG)?
A) $1T B) $5T C) $16T D) $50T

Quiz Questions (6–10)

Q6. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Q7. What is the projected market size for RWA tokenization by 2030 (BCG)?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q8. What percentage of staked ETH does Lido control?
A) 10%+ B) 20%+ C) 30%+ D) 50%+

Quiz Questions (6–10)

Q6. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Q7. What is the projected market size for RWA tokenization by 2030 (BCG)?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q8. What percentage of staked ETH does Lido control?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating centralization concerns.

Q9. What technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-sig

Quiz Questions (6–10)

Q6. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Q7. What is the projected market size for RWA tokenization by 2030 (BCG)?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q8. What percentage of staked ETH does Lido control?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating centralization concerns.

Q9. What technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-sig
Answer: B – ZK proofs enable privacy and scalability through ZK-rollups and private tx.

Q10. What is the estimated timeline for quantum computing to threaten ECDSA?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years

Quiz Questions (6–10)

Q6. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Q7. What is the projected market size for RWA tokenization by 2030 (BCG)?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q8. What percentage of staked ETH does Lido control?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating centralization concerns.

Q9. What technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-sig
Answer: B – ZK proofs enable privacy and scalability through ZK-rollups and private tx.

Q10. What is the estimated timeline for quantum computing to threaten ECDSA?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Quiz: CBDCs Future

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%

Quiz (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form

Quiz (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers

Quiz (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q4. What is China's CBDC called?
A) Digital Yuan B) e-CNY C) China Coin D) PBOC Token

(c) Joerg Osterrieder 2025

Quiz (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q4. What is China's CBDC called?
A) Digital Yuan B) e-CNY C) China Coin D) PBOC Token
Answer: B – China's CBDC is officially called e-CNY (electronic Chinese Yuan).

Q5. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+

Quiz (1–5)

Q1. What percentage of global GDP is represented by countries exploring CBDCs as of 2024?
A) 50% B) 70% C) 90% D) 100%
Answer: C – Over 130 countries representing 90% of global GDP are exploring CBDCs.

Q2. Which of the following is NOT a key characteristic of CBDCs?
A) Legal tender status B) Liability of central bank C) Must use DLT technology D) Electronic/digital form
Answer: C – CBDCs may use DLT but it is not required; technology choice varies by implementation.

Q3. Who are the primary users of wholesale CBDCs?
A) General public B) Financial institutions C) Retail merchants D) Individual consumers
Answer: B – Wholesale CBDCs are restricted to financial institutions for interbank settlement.

Q4. What is China's CBDC called?
A) Digital Yuan B) e-CNY C) China Coin D) PBOC Token
Answer: B – China's CBDC is officially called e-CNY (electronic Chinese Yuan).

Q5. How many wallets did China's e-CNY have by late 2024?
A) 50M+ B) 100M+ C) 260M+ D) 500M+
Answer: C – e-CNY had over 260 million wallets by late 2024, the largest CBDC pilot globally.

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned

Quiz (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency

Quiz (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030

Quiz (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – The Digital Euro decision is expected late 2025, with rollout planned for 2027-2028.

Q9. How does the Digital Euro handle privacy for small transactions?
A) Full KYC required B) Cash-like privacy C) No privacy D) Blockchain transparency

Quiz (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – The Digital Euro decision is expected late 2025, with rollout planned for 2027-2028.

Q9. How does the Digital Euro handle privacy for small transactions?
A) Full KYC required B) Cash-like privacy C) No privacy D) Blockchain transparency
Answer: B – Small transactions get cash-like privacy; large transactions require full AML compliance.

Q10. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading

Quiz (6–10)

Q6. What architecture does China's e-CNY use?
A) Fully decentralized B) Single-tier centralized C) Two-tier (PBOC wholesale, banks retail) D) Three-tier permissioned
Answer: C – e-CNY uses a two-tier system where PBOC handles wholesale and commercial banks handle retail distribution.

Q7. What privacy model does e-CNY implement?
A) Full anonymity B) Controllable anonymity C) Zero knowledge proofs D) Complete transparency
Answer: B – e-CNY uses "controllable anonymity" where the PBOC can see all transactions.

Q8. When is the Digital Euro decision expected?
A) 2024 B) Late 2025 C) 2027 D) 2030
Answer: B – The Digital Euro decision is expected late 2025, with rollout planned for 2027-2028.

Q9. How does the Digital Euro handle privacy for small transactions?
A) Full KYC required B) Cash-like privacy C) No privacy D) Blockchain transparency
Answer: B – Small transactions get cash-like privacy; large transactions require full AML compliance.

Q10. What is Project mBridge designed for?
A) Retail payments B) Cross-border CBDC settlements C) Stablecoin regulation D) NFT trading
Answer: B – mBridge is a multi-CBDC platform for cross-border payments and settlements.

Quiz (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand

Quiz (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T

Quiz (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q14. Which is NOT an advantage of RWA tokenization?
A) Fractional ownership B) 24/7 trading C) Guaranteed profits D) Programmable compliance

Quiz (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q14. Which is NOT an advantage of RWA tokenization?
A) Fractional ownership B) 24/7 trading C) Guaranteed profits D) Programmable compliance
Answer: C – Tokenization offers fractional ownership, 24/7 trading, and programmable compliance, but not guaranteed profits.

Q15. What percentage of staked ETH does Lido control, raising centralization concerns?
A) 10%+ B) 20%+ C) 30%+ D) 50%+

Quiz (11–15)

Q11. Which countries are NOT participants in Project mBridge?
A) China, Thailand B) UAE, Saudi Arabia C) USA, EU D) Hong Kong, Thailand
Answer: C – mBridge participants include China, Hong Kong, Thailand, UAE, and Saudi Arabia; not USA or EU.

Q12. When was the mBridge MVP launched?
A) January 2024 B) June 2024 C) December 2024 D) Not yet launched
Answer: B – The mBridge MVP was launched in June 2024 with live transactions completed.

Q13. What is projected market size for RWA tokenization by 2030 according to BCG?
A) $1T B) $5T C) $16T D) $50T
Answer: C – BCG estimates real world asset tokenization will reach $16 trillion by 2030.

Q14. Which is NOT an advantage of RWA tokenization?
A) Fractional ownership B) 24/7 trading C) Guaranteed profits D) Programmable compliance
Answer: C – Tokenization offers fractional ownership, 24/7 trading, and programmable compliance, but not guaranteed profits.

Q15. What percentage of staked ETH does Lido control, raising centralization concerns?
A) 10%+ B) 20%+ C) 30%+ D) 50%+
Answer: C – Lido controls over 30% of staked ETH, creating validator concentration concerns.

(c) Joerg Osterrieder 2025

Quiz (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures

Quiz (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years

Quiz (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%

Quiz (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%
Answer: B – There are 50,000+ open blockchain jobs with 30%+ annual growth.

Q19. Which is NOT mentioned as an AI + Blockchain convergence use case?
A) Smart contract auditing B) Decentralized AI training C) Physical robot control D) AI agent payments

Quiz (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%
Answer: B – There are 50,000+ open blockchain jobs with 30%+ annual growth.

Q19. Which is NOT mentioned as an AI + Blockchain convergence use case?
A) Smart contract auditing B) Decentralized AI training C) Physical robot control D) AI agent payments
Answer: C – The lesson covers smart contract auditing, decentralized AI training, and AI agent payments, but not physical robot control.

Q20. What feature does e-CNY support that does NOT require internet connection?
A) International transfers B) Dual offline payment C) Smart contract execution D) Real-time auditing

Quiz (16–20)

Q16. What cryptographic technology enables both privacy and scalability without tradeoffs?
A) SHA-256 B) Zero-knowledge proofs C) RSA encryption D) Multi-signatures
Answer: B – Zero-knowledge proofs enable privacy and scalability simultaneously through ZK-rollups and private transactions.

Q17. What is the estimated timeline for quantum computing to threaten ECDSA signatures?
A) 2-5 years B) 5-10 years C) 10-20 years D) 50+ years
Answer: C – ECDSA signatures face quantum computing threats in a 10-20 year timeline.

Q18. How many open blockchain jobs exist globally with what annual growth rate?
A) 10,000+, 10% B) 50,000+, 30% C) 100,000+, 50% D) 500,000+, 100%
Answer: B – There are 50,000+ open blockchain jobs with 30%+ annual growth.

Q19. Which is NOT mentioned as an AI + Blockchain convergence use case?
A) Smart contract auditing B) Decentralized AI training C) Physical robot control D) AI agent payments
Answer: C – The lesson covers smart contract auditing, decentralized AI training, and AI agent payments, but not physical robot control.

Q20. What feature does e-CNY support that does NOT require internet connection?
A) International transfers B) Dual offline payment C) Smart contract execution D) Real-time auditing
Answer: B – e-CNY supports dual offline payment capability, allowing transactions without internet connection.

L48: Course Synthesis

Blockchain & Cryptocurrency: The Complete Journey

Blockchain & Cryptocurrency Course

December 2025

The Problem: How do all the pieces fit together?

Part 4/4: Course Synthesis (Integration)

The Challenge

After studying 49 lessons across blockchain, DeFi, NFTs, and regulation, how do we synthesize this knowledge into a coherent framework for evaluating any crypto project or protocol?

Why It Matters

- Without synthesis, we have scattered facts but no analytical framework
- The crypto industry evolves faster than our course content - we need tools for lifelong learning

What We Need

- A systematic lens for analyzing any blockchain system (The Cryptoeconomics Lens)
- Understanding of fundamental trade-offs across trust, value, risk, and design

The Cryptoeconomics Question

How can we apply consistent principles to evaluate systems from Bitcoin to DeFi to CBDCs?

Today's lesson: A unifying framework for the entire course journey (L01-L48)

Course Journey: Seven Modules

Module A: Foundations
Blockchain, cryptography, consensus (PoW/PoS)
Module B: Cryptocurrencies
Bitcoin, altcoins, mining, wallets
Module C: Ethereum & Smart Contracts
Solidity, dApps, EVM, The Merge
Module D: DeFi
DEXs, lending, stablecoins, yield farming

Module E: NFTs & Tokenization
NFT standards, marketplaces, tokenomics, DAOs
Module F: Advanced Topics
Layer 2 scaling, flash loans, security
Module G: Regulation & Future
Global frameworks, CBDCs, 2025+ trends

49 Lessons + 2 Workshops
Theory + Labs + Hands-on Solidity

Module A: Foundations – Key Takeaways

- **Blockchain = Distributed Ledger**: Immutable, transparent, decentralized
- **Cryptography**: Hashing (SHA-256), digital signatures (ECDSA), Merkle trees
- **Bitcoin Invention**: Satoshi Nakamoto's solution to double-spending
- **PoW Consensus**: Miners compete to solve hash puzzle, longest chain wins
- **PoS Evolution**: Energy-efficient, validators stake tokens
- **Byzantine Fault Tolerance**: 2/3 honest nodes required

- **Fundamental Insight**: Trust through math and game theory, not institutions

Module B: Cryptocurrencies – Key Takeaways

- **Bitcoin**: Digital gold, 21M supply cap, halving every 4 years
- **UTXO Model**: Transaction inputs/outputs, not account balances
- **Mining**: Hashrate competition, ASIC dominance, mining pools
- **Wallets**: Hot (online, convenient) vs cold (offline, secure)
- **Altcoins**: Litecoin (faster), Monero (privacy), Bitcoin Cash (bigger blocks)
- **Network Effects**: Bitcoin's first-mover advantage and brand recognition

- **Critical Lesson**: Private key = ownership; lose key = lose funds

Module C: Ethereum & Smart Contracts – Key Takeaways

- **Smart Contracts**: Self-executing code, unstoppable applications
- **Solidity**: Most popular smart contract language (JavaScript-like)
- **EVM**: Turing-complete virtual machine, gas mechanism prevents infinite loops
- **dApps**: Frontend + smart contract backend (MetaMask integration)
- **The Merge (2022)**: Ethereum switched from PoW to PoS (99% energy reduction)
- **ERC Standards**: ERC-20 (tokens), ERC-721 (NFTs), ERC-1155 (multi-token)

- **Paradigm Shift**: From "code is code" to "code is law"

Module D: DeFi – Key Takeaways

- **DeFi = Open Financial System**: No intermediaries, permissionless
- **AMMs (Uniswap)**: x * y = k, liquidity pools replace order books
- **Lending (Aave, Compound)**: Over-collateralized loans, algorithmic interest rates
- **Stablecoins**: USDC (fiat-backed), DAI (crypto-collateralized), UST (algorithmic, failed)
- **Yield Farming**: Liquidity mining, APY chasing, impermanent loss risk
- **Derivatives**: Perpetual futures (funding rates), options (Deribit, Opyn)
- **TVL**: $100B+ locked in DeFi protocols (peak 2021, recovered 2024)

- **Innovation vs Risk**: Composability enables innovation, also cascading failures

Module E: NFTs & Tokenization – Key Takeaways

- **NFTs**: Unique tokens, provable ownership, on-chain metadata
- **Use Cases**: Digital art, gaming assets, memberships, ticketing
- **Marketplaces**: OpenSea, Blur, Magic Eden (Solana)
- **Royalties**: Creators earn on secondary sales (on-chain enforcement)
- **Tokenomics**: Token design, utility vs governance, vesting schedules
- **DAOs**: On-chain governance, token-weighted voting, treasury management
- **2021-2022 Boom/Bust**: $25B NFT market peak, 90%+ correction, niche survival

- **Lasting Impact**: Digital ownership infrastructure, beyond speculative JPEGs

Module F: Advanced Topics – Key Takeaways

- **Layer 2 Scaling**:
  - Optimistic Rollups (7-day withdrawal, fraud proofs)
  - ZK-Rollups (instant finality, validity proofs)
  - State channels (Lightning Network for Bitcoin)
- **Flash Loans**: Uncollateralized, atomic transactions (arbitrage, attacks)
- **Composability**: DeFi as "money legos" – powerful but risky
- **Smart Contract Security**:
  - Reentrancy (The DAO hack), oracle manipulation, access control
  - Tools: Slither, Mythril, formal verification
  - Defense in depth: Audits + bug bounties + monitoring
- **Critical Lesson**: $3B+ lost to exploits; security is paramount

Module G: Regulation & Future – Key Takeaways

- **Regulatory Spectrum**: Hostile (China ban) to permissive (Switzerland, Singapore)
- **US**: Fragmented (SEC vs CFTC), regulation by enforcement
- **EU MiCA**: Comprehensive framework, stablecoin focus, CASP licensing
- **Switzerland**: Principles-based, clear token classification, DLT Act
- **CBDCs**: 130+ countries exploring, e-CNY largest pilot
- **Future Trends**:
  - Institutional adoption, RWA tokenization, AI+crypto convergence
  - Account abstraction (UX breakthrough), modular blockchains
  - ZK proofs (privacy + scalability), DePIN (decentralized infrastructure)

- **Tension**: Innovation vs regulation, privacy vs compliance

Theme 1: Decentralization vs Efficiency Tradeoff

- **Blockchain Trilemma**: Decentralization, security, scalability (pick 2)
- **Bitcoin**: Maximally decentralized, sacrifices scalability (7 TPS)
- **Ethereum**: Decentralized, adding scalability via Layer 2
- **Solana**: High throughput (65,000 TPS), less decentralized (higher hardware requirements)
- **Centralized Exchanges**: Maximum efficiency, zero decentralization (FTX collapse risk)
- **Layer 2 Solutions**: Pragmatic compromise (rollups inherit L1 security)

- **Design Philosophy**: No perfect solution, context determines optimal tradeoff

Theme 2: Code is Law – Until It Isn't

- **Smart Contract Immutability**: Code executes exactly as written
- **The DAO Hack (2016)**: $60M drained via reentrancy
  - Community decision: Hard fork to reverse (Ethereum vs Ethereum Classic split)
  - "Code is law" vs "code has bugs, community decides"
- **Tornado Cash Sanctions (2022)**: US Treasury sanctioned smart contract
  - Debate: Can you sanction code? Is code speech or conduct?
- **Legal Enforcement**: SBF convicted despite decentralization rhetoric

- **Reality**: Code operates within legal and social contexts
- **Governance**: Most protocols have upgrade mechanisms (not truly immutable)

Theme 3: Speculation vs Utility

Speculation Dominates (2024):

- 90%+ transactions are trading
- Memecoins, pump-and-dump schemes
- Volatility hinders currency adoption

Utility Emerging:

- Stablecoins: $310B, real payments
- NFT ticketing adopted by sports teams
- DeFi: lending, derivatives work

Adoption S-Curve:

- 2010-2020: Early adopters, ideological
- 2024-2030: Institutional, utility-driven

Long-term Outlook:
Utility will dominate; speculation remains (like stock market)

Theme 4: Permissionless Innovation

TradFi vs DeFi:

- TradFi: Licenses, capital, compliance
- DeFi: Deploy contract, anyone can use

Innovation Examples:

- Uniswap: 2 devs, $100B+ volume
- Compound: Algorithmic interest rates
- Aave: Flash loans (impossible in TradFi)

Composability (Money Legos):

- Yearn: Aggregates lending protocols
- 1inch: Aggregates DEXs
- Curve Wars: Liquidity competition

Trade-off:
Exploits, scams, regulatory uncertainty

"Move fast and break things" applied to finance

Theme 5: Centralization Creep

Paradox: Decentralized protocols have centralized components

Examples:

- Exchanges: Binance/Coinbase (70%+)
- Stablecoins: Circle can freeze USDC
- Infrastructure: Infura, Alchemy RPCs
- Staking: Lido dominates Ethereum

Nakamoto Coefficient:
(Min entities to halt network)

- Bitcoin: 4 mining pools
- Ethereum: 3 entities
- Solana: 19 validators

Reality:
Decentralization is a spectrum, not binary

Theme 6: Privacy vs Transparency

Blockchain Reality:

- All transactions public (pseudonymous)
- Chainalysis/Elliptic track funds

Privacy Solutions:

- Monero: Ring signatures, stealth addresses
- Zcash: Optional zk-SNARKs
- Tornado Cash: Sanctioned mixer
- Aztec: ZK proofs on Ethereum

Regulatory Conflict:

- AML/CFT requirements
- Tax enforcement needs
- Human right to privacy
- Dissident/activist protection

Future: ZK proofs enable privacy + compliance (prove legality without revealing details)

What Blockchain Does Well

1. **Censorship Resistance:** No single point of control
2. **Programmable Money:** Smart contract logic
3. **Composability:** Permissionless integration
4. **Global Access:** Internet = access
5. **Transparency:** Auditable transactions
6. **24/7 Operation:** No market hours
7. **Fast Settlement:** Minutes vs days
8. **Capital Efficiency:** Flash loans, atomic swaps

What Blockchain Does Poorly

1. **Scalability:** 7-65K TPS limit
2. **UX:** Seed phrases, gas fees, no support
3. **Energy:** Bitcoin 150 TWh/year
4. **Volatility:** Unsuitable as currency
5. **Regulation:** Unclear legal status
6. **Fraud:** Irreversible, no recourse
7. **Complexity:** Steep learning curve
8. **Centralization:** Pools, staking concentration

Legitimate Use Cases (Where Blockchain Adds Value)

1. **Cross-Border Remittances:** Cheaper, faster than Western Union (USDC, Lightning)
2. **Inflation Hedge**: Store of value in unstable currencies (Argentina, Venezuela)
3. **Censorship Evasion:** Donations to dissidents (WikiLeaks, Ukraine war donations)
4. **Financial Inclusion**: Banking for unbanked (Africa, Southeast Asia)
5. **Tokenization of Assets:** Fractional ownership (real estate, art)
6. **Supply Chain Provenance:** Tracking goods (diamonds, food safety)
7. **Decentralized Identity:** Self-sovereign identity (no Facebook/Google control)
8. **DAOs:** Coordination without centralized hierarchy (GitcoinDAO, Uniswap governance)
9. **Gaming Economies:** True ownership of in-game assets (Axie Infinity model)

Questionable Use Cases (Blockchain Not Necessary)

1. **Most Supply Chains:** Centralized databases work fine (blockchain overkill)
2. **Voting:** Security and privacy challenges outweigh benefits
3. **Medical Records:** Privacy requirements conflict with blockchain transparency
4. **Most NFTs**: Simple database + digital signature suffices (no need for blockchain)
5. **Enterprise Blockchains**: Private blockchains = glorified shared databases
6. **IoT:** High transaction volume, low latency needs (blockchain too slow)
7. **Most "Blockchain for X"**: Marketing buzzword, no actual benefit

8. **Heuristic:** If you can use a database, use a database. Blockchain only when decentralization/censorship-resistance is critical.

The FTX Collapse: Lessons Learned

What Happened (Nov 2022):

- FTX commingled funds with Alameda
- Alameda lost billions (Luna, bad bets)
- Bank run after Binance CEO tweet
- $8B missing, SBF arrested

Key Lessons:

1. Not your keys, not your coins
2. Proof of reserves can be faked
3. Self-regulation failed
4. Offshore = less oversight
5. High yields = hidden risk

Industry Response: Merkle tree proofs, increased regulatory scrutiny

2024 Milestones: A Transformative Year

Q1 2024:

- **Jan**: SEC approves 11 Bitcoin ETFs
- BlackRock, Fidelity enter crypto
- \$50B+ AUM in first year
- **Mar**: Dencun upgrade (EIP-4844)
- L2 fees: \$0.50 $\rightarrow$ \$0.01

Q2-Q4 2024:

- **Apr**: Bitcoin 4th halving
- **Jul**: Ethereum ETFs approved
- **Nov**: Pro-crypto US administration
- **Dec**: MiCA full EU implementation

2025 Landscape: New Era Begins

- **Regulatory Shift (US)**:
  - Gary Gensler resigned as SEC Chair
  - Pro-crypto leadership expected
  - Stablecoin legislation priority
  - CBDC development paused
- **Institutional Reality**:
  - Bitcoin ETFs among largest commodity ETFs globally
  - Traditional asset managers offering crypto products
  - Banks exploring custody and trading services
- **Technical Progress**:
  - L2 ecosystem thriving (Base, Arbitrum, Optimism)
  - Restaking (EigenLayer) as major new primitive
  - Account abstraction adoption accelerating
- **Market Cycle**: Post-halving bull market dynamics

Course Content vs 2025 Reality

Topic	When Course Written	2025 Reality
Bitcoin ETFs	Speculative	Approved, $50B+ AUM
ETH staking	15M ETH staked	34M+ ETH staked
MiCA	Future framework	Fully implemented
US regulation	Hostile (Gensler)	Pro-crypto administration
Layer 2 fees	$0.50-2.00	$0.01-0.10 (post-Dencun)
DeFi TVL	Recovery phase	$80B+ TVL
Restaking	Emerging concept	$15B+ in EigenLayer
CBDCs	Racing ahead	US paused, EU preparing

Takeaway: Industry moves fast; stay current with primary sources

2025-2030: Key Questions

1. **Scaling:** Will Layer 2s solve Ethereum's scalability, or will alt-L1s dominate?
2. **Regulation:** Will global frameworks converge (MiCA template) or fragment?
3. **CBDCs:** Will they coexist with crypto, or attempt to crowd it out?
4. **Institutional Adoption:** Will $1T+ institutional capital enter crypto?
5. **DeFi vs CeFi:** Which model wins (composable protocols vs regulated intermediaries)?
6. **Privacy:** Can ZK proofs enable privacy without enabling crime?
7. **Interoperability:** Will cross-chain bridges remain attack vectors?
8. **Energy:** Will PoS adoption reduce environmental concerns?
9. **Quantum Threat:** Will post-quantum cryptography be deployed in time?
10. **Mainstream UX:** Will account abstraction achieve Web2-level usability?

Optimistic Scenario (2030)

- **Institutional Adoption:** Pension funds, sovereign wealth funds allocate 5-10% to crypto
- **Stablecoins:** $1T+ market cap, used globally for payments and remittances
- **Tokenization:** $10T+ real-world assets on-chain (real estate, bonds, equities)
- **Layer 2 Success:** Ethereum + rollups achieve 100,000+ TPS, fees ¡$0.01
- **Regulatory Clarity:** Global frameworks converge, DeFi compliance solutions emerge
- **Account Abstraction:** Wallets as easy as email (social recovery, gas abstraction)
- **Privacy + Compliance:** ZK proofs enable private, compliant transactions
- **CBDCs Coexist:** Central bank digital currencies complement, not replace, crypto
- **Mainstream Use:** 1B+ users (vs 500M in 2024)
- **Impact:** Financial system fundamentally transformed, more inclusive and efficient

Pessimistic Scenario (2030)

- **Regulatory Crackdown:** Major jurisdictions ban DeFi, privacy tools, self-custody
- **CBDC Monopoly:** Central banks outlaw competing stablecoins, crypto marginalized
- **Centralization Wins:** A few mega-platforms (Coinbase, Binance) dominate, surveillance standard
- **Scaling Failure:** Layer 2s too complex/fragmented, alt-L1s centralized, fees remain high
- **Security Catastrophe:** Major exploit (¿$10B) destroys trust, insurance unavailable
- **Quantum Breakthrough:** ECDSA broken, mass theft before migration complete
- **Environmental Backlash:** PoW banned globally, PoS attacked as plutocracy
- **Stablecoin Collapse:** Tether/Circle fail, contagion wipes out DeFi
- **User Apathy:** Complexity, scams, volatility drive users back to TradFi
- **Niche Survival:** Crypto becomes niche tool (like Tor), not mainstream finance

Realistic Scenario (2030)

- **Hybrid System:** Regulated CeFi + permissionless DeFi coexist
- **Institutional Participation:** Via compliant on/off ramps, tokenized securities
- **Stablecoins:** Regulated (MiCA-style), dominate crypto payments ($500B market cap)
- **Layer 2 Maturity**: Optimistic + ZK rollups achieve 50,000 TPS, fees $0.10
- **Selective Regulation:** Retail-facing services regulated (exchanges, wallets), protocols mostly exempt
- **Privacy Constrained:** KYC for fiat on/off ramps, some privacy tools banned
- **CBDCs Launched:** But limited adoption (prefer private stablecoins/crypto)
- **Use Cases Validated:** Remittances, tokenization, DAOs mainstream; speculation remains large
- **Users:** 750M (50% growth from 2024), still ¡10% global population
- **Conclusion:** Crypto as parallel financial system, not replacement

Problem Solved? The Cryptoeconomics Synthesis

The Original Problem

How do all the pieces fit together?

How This Course Solves It

- **The Cryptoeconomics Lens**: 6 questions for any system (Problem, Incentives, Costs/Benefits, Failures, Design, Alternatives)
- **Cross-Cutting Themes**: Decentralization vs efficiency, code as law, speculation vs utility, permissionless innovation, centralization creep, privacy vs transparency
- **Critical Framework**: What blockchain does well vs poorly, legitimate vs questionable use cases

Remaining Limitations

- Technology evolves faster than frameworks - 2024 brought Bitcoin ETFs, MiCA, Dencun upgrade (all post-course design)
- No single framework captures all trade-offs - context determines optimal solution

Open Questions

- What will the next breakthrough be? (2025-2030: scaling, privacy, regulation, or something unexpected?)
- Will crypto transform finance or remain a parallel system?

Synthesis provides tools for lifelong learning, but the crypto landscape continues to evolve

Final Thoughts: What Did We Learn?

1. **Technology Enables, Society Decides:** Blockchain is a tool, outcomes depend on adoption and regulation
2. **Decentralization is Hard:** Tradeoffs everywhere (speed, cost, security, usability)
3. **Finance is Being Rebuilt:** From first principles, in public, with open source
4. **Speculation Funds Innovation:** Bubbles are destructive but also fund R&D (dot-com parallel)
5. **Security is Existential:** One exploit can destroy years of progress
6. **Regulation is Inevitable:** Question is whether it enables or stifles innovation
7. **Privacy Matters:** But conflicts with AML/tax enforcement (unresolved tension)
8. **User Experience:** Crypto won't achieve mainstream adoption until UX matches Web2
9. **The Future is Uncertain:** Could be revolutionary or a niche curiosity

Critical Thinking: Question Everything

- **Don't Trust, Verify:** Crypto ethos applies to crypto itself
  - Verify token contracts before investing (scams everywhere)
  - Audit smart contracts before depositing funds
  - Check proof of reserves (exchanges, stablecoins)
- **Beware Hype Cycles**:
  - 2017: ICO mania (95%+ projects failed)
  - 2021: NFT boom (90%+ floor price collapse)
  - 2024: AI + crypto tokens surge (FET, RNDR, TAO up 500%+, AI agents trade autonomously)
- **Cui Bono (Who Benefits)?**:
  - Token launches: Founders, VCs dump on retail
  - Yield farming: Early LPs extract value from late entrants
  - Influencer shills: Paid promotions disguised as education
- **Intellectual Humility**: This field evolves rapidly, today's truth may be tomorrow's outdated belief

How to Stay Current

1. **Follow Builders, Not Influencers**:
   - Vitalik Buterin (Ethereum), developers over marketers
2. **Read Primary Sources**:
   - Whitepapers, protocol documentation, GitHub repos
   - Ethereum Research Forum, Bitcoin mailing list
3. **Use the Products**:
   - Try DeFi protocols (small amounts), deploy smart contracts, run a node
4. **Engage with Community**:
   - Discord servers, Twitter Crypto, local meetups
5. **Track On-Chain Data**:
   - Dune Analytics, Nansen, Glassnode (objective metrics)
6. **Continued Learning**:
   - Online courses, hackathons, security audits, governance participation

Parting Wisdom

"The best way to predict the future is to invent it."

– Alan Kay

"In the long run, the most important thing is not to make money, but to build systems that are more fair, more open, and more free."

– Crypto Ethos

"Stay curious. Stay skeptical. Stay building."

– Course Conclusion

Thank You

Thank you for completing this course!

You now have the foundational knowledge to:

- Understand blockchain technology and cryptocurrencies
- Build decentralized applications
- Participate in DeFi protocols
- Critically evaluate crypto projects
- Navigate the regulatory landscape
- Pursue a career in Web3

The journey has just begun.
Keep learning, keep building, keep questioning.

Contact: [Your contact information]
Course Materials: [GitHub/Website URL]

L48: Course Synthesis

Blockchain & Cryptocurrency: The Complete Journey

Blockchain & Cryptocurrency Course

December 2025

Learning Objectives

By the end of this lesson, you will be able to:

1. Synthesize key concepts from all 7 modules into a unified cryptoeconomics framework
2. Apply the Cryptoeconomics Lens (6 questions) to analyze any blockchain system
3. Evaluate cross-cutting trade-offs: decentralization vs efficiency, code as law vs legal compliance
4. Identify 2024–2025 milestones and project realistic future scenarios
5. Articulate a personal investment thesis using course frameworks

Building on L47: CBDCs and Future Trends

This final lesson integrates 49 lessons across 7 modules into a coherent analytical framework

Course Synthesis in a Nutshell

- After 49 lessons: "I finally understand cryptocurrency!"
- Reality: The more you learn, the more you realize how much more there is to learn

[COMIC: "I understand crypto now" confidence – Panel 1: Student before course: "Crypto is fake internet money." Panel 2: Student after L01: "I GET IT NOW!" Panel 3: Student after L48: "It's complicated... but I have a framework." Dunning-Kruger curve shown.]

[PLACEHOLDER] — The goal is not complete knowledge but a framework for continuous learning

The Problem: How do all the pieces fit together?

Part 4/4: Course Synthesis (Integration)

The Challenge

After studying 49 lessons across blockchain, DeFi, NFTs, and regulation, how do we synthesize this knowledge into a coherent framework for evaluating any crypto project or protocol?

Why It Matters

- Without synthesis, we have scattered facts but no analytical framework
- The crypto industry evolves faster than our course content - we need tools for lifelong learning

What We Need

- A systematic lens for analyzing any blockchain system (The Cryptoeconomics Lens)
- Understanding of fundamental trade-offs across trust, value, risk, and design

The Cryptoeconomics Question

How can we apply consistent principles to evaluate systems from Bitcoin to DeFi to CBDCs?

Today's lesson: A unifying framework for the entire course journey (L01-L48)

What Have We Learned Across Seven Modules?

Module A: Foundations
Blockchain, cryptography, consensus (PoW/PoS)
Module B: Cryptocurrencies
Bitcoin, altcoins, mining, wallets
Module C: Ethereum & Smart Contracts
Solidity, dApps, EVM, The Merge
Module D: DeFi
DEXs, lending, stablecoins, yield farming

Module E: NFTs & Tokenization
NFT standards, marketplaces, tokenomics, DAOs
Module F: Advanced Topics
Layer 2 scaling, flash loans, security
Module G: Regulation & Future
Global frameworks, CBDCs, 2025+ trends

49 Lessons + 2 Workshops
Theory + Labs + Hands-on Solidity

→ *Problem: How should governments regulate crypto? — Course Journey: Seven Modules The seven modules provide a unified framework: from foundational cryptography to advanced DeFi to regulation—all viewed through The Cryptoeconomics Lens*

Problem Check-In: Course Synthesis

Recall Our Problem

How should governments regulate crypto?

What We've Learned So Far

- Cross-cutting themes synthesize 49 lessons: Decentralization vs efficiency, code as law, speculation vs utility, permissionless innovation
- Critical evaluation framework: What blockchain does well (censorship resistance, programmability) vs poorly (scalability, UX)
- The Cryptoeconomics Lens provides 6 questions applicable to any system—from Bitcoin to CBDCs—for lifelong learning

Still to Address

- 2024-2025 milestones (Bitcoin ETFs, MiCA, Dencun upgrade), realistic 2030 scenarios, and how to stay current as the field evolves
- Will crypto transform global finance or remain a parallel system? The frameworks from this course help you evaluate new developments

Think About

- Based on what you've seen, how would *you* solve this problem?
- What trade-offs do you expect?

Pause and reflect: How does what we've learned so far address "How should governments regulate crypto?"?

The Economics of Course Synthesis

Incentive Structure

- **Core Problem:** Managing systemic and idiosyncratic risks
- **Why act honestly?** Risk-adjusted returns, insurance mechanisms
- **Value Flow:** Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

$$\text{Attack Cost} > \text{Potential Gain}$$

Design Space: Course Synthesis

Alternatives Considered

1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

Trade-offs Made

- Every design optimizes some properties
- ... at the expense of others

Design Questions

- What would YOU change?
- What's optimized? What's sacrificed?
- Are there other approaches?

Key Insight

No Perfect Solution

All blockchain designs involve trade-offs between decentralization, security, and scalability.

Every design is a trade-off. Understanding alternatives reveals the "why" behind choices.

Failure Modes: Course Synthesis

Critical Failure Mode

- **What breaks:** Black swan events, cascading failures
- **Why it happens:** Economic incentives misaligned

Root Cause

- Assumption violated
- Incentive structure broken
- External shock

Historical Context

- Multiple real-world failures documented
- Patterns repeating across protocols

Early Warning Signs

- ! Unusual economic behavior
- ! Incentive misalignment
- ! Centralization drift

Prediction: What could cause this to fail? How would you detect it early?

What Are the Key Blockchain Fundamentals?

Core Building Blocks:

- **Distributed Ledger**: Immutable, transparent, decentralized
- **Cryptography**: SHA-256, ECDSA, Merkle trees
- **Bitcoin**: Satoshi's solution to double-spending

Consensus & Trust:

- **PoW**: Miners solve hash puzzles, longest chain wins
- **PoS**: Energy-efficient, validators stake tokens
- **BFT**: 2/3 honest nodes required

Fundamental Insight: Trust through math and game theory, not institutions

How Do Cryptocurrencies Actually Work?

Bitcoin & Transaction Model:

- **Bitcoin**: Digital gold, 21M cap, halving every 4 years
- **UTXO Model**: Inputs/outputs, not account balances
- **Mining**: Hashrate competition, ASIC dominance

Ecosystem:

- **Wallets**: Hot (online) vs cold (offline, secure)
- **Altcoins**: Litecoin, Monero, Bitcoin Cash
- **Network Effects**: First-mover advantage

Critical Lesson: Private key = ownership; lose key = lose funds

What Makes Smart Contracts Revolutionary?

Core Technology:

- **Smart Contracts**: Self-executing, unstoppable code
- **Solidity**: Most popular language (JS-like)
- **EVM**: Turing-complete, gas prevents infinite loops

Ecosystem & Evolution:

- **dApps**: Frontend + contract backend
- **The Merge (2022)**: PoW $\rightarrow$ PoS (99% energy cut)
- **ERC Standards**: ERC-20, ERC-721, ERC-1155

Paradigm Shift: From "code is code" to "code is law"

How Does DeFi Reconstruct Finance?

Core Primitives:

- **AMMs**: $x \cdot y = k$, pools replace order books
- **Lending**: Over-collateralized, algorithmic rates
- **Stablecoins**: Fiat-backed (USDC), crypto (DAI), algo (UST – failed)
- **Yield Farming**: Liquidity mining, impermanent loss

Scale & Risk:

- **Derivatives**: Perpetual futures, on-chain options
- **TVL**: $100B+ locked (peak 2021, recovered 2024)
- **Composability**: "Money legos" – powerful but risky

Innovation vs Risk: Composability enables innovation but also cascading failures

What Can NFTs and Tokens Enable?

NFTs & Digital Ownership:

- **NFTs**: Unique tokens, provable ownership
- **Use Cases**: Art, gaming, memberships, ticketing
- **Marketplaces**: OpenSea, Blur, Magic Eden
- **Royalties**: On-chain creator earnings

Token Economies & DAOs:

- **Tokenomics**: Utility vs governance, vesting
- **DAOs**: On-chain voting, treasury management
- **Boom/Bust**: \$25B peak $\rightarrow$ 90%+ correction

Lasting Impact: Digital ownership infrastructure, beyond speculative JPEGs

How Do We Scale and Secure Blockchains?

Layer 2 Scaling:

- Optimistic Rollups (fraud proofs, 7-day withdrawal)
- ZK-Rollups (validity proofs, instant finality)
- State channels (Lightning Network)
- Flash loans (uncollateralized, atomic)

Smart Contract Security:

- Reentrancy, oracle manipulation, access control
- Tools: Slither, Mythril, formal verification
- Defense: Audits + bug bounties + monitoring

Critical Lesson: $3B+ lost to exploits; composability enables innovation but also cascading failures

How Will Regulation Shape Crypto's Future?

Global Regulatory Landscape:

- **Spectrum**: China (ban) to Switzerland (permissive)
- **US**: SEC vs CFTC, regulation by enforcement
- **EU MiCA**: Stablecoin focus, CASP licensing
- **CBDCs**: 130+ countries exploring

Future Trends:

- Institutional adoption, RWA tokenization
- AI+crypto convergence, DePIN
- Account abstraction (UX breakthrough)
- ZK proofs (privacy + scalability)

Core Tension: Innovation vs regulation, privacy vs compliance

Why Can't We Have Full Decentralization AND Efficiency?

The Blockchain Trilemma:
Pick 2 of 3: Decentralization, Security, Scalability

- **Bitcoin**: Max decentralized, 7 TPS
- **Ethereum**: Decentralized + L2 scaling
- **Solana**: 65K TPS, less decentralized

Pragmatic Compromises:

- **CEXs**: Max efficiency, zero decentralization (FTX risk)
- **Layer 2**: Rollups inherit L1 security
- Context determines optimal trade-off

Design Philosophy: No perfect solution — every system optimizes for different points on the trilemma

When Does "Code is Law" Actually Apply?

The Ideal vs Reality:

- **Immutability**: Code executes exactly as written
- **DAO Hack (2016)**: $60M drained; hard fork reversed it (ETH vs ETC split)
- **SBF convicted**: Legal system overrides decentralization rhetoric

Open Debates:

- **Tornado Cash (2022)**: Can you sanction code?
- Most protocols have upgrade mechanisms (not truly immutable)
- Code operates within legal and social contexts

Reality: "Code is law" is an aspiration — code has bugs, and communities decide how to respond

Will Crypto Ever Move Beyond Speculation?

Speculation Dominates (2024):

- 90%+ transactions are trading
- Memecoins, pump-and-dump schemes
- Volatility hinders currency adoption

Utility Emerging:

- Stablecoins: $310B, real payments
- NFT ticketing adopted by sports teams
- DeFi: lending, derivatives work

Adoption S-Curve:

- 2010-2020: Early adopters, ideological
- 2024-2030: Institutional, utility-driven

Long-term Outlook:
Utility will dominate; speculation remains (like stock market)

What Does Permissionless Innovation Enable?

TradFi (Traditional Finance, i.e., banks, brokers, exchanges) vs DeFi:

- TradFi: Licenses, capital, compliance
- DeFi: Deploy contract, anyone can use

Innovation Examples:

- Uniswap: 2 devs, $100B+ volume
- Compound: Algorithmic interest rates
- Aave: Flash loans (impossible in TradFi)

Composability (Money Legos):

- Yearn: Aggregates lending protocols
- 1inch: Aggregates DEXs
- Curve Wars: Liquidity competition

Trade-off:
Exploits, scams, regulatory uncertainty

"Move fast and break things" applied to finance

Why Does Centralization Keep Emerging?

Paradox: Decentralized protocols have centralized components

Examples:

- Exchanges: Binance/Coinbase (70%+)
- Stablecoins: Circle can freeze USDC
- Infrastructure: Infura, Alchemy RPCs
- Staking: Lido dominates Ethereum

Nakamoto Coefficient:
(Min entities to halt network)

- Bitcoin: 4 mining pools
- Ethereum: 3 entities
- Solana: 19 validators

Reality:
Decentralization is a spectrum, not binary

Can Blockchain Provide Both Privacy and Transparency?

Blockchain Reality:

- All transactions public (pseudonymous)
- Chainalysis/Elliptic track funds

Privacy Solutions:

- Monero: Ring signatures, stealth addresses
- Zcash: Optional zk-SNARKs
- Tornado Cash: Sanctioned mixer
- Aztec: ZK proofs on Ethereum

Regulatory Conflict:

- AML/CFT requirements
- Tax enforcement needs
- Human right to privacy
- Dissident/activist protection

Future: ZK proofs enable privacy + compliance (prove legality without revealing details)

What Blockchain Does Well

1. **Censorship Resistance:** No single point of control
2. **Programmable Money:** Smart contract logic
3. **Composability:** Permissionless integration
4. **Global Access:** Internet = access
5. **Transparency:** Auditable transactions
6. **24/7 Operation:** No market hours
7. **Fast Settlement:** Minutes vs days
8. **Capital Efficiency:** Flash loans, atomic swaps

What Blockchain Does Poorly

1. **Scalability:** 7-65K TPS limit
2. **UX:** Seed phrases, gas fees, no support
3. **Energy:** Bitcoin 150 TWh/year
4. **Volatility:** Unsuitable as currency
5. **Regulation:** Unclear legal status
6. **Fraud:** Irreversible, no recourse
7. **Complexity:** Steep learning curve
8. **Centralization:** Pools, staking concentration

When Does Blockchain Actually Add Value?

Financial Applications:

- **Remittances**: Cheaper, faster (USDC, Lightning)
- **Inflation Hedge**: Store of value (Argentina, Venezuela)
- **Censorship Evasion**: Dissident donations
- **Financial Inclusion**: Banking the unbanked
- **Asset Tokenization**: Fractional ownership

Non-Financial Applications:

- **Supply Chain**: Provenance tracking
- **Decentralized Identity**: Self-sovereign, no gatekeepers
- **DAOs**: Coordination without hierarchy
- **Gaming**: True ownership of in-game assets

Heuristic: Blockchain adds value when censorship resistance or trustless coordination is critical

When is Blockchain Just Marketing Hype?

Overhyped Use Cases:

- **Supply Chains**: Centralized DBs work fine
- **Voting**: Privacy challenges outweigh benefits
- **Medical Records**: Transparency conflicts with privacy
- **Most NFTs**: Database + signature suffices

More Hype Than Substance:

- **Enterprise Blockchains**: Glorified shared databases
- **IoT**: Too slow for high-volume, low-latency needs
- **"Blockchain for X"**: Often a marketing buzzword

Heuristic: If you can use a database, use a database. Blockchain only when decentralization is critical.

What Did FTX Teach Us?

What Happened (Nov 2022):

- FTX commingled funds with Alameda
- Alameda lost billions (Luna, bad bets)
- Bank run after Binance CEO tweet
- $8B missing, SBF arrested

Key Lessons:

1. Not your keys, not your coins
2. Proof of reserves can be faked
3. Self-regulation failed
4. Offshore = less oversight
5. High yields = hidden risk

Industry Response: Merkle tree proofs, increased regulatory scrutiny

What Made 2024 Transformative for Crypto?

Q1 2024:

- **Jan**: SEC approves 11 Bitcoin ETFs
- BlackRock, Fidelity enter crypto
- \$50B+ AUM in first year
- **Mar**: Dencun upgrade (EIP-4844, an Ethereum upgrade that dramatically reduced Layer 2 transaction fees)
- L2 fees: \$0.50 $\rightarrow$ \$0.01

Q2-Q4 2024:

- **Apr**: Bitcoin 4th halving
- **Jul**: Ethereum ETFs approved
- **Nov**: Pro-crypto US administration
- **Dec**: MiCA full EU implementation

What's Changing in the 2025 Landscape?

Regulatory & Institutional:

- US: Pro-crypto leadership post-Gensler
- Stablecoin legislation priority, CBDC paused
- Bitcoin ETFs among largest commodity ETFs
- Banks exploring custody and trading

Technical & Market:

- L2 thriving: Base, Arbitrum, Optimism
- Restaking (EigenLayer) as new primitive
- Account abstraction accelerating
- Post-halving bull market dynamics

2025 marks a shift: institutional infrastructure, regulatory clarity, and L2 maturity converge

How Has Reality Evolved Since Course Design?

Topic	When Course Written	2025 Reality
Bitcoin ETFs	Speculative	Approved, $50B+ AUM
ETH staking	15M ETH staked	34M+ ETH staked
MiCA	Future framework	Fully implemented
US regulation	Hostile (Gensler)	Pro-crypto administration
Layer 2 fees	$0.50-2.00	$0.01-0.10 (post-Dencun)
DeFi TVL	Recovery phase	$80B+ TVL
Restaking	Emerging concept	$15B+ in EigenLayer
CBDCs	Racing ahead	US paused, EU preparing

Takeaway: Industry moves fast; stay current with primary sources

What Are the Critical Questions for 2025-2030?

Technology & Scaling:

- Will L2s solve scalability or alt-L1s dominate?
- Can ZK proofs enable privacy + compliance?
- Will cross-chain bridges remain attack vectors?
- Will post-quantum crypto deploy in time?
- Will account abstraction achieve Web2 UX?

Markets & Regulation:

- Will global regulation converge (MiCA) or fragment?
- Will CBDCs coexist with or crowd out crypto?
- Will \$1T+ institutional capital enter?
- DeFi vs CeFi: which model wins?
- Will PoS adoption resolve energy concerns?

These open questions define the next chapter of crypto — use the Cryptoeconomics Lens to evaluate them

What's the Best-Case Scenario for 2030?

Adoption & Scale:

- Institutional: Pension/sovereign funds allocate 5–10%
- Stablecoins: \$1T+ cap, global payments
- Tokenization: \$10T+ real-world assets on-chain
- L2 Success: 100,000+ TPS, fees <\$0.01
- Mainstream: 1B+ users (vs 500M in 2024)

Infrastructure & Governance:

- Regulatory clarity with global convergence
- Wallets as easy as email (account abstraction)
- ZK proofs: privacy + compliance together
- CBDCs complement, not replace, crypto

Best case: Financial system fundamentally transformed — more inclusive and efficient

What's the Worst-Case Scenario for 2030?

Regulatory & Market Risks:

- Crackdown: DeFi, privacy tools, self-custody banned
- CBDC monopoly outlaws competing stablecoins
- Centralization: Coinbase/Binance dominate
- Stablecoin collapse triggers DeFi contagion
- User apathy: complexity drives users to TradFi

Technical & Security Risks:

- L2s too complex/fragmented, fees stay high
- Major exploit (>$10B) destroys trust
- Quantum breaks ECDSA before migration
- PoW banned, PoS attacked as plutocracy

Worst case: Crypto becomes a niche tool (like Tor), not mainstream finance

What's the Most Likely Scenario for 2030?

Market & Adoption:

- Hybrid: Regulated CeFi + permissionless DeFi
- Stablecoins: Regulated, $500B cap, payments
- 750M users (50% growth), <10% global pop
- Use cases validated: remittances, tokenization, DAOs

Technology & Regulation:

- L2 maturity: 50,000 TPS, $0.10 fees
- Selective regulation: retail-facing regulated, protocols exempt
- Privacy constrained: KYC on/off ramps
- CBDCs launched but limited adoption

Most likely: Crypto as parallel financial system, not replacement — institutional via compliant ramps

Problem Solved? The Cryptoeconomics Synthesis

The Original Problem

How do all the pieces fit together?

How This Course Solves It

- **The Cryptoeconomics Lens**: 6 questions for any system (Problem, Incentives, Costs/Benefits, Failures, Design, Alternatives)
- **Cross-Cutting Themes**: Decentralization vs efficiency, code as law, speculation vs utility, permissionless innovation, centralization creep, privacy vs transparency
- **Critical Framework**: What blockchain does well vs poorly, legitimate vs questionable use cases

Remaining Limitations

- Technology evolves faster than frameworks - 2024 brought Bitcoin ETFs, MiCA, Dencun upgrade (all post-course design)
- No single framework captures all trade-offs - context determines optimal solution

Open Questions

- What will the next breakthrough be? (2025-2030: scaling, privacy, regulation, or something unexpected?)
- Will crypto transform finance or remain a parallel system?

Synthesis provides tools for lifelong learning, but the crypto landscape continues to evolve

Course Synthesis: The Journey Complete

- From "What is blockchain?" (L01) to "How do all the pieces fit together?" (L48)
- You now have the frameworks to evaluate any crypto project or protocol

[COMIC: "Learning journey recap" – A winding path from L01 to L48 with milestones: "Hash functions" (mountain), "Bitcoin" (coin), "Smart contracts" (robot), "DeFi" (money legos), "NFTs" (picture frame), "Regulation" (gavel), "Synthesis" (puzzle complete). Student at end with graduation cap, holding "The Cryptoeconomics Lens".]

[PLACEHOLDER] — The course gave you frameworks; the real learning continues as you apply them

What Are the Core Lessons from This Course?

Technology & Design:

- Technology enables, society decides
- Decentralization is hard (speed, cost, security trade-offs)
- Finance rebuilt from first principles, in public
- Security is existential (one exploit destroys years)
- UX must match Web2 for mainstream adoption

Markets & Society:

- Speculation funds innovation (dot-com parallel)
- Regulation is inevitable (enable or stifle?)
- Privacy matters but conflicts with AML
- The future is uncertain: revolutionary or niche?

These 9 lessons form the synthesis of 49 lessons across 7 modules

How Should You Evaluate Crypto Projects?

Don't Trust, Verify:

- Verify token contracts before investing
- Audit smart contracts before depositing
- Check proof of reserves (exchanges, stablecoins)

Beware Hype Cycles:

- 2017: ICO mania (95%+ failed)
- 2021: NFT boom (90%+ collapse)
- 2024: AI+crypto surge (FET, RNDR, TAO)

Cui Bono (Who Benefits)?

- Token launches: Founders/VCs dump on retail
- Yield farming: Early LPs extract from late entrants
- Influencer shills: Paid promotions as "education"

Intellectual Humility: This field evolves rapidly; today's truth may be tomorrow's outdated belief

How Can You Keep Learning About Crypto?

Learn from Primary Sources:

- Follow builders, not influencers (Vitalik, developers)
- Read whitepapers, protocol docs, GitHub repos
- Track on-chain data: Dune, Nansen, Glassnode

Hands-On Engagement:

- Try DeFi protocols (small amounts), deploy contracts
- Join communities: Discord, Twitter Crypto, meetups
- Participate: hackathons, audits, governance

The best way to learn crypto is to use crypto — start with testnets, then small mainnet amounts

Key Takeaways

What Blockchain Delivers:

- Permissionless, censorship-resistant value transfer
- Programmable money via smart contracts
- Transparent, auditable financial infrastructure
- New coordination mechanisms (DAOs, tokens)

What Remains Unsolved:

- Scalability–security–decentralization trilemma
- User experience gap vs. traditional finance
- Regulatory uncertainty across jurisdictions
- Bridging speculation and real-world utility

Blockchain is a tool, not a solution—its value depends on thoughtful application to real problems

Parting Wisdom

"The best way to predict the future is to invent it."

– Alan Kay

"In the long run, the most important thing is not to make money, but to build systems that are more fair, more open, and more free."

– Crypto Ethos

"Stay curious. Stay skeptical. Stay building."

– Course Conclusion

Thank you for completing this course!

You now have the foundational knowledge to:

- Understand blockchain technology and cryptocurrencies
- Build decentralized applications
- Participate in DeFi protocols
- Critically evaluate crypto projects
- Navigate the regulatory landscape
- Pursue a career in Web3

The journey has just begun.
Keep learning, keep building, keep questioning.

Contact: [Your contact information]
Course Materials: [GitHub/Website URL]

L48: Course Synthesis

Mini-Lecture – Module G: Regulation & Future

Blockchain & Cryptocurrency Course

January 2026

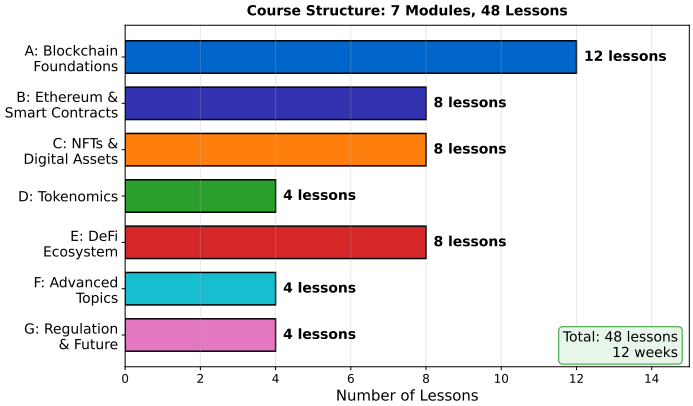
(c) Joerg Osterrieder 2025

Learning Objectives

By the end of this mini-lecture, you will be able to:

- Synthesize key takeaways from all seven course modules
- Identify cross-cutting themes (trilemma, code-is-law, centralization)
- Evaluate what blockchain does well vs poorly
- Apply critical thinking to evaluate crypto projects and trends

Course Journey: Seven Modules



Foundations → Crypto → Ethereum → DeFi → NFTs → Advanced → Future

Module Key Takeaways

A-C (Foundations):

- Blockchain = trust through math; PoW/PoS consensus
- Bitcoin: 21M cap, UTXOs; Ethereum: EVM, smart contracts

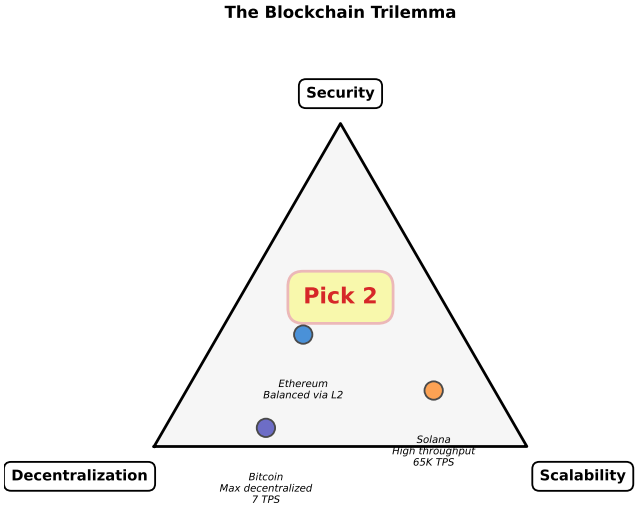
D-E (Applications):

- DeFi: AMMs, lending, stablecoins; TVL $100B+
- NFTs: Digital ownership, tokenomics, DAOs

F-G (Advanced):

- Layer 2: Rollups for scalability (Dencun: 90% fee reduction)
- Security: $3B+ lost to exploits; audits essential
- Regulation: MiCA (EU), US shifting pro-crypto (2025)

Cross-Cutting Theme: The Trilemma



No perfect solution: Bitcoin (decentralized), Solana (fast), L2 (compromise).

Cross-Cutting Themes

Code is Law – Until It Isn't

- DAO hack (2016): Community chose fork over "immutability"
- Tornado Cash sanctioned; SBF convicted

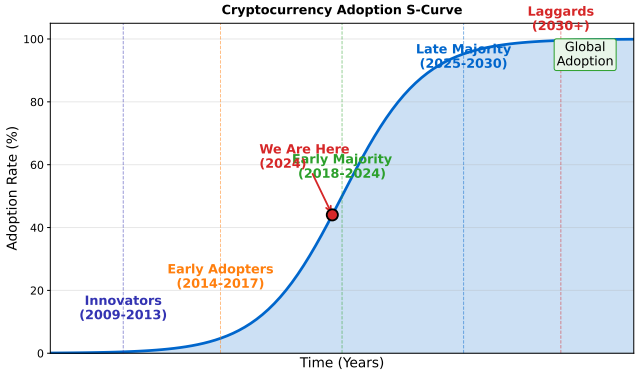
Centralization Creep

- Exchanges dominate (Binance 70%+); Circle can freeze USDC
- Nakamoto coefficient: BTC 4 pools, ETH 3 entities

Speculation vs Utility

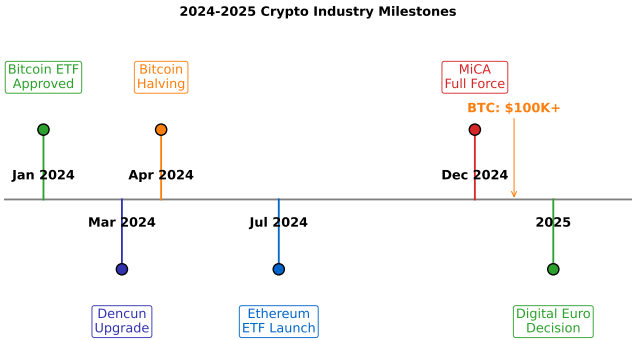
- 90%+ trading is speculation; but stablecoins ($310B) have real use

Speculation vs Utility: The S-Curve



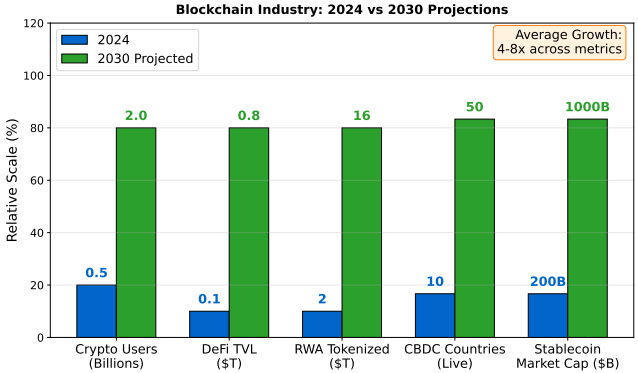
2024-2030: Crossing the chasm from speculation to institutional/utility.

2024-2025: Transformative Years



Bitcoin ETF approval, Dencun upgrade, MiCA implementation, pro-crypto US shift.

2030 Scenarios



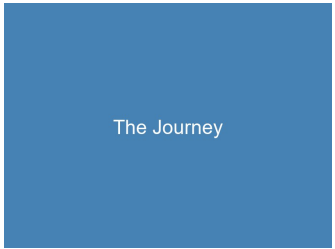
Realistic: Hybrid CeFi/DeFi, regulated stablecoins, 750M users, parallel system.

Key Takeaways

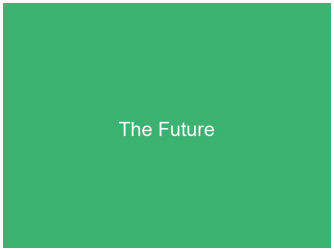
1. **Technology Enables, Society Decides:** Outcomes depend on adoption & regulation
2. **Decentralization is Hard:** Tradeoffs everywhere (speed, cost, security, UX)
3. **Security is Existential:** One exploit can destroy years of progress
4. **Speculation Funds Innovation:** Bubbles destructive but fund R&D
5. **Stay Curious, Stay Skeptical:** Verify, don't trust hype cycles

Don't Trust, Verify. Keep learning, keep building, keep questioning.

Course Synthesis



The Journey



The Future

Blockchain Tech

Images: Unsplash (CC0)

Quiz (1/2)

Q1. What is the blockchain trilemma?
A) Three blockchains B) Cannot optimize decentralization + security + scalability C) Three tokens D) Three layers

Quiz (1/2)

Q1. What is the blockchain trilemma?
A) Three blockchains B) Cannot optimize decentralization + security + scalability C) Three tokens D) Three layers
Answer: B – Must sacrifice one of the three properties.

Q2. What did The DAO hack (2016) demonstrate?
A) Code is perfect B) Immutability can be overridden by community C) Ethereum is insecure D) Bitcoin is better

Quiz (1/2)

Q1. What is the blockchain trilemma?
A) Three blockchains B) Cannot optimize decentralization + security + scalability C) Three tokens D) Three layers
Answer: B – Must sacrifice one of the three properties.

Q2. What did The DAO hack (2016) demonstrate?
A) Code is perfect B) Immutability can be overridden by community C) Ethereum is insecure D) Bitcoin is better
Answer: B – Community chose to fork, showing "code is law" has limits.

Q3. What is the Nakamoto coefficient?
A) Mining difficulty B) Minimum entities to halt network C) Token supply D) Block size

Quiz (1/2)

Q1. What is the blockchain trilemma?
A) Three blockchains B) Cannot optimize decentralization + security + scalability C) Three tokens D) Three layers
Answer: B – Must sacrifice one of the three properties.

Q2. What did The DAO hack (2016) demonstrate?
A) Code is perfect B) Immutability can be overridden by community C) Ethereum is insecure D) Bitcoin is better
Answer: B – Community chose to fork, showing "code is law" has limits.

Q3. What is the Nakamoto coefficient?
A) Mining difficulty B) Minimum entities to halt network C) Token supply D) Block size
Answer: B – Measures decentralization by minimum entities to control 51%.

Q4. What milestone occurred in January 2024?
A) The Merge B) Bitcoin halving C) Spot Bitcoin ETF approval D) MiCA passed

Quiz (1/2)

Q1. What is the blockchain trilemma?
A) Three blockchains B) Cannot optimize decentralization + security + scalability C) Three tokens D) Three layers
Answer: B – Must sacrifice one of the three properties.

Q2. What did The DAO hack (2016) demonstrate?
A) Code is perfect B) Immutability can be overridden by community C) Ethereum is insecure D) Bitcoin is better
Answer: B – Community chose to fork, showing "code is law" has limits.

Q3. What is the Nakamoto coefficient?
A) Mining difficulty B) Minimum entities to halt network C) Token supply D) Block size
Answer: B – Measures decentralization by minimum entities to control 51%.

Q4. What milestone occurred in January 2024?
A) The Merge B) Bitcoin halving C) Spot Bitcoin ETF approval D) MiCA passed
Answer: C – SEC approved 11 spot Bitcoin ETFs.

Q5. What did Dencun upgrade (March 2024) achieve?
A) PoS transition B) 90%+ L2 fee reduction C) Bitcoin compatibility D) NFT standard

Quiz (1/2)

Q1. What is the blockchain trilemma?
A) Three blockchains B) Cannot optimize decentralization + security + scalability C) Three tokens D) Three layers
Answer: B – Must sacrifice one of the three properties.

Q2. What did The DAO hack (2016) demonstrate?
A) Code is perfect B) Immutability can be overridden by community C) Ethereum is insecure D) Bitcoin is better
Answer: B – Community chose to fork, showing "code is law" has limits.

Q3. What is the Nakamoto coefficient?
A) Mining difficulty B) Minimum entities to halt network C) Token supply D) Block size
Answer: B – Measures decentralization by minimum entities to control 51%.

Q4. What milestone occurred in January 2024?
A) The Merge B) Bitcoin halving C) Spot Bitcoin ETF approval D) MiCA passed
Answer: C – SEC approved 11 spot Bitcoin ETFs.

Q5. What did Dencun upgrade (March 2024) achieve?
A) PoS transition B) 90%+ L2 fee reduction C) Bitcoin compatibility D) NFT standard
Answer: B – Proto-danksharding reduced L2 fees from \$0.50 to \$0.01.

Quiz (2/2)

Q6. What is the realistic 2030 scenario?
A) Crypto banned B) Full replacement of TradFi C) Hybrid CeFi/DeFi coexistence D) Only CBDCs survive

Quiz (2/2)

Q6. What is the realistic 2030 scenario?
A) Crypto banned B) Full replacement of TradFi C) Hybrid CeFi/DeFi coexistence D) Only CBDCs survive
Answer: C – Regulated + permissionless systems will coexist.

Q7. What percentage of crypto transactions are speculation (2024)?
A) 10% B) 50% C) 75% D) 90%+

Quiz (2/2)

Q6. What is the realistic 2030 scenario?
A) Crypto banned B) Full replacement of TradFi C) Hybrid CeFi/DeFi coexistence D) Only CBDCs survive
Answer: C – Regulated + permissionless systems will coexist.

Q7. What percentage of crypto transactions are speculation (2024)?
A) 10% B) 50% C) 75% D) 90%+
Answer: D – Trading/speculation dominates; utility emerging.

Q8. What is the FTX collapse's main lesson?
A) DeFi is safe B) Not your keys, not your coins C) Exchanges are trustworthy D) Proof of reserves works

Quiz (2/2)

Q6. What is the realistic 2030 scenario?
A) Crypto banned B) Full replacement of TradFi C) Hybrid CeFi/DeFi coexistence D) Only CBDCs survive
Answer: C – Regulated + permissionless systems will coexist.

Q7. What percentage of crypto transactions are speculation (2024)?
A) 10% B) 50% C) 75% D) 90%+
Answer: D – Trading/speculation dominates; utility emerging.

Q8. What is the FTX collapse's main lesson?
A) DeFi is safe B) Not your keys, not your coins C) Exchanges are trustworthy D) Proof of reserves works
Answer: B – Custodial risk; self-custody is safer.

Q9. What stablecoin market cap indicates real utility?
A) $10B B) $50B C) $310B D) $1T

Quiz (2/2)

Q6. What is the realistic 2030 scenario?
A) Crypto banned B) Full replacement of TradFi C) Hybrid CeFi/DeFi coexistence D) Only CBDCs survive
Answer: C – Regulated + permissionless systems will coexist.

Q7. What percentage of crypto transactions are speculation (2024)?
A) 10% B) 50% C) 75% D) 90%+
Answer: D – Trading/speculation dominates; utility emerging.

Q8. What is the FTX collapse's main lesson?
A) DeFi is safe B) Not your keys, not your coins C) Exchanges are trustworthy D) Proof of reserves works
Answer: B – Custodial risk; self-custody is safer.

Q9. What stablecoin market cap indicates real utility?
A) $10B B) $50B C) $310B D) $1T
Answer: C – $310B stablecoin market (Dec 2025) shows payment use.

Q10. Best way to stay current in crypto?
A) Follow influencers B) Read primary sources, use products C) Watch price charts D) Wait for news

Quiz (2/2)

Q6. What is the realistic 2030 scenario?
A) Crypto banned B) Full replacement of TradFi C) Hybrid CeFi/DeFi coexistence D) Only CBDCs survive
Answer: C – Regulated + permissionless systems will coexist.

Q7. What percentage of crypto transactions are speculation (2024)?
A) 10% B) 50% C) 75% D) 90%+
Answer: D – Trading/speculation dominates; utility emerging.

Q8. What is the FTX collapse's main lesson?
A) DeFi is safe B) Not your keys, not your coins C) Exchanges are trustworthy D) Proof of reserves works
Answer: B – Custodial risk; self-custody is safer.

Q9. What stablecoin market cap indicates real utility?
A) $10B B) $50B C) $310B D) $1T
Answer: C – $310B stablecoin market (Dec 2025) shows payment use.

Q10. Best way to stay current in crypto?
A) Follow influencers B) Read primary sources, use products C) Watch price charts D) Wait for news
Answer: B – Whitepapers, GitHub, hands-on experience.

Thank you for completing this course!

Keep learning, keep building, keep questioning.

The journey has just begun.

Quiz: Course Synthesis

Instructions: 10 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the fundamental trade-off described by the blockchain trilemma?
A) Cost, speed, privacy B) Security, decentralization, scalability C) Transparency, immutability D) Energy, throughput

Quiz (1–5)

Q1. What is the fundamental trade-off described by the blockchain trilemma?
A) Cost, speed, privacy B) Security, decentralization, scalability C) Transparency, immutability D) Energy, throughput
Answer: B – Cannot optimize all three: security, decentralization, or scalability.

Q2. What consensus mechanism did Ethereum switch to in The Merge?
A) Proof of Work B) Proof of Stake C) Proof of Authority D) Byzantine Fault Tolerance

Quiz (1–5)

Q1. What is the fundamental trade-off described by the blockchain trilemma?
A) Cost, speed, privacy B) Security, decentralization, scalability C) Transparency, immutability D) Energy, throughput
Answer: B – Cannot optimize all three: security, decentralization, or scalability.

Q2. What consensus mechanism did Ethereum switch to in The Merge?
A) Proof of Work B) Proof of Stake C) Proof of Authority D) Byzantine Fault Tolerance
Answer: B – PoS achieved 99% energy reduction from PoW.

Q3. Which ERC standard is used for fungible tokens?
A) ERC-721 B) ERC-1155 C) ERC-20 D) ERC-777

Quiz (1–5)

Q1. What is the fundamental trade-off described by the blockchain trilemma?
A) Cost, speed, privacy B) Security, decentralization, scalability C) Transparency, immutability D) Energy, throughput
Answer: B – Cannot optimize all three: security, decentralization, or scalability.

Q2. What consensus mechanism did Ethereum switch to in The Merge?
A) Proof of Work B) Proof of Stake C) Proof of Authority D) Byzantine Fault Tolerance
Answer: B – PoS achieved 99% energy reduction from PoW.

Q3. Which ERC standard is used for fungible tokens?
A) ERC-721 B) ERC-1155 C) ERC-20 D) ERC-777
Answer: C – ERC-20 for fungible; ERC-721 for NFTs.

Q4. What AMM formula do DEXs like Uniswap use?
A) $x + y = k$ B) $x * y = k$ C) $x - y = k$ D) $x / y = k$

Quiz (1–5)

Q1. What is the fundamental trade-off described by the blockchain trilemma?
A) Cost, speed, privacy B) Security, decentralization, scalability C) Transparency, immutability D) Energy, throughput
Answer: B – Cannot optimize all three: security, decentralization, scalability.

Q2. What consensus mechanism did Ethereum switch to in The Merge?
A) Proof of Work B) Proof of Stake C) Proof of Authority D) Byzantine Fault Tolerance
Answer: B – PoS achieved 99% energy reduction from PoW.

Q3. Which ERC standard is used for fungible tokens?
A) ERC-721 B) ERC-1155 C) ERC-20 D) ERC-777
Answer: C – ERC-20 for fungible; ERC-721 for NFTs.

Q4. What AMM formula do DEXs like Uniswap use?
A) x + y = k B) x * y = k C) x - y = k D) x / y = k
Answer: B – Constant product: x * y = k maintains liquidity.

Q5. What EU crypto regulation was fully implemented in December 2024?
A) FATF Guidelines B) MiCA C) Basel III D) Dodd-Frank

Quiz (1–5)

Q1. What is the fundamental trade-off described by the blockchain trilemma?
A) Cost, speed, privacy B) Security, decentralization, scalability C) Transparency, immutability D) Energy, throughput
Answer: B – Cannot optimize all three: security, decentralization, scalability.

Q2. What consensus mechanism did Ethereum switch to in The Merge?
A) Proof of Work B) Proof of Stake C) Proof of Authority D) Byzantine Fault Tolerance
Answer: B – PoS achieved 99% energy reduction from PoW.

Q3. Which ERC standard is used for fungible tokens?
A) ERC-721 B) ERC-1155 C) ERC-20 D) ERC-777
Answer: C – ERC-20 for fungible; ERC-721 for NFTs.

Q4. What AMM formula do DEXs like Uniswap use?
A) $x + y = k$ B) $x * y = k$ C) $x - y = k$ D) $x / y = k$
Answer: B – Constant product: $x * y = k$ maintains liquidity.

Q5. What EU crypto regulation was fully implemented in December 2024?
A) FATF Guidelines B) MiCA C) Basel III D) Dodd-Frank
Answer: B – Markets in Crypto-Assets provides comprehensive framework.

Quiz (6–10)

Q6. What is the withdrawal period for Optimistic Rollups?
A) Instant B) 1 day C) 7 days D) 30 days

Quiz (6–10)

Q6. What is the withdrawal period for Optimistic Rollups?
A) Instant B) 1 day C) 7 days D) 30 days
Answer: C – 7-day challenge period before withdrawals finalize.

Q7. What 2016 event led to Ethereum's hard fork?
A) Mt. Gox hack B) The DAO hack C) Parity freeze D) Terra collapse

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the withdrawal period for Optimistic Rollups?
A) Instant B) 1 day C) 7 days D) 30 days
Answer: C – 7-day challenge period before withdrawals finalize.

Q7. What 2016 event led to Ethereum's hard fork?
A) Mt. Gox hack B) The DAO hack C) Parity freeze D) Terra collapse
Answer: B – $60M drained, controversial fork to reverse theft.

Q8. What percentage of staked ETH does Lido control?
A) 10% B) 20% C) 30%+ D) 50%+

Quiz (6–10)

Q6. What is the withdrawal period for Optimistic Rollups?
A) Instant B) 1 day C) 7 days D) 30 days
Answer: C – 7-day challenge period before withdrawals finalize.

Q7. What 2016 event led to Ethereum's hard fork?
A) Mt. Gox hack B) The DAO hack C) Parity freeze D) Terra collapse
Answer: B – $60M drained, controversial fork to reverse theft.

Q8. What percentage of staked ETH does Lido control?
A) 10% B) 20% C) 30%+ D) 50%+
Answer: C – Over 30%, raising centralization concerns.

Q9. What is the Nakamoto Coefficient?
A) Hash rate metric B) Measure of decentralization C) Transaction speed D) Energy efficiency

Quiz (6–10)

Q6. What is the withdrawal period for Optimistic Rollups?
A) Instant B) 1 day C) 7 days D) 30 days
Answer: C – 7-day challenge period before withdrawals finalize.

Q7. What 2016 event led to Ethereum's hard fork?
A) Mt. Gox hack B) The DAO hack C) Parity freeze D) Terra collapse
Answer: B – $60M drained, controversial fork to reverse theft.

Q8. What percentage of staked ETH does Lido control?
A) 10% B) 20% C) 30%+ D) 50%+
Answer: C – Over 30%, raising centralization concerns.

Q9. What is the Nakamoto Coefficient?
A) Hash rate metric B) Measure of decentralization C) Transaction speed D) Energy efficiency
Answer: B – Minimum entities needed to compromise network.

Q10. What is the recommended blockchain use case heuristic?
A) Always use blockchain B) If a database works, use it C) Only for finance D) Never centralized

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What is the withdrawal period for Optimistic Rollups?
A) Instant B) 1 day C) 7 days D) 30 days
Answer: C – 7-day challenge period before withdrawals finalize.

Q7. What 2016 event led to Ethereum's hard fork?
A) Mt. Gox hack B) The DAO hack C) Parity freeze D) Terra collapse
Answer: B – $60M drained, controversial fork to reverse theft.

Q8. What percentage of staked ETH does Lido control?
A) 10% B) 20% C) 30%+ D) 50%+
Answer: C – Over 30%, raising centralization concerns.

Q9. What is the Nakamoto Coefficient?
A) Hash rate metric B) Measure of decentralization C) Transaction speed D) Energy efficiency
Answer: B – Minimum entities needed to compromise network.

Q10. What is the recommended blockchain use case heuristic?
A) Always use blockchain B) If a database works, use it C) Only for finance D) Never centralized
Answer: B – If a database suffices, blockchain adds unnecessary complexity.

W01: Deploy Your First Smart Contract

Module H: Hands-On Workshops

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Smart Contract Deployment in a Nutshell

- Every developer remembers their first “Hello World” – but on blockchain, your code lives forever
- The moment you click “Deploy” and see that green checkmark: you just became a blockchain developer

[COMIC: Developer celebrates “Hello World” achievement on blockchain – confetti, champagne, green checkmark on screen. Caption: “My code will outlive me!”]

[PLACEHOLDER] — Your first deployment is a rite of passage into Web3 development

The Problem: How do you deploy code to a global, censorship-resistant computer?

The Challenge
Traditional software runs on servers you (or a company) control. What if you want code that:

- Runs exactly as written, forever
- Cannot be censored or shut down
- Is verifiable by anyone

Why It Matters

- DeFi, NFTs, DAOs — all built on smart contracts
- $100B+ value secured by deployed code

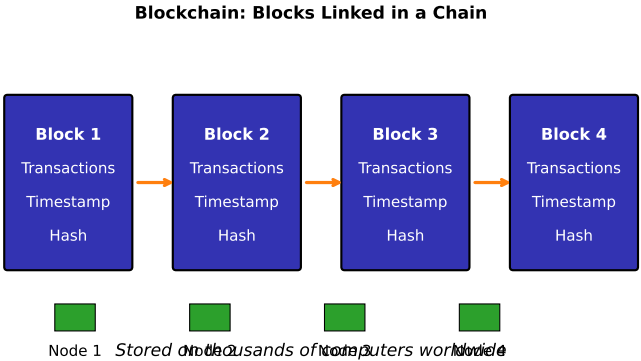
What We Need

- Testnet environment (no real money at risk)
- Wallet to sign transactions
- Code editor and deployment interface

The Cryptoeconomics Question
How do economic incentives ensure your deployed code runs correctly?

Today's workshop: Deploy your first smart contract to Ethereum's Sepolia testnet in 15 minutes

What is a Blockchain?



Your code will be stored permanently on this global network of computers

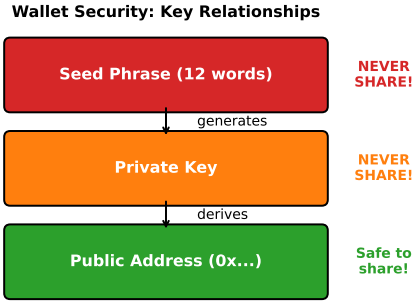
What is a Smart Contract?

Smart Contract: Code on the Blockchain

Immutable	**Public**	**Deterministic**	**Permanent**
Cannot be changed	Anyone can call	Same input = same output	Exists forever

Today you'll deploy your own smart contract – same tech behind DeFi, NFTs, DAOs

What is a Crypto Wallet?



Public address = Your identity on blockchain (like email address)

MetaMask = browser wallet that signs transactions and connects to websites

Why Do We Need Two Networks? Testnet vs Mainnet

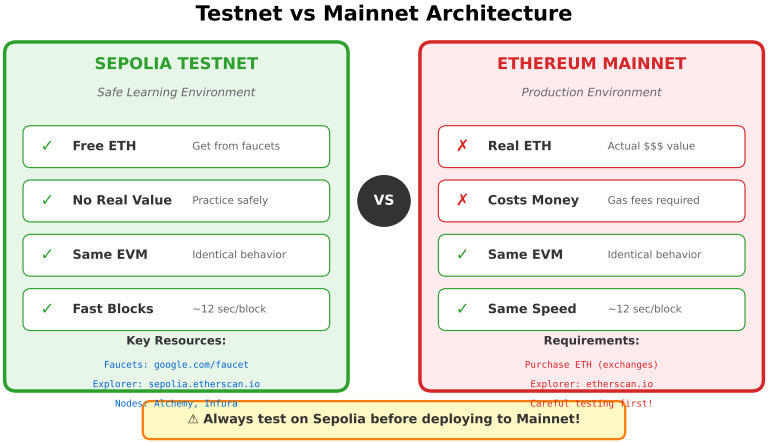
We use SEPOLIA TESTNET for learning:

Aspect	Testnet (Sepolia)	Mainnet
ETH Value	Free, no real value	Real money ($$$)
Purpose	Learning, testing	Production
Mistakes	Cost nothing	Can lose funds

Important: Never deploy practice code to mainnet – you could lose real money!

Sepolia ETH is free from faucets; mainnet ETH must be purchased

How Does Sepolia Architecture Compare to Mainnet?



Both networks use the same EVM – code works identically on testnet and mainnet

Workshop Objectives

By the end of this workshop, you will:

- Set up MetaMask wallet connected to Sepolia testnet
- Write a simple Solidity smart contract
- Compile and deploy using Remix IDE
- Interact with your deployed contract
- Verify your contract on Etherscan

Deliverable: Your contract address on Sepolia + screenshot

Estimated time: 45-60 minutes

What Do You Need Before Starting?

Before starting, ensure you have:

1. Chrome, Firefox, or Brave browser
2. MetaMask extension installed
3. Sepolia test ETH (we'll get this together)
4. Basic understanding of Solidity (from L15)

No coding experience required! We'll guide you step-by-step.

All tools are free and browser-based

How Do You Set Up MetaMask?

Install MetaMask:

1. Go to `metamask.io`
2. Click “Download” and add browser extension
3. Create new wallet (save seed phrase securely!)
4. Set a strong password

Switch to Sepolia Testnet:

1. Click network dropdown (top left)
2. Enable “Show test networks” in settings
3. Select “Sepolia”

NEVER share your seed phrase with anyone!

Why Do We Need ETH? (Gas Explained)

What is Gas?

- Fee paid to process your transaction on the blockchain
- Compensates the computers running the network
- More complex operations = more gas required

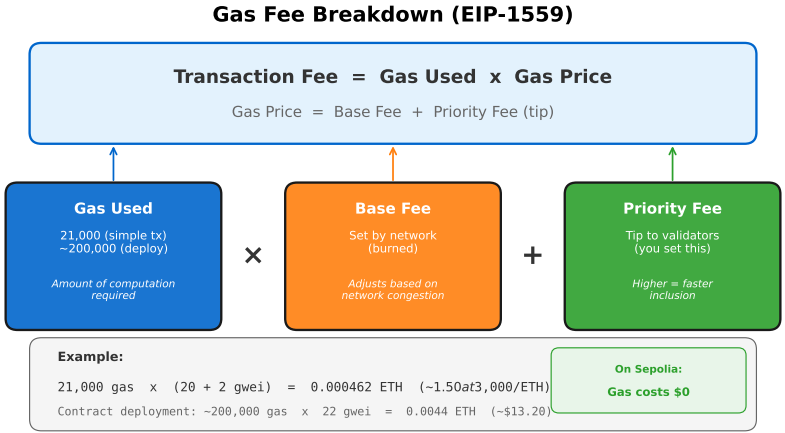
When Do You Pay Gas?

- **Deploying** a contract (one-time cost)
- **Writing** data (changing blockchain state)
- **Reading** data is FREE (no gas needed)

For This Workshop: We use free test ETH, so gas costs nothing real!

*On mainnet, gas fees range from **$1-$50+** depending on network congestion*

How Are Gas Fees Calculated Under EIP-1559?



On Sepolia testnet, gas is free – but understanding fees prepares you for mainnet

Where Can You Get Free Test ETH?

Primary Faucets (try in order):

1. Google Cloud: `cloud.google.com/application/web3/faucet/ethereum/sepolia`
2. Alchemy: `sepoliafaucet.com`
3. Infura: `infura.io/faucet/sepolia`

Backup Faucets (if primary fails):

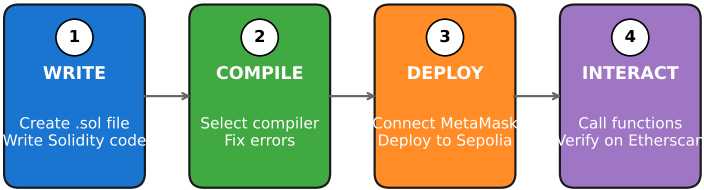
- QuickNode: `faucet.quicknode.com/ethereum/sepolia`
- Chainlink: `faucets.chain.link/sepolia`

Faucet rate limited? Try a different one! Most limit 0.1 ETH per day.

You need 0.01 ETH for this workshop

What Does the Development Workflow Look Like in Remix?

Remix IDE Development Workflow



Each step in Remix IDE - all in your browser!

Remix IDE handles everything in your browser - no installation needed

How Does Remix IDE Work?

Go to: `remix.ethereum.org`

Interface Overview:

- **File Explorer** (left): Create and manage .sol files
- **Editor** (center): Write your Solidity code
- **Compiler** (left sidebar): Compile your contract
- **Deploy** (left sidebar): Deploy to blockchain

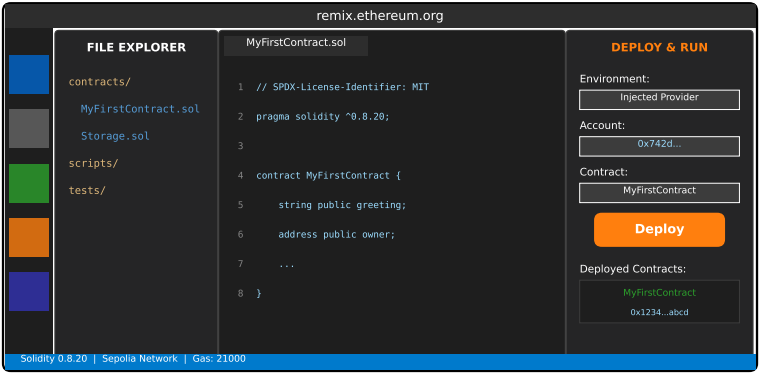
Create new file:

1. Click “contracts” folder
2. Click “New File” icon
3. Name it: `MyFirstContract.sol`

Remix auto-saves your work in browser storage

What Are the Key Components of the Remix Interface?

Remix IDE Interface Overview



Key panels: File Explorer (left), Editor (center), Deploy & Run (right sidebar)

What Are the Parts of a Solidity Contract?

Every Solidity file has three parts:

1. **License** (required):
   - `// SPDX-License-Identifier: MIT`
   - Declares your code is open source
2. **Compiler Version**:
   - `pragma solidity ^0.8.20;`
   - Tells Remix which Solidity version to use
3. **Contract Block**:
   - `contract MyContract { ... }`
   - Contains all your code

Think of a contract like a class in other programming languages

What Goes Inside Your Contract?

Inside your contract:

State Variables – Data stored permanently on blockchain:

- `string public greeting;` – A text value anyone can read
- `address public owner;` – A wallet/contract address

Constructor – Runs ONCE when contract is deployed:

- Sets up initial values
- Parameters come from deployment inputs

Functions – Code others can call:

- `public` = anyone can call
- Can read or change state variables

See L15 for detailed Solidity fundamentals

What Code Do You Need to Write?

Copy this code into Remix:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract MyFirstContract {
    string public greeting;
    string public ownerName;
    address public owner;

    constructor(string memory _name) {
        owner = msg.sender;
        ownerName = _name;
        greeting = "Hello, Blockchain!";
    }

    function setGreeting(string memory _greeting) public {
        greeting = _greeting;
    }
}
```

Full template available in contracts/MyFirstContract.sol

What Does Each Line of Code Do?

Line-by-line breakdown:

`string public greeting;`
→ A text variable anyone can read

`address public owner;`
→ Stores who deployed the contract

`constructor(string memory _name)`
→ Runs once; _name is what YOU type when deploying

`owner = msg.sender;`
→ `msg.sender` = YOUR wallet address (automatic!)

`function setGreeting(...) public`
→ Anyone can call this to change the greeting

msg.sender is a special variable Solidity provides automatically

Why Do You Need to Compile Your Contract?

What is Compilation?

- Translates human-readable Solidity into machine code (bytecode)
- Bytecode is what actually runs on Ethereum
- Like translating English to a language computers understand

In Remix:

1. Click "Solidity Compiler" icon (left sidebar)
2. Select compiler version: `0.8.20`
3. Click "Compile MyFirstContract.sol"
4. Green checkmark = success!

Errors? Red = syntax error (check semicolons, brackets)

Yellow warnings are usually okay to ignore

What Does “Deploy” Mean?

Deployment = Publishing your contract to the blockchain

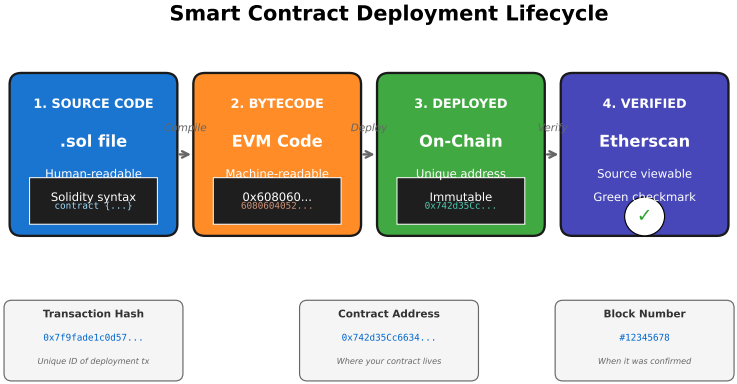
What happens:

1. Your compiled bytecode is sent to the network
2. It’s stored permanently at a unique address (0x...)
3. Anyone can now interact with your contract
4. You CANNOT change or delete it (immutable!)

Key Point: Deployment is permanent! Once deployed, your contract exists forever on the blockchain.

This is why we test on Sepolia first – mistakes on mainnet are forever

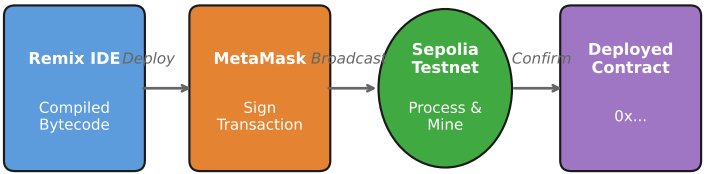
What Happens During the Contract Lifecycle?



Source code becomes bytecode, deployed to unique address, then verified on Etherscan

How Does the Deployment Process Flow?

Smart Contract Deployment Flow



Gas Fee: ~0.001 ETH (free on testnet!)

MetaMask signs the transaction, Sepolia processes it, you get a contract address

What is a Transaction?

Transaction = A request to change something on the blockchain

Examples of transactions:

- Deploying a new contract (what we're doing!)
- Calling a function that changes data
- Sending ETH to someone

NOT a transaction: Reading data (free, no signature needed)

Why does MetaMask pop up?

- You're authorizing the blockchain change
- You're agreeing to pay the gas fee
- Your private key signs the transaction

Every transaction is recorded publicly and permanently

How Do You Deploy to Sepolia?

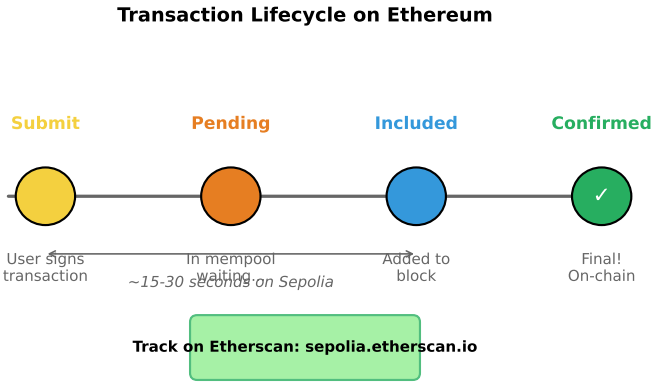
In Remix:

1. Click "Deploy & Run" icon (left sidebar)
2. Environment: Select "Injected Provider - MetaMask"
3. MetaMask popup: Click "Connect"
4. Verify: Network shows "Sepolia"
5. Enter your name in the `_name` field
6. Click "Deploy"
7. MetaMask popup: Click "Confirm"

Wait 15-30 seconds for confirmation!

You'll pay gas from your Sepolia test ETH

How Is Your Transaction Confirmed?



Your contract is now permanently on the Sepolia blockchain!

How Do You Interact With Your Deployed Contract?

After deployment, in Remix:

1. See your contract under "Deployed Contracts"
2. Click to expand
3. **Read functions** (blue buttons):
   - Click `greeting` – shows "Hello, Blockchain!"
   - Click `ownerName` – shows your name
   - Click `owner` – shows your wallet address
4. **Write functions** (orange buttons):
   - Enter new text in `setGreeting` field
   - Click button, confirm in MetaMask
   - Wait for confirmation, then click `greeting` again

Blue = free (view only), Orange = costs gas (state change)

How Can You View Your Contract Publicly?

Find your contract:

1. Copy contract address from Remix (click copy icon)
2. Go to `sepolia.etherscan.io`
3. Paste address in search bar
4. View your contract page!

What you'll see:

- Contract creation transaction
- All function calls you made
- Contract balance (0 ETH)

Etherscan is the public record of all blockchain activity

Workshop Deliverables

To complete this workshop, submit:

1. Your deployed contract address on Sepolia
   - Format: `0x...` (42 characters)
2. Screenshot showing:
   - Your contract in Remix with your name
   - Etherscan page showing your contract

Bonus (optional):

- Add a `setName()` function to change owner name
- Call your classmate's contract

See lab_guide.md for detailed step-by-step instructions

What Do Common Error Messages Mean?

Error Message	Solution
“Insufficient funds for gas”	Get more ETH from faucet (try backup list)
“Transaction underpriced”	Wait 30s and retry, network is busy
“Nonce too high/low”	Reset MetaMask: Settings ¿ Advanced ¿ Clear Activity
“execution reverted”	Check function inputs are correct
“ParserError: Expected ‘;’ ’	Add missing semicolon at end of line
“DeclarationError”	Variable name typo or undeclared

MetaMask popup doesn’t appear?

1. Check MetaMask extension is unlocked
2. Refresh Remix and reconnect
3. Try different browser (Chrome recommended)

What You Just Accomplished!

You just:

- Created your blockchain identity (wallet)
- Wrote actual Solidity smart contract code
- Deployed a program that lives FOREVER on Ethereum
- Joined 200M+ smart contract users worldwide

Your contract will exist as long as Ethereum exists!

This is the same technology behind:

- DeFi protocols managing $100B+ in assets
- NFT marketplaces
- DAOs governing organizations

You've taken your first step into blockchain development

The Reality of Deployment in a Nutshell

- That moment when you deploy your first contract and realize gas fees are real (even on testnet, the lesson sticks)
- "Wait, I can't undo this?" – immutability hits different when it's your code

[COMIC: Developer staring at MetaMask gas estimate in shock, coffee cup frozen mid-sip. Caption: "0.003 ETH just to say Hello World?!"]

[PLACEHOLDER] — On mainnet, gas optimization becomes an art form – every byte costs real money

Summary

What you learned:

- Set up MetaMask and connected to Sepolia testnet
- Wrote a Solidity smart contract with state variables
- Compiled and deployed using Remix IDE
- Interacted with your live contract on the blockchain
- Verified your contract on Etherscan

Next Workshop: W02 - Create Your Own Cryptocurrency (ERC-20 token)

Congratulations! You deployed your first smart contract!

Glossary: Key Terms

Term	Definition
Blockchain	Distributed database of linked blocks
Smart Contract	Code stored and executed on blockchain
Wallet	Software managing your blockchain identity
Seed Phrase	12 words that generate your private key
Gas	Fee paid for blockchain operations
Testnet	Practice network with free fake ETH
Deploy	Publishing your contract to blockchain
Etherscan	Website to view blockchain activity

Refer back to this when you encounter unfamiliar terms

(c) Joerg Osterrieder 2025

Next Steps

Continue Learning:

1. Complete W02 (Create Your Own Cryptocurrency)
2. Review L15 (Solidity Fundamentals) for deeper understanding
3. Try modifying your contract (add new functions!)

Explore Further:

- L17: ERC-20 Token Standard (theory behind W02)
- L43: Smart Contract Security
- Remix documentation: `remix-ide.readthedocs.io`

Challenge: Add a `setName()` function that only the owner can call!

Keep building – every expert started exactly where you are now

Questions for Reflection

1. Why does calling `setGreeting()` cost gas but reading `greeting` is free?
2. What happens to your contract if you lose access to your MetaMask wallet?
3. Why is the constructor only called once?
4. How would you make only the owner able to change the greeting?
5. What's the difference between Sepolia testnet and Ethereum mainnet?

(c) Joerg Osterrieder 2025

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH
C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone
C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day
C) Only once, when the contract is deployed D) Never
Answer: C – Constructor runs exactly once during deployment to initialize state.

Q5. What does `msg.sender` represent in Solidity?
A) The contract creator only B) The blockchain network
C) The wallet address calling the function D) The gas price
Answer: C – `msg.sender` is the address of whoever initiated the current transaction.

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan
C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute
C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours
C) No, it is immutable and permanent D) Only the owner can delete it
Answer: C – Deployed contracts are permanent; you cannot change or delete bytecode.

Q10. What should you NEVER share with anyone?
A) Contract address B) Etherscan link
C) Your 12-word seed phrase D) Your public wallet address
Answer: C – Seed phrase = full control of your wallet. Anyone with it can steal your funds.

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions
C) Ethereum compiler D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code
C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free
C) Deployment actions D) Compilation errors
Answer: B – Blue = view-only (no state change, no gas). Orange = write (costs gas).

Q15. What is a transaction in blockchain?
A) Only sending ETH to someone B) Any request to change blockchain state
C) Reading data from a contract D) Compiling code
Answer: B – Transactions include deploying contracts, calling state-changing functions, and transfers.

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; `^` means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version
C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address
C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation
C) Better security D) Required by law
Answer: B – Testnets let you practice without risking real money.

Q20. What does `string memory _name` mean in the constructor?
A) Permanent storage on blockchain B) Temporary parameter passed during deployment
C) Owner's address D) Gas setting
Answer: B – `memory` means temporary; `_name` is input you provide when deploying.

W01: Deploy Your First Smart Contract

Module H: Hands-On Workshops

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

(c) Joerg Osterrieder 2026

Learning Objectives

By the end of this workshop, you will be able to:

1. Deploy a smart contract to Ethereum Sepolia testnet using Remix IDE
2. Interact with deployed contracts: read state, send transactions, verify on Etherscan
3. Explain the relationship between gas, transaction fees, and network congestion
4. Distinguish between contract deployment and contract interaction transactions

Prerequisites: Chrome/Firefox/Brave browser, internet connection

---

Estimated time: 45–60 minutes — No prior coding experience required

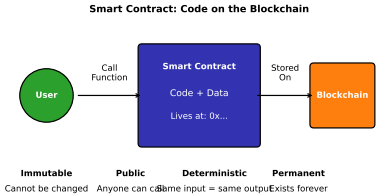
(c) Joerg Osterrieder 2026

Your First Blockchain Moment

Imagine this:

- You write a few lines of code
- You click one button
- Your code now runs on a network of thousands of computers worldwide
- No one – not even you – can delete or change it

That is what you will do today.



Your first deployment is a rite of passage into Web3 development

The Problem: How do you deploy code to a global, censorship-resistant computer?

The Challenge
Traditional software runs on servers you (or a company) control. What if you want code that:

- Runs exactly as written, forever
- Cannot be censored or shut down
- Is verifiable by anyone

Why It Matters

- DeFi, NFTs, DAOs — all built on smart contracts
- $100B+ value secured by deployed code

What We Need

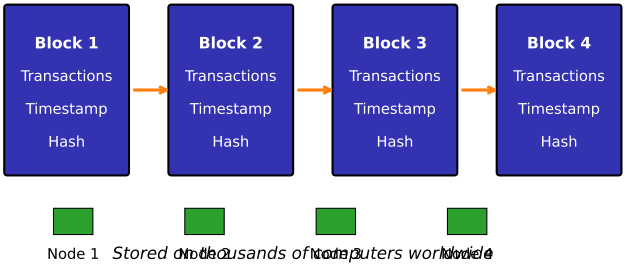
- Testnet environment (no real money at risk)
- Wallet to sign transactions
- Code editor and deployment interface

The Cryptoeconomics Question
How do economic incentives ensure your deployed code runs correctly?

Today's workshop: Deploy your first smart contract to Ethereum's Sepolia testnet (45-60 minutes)

What is a Blockchain?

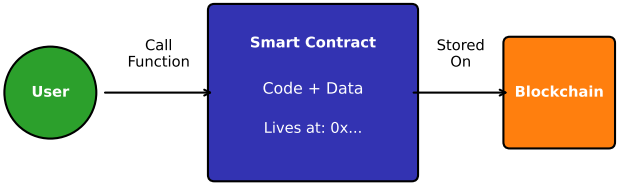
Blockchain: Blocks Linked in a Chain



Your code will be stored permanently on this global network of computers

What is a Smart Contract?

Smart Contract: Code on the Blockchain



Immutable	**Public**	**Deterministic**	**Permanent**
Cannot be changed	Anyone can call	Same input = same output	Exists forever

Today you'll deploy your own smart contract – same tech behind DeFi, NFTs, DAOs

Discovery: What Would YOU Put on a Permanent Computer?

Think About It:
If you could store ONE piece of information that no one could change or delete, what would you choose?

Predict:

- What kinds of information benefit from being permanent?
- What are the risks of permanence?

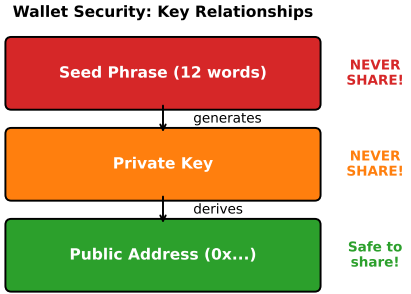
Discuss with your neighbor:

- Would you store a promise? A record? A rule?
- Why might a business want permanent, public records?

Key Insight: Smart contracts are exactly this – permanent rules and records that run automatically.

Discovery moment: Your intuition about permanent data is the foundation of smart contracts

What is a Crypto Wallet?



Public address = Your identity on blockchain (like email address)

MetaMask = browser wallet that signs transactions and connects to websites

Why Do We Need Two Networks? Testnet vs Mainnet

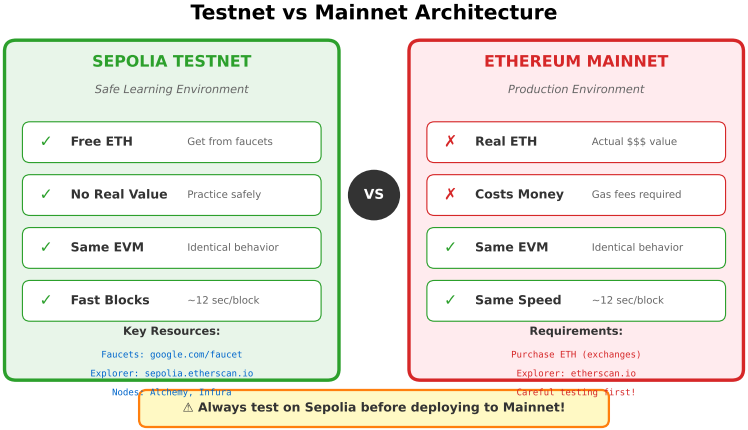
We use SEPOLIA TESTNET for learning:

Aspect	Testnet (Sepolia)	Mainnet
ETH Value	Free, no real value	Real money ($$$)
Purpose	Learning, testing	Production
Mistakes	Cost nothing	Can lose funds

Important: Never deploy practice code to mainnet – you could lose real money!

Sepolia ETH is free from faucets; mainnet ETH must be purchased

How Does Sepolia Architecture Compare to Mainnet?



Both networks use the same EVM – code works identically on testnet and mainnet

Workshop Objectives

By the end of this workshop, you will:

- Set up MetaMask wallet connected to Sepolia testnet
- Write a simple Solidity smart contract
- Compile and deploy using Remix IDE
- Interact with your deployed contract
- Verify your contract on Etherscan

Deliverable: Your contract address on Sepolia + screenshot

Estimated time: 45-60 minutes

(c) Joerg Osterrieder 2026

What Do You Need Before Starting?

All you need:

1. A laptop with Chrome, Firefox, or Brave browser
2. An internet connection
3. Curiosity about blockchain technology

No coding experience required! We will learn everything step-by-step together.

We will set up together in class:

- MetaMask wallet (free browser extension)
- Sepolia test ETH (free, no real money)

All tools are free and browser-based – nothing to install besides a browser extension

How Do You Set Up MetaMask?

Install MetaMask:

1. Go to `metamask.io`
2. Click “Download” and add browser extension
3. Create new wallet (save seed phrase securely!)
4. Set a strong password

Switch to Sepolia Testnet:

1. Click network dropdown (top left)
2. Enable “Show test networks” in settings
3. Select “Sepolia”

NEVER share your seed phrase with anyone!

Why Do We Need ETH? (Gas Explained)

What is Gas?

- Fee paid to process your transaction on the blockchain
- Compensates the computers running the network
- More complex operations = more gas required

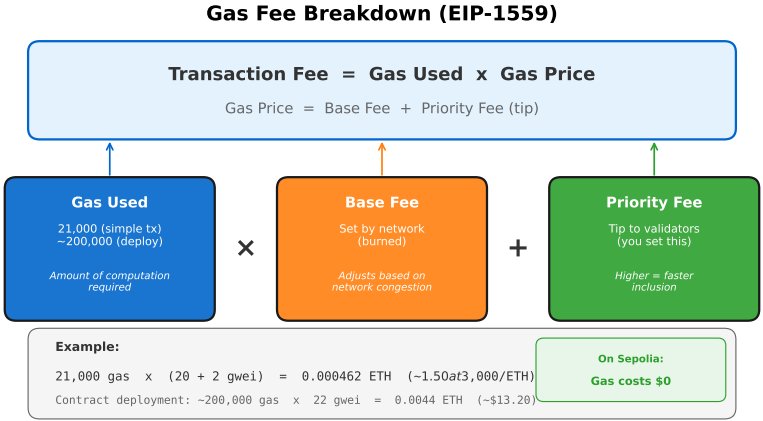
When Do You Pay Gas?

- **Deploying** a contract (one-time cost)
- **Writing** data (changing blockchain state)
- **Reading** data is FREE (no gas needed)

For This Workshop: We use free test ETH, so gas costs nothing real!

On mainnet, gas fees range from $1-$50+ depending on network congestion

How Are Gas Fees Calculated Under EIP-1559?



On Sepolia testnet, gas is free – but understanding fees prepares you for mainnet

Where Can You Get Free Test ETH?

Primary Faucets (try in order):

1. Google Cloud: `cloud.google.com/application/web3/faucet/ethereum/sepolia`
2. Alchemy: `sepoliafaucet.com`
3. Infura: `infura.io/faucet/sepolia`

Backup Faucets (if primary fails):

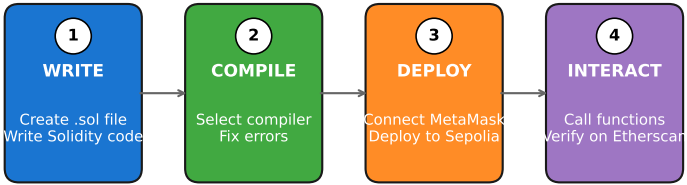
- QuickNode: `faucet.quicknode.com/ethereum/sepolia`
- Chainlink: `faucets.chain.link/sepolia`

Faucet rate limited? Try a different one! Most limit 0.1 ETH per day.

You need 0.01 ETH for this workshop

What Does the Development Workflow Look Like in Remix?

Remix IDE Development Workflow



Each step in Remix IDE - all in your browser!

Remix IDE handles everything in your browser - no installation needed

How Does Remix IDE Work?

Go to: `remix.ethereum.org`

Interface Overview:

- **File Explorer** (left): Create and manage .sol files
- **Editor** (center): Write your Solidity code
- **Compiler** (left sidebar): Compile your contract
- **Deploy** (left sidebar): Deploy to blockchain

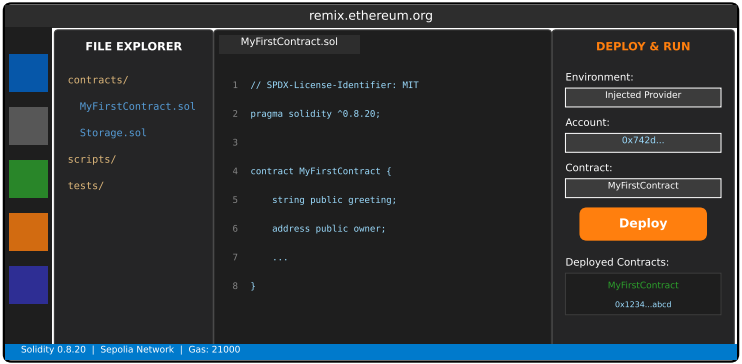
Create new file:

1. Click “contracts” folder
2. Click “New File” icon
3. Name it: `MyFirstContract.sol`

Remix auto-saves your work in browser storage

What Are the Key Components of the Remix Interface?

Remix IDE Interface Overview



Key panels: File Explorer (left), Editor (center), Deploy & Run (right sidebar)

What Are the Parts of a Solidity Contract?

Every Solidity file has three parts:

1. **License** (required):
   - `// SPDX-License-Identifier: MIT`
   - Declares your code is open source
2. **Compiler Version**:
   - `pragma solidity ^0.8.20;`
   - Tells Remix which Solidity version to use
3. **Contract Block**:
   - `contract MyContract { ... }`
   - Contains all your code

Think of a contract as a set of rules that everyone on the network agrees to follow

What Goes Inside Your Contract?

Inside your contract:

State Variables – Data stored permanently on blockchain:

- `string public greeting;` – A text value anyone can read
- `address public owner;` – A wallet/contract address

Constructor – Runs ONCE when contract is deployed:

- Sets up initial values
- Parameters come from deployment inputs

Functions – Code others can call:

- `public` = anyone can call
- Can read or change state variables

These building blocks are all you need to write your first contract

Let's Build Your Contract Step by Step

Before copying: Can you guess what each part does?

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

contract MyFirstContract {
    string public greeting;
    string public ownerName;
    address public owner;

    constructor(string memory _name) {
        owner = msg.sender;
        ownerName = _name;
        greeting = "Hello, Blockchain!";
    }

    function setGreeting(string memory _greeting) public {
        greeting = _greeting;
    }
}
```

After copying, read each line – can you explain what it does before looking at the next slide?

What Does Each Line of Code Do?

Line-by-line breakdown:

`string public greeting;`
→ A text variable anyone can read

`address public owner;`
→ Stores who deployed the contract

`constructor(string memory _name)`
→ Runs once; _name is what YOU type when deploying

`owner = msg.sender;`
→ `msg.sender` = YOUR wallet address (automatic!)

`function setGreeting(...) public`
→ Anyone can call this to change the greeting

---

msg.sender is a special variable Solidity provides automatically

Why Do You Need to Compile Your Contract?

What is Compilation?

- Translates human-readable Solidity into machine code (bytecode)
- Bytecode is what actually runs on Ethereum
- Like translating English to a language computers understand

In Remix:

1. Click "Solidity Compiler" icon (left sidebar)
2. Select compiler version: `0.8.20`
3. Click "Compile MyFirstContract.sol"
4. Green checkmark = success!

Errors? Red = syntax error (check semicolons, brackets)

Yellow warnings are usually okay to ignore

Discovery: Predict Before You Deploy

Before clicking "Deploy", make your predictions:

Predict:

- What will happen when you click Deploy?
- Will MetaMask ask you something? What?
- How long will it take?
- What will appear in Remix after deployment?

Write down your guesses:

- MetaMask will show: _____
- Wait time will be: _____ seconds
- After deployment I will see: _____

Now deploy and compare your predictions to reality!

Discovery moment: Predictions activate deeper learning – right or wrong, you learn more

What Does “Deploy” Mean?

Deployment = Publishing your contract to the blockchain

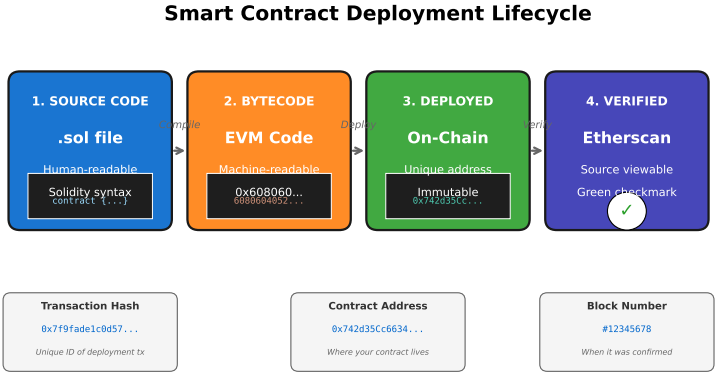
What happens:

1. Your compiled bytecode is sent to the network
2. It’s stored permanently at a unique address (0x...)
3. Anyone can now interact with your contract
4. You CANNOT change or delete it (immutable!)

Key Point: Deployment is permanent! Once deployed, your contract exists forever on the blockchain.

This is why we test on Sepolia first – mistakes on mainnet are forever

What Happens During the Contract Lifecycle?

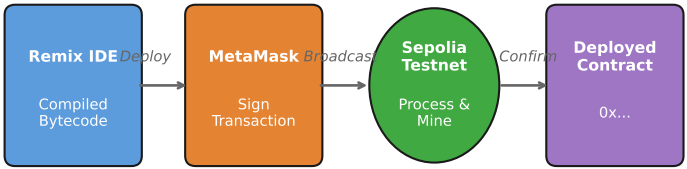


Each stage is permanent and auditable on the blockchain

Source code becomes bytecode, deployed to unique address, then verified on Etherscan

How Does the Deployment Process Flow?

Smart Contract Deployment Flow



Gas Fee: ~0.001 ETH (free on testnet!)

MetaMask signs the transaction, Sepolia processes it, you get a contract address

What is a Transaction?

Transaction = A request to change something on the blockchain

Examples of transactions:

- Deploying a new contract (what we're doing!)
- Calling a function that changes data
- Sending ETH to someone

NOT a transaction: Reading data (free, no signature needed)

Why does MetaMask pop up?

- You're authorizing the blockchain change
- You're agreeing to pay the gas fee
- Your private key signs the transaction

Every transaction is recorded publicly and permanently

How Do You Deploy to Sepolia?

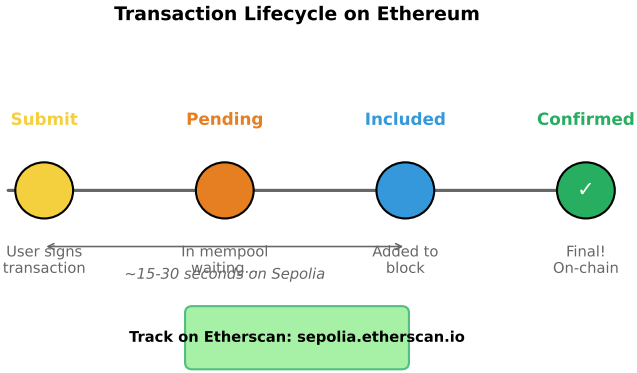
In Remix:

1. Click "Deploy & Run" icon (left sidebar)
2. Environment: Select "Injected Provider - MetaMask"
3. MetaMask popup: Click "Connect"
4. Verify: Network shows "Sepolia"
5. Enter your name in the `_name` field
6. Click "Deploy"
7. MetaMask popup: Click "Confirm"

Wait 15-30 seconds for confirmation!

You'll pay gas from your Sepolia test ETH

How Is Your Transaction Confirmed?



Your contract is now permanently on the Sepolia blockchain!

How Do You Interact With Your Deployed Contract?

After deployment, in Remix:

1. See your contract under "Deployed Contracts"
2. Click to expand
3. **Read functions** (blue buttons):
   - Click `greeting` – shows "Hello, Blockchain!"
   - Click `ownerName` – shows your name
   - Click `owner` – shows your wallet address
4. **Write functions** (orange buttons):
   - Enter new text in `setGreeting` field
   - Click button, confirm in MetaMask
   - Wait for confirmation, then click `greeting` again

Blue = free (view only), Orange = costs gas (state change)

Discovery: Why Did MetaMask Pop Up for One But Not the Other?

Observe:

- Clicking `greeting` (blue) – no MetaMask popup, instant result
- Clicking `setGreeting` (orange) – MetaMask popup, wait for confirmation

Reflect: Why the difference?

Think about it:

- What is different about reading vs writing?
- Why would writing cost money (gas)?
- Who pays, and why?

The economic insight:

- Reading = looking at data (free)
- Writing = changing the global ledger
- Someone must pay computers to process changes

Discovery moment: The read/write distinction is fundamental to ALL blockchain economics

How Can You View Your Contract Publicly?

Find your contract:

1. Copy contract address from Remix (click copy icon)
2. Go to `sepolia.etherscan.io`
3. Paste address in search bar
4. View your contract page!

What you'll see:

- Contract creation transaction
- All function calls you made
- Contract balance (0 ETH)

Etherscan is the public record of all blockchain activity

Discovery: What Can You Find About Your Contract?

Explore Etherscan and answer these questions:

1. Can you find the EXACT moment your contract was created?
2. Can you see your wallet address as the creator?
3. Can you find the setGreeting transaction you made?
4. What is the "gas used" for your deployment?

Reflect:

- Everything you did is PUBLIC and PERMANENT
- Anyone in the world can see your contract right now
- This is what "transparency" means on blockchain

Try it: Share your contract address with a classmate – can they read your greeting?

Discovery moment: Blockchain transparency means ALL actions are publicly auditable forever

Workshop Deliverables

To complete this workshop, submit:

1. Your deployed contract address on Sepolia
   - Format: `0x...` (42 characters)
2. Screenshot showing:
   - Your contract in Remix with your name
   - Etherscan page showing your contract

Bonus (optional):

- Add a `setName()` function to change owner name
- Call your classmate's contract

See lab_guide.md for detailed step-by-step instructions

What Do Common Error Messages Mean?

Error Message	Solution
“Insufficient funds for gas”	Get more ETH from faucet (try backup list)
“Transaction underpriced”	Wait 30s and retry, network is busy
“Nonce too high/low”	Reset MetaMask: Settings ¿ Advanced ¿ Clear Activity
“execution reverted”	Check function inputs are correct
“ParserError: Expected ‘;’”	Add missing semicolon at end of line
“DeclarationError”	Variable name typo or undeclared

MetaMask popup doesn’t appear?

1. Check MetaMask extension is unlocked
2. Refresh Remix and reconnect
3. Try different browser (Chrome recommended)

(c) Joerg Osterrieder 2026

What You Just Accomplished!

You just:

- Created your blockchain identity (wallet)
- Wrote actual Solidity smart contract code
- Deployed a program that lives FOREVER on Ethereum
- Joined 200M+ smart contract users worldwide

Your contract will exist as long as Ethereum exists!

This is the same technology behind:

- DeFi protocols managing $100B+ in assets
- NFT marketplaces
- DAOs governing organizations

You've taken your first step into blockchain development

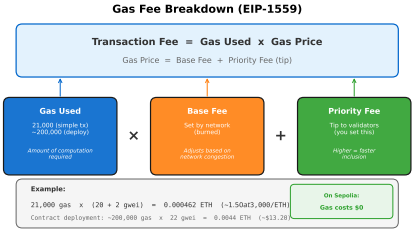
The Reality Check

What you just experienced:

- Deploying code costs real money on mainnet
- Once deployed, there is no “undo” button
- Every action is permanently recorded
- This is why we practice on testnet first

On mainnet:

- Gas optimization becomes an art form
- Every byte of storage costs real ETH
- Bugs can mean lost funds – forever



The skills you practiced today are identical to professional smart contract development

Problem Check-In: First Smart Contract

What We Solved:

- Deployed trustless code that executes automatically
- Verified contract behavior on public testnet
- Experienced the deploy-interact-verify workflow

What Remains:

- Gas optimization for real deployments
- Security auditing before mainnet
- Testing frameworks beyond manual verification

This workshop demonstrated: code is law in practice — once deployed, the contract executes as written

(c) Joerg Osterrieder 2026

The Economics of Smart Contract Deployment

Incentive Structure

- **Core Problem:** Who pays for permanent, global code execution?
- **Gas mechanism:** Users pay validators for computation and storage
- **Value Flow:** Deployers pay gas $\rightarrow$ validators earn fees $\rightarrow$ network remains secure

Economic Security

- Gas prevents spam (infinite loops cost infinite gas)
- EIP-1559: Base fee burned, reducing ETH supply

Key Economic Question

Who Pays, Who Earns?

Users pay gas for deployment and state changes. Validators earn fees for processing transactions. Reading state is free (no computation cost to network).

Design Principle

$$\text{Gas Cost} \propto \text{Computation} + \text{Storage}$$

The gas mechanism aligns incentives: users pay for resources, validators are compensated for processing

Design Space: Smart Contract Deployment

Platform Choices

1. **Ethereum Mainnet**: Maximum security, higher gas costs
2. **Layer 2 (Arbitrum, Base)**: Lower fees, inherit L1 security
3. **Alt-L1 (Solana, Avalanche)**: Different trade-offs in speed vs decentralization

Trade-offs

- More decentralization = higher deployment costs
- Testnets: Free but no economic security

Design Questions

- Should all contracts be immutable, or allow upgrades?
- How much should deployment cost to prevent spam?
- Should storage have ongoing rent or one-time cost?

Key Insight

Permanence Has a Price

Immutable deployment means bugs are forever. This is why testnets exist and audits matter.

Every deployment platform trades off cost, security, decentralization, and speed

Failure Modes: Smart Contract Deployment

Critical Failure Modes

- **What breaks:** Bugs in deployed code cannot be fixed
- **Why it matters:** $60M lost in The DAO hack (2016) due to reentrancy bug

Common Deployment Errors

- Wrong constructor parameters (permanent)
- Deploying to wrong network (mainnet instead of testnet)
- Insufficient gas causing failed transactions

Historical Context

- Parity wallet bug (2017): $280M locked forever
- Wormhole bridge (2022): $320M exploit
- Pattern: Most exploits target deployed contract logic

Early Warning Signs

- ! Unaudited code deployed with real funds
- ! No testnet deployment before mainnet
- ! Missing access controls on critical functions

Defense: Always deploy to testnet first, get audits for mainnet, use established libraries (OpenZeppelin)

(c) Joerg Osterrieder 2026

Summary

What you learned:

- Set up MetaMask and connected to Sepolia testnet
- Wrote a Solidity smart contract with state variables
- Compiled and deployed using Remix IDE
- Interacted with your live contract on the blockchain
- Verified your contract on Etherscan

Next Workshop: W02 - Create Your Own Cryptocurrency (ERC-20 token)

Congratulations! You deployed your first smart contract!

(c) Joerg Osterrieder 2026

Glossary: Key Terms

Term	Definition
Blockchain	Distributed database of linked blocks
Smart Contract	Code stored and executed on blockchain
Wallet	Software managing your blockchain identity
Seed Phrase	12 words that generate your private key
Gas	Fee paid for blockchain operations
Testnet	Practice network with free fake ETH
Deploy	Publishing your contract to blockchain
Etherscan	Website to view blockchain activity

Refer back to this when you encounter unfamiliar terms

(c) Joerg Osterrieder 2026

Next Steps

Continue Learning:

1. Complete W02 (Create Your Own Cryptocurrency)
2. Try modifying your contract (add new functions!)
3. Explore Remix documentation: `remix-ide.readthedocs.io`

Want to Go Deeper?

- The course covers Solidity fundamentals in detail (Module B)
- Smart contract security is covered later (Module F)
- Explore the Solidity docs: `docs.soliditylang.org`

Challenge: Add a `setName()` function that only the owner can call! (See `contracts/MyFirstContract_Extended.sol` for the solution.)

Keep building – every expert started exactly where you are now

Questions for Reflection

1. Why does calling `setGreeting()` cost gas but reading `greeting` is free?
2. What happens to your contract if you lose access to your MetaMask wallet?
3. Why is the constructor only called once?
4. How would you make only the owner able to change the greeting?
5. What's the difference between Sepolia testnet and Ethereum mainnet?

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH
C) Sepolia is more secure D) They are identical

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH
C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone
C) Automatically creates a getter function D) Hides it from view

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH
C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone
C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day
C) Only once, when the contract is deployed D) Never

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH
C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone
C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day
C) Only once, when the contract is deployed D) Never
Answer: C – Constructor runs exactly once during deployment to initialize state.

Q5. What does `msg.sender` represent in Solidity?
A) The contract creator only B) The blockchain network
C) The wallet address calling the function D) The gas price

Quiz Questions (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions
C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH
C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone
C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day
C) Only once, when the contract is deployed D) Never
Answer: C – Constructor runs exactly once during deployment to initialize state.

Q5. What does `msg.sender` represent in Solidity?
A) The contract creator only B) The blockchain network
C) The wallet address calling the function D) The gas price
Answer: C – `msg.sender` is the address of whoever initiated the current transaction.

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan
C) Calling `setGreeting()` to change state D) Compiling in Remix

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan
C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute
C) Create a backup D) Test gas costs

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan
C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute
C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours
C) No, it is immutable and permanent D) Only the owner can delete it

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan
C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute
C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours
C) No, it is immutable and permanent D) Only the owner can delete it
Answer: C – Deployed contracts are permanent; you cannot change or delete bytecode.

Q10. What should you NEVER share with anyone?
A) Contract address B) Etherscan link
C) Your 12-word seed phrase D) Your public wallet address

Quiz Questions (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code
C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan
C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute
C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours
C) No, it is immutable and permanent D) Only the owner can delete it
Answer: C – Deployed contracts are permanent; you cannot change or delete bytecode.

Q10. What should you NEVER share with anyone?
A) Contract address B) Etherscan link
C) Your 12-word seed phrase D) Your public wallet address
Answer: C – Seed phrase = full control of your wallet. Anyone with it can steal your funds.

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions
C) Ethereum compiler D) Wallet provider

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions
C) Ethereum compiler D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code
C) Solidity version D) Gas limit

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions
C) Ethereum compiler D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code
C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free
C) Deployment actions D) Compilation errors

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions
C) Ethereum compiler D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code
C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free
C) Deployment actions D) Compilation errors
Answer: B – Blue = view-only (no state change, no gas). Orange = write (costs gas).

Q15. What is a transaction in blockchain?
A) Only sending ETH to someone B) Any request to change blockchain state
C) Reading data from a contract D) Compiling code

(c) Joerg Osterrieder 2026

Quiz Questions (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain
C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions
C) Ethereum compiler D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code
C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free
C) Deployment actions D) Compilation errors
Answer: B – Blue = view-only (no state change, no gas). Orange = write (costs gas).

Q15. What is a transaction in blockchain?
A) Only sending ETH to someone B) Any request to change blockchain state
C) Reading data from a contract D) Compiling code
Answer: B – Transactions include deploying contracts, calling state-changing functions, and transfers.

(c) Joerg Osterrieder 2026

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` **specify?**
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version
C) Get more test ETH from a faucet D) Restart computer

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version
C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address
C) Contract is saved on your computer D) Etherscan approves it

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version
C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address
C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation
C) Better security D) Required by law

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version
C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address
C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation
C) Better security D) Required by law
Answer: B – Testnets let you practice without risking real money.

Q20. What does `string memory _name` mean in the constructor?
A) Permanent storage on blockchain B) Temporary parameter passed during deployment
C) Owner's address D) Gas setting

Quiz Questions (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name
C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version
C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address
C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation
C) Better security D) Required by law
Answer: B – Testnets let you practice without risking real money.

Q20. What does `string memory _name` mean in the constructor?
A) Permanent storage on blockchain B) Temporary parameter passed during deployment
C) Owner's address D) Gas setting
Answer: B – `memory` means temporary; `_name` is input you provide when deploying.

Quiz: First Smart Contract

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions C) Writing smart contracts D) Storing files on blockchain

Quiz (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH C) Sepolia is more secure D) They are identical

Quiz (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone C) Automatically creates a getter function D) Hides it from view

Quiz (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day C) Only once, when the contract is deployed D) Never

Quiz (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day C) Only once, when the contract is deployed D) Never
Answer: C – Constructor runs exactly once during deployment to initialize state.

Q5. What does `msg.sender` represent in Solidity?
A) The contract creator only B) The blockchain network C) The wallet address calling the function D) The gas price

Quiz (1–5)

Q1. What is the primary purpose of MetaMask in blockchain development?
A) Mining cryptocurrency B) Managing your blockchain identity and signing transactions C) Writing smart contracts D) Storing files on blockchain
Answer: B – MetaMask is a wallet that stores your private key and signs transactions.

Q2. What is the main difference between Sepolia testnet and Ethereum mainnet?
A) Sepolia is faster B) Mainnet uses real money with value, Sepolia uses free test ETH C) Sepolia is more secure D) They are identical
Answer: B – Testnet ETH is free and has no real-world value, used for safe practice.

Q3. In Solidity, what does the `public` keyword do for a state variable?
A) Deletes it after use B) Makes it modifiable by anyone C) Automatically creates a getter function D) Hides it from view
Answer: C – `public` auto-generates a free read function for the variable.

Q4. When is the `constructor` function executed?
A) Every time someone calls the contract B) Once per day C) Only once, when the contract is deployed D) Never
Answer: C – Constructor runs exactly once during deployment to initialize state.

Q5. What does `msg.sender` represent in Solidity?
A) The contract creator only B) The blockchain network C) The wallet address calling the function D) The gas price
Answer: C – `msg.sender` is the address of whoever initiated the current transaction.

Quiz (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code C) Type of cryptocurrency
D) Compiler setting

Quiz (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code C) Type of cryptocurrency
D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan C) Calling `setGreeting()` to change state
D) Compiling in Remix

Quiz (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute C) Create a backup D) Test gas costs

Quiz (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours C) No, it is immutable and permanent D) Only the owner can delete it

Quiz (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours C) No, it is immutable and permanent D) Only the owner can delete it
Answer: C – Deployed contracts are permanent; you cannot change or delete bytecode.

Q10. What should you NEVER share with anyone?
A) Contract address B) Etherscan link C) Your 12-word seed phrase D) Your public wallet address

Quiz (6–10)

Q6. What is gas in the Ethereum context?
A) Physical fuel for servers B) Fee paid to process transactions and execute code C) Type of cryptocurrency D) Compiler setting
Answer: B – Gas compensates miners/validators for computational work.

Q7. Which operation costs gas?
A) Reading a public variable B) Viewing your contract on Etherscan C) Calling `setGreeting()` to change state D) Compiling in Remix
Answer: C – Writing data to blockchain requires gas; reads are free.

Q8. What is the purpose of compilation in Remix?
A) Upload to GitHub B) Translate Solidity to bytecode the EVM can execute C) Create a backup D) Test gas costs
Answer: B – Compilation converts human-readable code to machine-executable bytecode.

Q9. After deploying a contract, can you delete or modify its code?
A) Yes, anytime B) Only within 24 hours C) No, it is immutable and permanent D) Only the owner can delete it
Answer: C – Deployed contracts are permanent; you cannot change or delete bytecode.

Q10. What should you NEVER share with anyone?
A) Contract address B) Etherscan link C) Your 12-word seed phrase D) Your public wallet address
Answer: C – Seed phrase = full control of your wallet. Anyone with it can steal your funds.

Quiz (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain C) It's a testing mode
D) Downloads MetaMask

Quiz (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain C) It's a testing mode
D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions C) Ethereum compiler
D) Wallet provider

Quiz (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain C) It's a testing mode
D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions C) Ethereum compiler
D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code C) Solidity version D) Gas limit

Quiz (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain C) It's a testing mode D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions C) Ethereum compiler D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free C) Deployment actions D) Compilation errors

Quiz (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain C) It's a testing mode
D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions C) Ethereum compiler
D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free C) Deployment actions D) Compilation errors
Answer: B – Blue = view-only (no state change, no gas). Orange = write (costs gas).

Q15. What is a transaction in blockchain?
A) Only sending ETH to someone B) Any request to change blockchain state C) Reading data from a contract
D) Compiling code

Quiz (11–15)

Q11. In Remix, what does "Injected Provider - MetaMask" mean?
A) Remix simulates MetaMask B) MetaMask provides connection to real blockchain C) It's a testing mode
D) Downloads MetaMask
Answer: B – Injected Provider connects Remix to the network through your MetaMask wallet.

Q12. What is Etherscan?
A) Antivirus for blockchain B) Block explorer showing all public blockchain transactions C) Ethereum compiler
D) Wallet provider
Answer: B – Etherscan displays public records of all transactions, contracts, and addresses.

Q13. What does SPDX-License-Identifier specify?
A) Your identity B) Open-source license for your code C) Solidity version D) Gas limit
Answer: B – Declares licensing terms (e.g., MIT) for code sharing and reuse.

Q14. In Remix, blue buttons represent:
A) Functions that cost gas B) View/read functions that are free C) Deployment actions D) Compilation errors
Answer: B – Blue = view-only (no state change, no gas). Orange = write (costs gas).

Q15. What is a transaction in blockchain?
A) Only sending ETH to someone B) Any request to change blockchain state C) Reading data from a contract
D) Compiling code
Answer: B – Transactions include deploying contracts, calling state-changing functions, and transfers.

Quiz (16–20)

Q16. What does `pragma solidity ^0.8.20;` **specify?**
A) License type B) Contract name C) Minimum Solidity compiler version D) Gas limit

Quiz (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but $<$0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version C) Get more test ETH from a faucet D) Restart computer

Quiz (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address C) Contract is saved on your computer D) Etherscan approves it

Quiz (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation C) Better security D) Required by law

Quiz (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation C) Better security D) Required by law
Answer: B – Testnets let you practice without risking real money.

Q20. What does `string memory _name` mean in the constructor?
A) Permanent storage on blockchain B) Temporary parameter passed during deployment C) Owner's address D) Gas setting

Quiz (16–20)

Q16. What does `pragma solidity ^0.8.20;` specify?
A) License type B) Contract name C) Minimum Solidity compiler version D) Gas limit
Answer: C – Pragma sets compiler version; ^ means 0.8.20 or higher (but <0.9.0).

Q17. If you get "Insufficient funds for gas" error, what should you do?
A) Delete MetaMask B) Change compiler version C) Get more test ETH from a faucet D) Restart computer
Answer: C – You need ETH to pay gas fees; use faucets to get free testnet ETH.

Q18. What happens during contract deployment?
A) Code is emailed to miners B) Bytecode is sent to network and stored at new address C) Contract is saved on your computer D) Etherscan approves it
Answer: B – Deployment creates a permanent on-chain contract at a unique address (0x...).

Q19. Why do we use testnets for learning?
A) Faster than mainnet B) Mistakes cost nothing; free ETH for safe experimentation C) Better security D) Required by law
Answer: B – Testnets let you practice without risking real money.

Q20. What does `string memory _name` mean in the constructor?
A) Permanent storage on blockchain B) Temporary parameter passed during deployment C) Owner's address D) Gas setting
Answer: B – `memory` means temporary; `_name` is input you provide when deploying.

W02: Create Your Own Cryptocurrency

Module H: Hands-On Workshops

Blockchain & Cryptocurrency Course

December 2025

(c) Joerg Osterrieder 2025

Token Creation in a Nutshell

- "I'm launching my own cryptocurrency!" – the excitement is real, the responsibility is bigger
- Creating a token takes 15 minutes; understanding tokenomics takes years

[COMIC: Enthusiastic person announcing "I'm launching a token!" to friends, eyes sparkling, holding laptop triumphantly. Caption: "To the moon!"]

[PLACEHOLDER] — The technical barrier to token creation is gone – the economic design challenge remains

The Problem: How do you create a digital currency without a central bank?

The Challenge
Traditional currencies require:

- Central authority to issue and manage supply
- Trust in institutions not to inflate away value
- Banking infrastructure for transfers

Why It Matters

- Anyone can create programmable money
- $1T+ market cap in ERC-20 tokens
- Foundation of DeFi, DAOs, and token economies

What We Need

- Standardized interface (ERC-20)
- Audited, secure code (OpenZeppelin)
- Deployment and distribution mechanism

The Cryptoeconomics Question
How do token economics (supply, distribution, utility) determine value?

Today's workshop: Create your own ERC-20 token in 30 minutes

Workshop Objectives

By the end of this workshop, you will:

- Understand the ERC-20 token standard
- Use OpenZeppelin's audited contracts
- Deploy your own cryptocurrency on Sepolia
- Add your token to MetaMask wallet
- Transfer tokens to a classmate

Deliverable: Token contract address + proof of transfer

Estimated time: 60 minutes

What Do You Need Before Starting?

Required (from W01):

1. MetaMask wallet connected to Sepolia
2. Sepolia test ETH (0.05+ ETH recommended)
3. Familiarity with Remix IDE

If you haven't done W01:

- Complete W01 first, or
- Follow the MetaMask/Sepolia setup in W01 slides

This workshop builds on W01 skills

What Makes a Token Different from a Coin?

Definition: A digital asset created on an existing blockchain.

Token vs Coin:

- **Coin**: Native currency of a blockchain (ETH, BTC)
- **Token**: Created using smart contracts on a blockchain

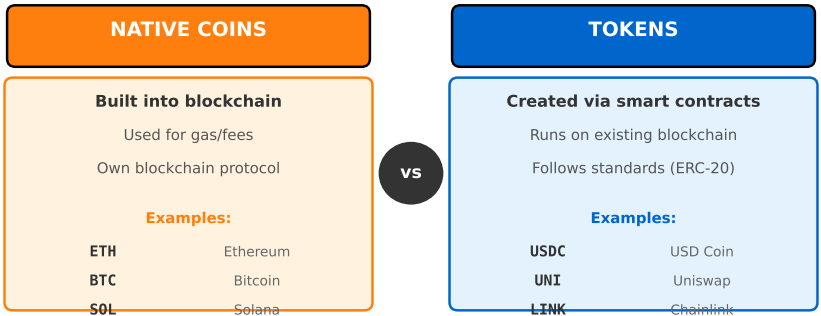
What tokens represent:

- Currency (stablecoins like USDC)
- Ownership (shares in a project)
- Access rights (membership, services)
- Voting power (governance)

Today you'll create your own token on Ethereum's Sepolia testnet

How Do Tokens Differ from Coins?

Coin vs Token: What's the Difference?



Key Difference:

Coins = Native currency | Tokens = Built on top of a blockchain

Coins are native to blockchains; tokens are built on top using smart contracts

(c) Joerg Osterrieder 2025

Why Would You Create Your Own Token?

Real-world use cases:

- **Startups**: Fundraising and community building
- **Games**: In-game currency and rewards
- **DAOs**: Governance and voting rights
- **Loyalty Programs**: Points and rewards
- **Payments**: Stablecoins for transactions

Today's goal:

- Create YOUR token with custom name and symbol
- Experience the full deployment process
- Transfer tokens to prove ownership works

Same process used for billions of dollars in real tokens

How Does Contract Inheritance Work?

Problem: Writing ERC-20 from scratch = 200+ lines of code
Solution: Inherit from OpenZeppelin's tested code!

What `is` does:

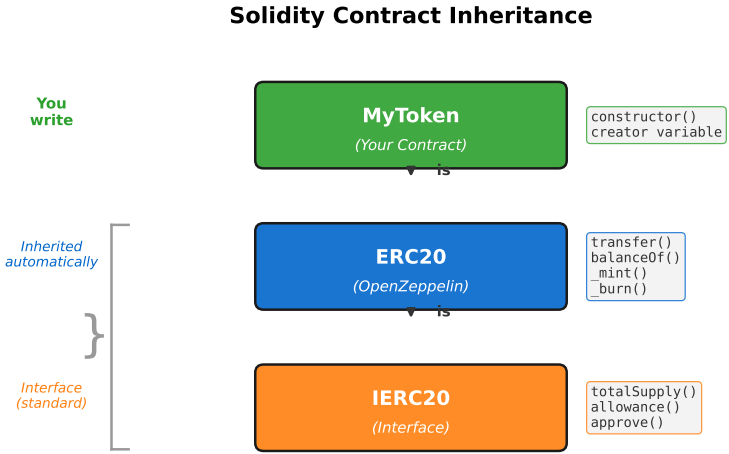
```
contract MyToken is ERC20 { ... }
```

- MyToken **inherits** all functions from ERC20
- Your contract automatically has transfer(), balanceOf(), etc.
- You only write what's different (constructor)

Analogy: Like a child inheriting traits from parents – you get everything they have, plus your own additions.

Inheritance is fundamental to Solidity and all object-oriented programming

Inheritance Hierarchy Visualization



Your contract inherits all functionality from ERC20, which implements the IERC20 interface

How Do You Import OpenZeppelin Contracts?

What happens when you write:

```
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
```

Step by step:

1. Remix sees the `@openzeppelin` prefix
2. Remix downloads the code from NPM (package manager)
3. The ERC20.sol file becomes available to your contract
4. You can now use `is ERC20` to inherit

Why this matters:

- You don't need to install anything locally
- Always gets the latest audited version
- Same code used by major DeFi projects

Remix handles package management automatically – just type and wait 10-20 seconds

What Parameters Does Your Token Need?

A constructor runs ONCE when the contract deploys.

```
constructor(
    string memory name,    // "Alice Coin"
    string memory symbol,  // "ALICE"
    uint256 initialSupply  // 1000000
) ERC20(name, symbol) {
    _mint(msg.sender, initialSupply * 10 ** decimals());
}
```

What each parameter does:

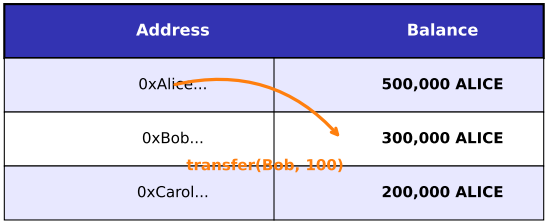
- **name**: Human-readable name (shown in wallets)
- **symbol**: Ticker symbol (like stock symbols: AAPL, GOOG)
- **initialSupply**: How many tokens to create

Important: These values are PERMANENT after deployment!

Choose carefully – you cannot change name, symbol, or initial supply later

How Token Balances Work

ERC-20 Token: Internal Balance Ledger



Smart contract stores: mapping(address => uint256) balances

Total Supply = Sum of all balances = 1,000,000 ALICE

The smart contract maintains a ledger (mapping) of who owns how many tokens

How Do Mint and Burn Functions Work?

Mint = Create new tokens from nothing

- Increases total supply
- New tokens go to a specified address
- In our contract: `_mint(msg.sender, amount)`

Burn = Destroy tokens permanently

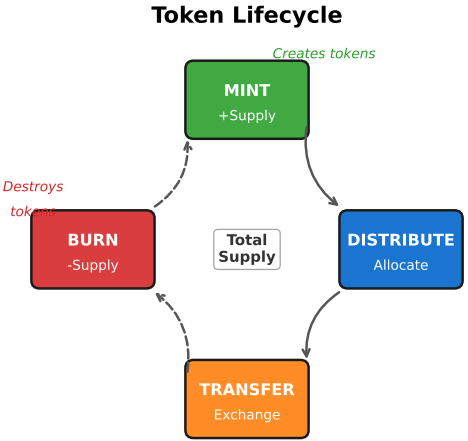
- Decreases total supply
- Tokens are removed forever
- Often sends to address(0) – the "black hole"

In our token:

- We mint ALL tokens in constructor (one-time)
- Basic version has no burn function
- Bonus: Add these features yourself!

Mint/burn control is critical for tokenomics – who can create/destroy?

What Journey Does a Token Take?



Solid arrows = typical flow | Dashed = optional (deflationary/inflationary)

Tokens follow a lifecycle: creation (mint) through distribution, transfer, and optional destruction (burn)

How Do You Find Someone's Wallet Address?

When transferring tokens, you need the recipient's address:

Address format:

- Always starts with `0x`
- Followed by 40 hexadecimal characters
- Example: `0xAb5801a7D398351b8bE11C439e05C5B3259aeC9B`
- Total: 42 characters

Critical warnings:

- Double-check the address before sending!
- Transactions cannot be reversed
- Tokens sent to wrong address = lost forever
- Copy-paste to avoid typos

Get your classmate's address from MetaMask: click account name to copy

What is ERC-20?

ERC-20 = Ethereum Request for Comments #20

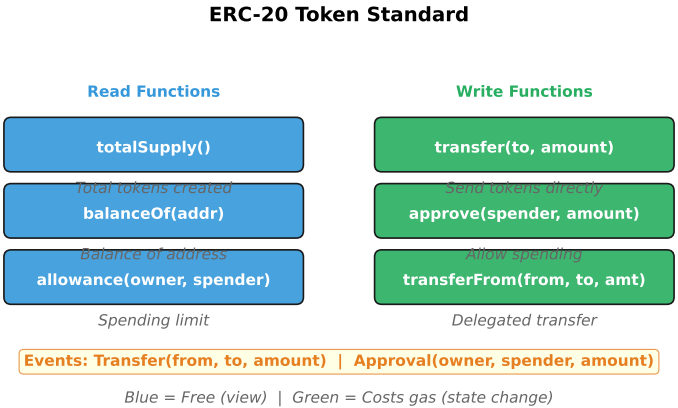
- Standard interface for fungible tokens
- Published in 2015, widely adopted since 2017
- Used by: USDC, LINK, UNI, DAI, and 500,000+ tokens

Fungible means:

- Every token is identical and interchangeable
- Like dollars: one $1 bill = any other $1 bill
- Unlike NFTs where each token is unique

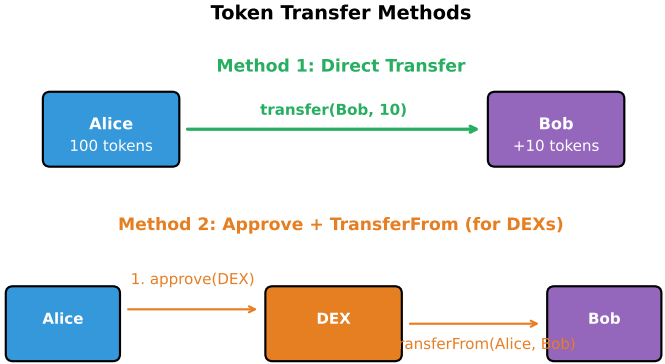
See L17 for detailed ERC-20 coverage

What Functions Must Every ERC-20 Token Have?



These 6 functions + 2 events define the ERC-20 standard

How Can You Move Tokens Between Wallets?



Direct transfer for simple sends; approve pattern for DEXs and DeFi

Why Are There Two Ways to Transfer Tokens?

Two ways to move tokens:

1. **transfer(to, amount)** – Direct send
   - YOU send YOUR tokens to someone
   - Simple: one transaction
   - Used in: peer-to-peer transfers

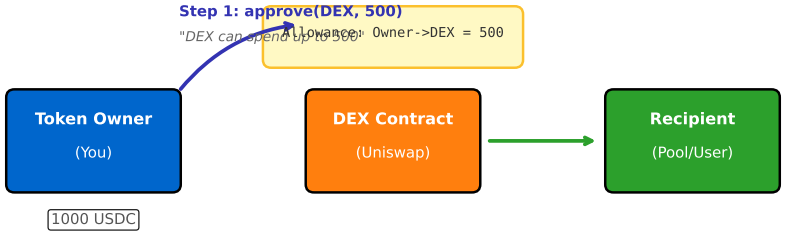
2. **approve() + transferFrom()** – Allow someone else
   - Step 1: You approve an app to spend X tokens
   - Step 2: App calls transferFrom() to take them
   - Used in: DEXs (Uniswap), DeFi protocols (Aave)

Why approve pattern? Apps can't just take tokens – you must authorize first!

Always check what you're approving – unlimited approvals can be risky

How Does the Approve Pattern Work?

The Approve + TransferFrom Pattern



Why? Smart contracts cannot initiate transactions - they need permission first

Used by: Uniswap, Aave, Compound, and every DeFi protocol

The two-step pattern lets smart contracts move tokens on your behalf after explicit approval

(c) Joerg Osterrieder 2025

Why Should You Use Audited Code?

Smart contract audits:

- Security experts review code for vulnerabilities
- Look for bugs, exploits, logic errors
- Cost: $10k - $500k+ per audit
- Takes weeks to months

Why OpenZeppelin is trusted:

- Audited by multiple security firms
- Used by major projects (Aave, Compound, OpenSea)
- Open source – anyone can review
- Battle-tested with billions of dollars at stake

Lesson: Never deploy unaudited code with real money!

For learning on testnet, unaudited code is fine – but mainnet requires audits

What is OpenZeppelin?

OpenZeppelin Contracts:

- Library of secure, audited smart contracts
- Used by 95%+ of Ethereum projects
- Open source, MIT licensed
- Battle-tested with billions of dollars secured

Why use OpenZeppelin?

- Don't reinvent the wheel
- Professional security audits
- Follows best practices
- Saves weeks of development time

Website: openzeppelin.com/contracts

How Do You Use OpenZeppelin Contracts?

Importing in Remix:

```
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
```

Remix automatically fetches from NPM!

Inheriting the contract:

```
contract MyToken is ERC20 {
    constructor() ERC20("Token Name", "SYMBOL") {
        _mint(msg.sender, 1000000 * 10 ** decimals());
    }
}
```

That's it! You inherit all 6 ERC-20 functions automatically.

OpenZeppelin handles all the complex logic for you

What Should You Name Your Token?

You need to decide:

Parameter	Example
Name	"Alice Coin"
Symbol	"ALICE"
Initial Supply	1,000,000

Naming tips:

- Name: Your name, project name, fun name
- Symbol: 3-5 uppercase letters (like stock tickers)
- Supply: How many tokens to create (you own 100%)

These are permanently set at deployment

Why Do Tokens Use 18 Decimals?

ERC-20 tokens use 18 decimals (like ETH):

- 1 token = 1,000,000,000,000,000,000 (10^18) smallest units
- Similar to 1 dollar = 100 cents

Why this matters:

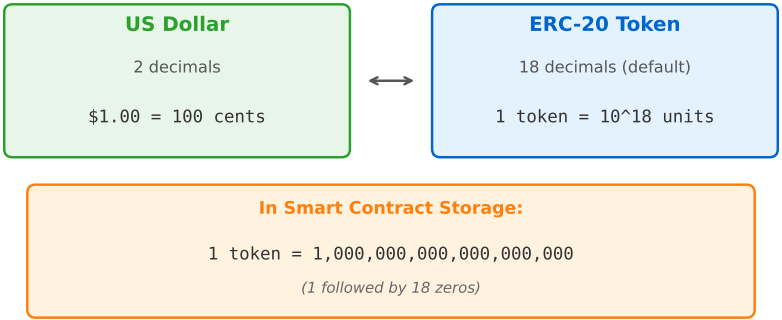
- When you mint 1,000,000 tokens...
- Actually creating: 1,000,000 $\times$ 10^18 units
- Code: `initialSupply * 10 ** decimals()`

Don't worry: Wallets display the human-readable number!

Some tokens use fewer decimals (USDC uses 6)

Why Use 18 Decimals for Token Math?

Understanding Token Decimals



`Code: amount * 10 ** decimals()`

Why? Integer math avoids floating-point errors in financial calculations

Using integer math with 18 decimals avoids floating-point errors in financial calculations

(c) Joerg Osterrieder 2025

What Code Creates Your Token?

Copy this code into Remix:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract MyToken is ERC20 {
    address public creator;

    constructor(
        string memory name,
        string memory symbol,
        uint256 initialSupply
    ) ERC20(name, symbol) {
        creator = msg.sender;
        _mint(msg.sender, initialSupply * 10 ** decimals());
    }
}
```

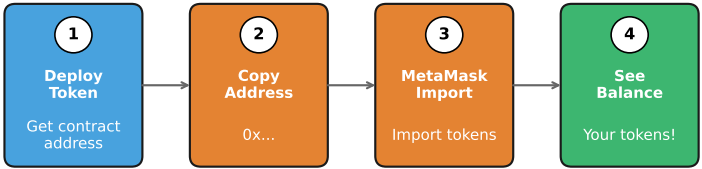
Full template in contracts/MyToken.sol

How Do You Deploy Your Token?

1. **Open Remix IDE** (`remix.ethereum.org`)
   1. Create new file: `MyToken.sol`
   2. Paste the contract code
   3. Wait for OpenZeppelin to download (10-20 seconds)
2. **Compile**
   1. Click Solidity Compiler icon
   2. Select version 0.8.20
   3. Click "Compile MyToken.sol"
3. **Deploy**
   1. Environment: "Injected Provider - MetaMask"
   2. Enter: `"Your Token Name", "SYMBOL", 1000000`
   3. Click Deploy, confirm in MetaMask

How Do You See Your Token in MetaMask?

Adding Your Token to MetaMask



MetaMask > Import tokens > Paste contract address

Name and symbol auto-populate from the contract!

Your tokens won't show in MetaMask until you import them

How Do You Add Your Token to MetaMask?

After deployment:

1. Copy your token contract address from Remix
2. Open MetaMask
3. Scroll down, click “Import tokens”
4. Paste the contract address
5. Name and symbol auto-populate!
6. Click “Add Custom Token”
7. Click “Import Tokens”

You should see:

- Your token with the symbol you chose
- Full balance (all tokens minted to you)

Each wallet needs to import the token to see it

How Do You Send Tokens to Someone Else?

Option 1: Using MetaMask

1. Click your token in MetaMask
2. Click "Send"
3. Enter classmate's wallet address
4. Enter amount (e.g., 100 tokens)
5. Confirm transaction

Option 2: Using Remix

1. Expand your deployed contract
2. Find `transfer` function
3. Enter: recipient address, amount (with 18 decimals!)
4. Click transfer, confirm in MetaMask

Your classmate must import your token to see it in their wallet

How Can You Verify Your Token on Etherscan?

View your token:

1. Go to `sepolia.etherscan.io`
2. Search for your contract address
3. Click “Token” tab to see token info

You’ll see:

- Token name and symbol
- Total supply
- Holder count
- All transfer transactions

Optional: Verify source code to make contract readable

Etherscan auto-detects ERC-20 tokens

Workshop Deliverables

To complete this workshop, submit:

1. Your token contract address on Sepolia
   - Format: `0x...` (42 characters)
2. Proof of token transfer:
   - Etherscan link to transfer transaction, OR
   - Screenshot of MetaMask showing sent tokens

Bonus (optional):

- Add a `mint()` function (owner only)
- Add a `burn()` function
- Create a token with custom decimals

See lab_guide.md for detailed instructions

Real-World Token Examples

Popular ERC-20 tokens built this way:

Token	Symbol	Market Cap
Tether	USDT	$139B
USD Coin	USDC	$42B
Chainlink	LINK	$14B
Uniswap	UNI	$7B
Dai	DAI	$5B

They all started the same way you just did!
(Just with more features and real money)

Market caps as of December 2024

What Advanced Features Can You Add?

OpenZeppelin Extensions:

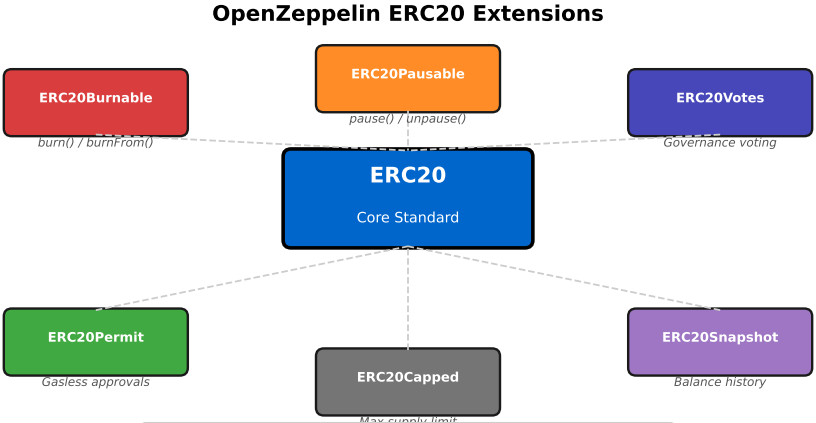
- **ERC20Burnable**: Allow token burning
- **ERC20Pausable**: Pause all transfers
- **ERC20Votes**: Governance voting power
- **ERC20Permit**: Gasless approvals (EIP-2612)

Additional Features:

- Ownable: Restrict admin functions
- AccessControl: Role-based permissions
- Timelocks: Delayed execution

See OpenZeppelin documentation for full list

What Advanced Features Can You Add?



Mix and match extensions to build feature-rich tokens with audited, secure code

What You Just Accomplished!

Celebrate – you just:

1. Understood the ERC-20 token standard
2. Used professional-grade OpenZeppelin contracts
3. Deployed YOUR OWN cryptocurrency to the blockchain
4. Imported your token into MetaMask
5. Transferred tokens to another person
6. Verified everything on Etherscan

Skills gained:

- Token creation and deployment
- Contract inheritance and imports
- Token management in wallets

Same skills used by teams launching real tokens worth millions!

Glossary: Key Terms

Term	Definition
Token	Digital asset on existing blockchain
ERC-20	Standard interface for fungible tokens
Fungible	Interchangeable (1 token = any other token)
Mint	Create new tokens (increases supply)
Burn	Destroy tokens (decreases supply)
Inherit	Get functionality from parent contract
Constructor	Code that runs once at deployment
Decimals	Smallest unit (18 = like ETH)

Remember: Token $\neq$ Coin. Tokens are created ON blockchains.

Refer back to this slide when terminology gets confusing

Next Steps

Extend your knowledge:

- Add mint/burn functions to your token
- Explore ERC-721 (NFTs) – non-fungible tokens
- Learn about token economics (tokenomics)
- Study DeFi protocols that use ERC-20 (Uniswap, Aave)

Resources:

- OpenZeppelin Docs: `docs.openzeppelin.com`
- Solidity Docs: `docs.soliditylang.org`
- EIP-20 Standard: `eips.ethereum.org/EIPS/eip-20`

Course continues with: Module C (NFTs), Module E (DeFi)

Keep experimenting on testnet – mistakes cost nothing!

Token Responsibility in a Nutshell

- Creating a token is easy; creating a token people trust is hard
- With great minting power comes great responsibility – and possibly regulatory scrutiny

[COMIC: Person holding newly minted token, surrounded by warning signs: "Securities Law?", "Tokenomics?", "Liquidity?", "Rug pull accusations?". Caption: "Maybe I should have read the fine print..."]

[PLACEHOLDER] — Technical creation is step one; economic design, legal compliance, and community trust are the real challenges

Summary

What you accomplished:

- Created your own ERC-20 cryptocurrency
- Used OpenZeppelin's audited contracts
- Deployed to Sepolia testnet
- Added token to MetaMask wallet
- Transferred tokens to another wallet

Key concepts:

- ERC-20 = standard token interface
- OpenZeppelin = secure, audited implementations
- Decimals = 18 (like ETH)
- Import token in MetaMask to see balance

Congratulations! You created your own cryptocurrency!

Questions for Reflection

1. Why do ERC-20 tokens use 18 decimals by default?
2. What's the difference between `transfer` and `transferFrom`?
3. Why would you use OpenZeppelin instead of writing your own ERC-20?
4. How would you add a function to mint new tokens?
5. What happens if someone sends tokens to an address that never imports them?

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency
C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing
C) Transfers tokens D) Approves token spending
Answer: B – Mint creates new tokens and increases total supply.

Q5. Which keyword allows a contract to inherit from another?
A) extends B) inherits C) is D) from
Answer: C – The `is` keyword enables inheritance (e.g., `contract MyToken is ERC20`).

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX
D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique
C) Every token is identical and interchangeable D) Can be burned
Answer: C – Fungible means all tokens are identical, like dollars (unlike NFTs).

Q10. How many characters does an Ethereum address contain?
A) 20 B) 32 C) 40 D) 42
Answer: D – Ethereum addresses are 42 characters (0x + 40 hexadecimal characters).

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address
C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby
Answer: C – Sepolia is the recommended Ethereum testnet (Goerli, Ropsten, Rinkeby deprecated).

Q15. What happens to tokens sent to an address that never imports them?
A) Tokens return to sender B) Tokens are burned
C) Tokens remain in contract D) Tokens are in that address but invisible in UI
Answer: D – Tokens exist on-chain but won't show in wallet UI until imported.

Quiz Questions (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call
C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect
Answer: C – Burning destroys tokens permanently, reducing total supply.

Q20. Which OpenZeppelin extension enables governance voting?
A) ERC20Burnable B) ERC20Pausable C) ERC20Votes D) ERC20Permit
Answer: C – `ERC20Votes` adds governance voting power functionality.

W02: Create Your Own Cryptocurrency

Module H: Hands-On Workshops

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

(c) Joerg Osterrieder 2026

Learning Objectives

By the end of this workshop, you will be able to:

1. Create and deploy an ERC-20 token on Ethereum Sepolia testnet using OpenZeppelin
2. Explain how contract inheritance enables reuse of audited, battle-tested code
3. Transfer tokens between wallets and verify transactions on Etherscan
4. Analyze token economics: supply, decimals, and the relationship between technical parameters and value

Prerequisites: MetaMask wallet with Sepolia ETH (from W01)

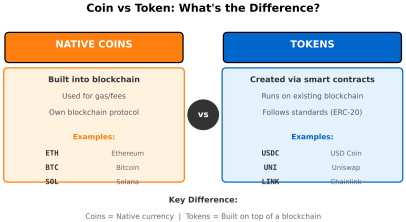
Estimated time: 60 minutes — Same technology behind USDC ($42B) and UNI ($7B)

Your Own Cryptocurrency – Seriously

What if you could:

- Create your own digital currency
- Define how many units exist
- Send it to anyone in the world
- All in under 30 minutes?

That is exactly what you will do today.
Same technology behind USDC ($42B), UNI ($7B), and 500,000+ real tokens.



The technical barrier to token creation is gone – the economic design challenge remains

The Problem: How do you create a digital currency without a central bank?

The Challenge
Traditional currencies require:

- Central authority to issue and manage supply
- Trust in institutions not to inflate away value
- Banking infrastructure for transfers

Why It Matters

- Anyone can create programmable money
- $1T+ market cap in ERC-20 tokens
- Foundation of DeFi, DAOs, and token economies

What We Need

- Standardized interface (ERC-20)
- Audited, secure code (OpenZeppelin)
- Deployment and distribution mechanism

The Cryptoeconomics Question
How do token economics (supply, distribution, utility) determine value?

Today's workshop: Create your own ERC-20 token in 30 minutes

(c) Joerg Osterrieder 2026

Workshop Objectives

By the end of this workshop, you will:

- Understand the ERC-20 token standard
- Use OpenZeppelin's audited contracts
- Deploy your own cryptocurrency on Sepolia
- Add your token to MetaMask wallet
- Transfer tokens to a classmate

Deliverable: Token contract address + proof of transfer

Estimated time: 60 minutes

(c) Joerg Osterrieder 2026

What Do You Need Before Starting?

All you need:

1. MetaMask wallet with Sepolia test ETH
2. Familiarity with Remix IDE (from W01, or we will set up together)

New to MetaMask or Remix?

- No problem – your instructor will help you set up
- Follow the quick-start guide in the lab guide

No prior knowledge of tokens or ERC-20 required!
We will learn what tokens are and how they work, step by step.

If you completed W01, you are fully prepared. If not, we will get you up to speed.

What Makes a Token Different from a Coin?

Definition: A digital asset created on an existing blockchain.

Token vs Coin:

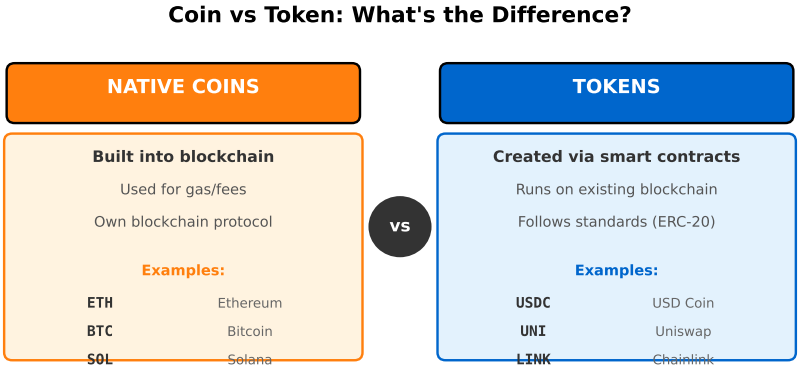
- **Coin**: Native currency of a blockchain (ETH, BTC)
- **Token**: Created using smart contracts on a blockchain

What tokens represent:

- Currency (stablecoins like USDC)
- Ownership (shares in a project)
- Access rights (membership, services)
- Voting power (governance)

Today you'll create your own token on Ethereum's Sepolia testnet

How Do Tokens Differ from Coins?



Coins are native to blockchains; tokens are built on top using smart contracts

(c) Joerg Osterrieder 2026

Discovery: Tokens Are Everywhere – Can You Spot Them?

Think about these real-world examples:

Which are "tokens"?

- Airline miles
- Casino chips
- Gift cards
- Concert tickets
- Loyalty points

Discuss:

- What makes them different from cash?
- Who controls their supply?
- Can you trade them with anyone?
- What happens if the company disappears?

Key Insight: Blockchain tokens solve the trust problem – no company needed to manage them.

Discovery moment: You already understand tokens – blockchain just makes them programmable

(c) Joerg Osterrieder 2026

Why Would You Create Your Own Token?

Real-world use cases:

- **Startups**: Fundraising and community building
- **Games**: In-game currency and rewards
- **DAOs**: Governance and voting rights
- **Loyalty Programs**: Points and rewards
- **Payments**: Stablecoins for transactions

Today's goal:

- Create YOUR token with custom name and symbol
- Experience the full deployment process
- Transfer tokens to prove ownership works

Same process used for billions of dollars in real tokens

How Does Contract Inheritance Work?

Problem: Writing ERC-20 from scratch = 200+ lines of code
Solution: Inherit from OpenZeppelin's tested code!

What `is` does:

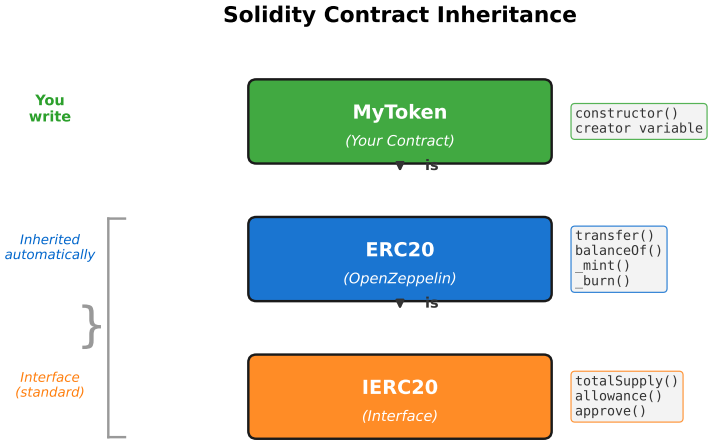
```
contract MyToken is ERC20 { ... }
```

- MyToken **inherits** all functions from ERC20
- Your contract automatically has transfer(), balanceOf(), etc.
- You only write what's different (constructor)

Analogy: Like a child inheriting traits from parents – you get everything they have, plus your own additions.

Inheritance is fundamental to Solidity and all object-oriented programming

Inheritance Hierarchy Visualization



Your contract inherits all functionality from ERC20, which implements the IERC20 interface

How Do You Import OpenZeppelin Contracts?

What happens when you write:

```
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
```

Step by step:

1. Remix sees the `@openzeppelin` prefix
2. Remix downloads the code from NPM (package manager)
3. The ERC20.sol file becomes available to your contract
4. You can now use `is ERC20` to inherit

Why this matters:

- You don't need to install anything locally
- Always gets the latest audited version
- Same code used by major DeFi projects

Remix handles package management automatically – just type and wait 10-20 seconds

What Parameters Does Your Token Need?

A constructor runs ONCE when the contract deploys.

```
constructor(
    string memory name,    // "Alice Coin"
    string memory symbol,  // "ALICE"
    uint256 initialSupply  // 1000000
) ERC20(name, symbol) {
    _mint(msg.sender, initialSupply * 10 ** decimals());
}
```

What each parameter does:

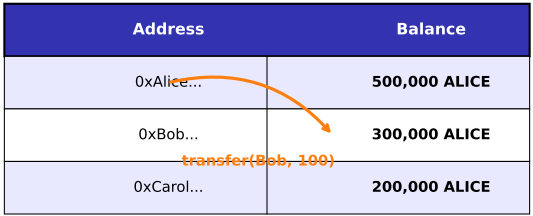
- **name**: Human-readable name (shown in wallets)
- **symbol**: Ticker symbol (like stock symbols: AAPL, GOOG)
- **initialSupply**: How many tokens to create

Important: These values are PERMANENT after deployment!

Choose carefully – you cannot change name, symbol, or initial supply later

How Token Balances Work

ERC-20 Token: Internal Balance Ledger



Smart contract stores: mapping(address => uint256) balances

Total Supply = Sum of all balances = 1,000,000 ALICE

The smart contract maintains a ledger (mapping) of who owns how many tokens

How Do Mint and Burn Functions Work?

Mint = Create new tokens from nothing

- Increases total supply
- New tokens go to a specified address
- In our contract: `_mint(msg.sender, amount)`

Burn = Destroy tokens permanently

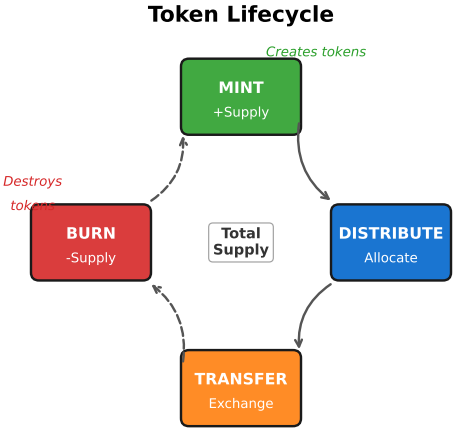
- Decreases total supply
- Tokens are removed forever
- Often sends to address(0) – the "black hole"

In our token:

- We mint ALL tokens in constructor (one-time)
- Basic version has no burn function
- Bonus: Add these features yourself!

Mint/burn control is critical for tokenomics – who can create/destroy?

What Journey Does a Token Take?



Tokens follow a lifecycle: creation (mint) through distribution, transfer, and optional destruction (burn)

(c) Joerg Osterrieder 2026

How Do You Find Someone's Wallet Address?

When transferring tokens, you need the recipient's address:

Address format:

- Always starts with `0x`
- Followed by 40 hexadecimal characters
- Example: `0xAb5801a7D398351b8bE11C439e05C5B3259aeC9B`
- Total: 42 characters

Critical warnings:

- Double-check the address before sending!
- Transactions cannot be reversed
- Tokens sent to wrong address = lost forever
- Copy-paste to avoid typos

Get your classmate's address from MetaMask: click account name to copy

What is ERC-20?

ERC-20 = Ethereum Request for Comments #20

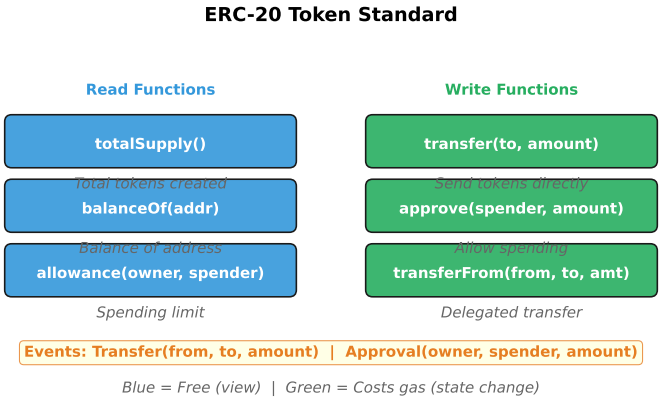
- Standard interface for fungible tokens
- Published in 2015, widely adopted since 2017
- Used by: USDC, LINK, UNI, DAI, and 500,000+ tokens

Fungible means:

- Every token is identical and interchangeable
- Like dollars: one $1 bill = any other $1 bill
- Unlike NFTs where each token is unique

ERC-20 is the foundation – we will learn everything you need in this workshop

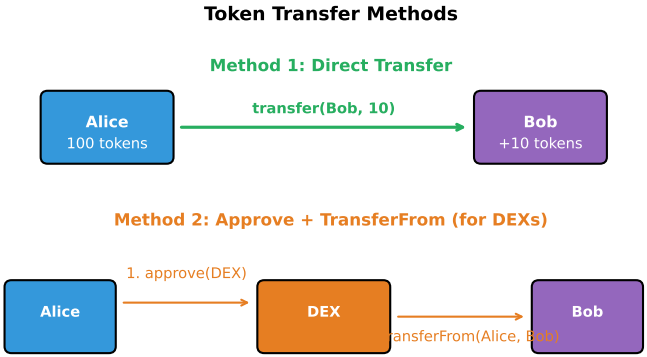
What Functions Must Every ERC-20 Token Have?



These 6 functions + 2 events define the ERC-20 standard

(c) Joerg Osterrieder 2026

How Can You Move Tokens Between Wallets?



Direct transfer for simple sends; approve pattern for DEXs and DeFi

Why Are There Two Ways to Transfer Tokens?

Two ways to move tokens:

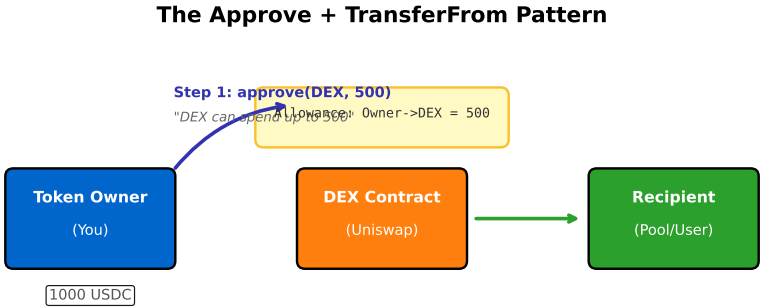
1. **transfer(to, amount)** – Direct send
   - YOU send YOUR tokens to someone
   - Simple: one transaction
   - Used in: peer-to-peer transfers

2. **approve() + transferFrom()** – Allow someone else
   - Step 1: You approve an app to spend X tokens
   - Step 2: App calls transferFrom() to take them
   - Used in: DEXs (Uniswap), DeFi protocols (Aave)

Why approve pattern? Apps can't just take tokens – you must authorize first!

Always check what you're approving – unlimited approvals can be risky

How Does the Approve Pattern Work?



Why? Smart contracts cannot initiate transactions - they need permission first

Used by: Uniswap, Aave, Compound, and every DeFi protocol

The two-step pattern lets smart contracts move tokens on your behalf after explicit approval

(c) Joerg Osterrieder 2026

Why Should You Use Audited Code?

Smart contract audits:

- Security experts review code for vulnerabilities
- Look for bugs, exploits, logic errors
- Cost: $10k - $500k+ per audit
- Takes weeks to months

Why OpenZeppelin is trusted:

- Audited by multiple security firms
- Used by major projects (Aave, Compound, OpenSea)
- Open source – anyone can review
- Battle-tested with billions of dollars at stake

Lesson: Never deploy unaudited code with real money!

For learning on testnet, unaudited code is fine – but mainnet requires audits

What is OpenZeppelin?

OpenZeppelin Contracts:

- Library of secure, audited smart contracts
- Used by 95%+ of Ethereum projects
- Open source, MIT licensed
- Battle-tested with billions of dollars secured

Why use OpenZeppelin?

- Don't reinvent the wheel
- Professional security audits
- Follows best practices
- Saves weeks of development time

Website: openzeppelin.com/contracts

How Do You Use OpenZeppelin Contracts?

Importing in Remix:

```
import "@openzeppelin/contracts/token/ERC20/ERC20.sol";
```

Remix automatically fetches from NPM!

Inheriting the contract:

```
contract MyToken is ERC20 {
    constructor() ERC20("Token Name", "SYMBOL") {
        _mint(msg.sender, 1000000 * 10 ** decimals());
    }
}
```

That's it! You inherit all 6 ERC-20 functions automatically.

OpenZeppelin handles all the complex logic for you

What Should You Name Your Token?

You need to decide:

Parameter	Example
Name	"Alice Coin"
Symbol	"ALICE"
Initial Supply	1,000,000

Naming tips:

- Name: Your name, project name, fun name
- Symbol: 3-5 uppercase letters (like stock tickers)
- Supply: How many tokens to create (you own 100%)

These are permanently set at deployment

Why Do Tokens Use 18 Decimals?

ERC-20 tokens use 18 decimals (like ETH):

- 1 token = 1,000,000,000,000,000,000 (10^18) smallest units
- Similar to 1 dollar = 100 cents

Why this matters:

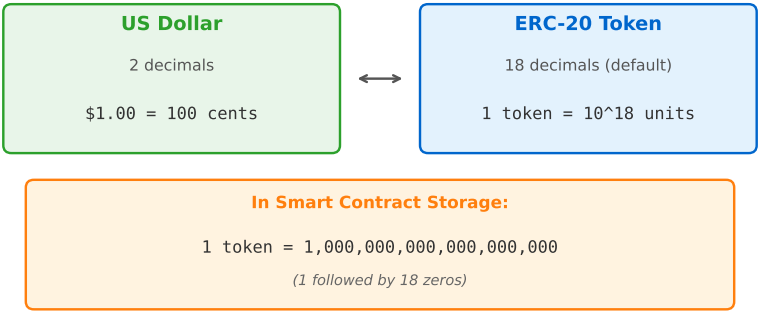
- When you mint 1,000,000 tokens...
- Actually creating: 1,000,000 $\times$ 10^18 units
- Code: `initialSupply * 10 ** decimals()`

Don't worry: Wallets display the human-readable number!

Some tokens use fewer decimals (USDC uses 6)

Why Use 18 Decimals for Token Math?

Understanding Token Decimals



`Code: amount * 10 ** decimals()`

Why? Integer math avoids floating-point errors in financial calculations

Using integer math with 18 decimals avoids floating-point errors in financial calculations

(c) Joerg Osterrieder 2026

What Code Creates Your Token?

Copy this code into Remix:

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

import "@openzeppelin/contracts/token/ERC20/ERC20.sol";

contract MyToken is ERC20 {
    address public creator;

    constructor(
        string memory name,
        string memory symbol,
        uint256 initialSupply
    ) ERC20(name, symbol) {
        creator = msg.sender;
        _mint(msg.sender, initialSupply * 10 ** decimals());
    }
}
```

Full template in contracts/MyToken.sol

Discovery: Predict What Your Token Will Do

Before deploying, predict:

Your predictions:

- Who will own all the tokens initially?
- How many tokens will exist?
- Can you create more tokens later?
- Can you change the token name later?

Write your guesses:

- Initial owner: _____
- Total supply: _____
- Can create more: Yes / No
- Can rename: Yes / No

Deploy now and check your predictions!

Discovery moment: Understanding what is fixed at deployment vs changeable is crucial for token design

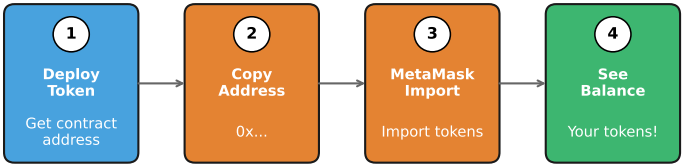
(c) Joerg Osterrieder 2026

How Do You Deploy Your Token?

1. **Open Remix IDE** (`remix.ethereum.org`)
   1. Create new file: `MyToken.sol`
   2. Paste the contract code
   3. Wait for OpenZeppelin to download (10-20 seconds)
2. **Compile**
   1. Click Solidity Compiler icon
   2. Select version 0.8.20
   3. Click “Compile MyToken.sol”
3. **Deploy**
   1. Environment: “Injected Provider - MetaMask”
   2. Enter: `"Your Token Name", "SYMBOL", 1000000`
   3. Click Deploy, confirm in MetaMask

How Do You See Your Token in MetaMask?

Adding Your Token to MetaMask



MetaMask > Import tokens > Paste contract address

Name and symbol auto-populate from the contract!

Your tokens won't show in MetaMask until you import them

How Do You Add Your Token to MetaMask?

After deployment:

1. Copy your token contract address from Remix
2. Open MetaMask
3. Scroll down, click “Import tokens”
4. Paste the contract address
5. Name and symbol auto-populate!
6. Click “Add Custom Token”
7. Click “Import Tokens”

You should see:

- Your token with the symbol you chose
- Full balance (all tokens minted to you)

Each wallet needs to import the token to see it

How Do You Send Tokens to Someone Else?

Option 1: Using MetaMask

1. Click your token in MetaMask
2. Click "Send"
3. Enter classmate's wallet address
4. Enter amount (e.g., 100 tokens)
5. Confirm transaction

Option 2: Using Remix

1. Expand your deployed contract
2. Find `transfer` function
3. Enter: recipient address, amount (with 18 decimals!)
4. Click transfer, confirm in MetaMask

Your classmate must import your token to see it in their wallet

Discovery: What Just Happened When You Transferred?

Observe after your transfer:

Check these things:

- Your balance decreased by exactly 100
- Your classmate's balance increased by 100
- Total supply stayed the same
- A gas fee was charged

Reflect:

- Where did the tokens "move" to?
- Did any tokens get created or destroyed?
- Who verified the transfer was valid?
- Could you reverse the transfer?

Key Insight: Tokens do not physically move – the ledger (mapping) updates balances.

Discovery moment: Token transfers are ledger updates, just like a bank updating account numbers

How Can You Verify Your Token on Etherscan?

View your token:

1. Go to `sepolia.etherscan.io`
2. Search for your contract address
3. Click “Token” tab to see token info

You’ll see:

- Token name and symbol
- Total supply
- Holder count
- All transfer transactions

Optional: Verify source code to make contract readable

Etherscan auto-detects ERC-20 tokens

Workshop Deliverables

To complete this workshop, submit:

1. Your token contract address on Sepolia
   - Format: `0x...` (42 characters)
2. Proof of token transfer:
   - Etherscan link to transfer transaction, OR
   - Screenshot of MetaMask showing sent tokens

Bonus (optional):

- Add a `mint()` function (owner only)
- Add a `burn()` function
- Create a token with custom decimals

See lab_guide.md for detailed instructions

Real-World Token Examples

Popular ERC-20 tokens built this way:

Token	Symbol	Market Cap
Tether	USDT	$139B
USD Coin	USDC	$42B
Chainlink	LINK	$14B
Uniswap	UNI	$7B
Dai	DAI	$5B

They all started the same way you just did!
(Just with more features and real money)

Market caps approximate (verify current values at coingecko.com)

What Advanced Features Can You Add?

OpenZeppelin Extensions:

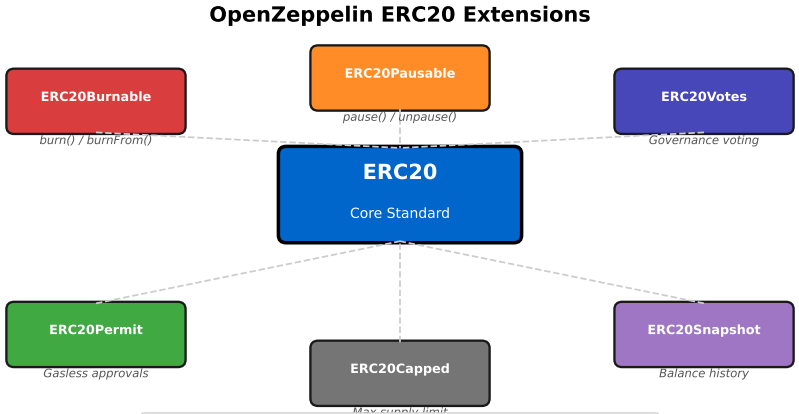
- **ERC20Burnable**: Allow token burning
- **ERC20Pausable**: Pause all transfers
- **ERC20Votes**: Governance voting power
- **ERC20Permit**: Gasless approvals (EIP-2612)

Additional Features:

- Ownable: Restrict admin functions
- AccessControl: Role-based permissions
- Timelocks: Delayed execution

See OpenZeppelin documentation for full list

What Advanced Features Can You Add?



Mix and match extensions to build feature-rich tokens with audited, secure code

What You Just Accomplished!

Celebrate – you just:

1. Understood the ERC-20 token standard
2. Used professional-grade OpenZeppelin contracts
3. Deployed YOUR OWN cryptocurrency to the blockchain
4. Imported your token into MetaMask
5. Transferred tokens to another person
6. Verified everything on Etherscan

Skills gained:

- Token creation and deployment
- Contract inheritance and imports
- Token management in wallets

Same skills used by teams launching real tokens worth millions!

Discovery: You Are Now a Token Creator – What Would You Build?

You now have the skills to create any ERC-20 token. What would YOU build?

Brainstorm use cases:

- A university loyalty token?
- A voting token for student government?
- A game currency for a project?
- A charity donation tracker?

Design questions:

- How many tokens would you create?
- Who should be able to mint more?
- Should tokens be burnable?
- What gives your token value?

The hard part is not the code – it is the economic design.

Discovery moment: Technical skills are step one; tokenomics is where the real challenge begins

Glossary: Key Terms

Term	Definition
Token	Digital asset on existing blockchain
ERC-20	Standard interface for fungible tokens
Fungible	Interchangeable (1 token = any other token)
Mint	Create new tokens (increases supply)
Burn	Destroy tokens (decreases supply)
Inherit	Get functionality from parent contract
Constructor	Code that runs once at deployment
Decimals	Smallest unit (18 = like ETH)

Remember: Token $\neq$ Coin. Tokens are created ON blockchains.

Refer back to this slide when terminology gets confusing

Next Steps

Extend your knowledge:

- Add mint/burn functions to your token
- Explore ERC-721 (NFTs) – non-fungible tokens
- Learn about token economics (tokenomics)
- Study DeFi protocols that use ERC-20 (Uniswap, Aave)

Resources:

- OpenZeppelin Docs: `docs.openzeppelin.com`
- Solidity Docs: `docs.soliditylang.org`
- EIP-20 Standard: `eips.ethereum.org/EIPS/eip-20`

In the course: Modules C (NFTs), D (Tokenomics), and E (DeFi) build on these foundations.

Keep experimenting on testnet – mistakes cost nothing!

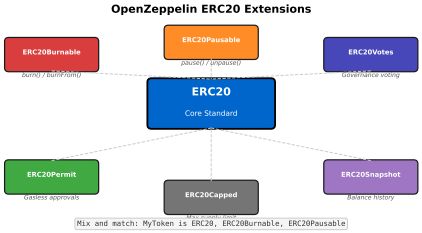
The Bigger Picture

Creating a token is easy. Building trust is hard:

- Anyone can create a token in minutes
- But why would anyone value it?
- Real tokens need: utility, community, legal compliance
- The code is 10% of the work

Questions to consider:

- What gives a token value?
- Who regulates token creation?
- What is a “rug pull” and how do you avoid it?



Technical creation is step one; economic design, legal compliance, and community trust are the real challenges

Problem Check-In: Create Your Cryptocurrency

What We Solved:

- Created programmable money without a central bank
- Used audited code (OpenZeppelin) for security
- Deployed and transferred tokens peer-to-peer

What Remains:

- Token economics design (what gives it value?)
- Legal compliance (securities law, MiCA)
- Community building and utility beyond speculation

Creating a token is easy — designing one that holds value requires solving economic, legal, and social challenges

(c) Joerg Osterrieder 2026

The Economics of Token Creation

Incentive Structure

- **Core Problem:** How do token economics determine value?
- **Supply design:** Fixed supply (deflationary) vs inflationary (ongoing minting)
- **Value Flow:** Creators set initial distribution; market determines price

Economic Security

- Audited code prevents infinite mint exploits
- approve() pattern prevents unauthorized transfers

Key Economic Question

What Gives a Token Value?

Utility (governance, access, payments), scarcity (fixed supply), and demand (network effects, speculation). Technical creation cost is near zero — economic design is everything.

Design Principle

$$\text{Token Value} = f(\text{Utility}, \text{Scarcity}, \text{Demand})$$

Anyone can create 1M tokens in minutes — the challenge is designing economics that sustain value

Design Space: Token Creation

Token Design Choices

1. **Fixed Supply** (Bitcoin model): Deflationary, scarcity-driven value
2. **Inflationary** (ETH pre-Merge): Ongoing issuance for validator rewards
3. **Elastic Supply** (Ampleforth): Algorithmic supply adjustment

Trade-offs

- Fixed supply: Scarcity vs liquidity challenges
- Minting rights: Centralized control vs community governance

Design Questions

- How many tokens should exist? (supply cap)
- Who can mint new tokens? (access control)
- Should tokens be burnable? (deflationary pressure)
- How should initial supply be distributed?

Key Insight

Code Sets Rules, Market Sets Price

The smart contract enforces supply rules; the market determines whether anyone values the token.

Every tokenomics decision is a trade-off between scarcity, utility, fairness, and flexibility

Failure Modes: Token Creation

Critical Failure Modes

- **Rug pull:** Creator mints unlimited tokens and dumps on buyers
- **Infinite mint exploit:** Bug allows unauthorized token creation

Historical Precedents

- **2017 ICO mania:** 95%+ of token projects failed or were scams
- **Squid Game token (2021):** Classic rug pull, $3.4M stolen
- **Cover Protocol (2020):** Infinite mint exploit drained funds

Regulatory Risks

- Tokens may be classified as securities (Howey test)
- EU MiCA requires licensing for token issuers
- US SEC enforcement actions against token creators

Early Warning Signs

! No token utility beyond speculation

! Concentrated ownership (founders hold 50%+)

! No vesting schedule for team tokens

Creating a token is trivial; creating one that is not a security, not a scam, and has real utility is the challenge

(c) Joerg Osterrieder 2026

Summary

What you accomplished:

- Created your own ERC-20 cryptocurrency
- Used OpenZeppelin's audited contracts
- Deployed to Sepolia testnet
- Added token to MetaMask wallet
- Transferred tokens to another wallet

Key concepts:

- ERC-20 = standard token interface
- OpenZeppelin = secure, audited implementations
- Decimals = 18 (like ETH)
- Import token in MetaMask to see balance

Congratulations! You created your own cryptocurrency!

Questions for Reflection

1. Why do ERC-20 tokens use 18 decimals by default?
2. What's the difference between `transfer` and `transferFrom`?
3. Why would you use OpenZeppelin instead of writing your own ERC-20?
4. How would you add a function to mint new tokens?
5. What happens if someone sends tokens to an address that never imports them?

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency
C) Coins are native, tokens are created via smart contracts D) No difference

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency
C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency
C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing
C) Transfers tokens D) Approves token spending

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency
C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing
C) Transfers tokens D) Approves token spending
Answer: B – Mint creates new tokens and increases total supply.

Q5. Which keyword allows a contract to inherit from another?
A) extends B) inherits C) is D) from

Quiz Questions (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20
C) Ethereum Regular Code 20 D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency
C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing
C) Transfers tokens D) Approves token spending
Answer: B – Mint creates new tokens and increases total supply.

Q5. Which keyword allows a contract to inherit from another?
A) extends B) inherits C) is D) from
Answer: C – The `is` keyword enables inheritance (e.g., `contract MyToken is ERC20`).

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX
D) A library of audited smart contracts

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX
D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX
D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique
C) Every token is identical and interchangeable D) Can be burned

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX
D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique
C) Every token is identical and interchangeable D) Can be burned
Answer: C – Fungible means all tokens are identical, like dollars (unlike NFTs).

Q10. How many characters does an Ethereum address contain?
A) 20 B) 32 C) 40 D) 42

Quiz Questions (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment
C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX
D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique
C) Every token is identical and interchangeable D) Can be burned
Answer: C – Fungible means all tokens are identical, like dollars (unlike NFTs).

Q10. How many characters does an Ethereum address contain?
A) 20 B) 32 C) 40 D) 42
Answer: D – Ethereum addresses are 42 characters (0x + 40 hexadecimal characters).

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens $= 1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address
C) The token symbol D) The block miner

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens $= 1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address
C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address
C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby
Answer: C – Sepolia is the recommended Ethereum testnet (Goerli, Ropsten, Rinkeby deprecated).

Q15. What happens to tokens sent to an address that never imports them?
A) Tokens return to sender B) Tokens are burned
C) Tokens remain in contract D) Tokens are in that address but invisible in UI

Quiz Questions (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code
C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address
C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby
Answer: C – Sepolia is the recommended Ethereum testnet (Goerli, Ropsten, Rinkeby deprecated).

Q15. What happens to tokens sent to an address that never imports them?
A) Tokens return to sender B) Tokens are burned
C) Tokens remain in contract D) Tokens are in that address but invisible in UI
Answer: D – Tokens exist on-chain but won't show in wallet UI until imported.

Quiz Questions (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin

Quiz Questions (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call
C) transfer() is for NFTs D) transferFrom() is faster

Quiz Questions (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call
C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP

Quiz Questions (16–20)

Q16. What does "audited" mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call
C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect

Quiz Questions (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call
C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect
Answer: C – Burning destroys tokens permanently, reducing total supply.

Q20. Which OpenZeppelin extension enables governance voting?
A) ERC20Burnable B) ERC20Pausable C) ERC20Votes D) ERC20Permit

Quiz Questions (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities
C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call
C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect
Answer: C – Burning destroys tokens permanently, reducing total supply.

Q20. Which OpenZeppelin extension enables governance voting?
A) ERC20Burnable B) ERC20Pausable C) ERC20Votes D) ERC20Permit
Answer: C – `ERC20Votes` adds governance voting power functionality.

Quiz: Create Your Cryptocurrency

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20 C) Ethereum Regular Code 20
D) Ethereum Resource Collection 20

Quiz (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20 C) Ethereum Regular Code 20
D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency C) Coins are native, tokens are created via smart contracts D) No difference

Quiz (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20 C) Ethereum Regular Code 20
D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18

Quiz (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20 C) Ethereum Regular Code 20
D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing C) Transfers tokens D) Approves token spending

Quiz (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20 C) Ethereum Regular Code 20
D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing C) Transfers tokens D) Approves token spending
Answer: B – Mint creates new tokens and increases total supply.

Q5. Which keyword allows a contract to inherit from another?
A) extends B) inherits C) is D) from

Quiz (1–5)

Q1. What does ERC-20 stand for?
A) Ethereum Request Contract-20 B) Ethereum Request for Comments 20 C) Ethereum Regular Code 20
D) Ethereum Resource Collection 20
Answer: B – ERC-20 is Ethereum Request for Comments #20, published in 2015.

Q2. What is the main difference between a coin and a token?
A) Coins are cheaper B) Tokens are native blockchain currency C) Coins are native, tokens are created via smart contracts D) No difference
Answer: C – Coins (ETH, BTC) are native to blockchains; tokens are created via smart contracts.

Q3. How many decimals does the default ERC-20 implementation use?
A) 6 B) 8 C) 12 D) 18
Answer: D – ERC-20 tokens use 18 decimals by default, similar to ETH.

Q4. What does the `_mint()` function do?
A) Destroys tokens B) Creates new tokens from nothing C) Transfers tokens D) Approves token spending
Answer: B – Mint creates new tokens and increases total supply.

Q5. Which keyword allows a contract to inherit from another?
A) extends B) inherits C) is D) from
Answer: C – The `is` keyword enables inheritance (e.g., `contract MyToken is ERC20`).

Quiz (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment C) Never runs D) Runs on every transfer

Quiz (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX D) A library of audited smart contracts

Quiz (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()

Quiz (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique C) Every token is identical and interchangeable D) Can be burned

Quiz (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique C) Every token is identical and interchangeable D) Can be burned
Answer: C – Fungible means all tokens are identical, like dollars (unlike NFTs).

Q10. How many characters does an Ethereum address contain?
A) 20 B) 32 C) 40 D) 42

(c) Joerg Osterrieder 2025

Quiz (6–10)

Q6. What happens when you deploy a smart contract constructor?
A) Runs every time a function is called B) Runs once at deployment C) Never runs D) Runs on every transfer
Answer: B – Constructors execute exactly once when the contract is deployed.

Q7. What is OpenZeppelin?
A) A blockchain B) A wallet C) A DEX D) A library of audited smart contracts
Answer: D – OpenZeppelin provides secure, audited smart contract libraries.

Q8. Which ERC-20 function is used for direct peer-to-peer transfers?
A) transferFrom() B) approve() C) transfer() D) send()
Answer: C – `transfer(to, amount)` sends your tokens directly to someone.

Q9. What does "fungible" mean in the context of ERC-20 tokens?
A) Can be traded B) Every token is unique C) Every token is identical and interchangeable D) Can be burned
Answer: C – Fungible means all tokens are identical, like dollars (unlike NFTs).

Q10. How many characters does an Ethereum address contain?
A) 20 B) 32 C) 40 D) 42
Answer: D – Ethereum addresses are 42 characters (0x + 40 hexadecimal characters).

(c) Joerg Osterrieder 2025

Quiz (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code C) Allow another address to spend your tokens D) Mint tokens

Quiz (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$

Quiz (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address C) The token symbol D) The block miner

Quiz (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby

Quiz (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby
Answer: C – Sepolia is the recommended Ethereum testnet (Goerli, Ropsten, Rinkeby deprecated).

Q15. What happens to tokens sent to an address that never imports them?
A) Tokens return to sender B) Tokens are burned C) Tokens remain in contract D) Tokens are in that address but invisible in UI

Quiz (11–15)

Q11. What is the purpose of the approve() function?
A) Approve a transaction B) Verify contract code C) Allow another address to spend your tokens D) Mint tokens
Answer: C – `approve()` grants permission for another address (e.g., DEX) to spend tokens.

Q12. If you mint 1,000,000 tokens, how many smallest units are created?
A) 1,000,000 B) 1,000,000,000 C) $1{,}000{,}000 \times 10^{18}$ D) $1{,}000{,}000 \times 10^{6}$
Answer: C – With 18 decimals, 1M tokens = $1{,}000{,}000 \times 10^{18}$ smallest units.

Q13. What does `msg.sender` represent in Solidity?
A) The contract address B) The caller's address C) The token symbol D) The block miner
Answer: B – `msg.sender` is the address of the account calling the function.

Q14. Which testnet did we use in this workshop?
A) Goerli B) Ropsten C) Sepolia D) Rinkeby
Answer: C – Sepolia is the recommended Ethereum testnet (Goerli, Ropsten, Rinkeby deprecated).

Q15. What happens to tokens sent to an address that never imports them?
A) Tokens return to sender B) Tokens are burned C) Tokens remain in contract D) Tokens are in that address but invisible in UI
Answer: D – Tokens exist on-chain but won't show in wallet UI until imported.

Quiz (16–20)

Q16. What does "audited" mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities C) Contract is deployed D) Contract uses OpenZeppelin

Quiz (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call C) transfer() is for NFTs D) transferFrom() is faster

Quiz (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP

Quiz (16–20)

Q16. What does "audited" mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect

Quiz (16–20)

Q16. What does "audited" mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect
Answer: C – Burning destroys tokens permanently, reducing total supply.

Q20. Which OpenZeppelin extension enables governance voting?
A) ERC20Burnable B) ERC20Pausable C) ERC20Votes D) ERC20Permit

Quiz (16–20)

Q16. What does “audited” mean for smart contracts?
A) Contract is compiled B) Security experts reviewed code for vulnerabilities C) Contract is deployed D) Contract uses OpenZeppelin
Answer: B – Audits involve security firms reviewing code for bugs and exploits.

Q17. What is the difference between transfer() and transferFrom()?
A) No difference B) transferFrom() requires prior approve() call C) transfer() is for NFTs D) transferFrom() is faster
Answer: B – `transferFrom()` requires the owner to `approve()` first (used by DEXs).

Q18. Which symbol is used for the Uniswap token?
A) UNI B) SWAP C) UNIV3 D) UNISWAP
Answer: A – Uniswap token uses symbol UNI ($7B market cap, Dec 2024).

Q19. What does burning a token do to total supply?
A) Increases it B) Keeps it the same C) Decreases it D) Has no effect
Answer: C – Burning destroys tokens permanently, reducing total supply.

Q20. Which OpenZeppelin extension enables governance voting?
A) ERC20Burnable B) ERC20Pausable C) ERC20Votes D) ERC20Permit
Answer: C – `ERC20Votes` adds governance voting power functionality.

W03: Mint Your First NFT

Module H: Hands-On Workshops

Prof. Dr. Jörg Osterrieder

BSc Blockchain, Crypto Economy & NFTs

Spring 2026

Learning Objectives

By the end of this workshop, you will be able to:

1. Deploy an ERC-721 NFT contract on Sepolia testnet using OpenZeppelin
2. Create and link NFT metadata (name, description, image) following the OpenSea standard
3. Mint a unique, verifiable digital token and verify ownership on Etherscan
4. Explain the relationship between on-chain tokens, off-chain metadata, and IPFS content addressing

Prerequisites: MetaMask wallet with Sepolia ETH (from W01/W02)

Estimated time: 60–75 minutes — Builds on W01 (contracts) and W02 (tokens)

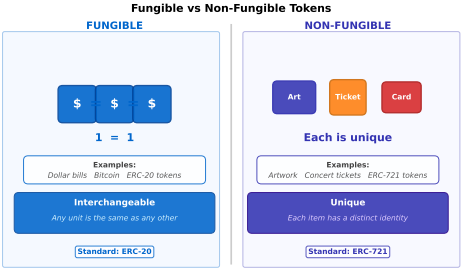
Your First Digital Collectible

Imagine this:

- What if you could create a unique digital item that proves your ownership on a blockchain?
- Not a copy – an original, verifiable, one-of-a-kind token
- Stored permanently, transferable, and visible to anyone

Today, you will do exactly that.

You will write a smart contract, mint a unique token, and verify it on Etherscan and OpenSea – all in about 60 minutes.



W03 builds on W01 (contracts) and W02 (tokens) – now we make them unique

The Problem: How Do You Prove Ownership of a Digital File?

The Challenge
Digital files can be copied infinitely at zero cost. There is:

- No built-in scarcity for digital content
- No provenance trail for creators
- No way to prove "this is the original"

Why It Matters

- Digital art and collectibles need verifiable ownership
- Gaming items need uniqueness and transferability
- Real-world assets need on-chain representation

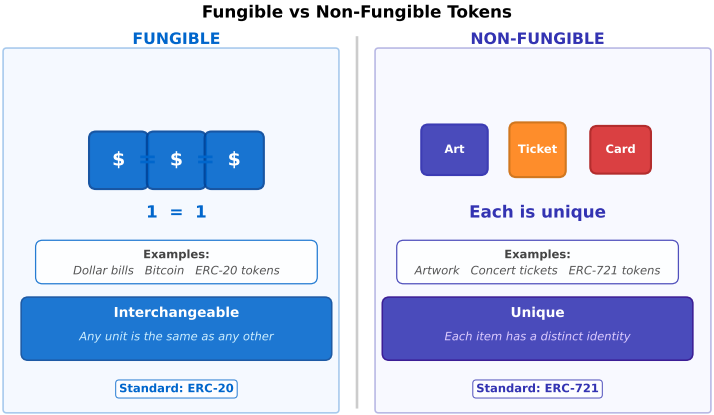
What We Need

- A smart contract standard for uniqueness (ERC-721)
- Metadata linking (name, description, image)
- Permanent, decentralized storage (IPFS)

The Cryptoeconomics Question
Who pays for digital uniqueness, and what economic value does verifiable ownership create?

Today's workshop: Mint your first NFT on Sepolia testnet (60–75 minutes)

Fungible vs Non-Fungible: Why Does It Matter?



ERC-20 = fungible (every token identical), ERC-721 = non-fungible (every token unique)

How Is ERC-721 Different from ERC-20?

ERC-20 vs ERC-721: Key Differences

Dimension	ERC-20 (Fungible)	ERC-721 (Non-Fungible)
Uniqueness	Identical tokens	Each token unique
Divisibility	Divisible (decimals)	Indivisible (whole)
Standard	ERC-20	ERC-721
Use Case	Currency, voting	Art, collectibles, gaming
Balance Type	Amount (uint256)	List of Token IDs
Key Function	transfer()	safeTransferFrom()

ERC-20 powers currencies and governance; ERC-721 powers ownership of unique items

6 key differences: unique IDs, metadata URIs, individual ownership, approval per token, no decimals, non-divisible

(c) Joerg Osterrieder 2026

Discovery: Can You Think of Non-Fungible Things in Your Life?

Think About It:
Not everything is interchangeable. Some things are unique by nature.

Predict:

- List 3 things you own that are NOT interchangeable
- What makes each one unique?
- Could you replace it with "an equivalent"?

Discuss with your neighbor:

- A concert ticket (specific seat, date)
- Your passport (unique to you)
- A hand-drawn sketch (one original)

(c) Joerg Osterrieder 2026

Discovery: Can You Think of Non-Fungible Things in Your Life?

Think About It:
Not everything is interchangeable. Some things are unique by nature.

Predict:

- List 3 things you own that are NOT interchangeable
- What makes each one unique?
- Could you replace it with "an equivalent"?

Discuss with your neighbor:

- A concert ticket (specific seat, date)
- Your passport (unique to you)
- A hand-drawn sketch (one original)

Key Insight: NFTs bring this concept of uniqueness to digital items – each token has a unique ID and metadata, just like each passport has a unique number.

Discovery moment: Non-fungibility is natural – blockchain simply makes it work for digital items

What Does an NFT Actually Contain?

An NFT has two layers – on-chain and off-chain:

On-Chain (stored on blockchain):

- Token ID (unique number: 0, 1, 2, ...)
- Owner address (who holds this token)
- tokenURI pointer (link to metadata)
- Transfer history (every sale/transfer)

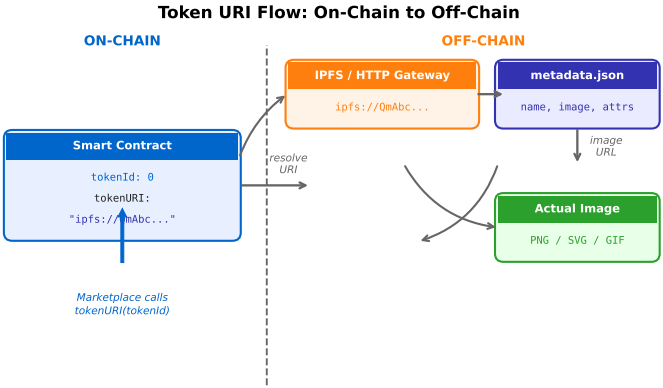
Off-Chain (stored elsewhere):

- Metadata JSON (name, description, attributes)
- Actual image or media file
- Stored on IPFS, web server, or cloud
- Linked by the tokenURI

Why this split? Storing images on-chain would cost thousands of dollars in gas. The token proves ownership; the metadata describes what you own.

The token itself lives on the blockchain; the art and metadata are stored elsewhere

How Does tokenURI Connect Your NFT to Its Art?



tokenURI is the bridge between on-chain token ownership and off-chain metadata/image content

Workshop Objectives

By the end of this workshop, you will:

1. Understand ERC-721 basics and how NFTs differ from fungible tokens
2. Create NFT metadata JSON following the OpenSea standard
3. Deploy an NFT contract on Sepolia testnet
4. Mint an NFT with metadata
5. View your NFT on Etherscan and OpenSea testnet

Deliverable: Contract address + minted tokenId + screenshot

Prerequisites: MetaMask wallet with Sepolia ETH (from W01/W02)

(c) Joerg Osterrieder 2026

What Do You Need Before Starting?

Prerequisites (from W01/W02):

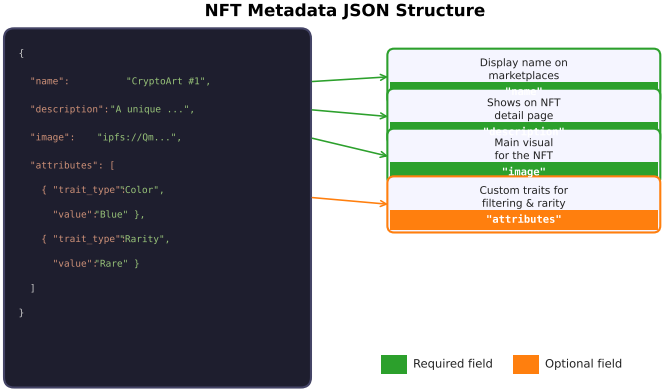
1. MetaMask wallet with Sepolia test ETH
2. Chrome, Firefox, or Brave browser
3. Remix IDE (`remix.ethereum.org`) – same as W01/W02
4. Curiosity (the most important tool)

Need Sepolia ETH? Use the same faucets from W01:

- Google Cloud: `cloud.google.com/application/web3/faucet/ethereum/sepolia`
- Alchemy: `sepoliafaucet.com`
- Chainlink: `faucets.chain.link/sepolia`

If you need Sepolia ETH, ask the instructor or visit a faucet (see lab guide)

What Goes Inside Your NFT Metadata?



OpenSea and other marketplaces read these fields to display your NFT

OpenSea metadata standard: name, description, image, and optional attributes array

How Do You Create Your Metadata?

NFT metadata follows a standard JSON format:

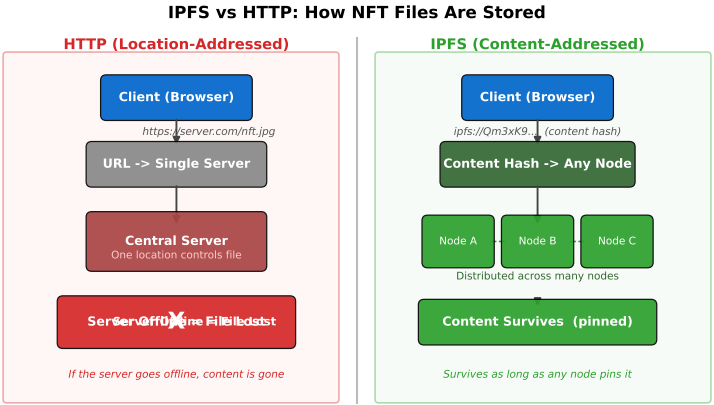
```
{
  "name": "My First NFT",
  "description": "Created during W03 Workshop",
  "image": "https://upload.wikimedia.org/wikipedia/commons
            /4/46/Bitcoin.svg",
  "attributes": [
    {"trait_type": "Course", "value": "Blockchain"},
    {"trait_type": "Workshop", "value": "W03"}
  ]
}
```

Use this ready-made URL directly:
https://digital-ai-finance.github.io/Cryptoeconomics-Blockchain/workshops/w03-example-metadata.json

---

Option A: Use the placeholder URL above. Option B: Upload your own to IPFS (see lab guide)

Why IPFS? Content Addressing vs Location Addressing



IPFS addresses content by its hash (permanent) – HTTP addresses by location (can change or disappear)

Discovery: How Many Lines of Code to Create a Unique Digital Item?

Think About It:
You are about to write a smart contract that creates unique, verifiable digital tokens.

Predict:

- How many lines of code do you think it takes to write an NFT smart contract?
- Write down your guess: _____ lines
- Compare with your neighbor

Consider:

- In W01, your first contract was 15 lines
- In W02, your ERC-20 token was about 20 lines
- NFTs seem more complex – unique IDs, metadata...

Discovery: How Many Lines of Code to Create a Unique Digital Item?

Think About It:
You are about to write a smart contract that creates unique, verifiable digital tokens.

Predict:

- How many lines of code do you think it takes to write an NFT smart contract?
- Write down your guess: _____ lines
- Compare with your neighbor

Consider:

- In W01, your first contract was 15 lines
- In W02, your ERC-20 token was about 20 lines
- NFTs seem more complex – unique IDs, metadata...

Answer: About 25 lines – thanks to OpenZeppelin! The audited library handles all the complex ERC-721 logic for you.

Discovery moment: Standing on the shoulders of giants – OpenZeppelin does the heavy lifting

What Are the Key Parts of an ERC-721 Contract?

Three essential building blocks:

1. **Import OpenZeppelin's ERC721URIStorage**
   - Audited, battle-tested code used by thousands of NFT projects
   - Handles ownership tracking, transfers, and metadata storage
2. **Token ID Counter (`_nextTokenId`)**
   - Auto-incrementing: first mint = token 0, second = token 1, ...
   - Each ID is unique within your collection
3. **`mintNFT()` Function**
   - Creates a new token and assigns it to the caller
   - Links off-chain metadata via tokenURI

Compare to W02 (ERC-20): Same pattern (import, state, functions), different standard.

OpenZeppelin provides audited building blocks – never write token standards from scratch

Let's Build Your NFT Contract Step by Step

Before copying into Remix, look at each section. Can you guess what each part does?

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.20;

import "@openzeppelin/contracts/token/ERC721/ERC721.sol";
import "@openzeppelin/contracts/token/ERC721/extensions/ERC721URIStorage.sol";

contract MyFirstNFT is ERC721URIStorage {
    uint256 private _nextTokenId;
    address public creator;

    constructor(string memory name, string memory symbol)
        ERC721(name, symbol)
    {
        creator = msg.sender;
    }

    function mintNFT(string memory tokenURI)
        public returns (uint256)
    {
        uint256 tokenId = _nextTokenId;
        _nextTokenId++;
        _safeMint(msg.sender, tokenId);
        _setTokenURI(tokenId, tokenURI);
        return tokenId;
    }
}
```

This is the complete contract – about 25 lines of actual code

What Does Each Line of Code Do?

Line-by-line breakdown:

`ERC721URIStorage`
→ Stores a unique metadata URI per token (unlike ERC-20's shared balance)

`uint256 private _nextTokenId;`
→ Auto-incrementing counter (token 0, 1, 2, ...)

`constructor(name, symbol) ERC721(name, symbol)`
→ Collection identity (e.g., "My Art Collection", "ART")

`_safeMint(msg.sender, tokenId);`
→ Creates the token and assigns it to YOUR wallet

`_setTokenURI(tokenId, tokenURI);`
→ Links off-chain metadata (JSON with name, image) to the token

`return tokenId;`
→ Returns the ID so you know which token was created

Compare to W02: ERC-20 tracks balances, ERC-721 tracks individual token ownership

How Do You Compile Your NFT Contract?

In Remix IDE:

1. File Explorer → contracts folder → create "`MyFirstNFT.sol`"
2. Paste the contract code from the previous slide
3. Click the Solidity Compiler tab (left sidebar icon)
4. Select compiler version: `0.8.20` (or later)
5. Click "Compile MyFirstNFT.sol"
6. Wait for OpenZeppelin to download (10–30 seconds first time)
7. Green checkmark = success!

Errors? Check:

- Solidity version matches `pragma` statement
- No typos in import paths (case-sensitive!)
- All brackets and semicolons are in place

If compilation fails: check Solidity version matches pragma, ensure no typos in import paths

Discovery: Predict Before You Deploy

Before clicking "Deploy", make your predictions:

Predict:

- What constructor parameters will you need?
- How many NFTs exist right after deployment?
- Will there be any tokens in your wallet?
- Will deployment cost more or less gas than W01?

Write down your guesses:

- Parameters: _____
- NFTs after deploy: _____
- My wallet has: _____ NFTs
- Gas compared to W01: _____

Discovery: Predict Before You Deploy

Before clicking "Deploy", make your predictions:

Predict:

- What constructor parameters will you need?
- How many NFTs exist right after deployment?
- Will there be any tokens in your wallet?
- Will deployment cost more or less gas than W01?

Write down your guesses:

- Parameters: _____
- NFTs after deploy: _____
- My wallet has: _____ NFTs
- Gas compared to W01: _____

Answers: Name + symbol (e.g., "My Art Collection", "ART"). Zero NFTs – the contract is deployed but empty, like an empty photo album. Gas will be higher because ERC-721 is more complex than W01's simple contract.

Discovery moment: Deploying a contract does not create any tokens – minting is a separate step

How Do You Deploy Your NFT Contract?

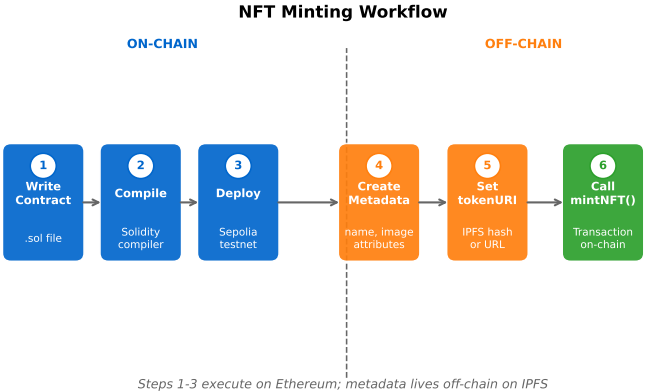
In Remix:

1. Click "Deploy & Run" tab (left sidebar)
2. Environment: Select "Injected Provider - MetaMask"
3. MetaMask popup: confirm you are on Sepolia network
4. Enter constructor parameters:
   - `name`: e.g., "My Art Collection"
   - `symbol`: e.g., "ART"
5. Click "Deploy"
6. MetaMask popup: confirm transaction (∼0.01 Sepolia ETH)
7. Wait 15–30 seconds for confirmation
8. Copy contract address from "Deployed Contracts" section

Important: Save your contract address – you will need it for Etherscan and OpenSea verification!

Save your contract address – you will need it for Etherscan and OpenSea verification

What Does the NFT Minting Workflow Look Like?



Complete flow: write contract, deploy, mint with metadata, verify on Etherscan and OpenSea

How Do You Mint Your First NFT?

The key moment – creating your unique token:

1. In Remix: expand your deployed contract (bottom of Deploy tab)
2. Find the `mintNFT` function (orange button = write function)
3. In the `tokenURI` input field, paste:
   `https://digital-ai-finance.github.io/Cryptoeconomics-Blockchain/workshops/w03-example-metadata.json`
4. Click "mintNFT"
5. MetaMask popup: confirm transaction
6. Wait for confirmation – check Remix console for green checkmark

Congratulations – you just created your first NFT!

Your token ID is `0` (the first token in your collection).

The mintNFT function calls _safeMint (creates token) and _setTokenURI (links metadata)

How Do You Verify Your NFT Exists?

Use Remix read functions (blue buttons – free, no gas):

1. Call `ownerOf(0)` → returns YOUR wallet address (you are the owner!)
2. Call `tokenURI(0)` → returns the metadata URI you provided
3. Call `balanceOf(your_address)` → returns 1 (you own one NFT)
4. Call `creator()` → returns your address (you deployed the contract)

What do these tell you?

- **ownerOf**: Proves who holds a specific token
- **tokenURI**: Shows where the metadata lives
- **balanceOf**: Counts how many NFTs an address owns

Read functions are free – they query blockchain state without creating transactions

Discovery: What Can Etherscan Tell You About Your NFT?

Explore and investigate:
Go to `sepolia.etherscan.io` and search for your contract address.

Find these on Etherscan:

1. The contract creation transaction
2. Your mint transaction
3. The tokenURI stored on-chain
4. Who owns token 0

Reflect:

- Everything is public and transparent
- Anyone can verify your NFT's ownership
- The entire history is permanently recorded
- This is what "trustless verification" means

(c) Joerg Osterrieder 2026

Discovery: What Can Etherscan Tell You About Your NFT?

Explore and investigate:
Go to `sepolia.etherscan.io` and search for your contract address.

Find these on Etherscan:

1. The contract creation transaction
2. Your mint transaction
3. The tokenURI stored on-chain
4. Who owns token 0

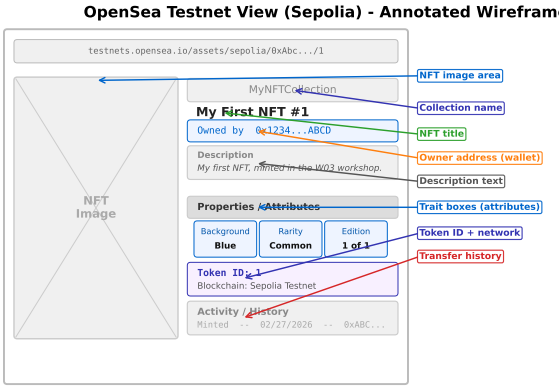
Reflect:

- Everything is public and transparent
- Anyone can verify your NFT's ownership
- The entire history is permanently recorded
- This is what "trustless verification" means

Key Insight: Blockchain transparency means NFT provenance is always verifiable – no need to trust a gallery or marketplace.

Discovery moment: On-chain transparency replaces institutional trust with cryptographic proof

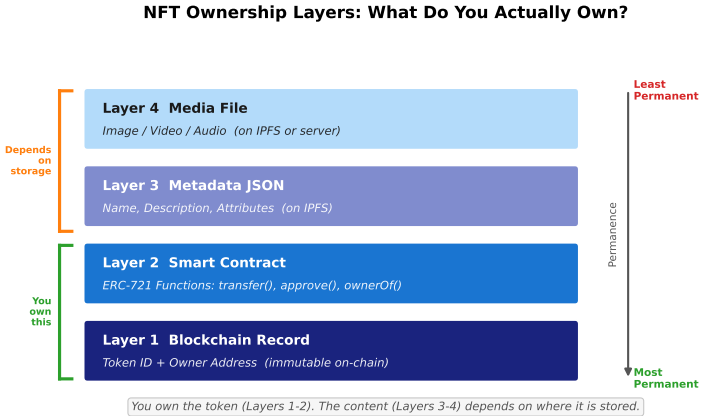
How Does Your NFT Appear on OpenSea?



View your NFT: Go to `testnets.opensea.io`, connect MetaMask, check your Profile.

OpenSea reads your contract's tokenURI, fetches the metadata JSON, and displays the image

What Do You Actually Own After Minting?



You own the token (on-chain record of ownership), NOT the image file itself – anyone can still view or copy the image

Workshop Deliverables

To complete this workshop, submit:

1. Contract address on Sepolia (from Remix "Deployed Contracts")
   - Format: `0x...` (42 characters)
2. Token ID of your minted NFT (should be 0 for first mint)
3. Screenshot of Etherscan OR OpenSea showing your NFT

Bonus (optional):

- Mint a second NFT with different metadata (token ID will be 1)
- Deploy the extended contract with royalties (see `contracts/MyFirstNFT_Extended.sol`)
- Set a 5% royalty using `setDefaultRoyalty(your_address, 500)`

All deliverables should reference the Sepolia testnet – never deploy to mainnet for workshops

What Do Common Error Messages Mean?

Error Message	Cause	Solution
"Insufficient funds"	Not enough Sepolia ETH	Visit faucet (sepoliafaucet.com)
"ERC721: invalid token ID"	Token does not exist	Check token ID (starts at 0)
"Execution reverted"	Contract logic error	Check constructor parameters
OpenSea not showing NFT	Indexing delay	Wait 5 min, refresh metadata
MetaMask "wrong network"	Not on Sepolia	Switch network in MetaMask

Still stuck?

1. Read the error message carefully – it usually tells you the fix
2. Check MetaMask is unlocked and on Sepolia
3. Try refreshing Remix and reconnecting MetaMask

Most errors have simple fixes – always read the error message carefully

What You Just Accomplished!

You just:

- Created an ERC-721 NFT collection from scratch
- Wrote metadata following the OpenSea standard
- Deployed a smart contract to Sepolia testnet
- Minted a unique, verifiable digital token
- Verified ownership on Etherscan
- Viewed your creation on OpenSea

These are the same skills behind CryptoPunks, BAYC, and digital art marketplaces.

The NFT ecosystem manages billions in value using the exact same tools and patterns you practiced today: OpenZeppelin, Remix, MetaMask, and ERC-721.

You used professional-grade tools (OpenZeppelin, Remix, MetaMask) – same as production NFT projects

The Reality Check

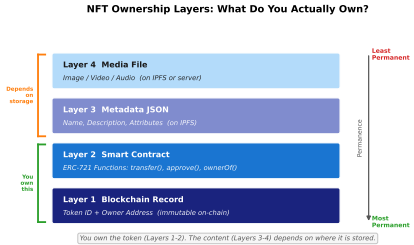
On Mainnet, things get real:

- Gas costs for minting: $5–20 per NFT
- Metadata storage costs matter (IPFS pinning services)
- Royalty enforcement varies by marketplace
- Floor price dynamics affect collection value

What changes on mainnet:

- Every byte of storage costs real ETH
- Metadata permanence becomes critical
- Security audits are essential before launch
- Marketing and community drive demand

The technical skills you practiced today are identical to professional NFT development.



Sepolia is free – mainnet deployment involves real economic considerations

Problem Check-In: Mint Your First NFT

What We Solved:

- Created verifiable digital uniqueness on blockchain
- Linked on-chain ownership to off-chain metadata
- Proved ownership via Etherscan and OpenSea

What Remains:

- Metadata permanence (IPFS pinning vs centralized hosting)
- Royalty enforcement across marketplaces
- Legal status of NFT ownership vs copyright

NFTs solve digital scarcity but do not solve copyright, permanence, or intrinsic value

(c) Joerg Osterrieder 2026

The Economics of NFT Minting

Incentive Structure

- **Core Problem:** Who pays for digital uniqueness, and what economic value does it create?
- **Minting cost:** Gas fee ($5–20 on mainnet) creates economic barrier against spam
- **Value Flow:** Creators pay gas → collectors pay purchase price → creators earn royalties

Economic Security

- ERC-721 enforces unique ownership per token ID
- On-chain provenance eliminates counterfeiting

Key Economic Question

What Creates NFT Value?

Scarcity (unique token IDs), provenance (verifiable ownership history), utility (access, membership), and social signaling (status, identity). The token is the proof; the value is social.

Design Principle

$$\text{NFT Value} = f(\text{Scarcity}, \text{Provenance}, \text{Utility})$$

Gas costs create a floor price for minting — on mainnet, every NFT must justify its creation cost

Design Space: NFT Minting

NFT Standard Choices

1. **ERC-721**: One token per ID, simple ownership model
2. **ERC-1155**: Multi-token (fungible + non-fungible in one contract)
3. **ERC-721A**: Gas-optimized batch minting (Azuki)

Metadata Storage Trade-offs

- IPFS: Content-addressed, decentralized, requires pinning
- On-chain: Permanent but extremely expensive
- Centralized server: Cheap but can disappear

Design Questions

- Should metadata be immutable or updatable?
- Open minting (anyone) or restricted (creator only)?
- Should royalties be on-chain (ERC-2981) or marketplace-enforced?

Key Insight

Permanence vs Flexibility

Immutable metadata guarantees authenticity but prevents fixes. Updatable metadata allows improvements but requires trust.

Every NFT design trades off permanence, cost, flexibility, and decentralization of metadata storage

(c) Joerg Osterrieder 2026

Failure Modes: NFT Minting

Critical Failure Modes

- **Metadata disappears:** Server goes offline, IPFS node stops pinning
- **Rug pull:** Creator abandons project after mint revenue

Historical Precedents

- **NFT winter (2022–23):** 90%+ of collections lost floor value
- **Centralized metadata:** Multiple projects lost images when hosting expired
- **Wash trading:** Fake volume inflated perceived demand

Ownership Misconceptions

- NFT $\neq$ copyright (you own the token, not the art)
- Anyone can still view and copy the image
- Legal rights depend on creator's license terms

Early Warning Signs

! Metadata on centralized servers (not IPFS)

! No utility beyond speculative resale

! Anonymous team with no track record

The token is permanent on-chain, but the value proposition depends on metadata permanence and real utility

(c) Joerg Osterrieder 2026

Summary and Key Takeaways

What you learned today:

1. ERC-721 creates unique, non-fungible tokens (unlike ERC-20)
2. NFT metadata (name, description, image) lives off-chain
3. tokenURI is the bridge connecting on-chain token to off-chain metadata
4. IPFS provides content-addressed, decentralized storage
5. Anyone can verify NFT ownership on-chain (Etherscan, OpenSea)

The progression:

- W01: Deploy a smart contract (your first on-chain code)
- W02: Create a fungible token (ERC-20, shared balances)
- W03: Mint a non-fungible token (ERC-721, unique ownership)

Next: Course Module C covers NFTs and Digital Assets in depth (8 lessons).

Key insight: NFTs prove digital ownership – the technology is simple, the implications are profound

Glossary: Key Terms

Term	Definition
NFT	Non-Fungible Token – unique digital asset on blockchain
ERC-721	Ethereum standard for non-fungible tokens
tokenURI	Function returning metadata URI for a specific token
Metadata JSON	Structured file with name, description, image, attributes
IPFS	InterPlanetary File System – decentralized content storage
Mint	Creating a new token on the blockchain
Token ID	Unique identifier for each token within a collection
OpenSea	Largest NFT marketplace (testnets.opensea.io for testing)
ERC-2981	Standard for on-chain royalty payment information
Content Addressing	Locating files by their content hash, not location

These terms appear throughout Module C (NFTs and Digital Assets)

(c) Joerg Osterrieder 2026

Next Steps and Resources

Continue Learning:

1. Course: Module C (NFTs and Digital Assets) – 8 lessons on NFT theory and practice
2. Try: Upload your own metadata to IPFS via Pinata (`pinata.cloud`, free tier)
3. Explore: ERC-1155 (multi-token standard) for gaming and batch operations
4. Study: NFT marketplace mechanics (royalties, auctions, floor prices)

Resources:

- OpenZeppelin docs: `docs.openzeppelin.com/contracts`
- EIP-721 specification: `eips.ethereum.org/EIPS/eip-721`
- Pinata IPFS: `pinata.cloud`
- OpenSea testnet: `testnets.opensea.io`

Challenge: Deploy the extended contract (`contracts/MyFirstNFT_Extended.sol`) and set up royalties!

The NFT ecosystem evolves rapidly – the fundamentals you learned today remain constant

Questions for Reflection

1. Why does minting an NFT cost gas but reading `ownerOf()` is free?
2. What happens to your NFT's image if the IPFS node stops pinning it?
3. If you transfer your NFT to someone else, can you still see the metadata?
4. Why would a creator want to set royalties (ERC-2981) on their NFT?
5. What is the difference between owning an NFT and owning the copyright to the artwork?

(c) Joerg Osterrieder 2026

Quiz Questions (1–5)

Q1. What does “non-fungible” mean?
A) Divisible into smaller units B) Identical and interchangeable
C) Each item is unique and not interchangeable D) Cannot be transferred

Quiz Questions (1–5)

Q1. What does “non-fungible” mean?
A) Divisible into smaller units B) Identical and interchangeable
C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777

Quiz Questions (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable
C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address
C) A URI pointing to the token's metadata D) The token's creation date

Quiz Questions (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable
C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address
C) A URI pointing to the token's metadata D) The token's creation date
Answer: C – tokenURI returns the link to off-chain metadata (name, description, image).

Q4. Where is NFT metadata typically stored?
A) On the Ethereum blockchain B) In the smart contract's storage
C) Off-chain (IPFS or web server) D) In the user's wallet

Quiz Questions (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable
C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address
C) A URI pointing to the token's metadata D) The token's creation date
Answer: C – tokenURI returns the link to off-chain metadata (name, description, image).

Q4. Where is NFT metadata typically stored?
A) On the Ethereum blockchain B) In the smart contract's storage
C) Off-chain (IPFS or web server) D) In the user's wallet
Answer: C – Storing images on-chain would cost thousands in gas; metadata lives off-chain.

Q5. What does _safeMint do?
A) Burns a token B) Transfers a token
C) Creates a new token and assigns it to an owner D) Updates the token's metadata

Quiz Questions (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable
C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address
C) A URI pointing to the token's metadata D) The token's creation date
Answer: C – tokenURI returns the link to off-chain metadata (name, description, image).

Q4. Where is NFT metadata typically stored?
A) On the Ethereum blockchain B) In the smart contract's storage
C) Off-chain (IPFS or web server) D) In the user's wallet
Answer: C – Storing images on-chain would cost thousands in gas; metadata lives off-chain.

Q5. What does _safeMint do?
A) Burns a token B) Transfers a token
C) Creates a new token and assigns it to an owner D) Updates the token's metadata
Answer: C – _safeMint creates a new token and assigns ownership to the specified address.

Quiz Questions (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address
C) Using an IP address for each file D) Using a database ID

Quiz Questions (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address
C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable
C) ERC721URIStorage D) ERC721Pausable

Quiz Questions (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address
C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable
C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does ownerOf(tokenId) return?
A) The token's metadata B) The token's creation date
C) The address that owns the token D) The token's transfer history

Quiz Questions (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address
C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable
C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does ownerOf(tokenId) return?
A) The token's metadata B) The token's creation date
C) The address that owns the token D) The token's transfer history
Answer: C – ownerOf returns the current owner's Ethereum address for that specific token.

Q9. Can you modify an NFT's metadata after minting?
A) No, it is permanently fixed B) Yes, by calling setTokenURI (if the contract allows)
C) Only the owner can modify it D) Only within the first 24 hours

Quiz Questions (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address
C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable
C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does ownerOf(tokenId) return?
A) The token's metadata B) The token's creation date
C) The address that owns the token D) The token's transfer history
Answer: C – ownerOf returns the current owner's Ethereum address for that specific token.

Q9. Can you modify an NFT's metadata after minting?
A) No, it is permanently fixed B) Yes, by calling setTokenURI (if the contract allows)
C) Only the owner can modify it D) Only within the first 24 hours
Answer: B – If the contract exposes setTokenURI, metadata can be updated; immutability depends on design.

Q10. Why does minting cost gas but viewing is free?
A) Minting creates a new block
B) Minting writes to blockchain state (costs gas); viewing reads existing state (free)
C) The network charges for all operations D) Only the first mint costs gas

Quiz Questions (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address
C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable
C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does ownerOf(tokenId) return?
A) The token's metadata B) The token's creation date
C) The address that owns the token D) The token's transfer history
Answer: C – ownerOf returns the current owner's Ethereum address for that specific token.

Q9. Can you modify an NFT's metadata after minting?
A) No, it is permanently fixed B) Yes, by calling setTokenURI (if the contract allows)
C) Only the owner can modify it D) Only within the first 24 hours
Answer: B – If the contract exposes setTokenURI, metadata can be updated; immutability depends on design.

Q10. Why does minting cost gas but viewing is free?
A) Minting creates a new block
B) Minting writes to blockchain state (costs gas); viewing reads existing state (free)
C) The network charges for all operations D) Only the first mint costs gas
Answer: B – Writing to blockchain requires validators to process and store changes; reading is local.

Quiz Questions (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image
C) hash, block, nonce D) from, to, value

Quiz Questions (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image
C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer
B) ERC-1155 supports both fungible and non-fungible tokens in one contract
C) ERC-721 is faster D) ERC-1155 only works on Layer 2

Quiz Questions (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image
C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer
B) ERC-1155 supports both fungible and non-fungible tokens in one contract
C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed
B) The token still exists on-chain but metadata may be inaccessible
C) The owner loses their token D) The blockchain automatically backs up the metadata

Quiz Questions (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image
C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer
B) ERC-1155 supports both fungible and non-fungible tokens in one contract
C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed
B) The token still exists on-chain but metadata may be inaccessible
C) The owner loses their token D) The blockchain automatically backs up the metadata
Answer: B – The on-chain token persists; only the off-chain metadata becomes unreachable.

Q14. What is the purpose of the token ID in an ERC-721 contract?
A) To set the token's price B) To uniquely identify each token in the collection
C) To determine gas costs D) To link to the owner's profile

Quiz Questions (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image
C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer
B) ERC-1155 supports both fungible and non-fungible tokens in one contract
C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed
B) The token still exists on-chain but metadata may be inaccessible
C) The owner loses their token D) The blockchain automatically backs up the metadata
Answer: B – The on-chain token persists; only the off-chain metadata becomes unreachable.

Q14. What is the purpose of the token ID in an ERC-721 contract?
A) To set the token's price B) To uniquely identify each token in the collection
C) To determine gas costs D) To link to the owner's profile
Answer: B – Each token ID is unique within the contract, enabling individual ownership tracking.

Q15. Why use OpenZeppelin instead of writing ERC-721 from scratch?
A) OpenZeppelin is free B) OpenZeppelin contracts are audited and battle-tested
C) OpenZeppelin is faster D) The Ethereum Foundation requires it

Quiz Questions (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image
C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer
B) ERC-1155 supports both fungible and non-fungible tokens in one contract
C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed
B) The token still exists on-chain but metadata may be inaccessible
C) The owner loses their token D) The blockchain automatically backs up the metadata
Answer: B – The on-chain token persists; only the off-chain metadata becomes unreachable.

Q14. What is the purpose of the token ID in an ERC-721 contract?
A) To set the token's price B) To uniquely identify each token in the collection
C) To determine gas costs D) To link to the owner's profile
Answer: B – Each token ID is unique within the contract, enabling individual ownership tracking.

Q15. Why use OpenZeppelin instead of writing ERC-721 from scratch?
A) OpenZeppelin is free B) OpenZeppelin contracts are audited and battle-tested
C) OpenZeppelin is faster D) The Ethereum Foundation requires it
Answer: B – Audited code reduces security risks; writing standards from scratch invites bugs.

Quiz Questions (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs
C) A metadata format D) A bridge protocol

Quiz Questions (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs
C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI
C) Only if using ERC-1155 D) Only the first 100 tokens

Quiz Questions (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs
C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI
C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer
B) Ensuring a node continues to store and serve specific content
C) Creating a backup on a centralized server D) Encrypting the file for privacy

Quiz Questions (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs
C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI
C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer
B) Ensuring a node continues to store and serve specific content
C) Creating a backup on a centralized server D) Encrypting the file for privacy
Answer: B – Pinning tells an IPFS node to keep content available; unpinned content may be garbage-collected.

Q19. Why is Etherscan useful for NFT verification?
A) It mints NFTs automatically
B) It shows all on-chain transactions, ownership, and contract code transparently
C) It stores NFT images D) It sets NFT prices

Quiz Questions (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs
C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI
C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer
B) Ensuring a node continues to store and serve specific content
C) Creating a backup on a centralized server D) Encrypting the file for privacy
Answer: B – Pinning tells an IPFS node to keep content available; unpinned content may be garbage-collected.

Q19. Why is Etherscan useful for NFT verification?
A) It mints NFTs automatically
B) It shows all on-chain transactions, ownership, and contract code transparently
C) It stores NFT images D) It sets NFT prices
Answer: B – Etherscan provides transparent, public access to all on-chain data and transaction history.

Q20. What is the fundamental difference between owning an NFT and owning the image file?
A) There is no difference
B) The NFT is a blockchain-verifiable ownership record; the image is a digital file anyone can copy
C) The image is more valuable D) NFTs automatically include copyright

(c) Joerg Osterrieder 2026

Quiz Questions (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs
C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI
C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer
B) Ensuring a node continues to store and serve specific content
C) Creating a backup on a centralized server D) Encrypting the file for privacy
Answer: B – Pinning tells an IPFS node to keep content available; unpinned content may be garbage-collected.

Q19. Why is Etherscan useful for NFT verification?
A) It mints NFTs automatically
B) It shows all on-chain transactions, ownership, and contract code transparently
C) It stores NFT images D) It sets NFT prices
Answer: B – Etherscan provides transparent, public access to all on-chain data and transaction history.

Q20. What is the fundamental difference between owning an NFT and owning the image file?
A) There is no difference
B) The NFT is a blockchain-verifiable ownership record; the image is a digital file anyone can copy
C) The image is more valuable D) NFTs automatically include copyright
Answer: B – NFT ownership is cryptographic proof on-chain; the underlying file can still be freely copied.

Quiz: Mint Your First NFT

Instructions: 20 multiple choice questions — Select the best answer — Answers revealed after each question

Quiz (1–5)

Q1. What does “non-fungible” mean?
A) Divisible into smaller units B) Identical and interchangeable C) Each item is unique and not interchangeable
D) Cannot be transferred

Quiz (1–5)

Q1. What does “non-fungible” mean?
A) Divisible into smaller units B) Identical and interchangeable C) Each item is unique and not interchangeable
D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777

Quiz (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address C) A URI pointing to the token's metadata D) The token's creation date

Quiz (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address C) A URI pointing to the token's metadata D) The token's creation date
Answer: C – tokenURI returns the link to off-chain metadata (name, description, image).

Q4. Where is NFT metadata typically stored?
A) On the Ethereum blockchain B) In the smart contract's storage C) Off-chain (IPFS or web server) D) In the user's wallet

Quiz (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address C) A URI pointing to the token's metadata D) The token's creation date
Answer: C – tokenURI returns the link to off-chain metadata (name, description, image).

Q4. Where is NFT metadata typically stored?
A) On the Ethereum blockchain B) In the smart contract's storage C) Off-chain (IPFS or web server) D) In the user's wallet
Answer: C – Storing images on-chain would cost thousands in gas; metadata lives off-chain.

Q5. What does `_safeMint` do?
A) Burns a token B) Transfers a token C) Creates a new token and assigns it to an owner D) Updates the token's metadata

Quiz (1–5)

Q1. What does "non-fungible" mean?
A) Divisible into smaller units B) Identical and interchangeable C) Each item is unique and not interchangeable D) Cannot be transferred
Answer: C – Non-fungible means each token is distinct and cannot be swapped 1:1 for another.

Q2. What standard defines NFTs on Ethereum?
A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-777
Answer: B – ERC-721 is the standard for non-fungible tokens; ERC-20 is for fungible tokens.

Q3. What does the tokenURI function return?
A) The token's price B) The owner's address C) A URI pointing to the token's metadata D) The token's creation date
Answer: C – tokenURI returns the link to off-chain metadata (name, description, image).

Q4. Where is NFT metadata typically stored?
A) On the Ethereum blockchain B) In the smart contract's storage C) Off-chain (IPFS or web server) D) In the user's wallet
Answer: C – Storing images on-chain would cost thousands in gas; metadata lives off-chain.

Q5. What does `_safeMint` do?
A) Burns a token B) Transfers a token C) Creates a new token and assigns it to an owner D) Updates the token's metadata
Answer: C – _safeMint creates a new token and assigns ownership to the specified address.

Quiz (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address C) Using an IP address for each file D) Using a database ID

Quiz (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable C) ERC721URIStorage D) ERC721Pausable

Quiz (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does `ownerOf(tokenId)` return?
A) The token's metadata B) The token's creation date C) The address that owns the token D) The token's transfer history

Quiz (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does `ownerOf(tokenId)` return?
A) The token's metadata B) The token's creation date C) The address that owns the token D) The token's transfer history
Answer: C – ownerOf returns the current owner's Ethereum address for that specific token.

Q9. Can you modify an NFT's metadata after minting?
A) No, it is permanently fixed B) Yes, by calling setTokenURI (if the contract allows) C) Only the owner can modify it D) Only within the first 24 hours

Quiz (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does `ownerOf(tokenId)` return?
A) The token's metadata B) The token's creation date C) The address that owns the token D) The token's transfer history
Answer: C – ownerOf returns the current owner's Ethereum address for that specific token.

Q9. Can you modify an NFT's metadata after minting?
A) No, it is permanently fixed B) Yes, by calling setTokenURI (if the contract allows) C) Only the owner can modify it D) Only within the first 24 hours
Answer: B – If the contract exposes setTokenURI, metadata can be updated; immutability depends on design.

Q10. Why does minting cost gas but viewing is free?
A) Minting creates a new block B) Minting writes to blockchain state (costs gas); viewing reads existing state (free)
C) The network charges for all operations D) Only the first mint costs gas

Quiz (6–10)

Q6. What is IPFS content addressing?
A) Using a domain name to locate files B) Using the content's hash as its address C) Using an IP address for each file D) Using a database ID
Answer: B – IPFS uses cryptographic hashes of content as addresses, ensuring immutability.

Q7. Which OpenZeppelin extension stores per-token metadata URIs?
A) ERC721Burnable B) ERC721Enumerable C) ERC721URIStorage D) ERC721Pausable
Answer: C – ERC721URIStorage adds a mapping from token ID to metadata URI string.

Q8. What does `ownerOf(tokenId)` return?
A) The token's metadata B) The token's creation date C) The address that owns the token D) The token's transfer history
Answer: C – ownerOf returns the current owner's Ethereum address for that specific token.

Q9. Can you modify an NFT's metadata after minting?
A) No, it is permanently fixed B) Yes, by calling setTokenURI (if the contract allows) C) Only the owner can modify it D) Only within the first 24 hours
Answer: B – If the contract exposes setTokenURI, metadata can be updated; immutability depends on design.

Q10. Why does minting cost gas but viewing is free?
A) Minting creates a new block B) Minting writes to blockchain state (costs gas); viewing reads existing state (free)
C) The network charges for all operations D) Only the first mint costs gas
Answer: B – Writing to blockchain requires validators to process and store changes; reading is local.

Quiz (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image C) hash, block, nonce D) from, to, value

Quiz (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer B) ERC-1155 supports both fungible and non-fungible tokens in one contract C) ERC-721 is faster D) ERC-1155 only works on Layer 2

(c) Joerg Osterrieder 2026

Quiz (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer B) ERC-1155 supports both fungible and non-fungible tokens in one contract C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed B) The token still exists on-chain but metadata may be inaccessible C) The owner loses their token D) The blockchain automatically backs up the metadata

(c) Joerg Osterrieder 2026

Quiz (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer B) ERC-1155 supports both fungible and non-fungible tokens in one contract C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed B) The token still exists on-chain but metadata may be inaccessible C) The owner loses their token D) The blockchain automatically backs up the metadata
Answer: B – The on-chain token persists; only the off-chain metadata becomes unreachable.

Q14. What is the purpose of the token ID in an ERC-721 contract?
A) To set the token's price B) To uniquely identify each token in the collection C) To determine gas costs D) To link to the owner's profile

Quiz (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer B) ERC-1155 supports both fungible and non-fungible tokens in one contract C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed B) The token still exists on-chain but metadata may be inaccessible C) The owner loses their token D) The blockchain automatically backs up the metadata
Answer: B – The on-chain token persists; only the off-chain metadata becomes unreachable.

Q14. What is the purpose of the token ID in an ERC-721 contract?
A) To set the token's price B) To uniquely identify each token in the collection C) To determine gas costs D) To link to the owner's profile
Answer: B – Each token ID is unique within the contract, enabling individual ownership tracking.

Q15. Why use OpenZeppelin instead of writing ERC-721 from scratch?
A) OpenZeppelin is free B) OpenZeppelin contracts are audited and battle-tested C) OpenZeppelin is faster D) The Ethereum Foundation requires it

Quiz (11–15)

Q11. Which JSON fields are standard in NFT metadata?
A) price, seller, buyer B) name, description, image C) hash, block, nonce D) from, to, value
Answer: B – The OpenSea metadata standard requires name, description, and image fields.

Q12. What is the key difference between ERC-721 and ERC-1155?
A) ERC-1155 is newer B) ERC-1155 supports both fungible and non-fungible tokens in one contract C) ERC-721 is faster D) ERC-1155 only works on Layer 2
Answer: B – ERC-1155 is a multi-token standard supporting fungible, non-fungible, and semi-fungible tokens.

Q13. What happens if the server hosting NFT metadata goes offline?
A) The NFT is destroyed B) The token still exists on-chain but metadata may be inaccessible C) The owner loses their token D) The blockchain automatically backs up the metadata
Answer: B – The on-chain token persists; only the off-chain metadata becomes unreachable.

Q14. What is the purpose of the token ID in an ERC-721 contract?
A) To set the token's price B) To uniquely identify each token in the collection C) To determine gas costs D) To link to the owner's profile
Answer: B – Each token ID is unique within the contract, enabling individual ownership tracking.

Q15. Why use OpenZeppelin instead of writing ERC-721 from scratch?
A) OpenZeppelin is free B) OpenZeppelin contracts are audited and battle-tested C) OpenZeppelin is faster D) The Ethereum Foundation requires it
Answer: B – Audited code reduces security risks; writing standards from scratch invites bugs.

Quiz (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs C) A metadata format D) A bridge protocol

Quiz (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI C) Only if using ERC-1155 D) Only the first 100 tokens

Quiz (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer B) Ensuring a node continues to store and serve specific content C) Creating a backup on a centralized server D) Encrypting the file for privacy

Quiz (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer B) Ensuring a node continues to store and serve specific content C) Creating a backup on a centralized server D) Encrypting the file for privacy
Answer: B – Pinning tells an IPFS node to keep content available; unpinned content may be garbage-collected.

Q19. Why is Etherscan useful for NFT verification?
A) It mints NFTs automatically B) It shows all on-chain transactions, ownership, and contract code transparently
C) It stores NFT images D) It sets NFT prices

Quiz (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer B) Ensuring a node continues to store and serve specific content C) Creating a backup on a centralized server D) Encrypting the file for privacy
Answer: B – Pinning tells an IPFS node to keep content available; unpinned content may be garbage-collected.

Q19. Why is Etherscan useful for NFT verification?
A) It mints NFTs automatically B) It shows all on-chain transactions, ownership, and contract code transparently C) It stores NFT images D) It sets NFT prices
Answer: B – Etherscan provides transparent, public access to all on-chain data and transaction history.

Q20. What is the fundamental difference between owning an NFT and owning the image file?
A) There is no difference B) The NFT is a blockchain-verifiable ownership record; the image is a digital file anyone can copy C) The image is more valuable D) NFTs automatically include copyright

Quiz (16–20)

Q16. What does ERC-2981 define?
A) A new token standard B) A royalty payment standard for NFTs C) A metadata format D) A bridge protocol
Answer: B – ERC-2981 standardizes on-chain royalty information so marketplaces can pay creators.

Q17. Can two NFTs in the same collection have different metadata?
A) No, all tokens share one metadata B) Yes, each token has its own tokenURI C) Only if using ERC-1155 D) Only the first 100 tokens
Answer: B – ERC721URIStorage maps each token ID to its own unique metadata URI.

Q18. What is "pinning" in the IPFS context?
A) Locking a token to prevent transfer B) Ensuring a node continues to store and serve specific content C) Creating a backup on a centralized server D) Encrypting the file for privacy
Answer: B – Pinning tells an IPFS node to keep content available; unpinned content may be garbage-collected.

Q19. Why is Etherscan useful for NFT verification?
A) It mints NFTs automatically B) It shows all on-chain transactions, ownership, and contract code transparently C) It stores NFT images D) It sets NFT prices
Answer: B – Etherscan provides transparent, public access to all on-chain data and transaction history.

Q20. What is the fundamental difference between owning an NFT and owning the image file?
A) There is no difference B) The NFT is a blockchain-verifiable ownership record; the image is a digital file anyone can copy C) The image is more valuable D) NFTs automatically include copyright
Answer: B – NFT ownership is cryptographic proof on-chain; the underlying file can still be freely copied.