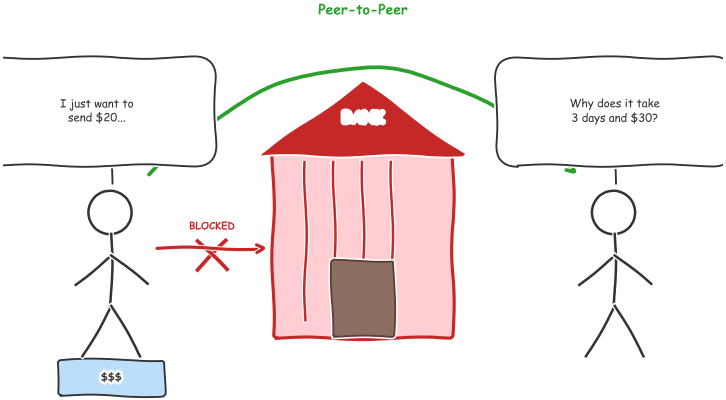
L01: Introduction to Blockchain – Technical Deep Dive

BSc Blockchain Course

Digital Finance

What If You Could Send Money Like Email?



What if we could skip the middleman entirely?

Imagine clicking "send" on a payment the way you send a message – no bank, no three-day wait, no hidden fees. That is the promise

Learning Objectives

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

1. **Describe** blockchain's core architecture and distinguish it from traditional databases. *[Understand]*
2. **Explain** how transactions are created, validated, and confirmed on a blockchain. *[Understand]*
3. **Calculate** basic blockchain metrics (confirmation time, hash rate, block reward). *[Apply]*
4. **Compare** centralized, distributed, and decentralized systems on trust, throughput, and resilience. *[Analyze]*
5. **Evaluate** whether a proposed use case genuinely requires blockchain technology. *[Evaluate]*

Bloom's levels covered: Understand, Apply, Analyze, Evaluate

These objectives map directly to quiz and exercise assessments.

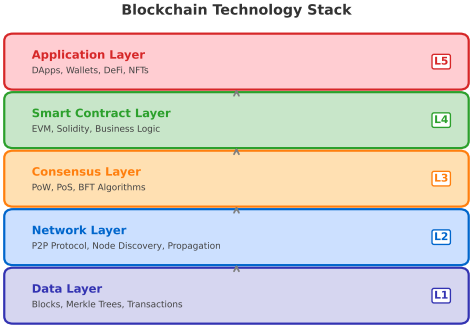
Where This Lesson Fits

This is Lesson 1 of a 12-lesson course that builds from the foundations of blockchain up through Bitcoin, Ethereum, DeFi, and tokenomics.

This lesson starts at: zero assumptions – we define every term from scratch.

By the end: you will know what a blockchain is, how transactions flow through one, and when it makes sense to use one.

Layer focus: Today we cover Layer 0 (network) and Layer 1 (consensus + data). Later lessons add smart contracts, tokens, and applications.



- **What you see:** A stack diagram showing blockchain layers from hardware up to applications.
- **Key pattern:** Each layer depends on the ones below it.
- **Takeaway:** Understanding Layer 0 and 1 is prerequisite to everything above.

Lessons 2–4 cover cryptography and consensus; Lessons 5–8 cover Ethereum and smart contracts.

Think About the Last Time You Sent Money Internationally

Take a moment and recall the last time you – or someone you know – needed to send money across borders.

Consider these questions:

- How many **days** did the transfer take?
- What **fees** were charged – and by how many intermediaries?
- Did you know the **exchange rate** before you hit "send," or did the final amount come as a surprise?
- What would have happened if the receiving bank had been **closed for a holiday**?

The average international wire transfer costs 6.2% in fees and takes 2–5 business days. A blockchain transfer can settle in under a minute for a fraction of a cent.

The question is not whether the technology works. The question is: *why do we still tolerate the old system?*

World Bank Remittance Prices Worldwide, Q4 2024: global average cost 6.2% for sending $200.

What Is a Blockchain? A Definition

Definition: Blockchain

A **blockchain** is an append-only (add-only, never delete) digital ledger (record book) that stores data in **blocks** linked together by **cryptographic hashes** (unique digital fingerprints). It is replicated across a **peer-to-peer network** (computers talking directly to each other) and uses a **consensus mechanism** (a voting rule) so all participants agree on which data is valid.

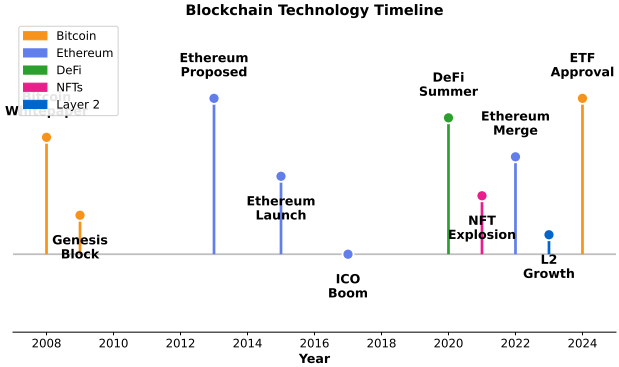
Four core properties:

1. **Decentralization:** No single company or government runs it – thousands of independent computers share the work.
2. **Immutability:** Once data is written, it cannot be changed or erased without redoing enormous amounts of computation.
3. **Transparency:** Every transaction is publicly visible to anyone who wants to check.
4. **Cryptographic security:** Mathematical puzzles protect the data instead of passwords or firewalls.

Blockchain combines ideas from 1991 (timestamping), 1997 (proof of work), and 2008 (Nakamoto consensus).

From Bitcoin to ETFs: Sixteen Years of Blockchain

- **2008–2015: Foundation era** – Bitcoin whitepaper, genesis block, and Ethereum launch established the core protocols still dominant today
- **2017–2021: Expansion era** – ICO boom, DeFi Summer, and NFT explosion brought speculative capital and mass awareness
- **2022–2024: Maturation era** – Ethereum Merge, Layer-2 scaling, and spot Bitcoin ETF approval marked institutional acceptance



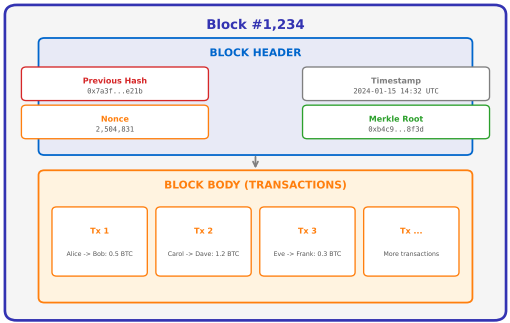
Each milestone built on the last: without Bitcoin's proof of concept, Ethereum's smart contracts and DeFi would not exist.

The Anatomy of a Block

Every block in the chain contains the same basic components. Think of each block as a sealed envelope that references the envelope before it.

Inside a single block:

- **Block header:** metadata including timestamp, difficulty target, and nonce (a number miners adjust)
- **Previous block hash:** the digital fingerprint of the block before this one – this is the "chain" in blockchain
- **Merkle root:** a single hash that summarizes all transactions in the block
- **Transaction list:** the actual transfer records



- **What you see:** A diagram of a single block showing header fields and transaction data.
- **Key pattern:** The previous-block hash creates a backward-pointing chain – change one block and every hash after it breaks.
- **Takeaway:** This structure is what makes blockchain tamper-evident, not tamper-proof.

Centralized vs Distributed vs Decentralized

These three network architectures differ in who controls the data and what happens when something fails.

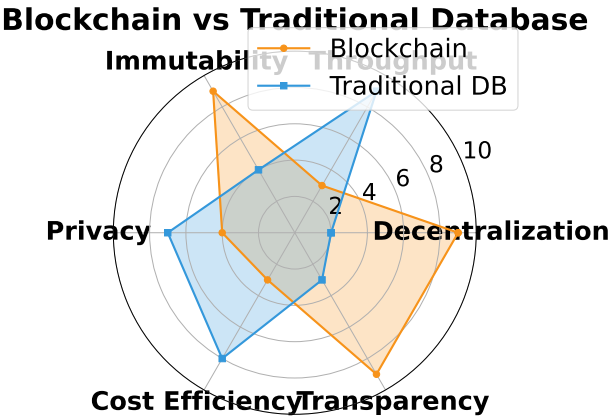
Dimension	Centralized	Distributed	Decentralized
Control	Single authority	Multiple coordinated	No single authority
Trust model	Trust the operator	Trust the consortium	Trust the protocol
Throughput	Very high (100K+ TPS)	High (10K+ TPS)	Low–moderate (7–65 TPS)
Failure mode	Single point of failure	Partial failure	Highly fault-tolerant
Examples	Visa, Google, a bank	AWS multi-region	Bitcoin, Ethereum

Key insight: "Distributed" and "decentralized" are **not the same thing.** A distributed system can still have a single owner (like Google's servers spread across data centers). A decentralized system has **no owner** – the rules are enforced by code, not by a company.

TPS = Transactions Per Second. Bitcoin averages 7 TPS; Visa peaks at 65,000 TPS.

Choosing the Right Tool: Blockchain vs Traditional Database

- **Blockchain excels** at decentralization, immutability, and transparency – scoring 9/10 on each – but pays a steep price in throughput (3/10) and cost efficiency (3/10)
- **Traditional databases** dominate on throughput (9/10) and cost efficiency (8/10) – the right choice whenever a trusted operator exists
- **The decision** turns on one question: do multiple distrusting parties need to write shared data? If yes, blockchain wins; if no, a database is faster and cheaper



Radar chart: each axis scored 1–10. The larger the shaded area for a dimension, the stronger that system is in that regard.

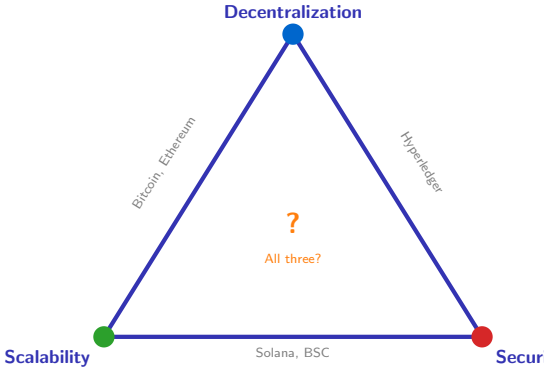
The Blockchain Trilemma

In 2017, Ethereum co-founder Vitalik Buterin observed that blockchains face a fundamental trade-off among three desirable properties:

1. **Decentralization:** Many independent nodes run the network – no single entity can censor or shut it down.
2. **Security:** The network resists attacks; transactions cannot be reversed once confirmed.
3. **Scalability:** The network processes a high volume of transactions quickly and cheaply.

The claim: You can optimize for any two, but the third will suffer.

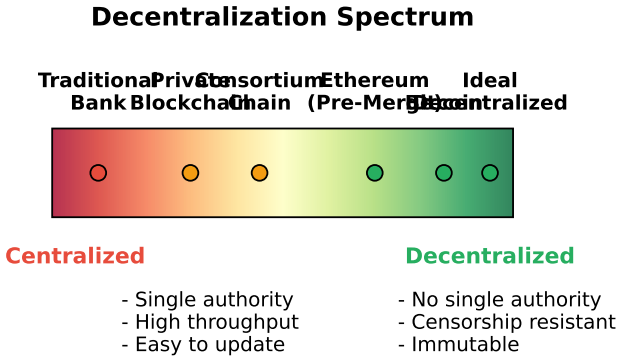
Bitcoin picks decentralization + security (but processes only 7 TPS).
Solana picks security + scalability (but has fewer validators).
No chain has solved all three simultaneously – yet.



The trilemma is a design heuristic, not a proven impossibility theorem. Layer-2 solutions attempt to circumvent it.

The Decentralization Spectrum: From Bank to Bitcoin

- **Not binary** – systems span a gradient from fully centralized (single authority, high throughput, easy to update) to fully decentralized (no authority, censorship-resistant, immutable)
- **Private and consortium chains** occupy the middle: known participants share governance, gaining some decentralization benefits while keeping higher speed
- **Bitcoin sits near the far end** – the most decentralized production network, with no single entity able to censor or reverse transactions



Hyperledger Fabric (used by IBM and Walmart) is a consortium chain – faster than Bitcoin but governed by a known set of companies.

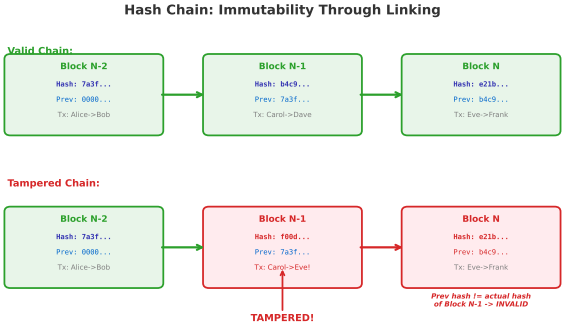
How Hash Chaining Makes Tampering Visible

A **hash function** takes any input (a transaction, a file, a block) and produces a fixed-length "fingerprint." Two critical properties:

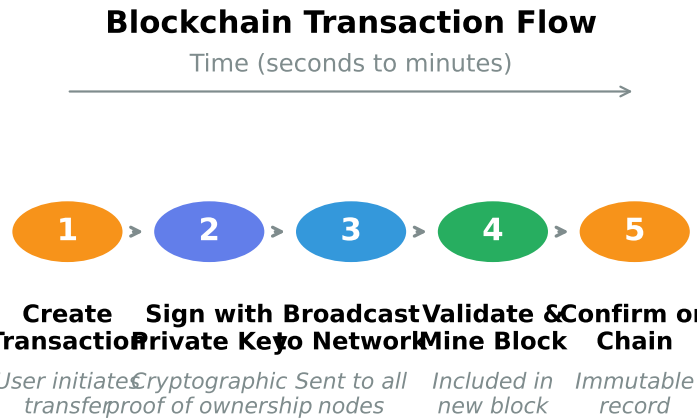
1. **Deterministic:** Same input always gives the same output.
2. **Avalanche effect:** Change one character in the input and the entire output changes unpredictably.

Because each block stores the hash of the *previous* block, altering any historical block would change its hash, which would break the link in the next block, which would break the one after that – a cascade of mismatches all the way to the present.

Result: Tampering is not impossible, but it is **immediately visible** to every node on the network.



- **What you see:** Three blocks linked by hash pointers, with the middle block tampered.
- **Key pattern:** The tampered block's hash no longer matches what Block 3 expects – the chain is broken.
- **Takeaway:** Hash chaining turns a data structure into a tamper-detection mechanism.



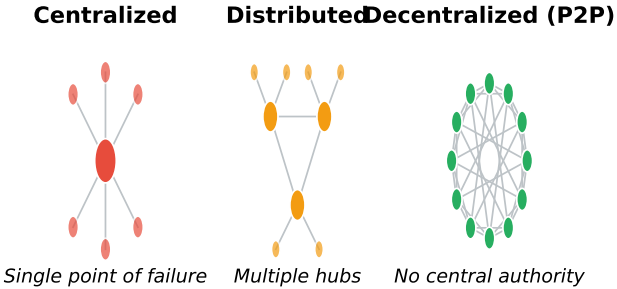
Five stages of a blockchain transaction:

1. **Create:** The sender specifies the recipient address and the amount to transfer.
2. **Sign:** The sender's private key (a secret number only the owner knows) generates a digital signature proving authorization.
3. **Broadcast:** The signed transaction is sent to nearby nodes, which relay it across the entire network.

Why Network Topology Determines Security

- **Centralized** networks route all traffic through one hub – efficient, but a single point of failure can bring down the entire system
- **Distributed** networks use multiple hubs connected to each other – more resilient, but each hub still controls its own cluster of nodes
- **Decentralized (P2P)** networks have no hubs at all – every node connects directly to peers, so there is no single target for an attacker to disable

Network Topology Comparison



Bitcoin's P2P network has over 50,000 reachable nodes worldwide – no single shutdown can stop it.

Confirmation Time: A Worked Example

Problem: How long must you wait before a Bitcoin or Ethereum transaction is considered irreversible (final)?

Bitcoin:

- Average block time = 10 minutes
- Industry standard = 6 confirmations (six blocks built on top of yours)

Confirmation Time: A Worked Example

Problem: How long must you wait before a Bitcoin or Ethereum transaction is considered irreversible (final)?

Bitcoin:

- Average block time = 10 minutes
- Industry standard = 6 confirmations (six blocks built on top of yours)

$$\underbrace{6 \text{ confirmations}}_{\text{security threshold}} \times \underbrace{10 \text{ min/block}}_{\text{average block time}} = \mathbf{60 \text{ minutes}}$$

Confirmation Time: A Worked Example

Problem: How long must you wait before a Bitcoin or Ethereum transaction is considered irreversible (final)?

Bitcoin:

- Average block time = 10 minutes
- Industry standard = 6 confirmations (six blocks built on top of yours)

$$\underbrace{6 \text{ confirmations}}_{\text{security threshold}} \times \underbrace{10 \text{ min/block}}_{\text{average block time}} = \mathbf{60 \text{ minutes}}$$

Ethereum (post-Merge):

- Average block time = 12 seconds
- Finality requires 2 epochs (an epoch = 32 slots of 12 seconds each)

Confirmation Time: A Worked Example

Problem: How long must you wait before a Bitcoin or Ethereum transaction is considered irreversible (final)?

Bitcoin:

- Average block time = 10 minutes
- Industry standard = 6 confirmations (six blocks built on top of yours)

$$\underbrace{6 \text{ confirmations}}_{\text{security threshold}} \times \underbrace{10 \text{ min/block}}_{\text{average block time}} = \mathbf{60 \text{ minutes}}$$

Ethereum (post-Merge):

- Average block time = 12 seconds
- Finality requires 2 epochs (an epoch = 32 slots of 12 seconds each)

$$\underbrace{2 \text{ epochs}}_{\text{finality rule}} \times \underbrace{32 \text{ slots}}_{\text{per epoch}} \times \underbrace{12 \text{ sec/slot}}_{\text{slot duration}} = 768 \text{ sec} \approx \mathbf{12.8 \text{ minutes}}$$

Confirmation Time: A Worked Example

Problem: How long must you wait before a Bitcoin or Ethereum transaction is considered irreversible (final)?

Bitcoin:

- Average block time = 10 minutes
- Industry standard = 6 confirmations (six blocks built on top of yours)

$$\underbrace{6 \text{ confirmations}}_{\text{security threshold}} \times \underbrace{10 \text{ min/block}}_{\text{average block time}} = \mathbf{60 \text{ minutes}}$$

Ethereum (post-Merge):

- Average block time = 12 seconds
- Finality requires 2 epochs (an epoch = 32 slots of 12 seconds each)

$$\underbrace{2 \text{ epochs}}_{\text{finality rule}} \times \underbrace{32 \text{ slots}}_{\text{per epoch}} \times \underbrace{12 \text{ sec/slot}}_{\text{slot duration}} = 768 \text{ sec} \approx \mathbf{12.8 \text{ minutes}}$$

Takeaway: Ethereum is roughly 5 times faster to finality than Bitcoin. For a coffee purchase, even 12.8 minutes is too slow – this is why Layer-2 solutions and payment channels exist.

Visa authorizes in 1–2 seconds. Speed vs. security is the fundamental trade-off.

Proof of Work vs Proof of Stake

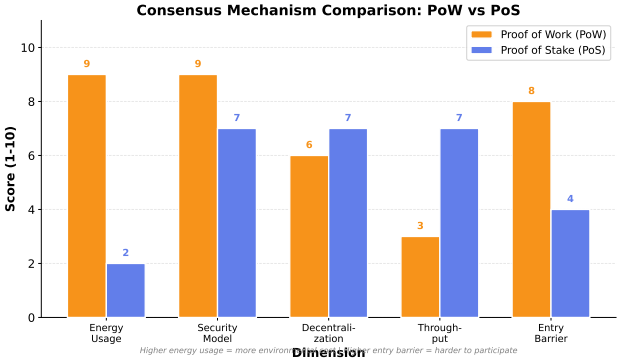
A **consensus mechanism** is the rule a blockchain uses to decide which computer gets to add the next block. The two dominant approaches:

Proof of Work (PoW):

- Miners compete to solve a mathematical puzzle
- Winner spends real electricity
- Attacking requires 51% of global computing power
- Used by: Bitcoin, Litecoin

Proof of Stake (PoS):

- Validators lock up ("stake") their own coins as collateral
- Protocol randomly selects who proposes the next block
- Attacking requires owning 33%+ of all staked coins
- Used by: Ethereum (since Sept 2022), Solana, Cardano



- **What you see:** A side-by-side comparison of PoW and PoS across energy, speed, and barrier to entry.
- **Key pattern:** PoS wins on energy and speed; PoW has a longer track record.
- **Takeaway:** The industry is moving toward PoS, but PoW remains Bitcoin's core security model.

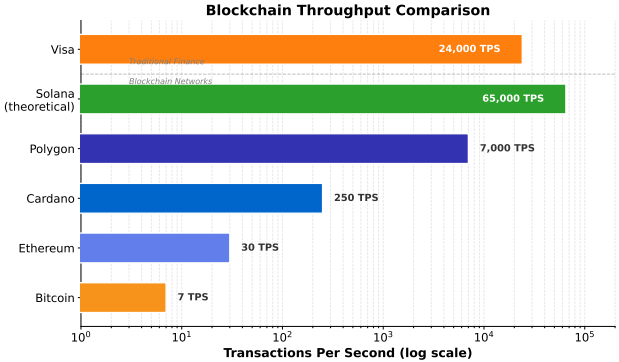
How Fast Can a Blockchain Process Transactions?

Throughput is measured in TPS (Transactions Per Second) – how many transfers the network can handle simultaneously.

The gap between blockchain and traditional systems is enormous:

- **Visa:** up to 65,000 TPS (typically 1,700 average)
- **Bitcoin:** approximately 7 TPS
- **Ethereum (L1):** approximately 15–30 TPS
- **Solana:** approximately 700–4,000 TPS

Why so slow? Every node must independently verify every transaction. More nodes = more security but less speed. This is the scalability leg of the trilemma in action.



- **What you see:** A bar chart comparing TPS across payment networks and blockchains.
- **Key pattern:** Traditional networks handle orders of magnitude more transactions than base-layer blockchains.
- **Takeaway:** Layer-2 solutions (Lightning, rollups) aim to bridge this gap without sacrificing security.

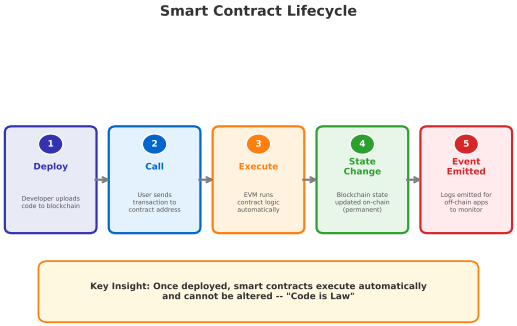
Smart Contracts: Code That Enforces Itself

A **smart contract** is a program stored on a blockchain that automatically executes when predetermined conditions are met. Think of it as a vending machine: insert the right coin, and the product comes out – no shopkeeper required.

Lifecycle of a smart contract:

1. **Deploy:** A developer writes code and uploads it to the blockchain. It gets its own address.
2. **Call:** A user sends a transaction to that address, triggering a function.
3. **Execute:** Every validator runs the code and verifies the result matches.
4. **State change:** The blockchain updates balances, ownership, or other data according to the code's logic.

Key property: Once deployed, the code cannot be changed by anyone – not even the developer. "Code is law."



- **What you see:** A flow diagram showing the four stages: Deploy, Call, Execute, State Change.
- **Key pattern:** Execution is deterministic – every node produces the same result.
- **Takeaway:** Smart contracts eliminate the need for a trusted intermediary to enforce agreements.

Block Reward and Mining Economics

Problem: Who pays the computers that secure the blockchain? And is it profitable?

Revenue side – Block reward:

- Current Bitcoin block reward = 3.125 BTC (halved every 210,000 blocks, roughly every 4 years)
- Assume 1 BTC = $60,000

Block Reward and Mining Economics

Problem: Who pays the computers that secure the blockchain? And is it profitable?

Revenue side – Block reward:

- Current Bitcoin block reward = 3.125 BTC (halved every 210,000 blocks, roughly every 4 years)
- Assume 1 BTC = $60,000

$$\underbrace{3.125\ \text{BTC}}_{\text{block reward}} \times \underbrace{\$60{,}000}_{\text{price per BTC}} = \mathbf{\$187{,}500\ \ \text{per block}}$$

Block Reward and Mining Economics

Problem: Who pays the computers that secure the blockchain? And is it profitable?

Revenue side – Block reward:

- Current Bitcoin block reward = 3.125 BTC (halved every 210,000 blocks, roughly every 4 years)
- Assume 1 BTC = \$60,000

$$\underbrace{3.125 \text{ BTC}}_{\text{block reward}} \times \underbrace{\$60{,}000}_{\text{price per BTC}} = \textbf{\$187,500 per block}$$

Cost side – Electricity:

- A modern mining rig (ASIC) uses about 3,000 watts and costs \$0.05/kWh to run
- Running 24/7 for one month: 3 kW $\times$ 720 hours $\times$ \$0.05 = \$108/month per rig
- Large mining farms operate 10,000+ rigs

Block Reward and Mining Economics

Problem: Who pays the computers that secure the blockchain? And is it profitable?

Revenue side – Block reward:

- Current Bitcoin block reward = 3.125 BTC (halved every 210,000 blocks, roughly every 4 years)
- Assume 1 BTC = \$60,000

$$\underbrace{3.125\ \text{BTC}}_{\text{block reward}} \times \underbrace{\$60{,}000}_{\text{price per BTC}} = \mathbf{\$187{,}500\ \ per\ block}$$

Cost side – Electricity:

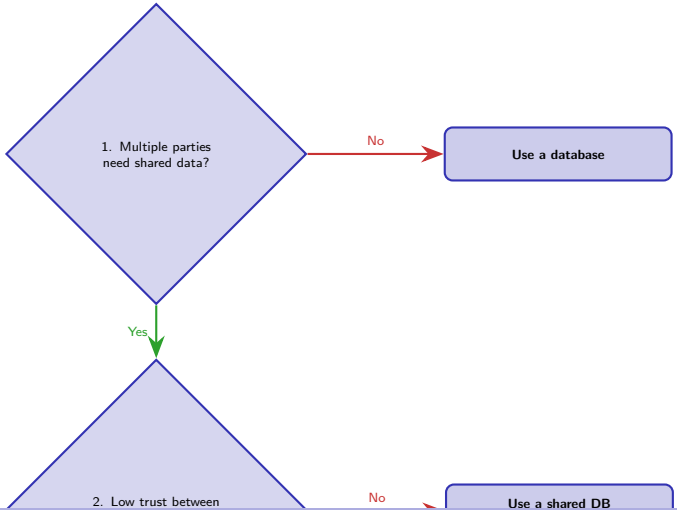
- A modern mining rig (ASIC) uses about 3,000 watts and costs \$0.05/kWh to run
- Running 24/7 for one month: 3 kW $\times$ 720 hours $\times$ \$0.05 = \$108/month per rig
- Large mining farms operate 10,000+ rigs

Takeaway: Mining is profitable only if electricity cost stays below the block reward. When Bitcoin's price drops or the reward halves, inefficient miners shut down – the network self-adjusts through **difficulty adjustment** (the puzzle gets easier when miners leave, harder when they join).

The next halving (reward drops to 1.5625 BTC) is expected around April 2028.

When to Use Blockchain: Decision Framework

Not every problem needs a blockchain. Before proposing one, ask these four questions in order. If any answer is “no,” a traditional database is probably the better choice.



What Happens When Someone Controls 51%?

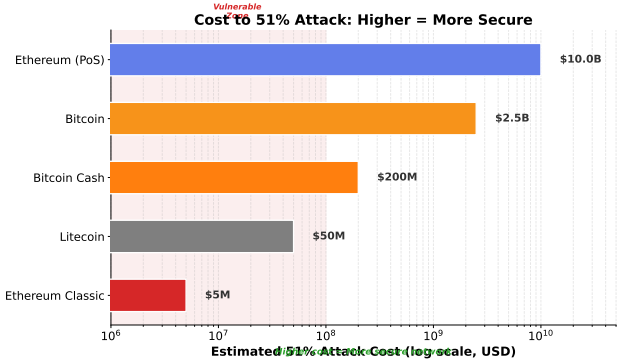
A **51% attack** occurs when a single entity gains majority control of a blockchain's consensus power – hash rate for PoW, or staked coins for PoS.

What the attacker can do:

- **Double-spend:** Send coins to a merchant, then rewrite history to get the coins back
- **Block transactions:** Refuse to include specific people's transactions in new blocks
- **Reorganize the chain:** Replace recent blocks with an alternative version

What the attacker cannot do:

- Steal coins from other wallets (private keys are still needed)
- Change the consensus rules (other nodes would reject invalid blocks)



- **What you see:** Common blockchain attack types ranked by cost and impact.
- **Key pattern:** 51% attacks are extremely expensive on large networks but cheap on small ones.
- **Takeaway:** Network size is the primary defense – Bitcoin has never been successfully 51%-attacked.

The DAO Hack: When Code Is Law Goes Wrong

In June 2016, an attacker exploited a bug in "The DAO" (Decentralized Autonomous Organization), a smart contract on Ethereum that functioned as a venture capital fund controlled by its investors.

What happened:

1. The DAO raised $150 million in Ether from 11,000 investors
2. A recursive call bug (reentrancy attack) let the attacker repeatedly withdraw funds before the balance was updated
3. The attacker drained $60 million – roughly 40% of the fund

The dilemma:

- **"Code is law" camp:** The attacker followed the contract's rules. No theft occurred – the code worked as written.
- **"Intent matters" camp:** The code had a bug. The community should fix it to protect investors.

Resolution: Ethereum performed a **hard fork** (a backward-incompatible rule change) to reverse the theft. Dissenters kept the original chain – that chain is now called **Ethereum Classic (ETC)**.

The DAO hack remains the defining "code is law" vs "social consensus" debate in blockchain history.

Scalability, Energy, and Regulation

Three categories of risk threaten blockchain adoption. Each has a different severity and a different mitigation path.

Challenge	Severity	Current Impact	Mitigation
Scalability	High	Bitcoin: 7 TPS; fees spike during congestion	Layer-2 (Lightning, rollups) Sharding (Ethereum roadmap)
Energy	Medium	Bitcoin mining uses roughly 150 TWh/year (comparable to Poland)	Proof of Stake (Ethereum cut energy 99.95%) Renewable mining incentives
Regulation	High	Varies by jurisdiction; some countries ban crypto, others embrace it	EU MiCA framework (2024); US clarity evolving; Industry self-regulation

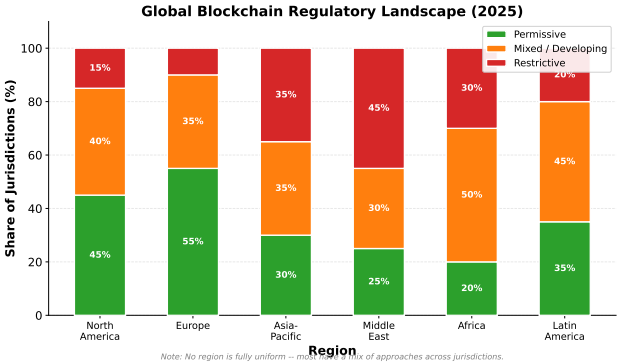
Key insight: Scalability and energy are *engineering* problems with known solution paths. Regulation is a *political* problem with no single answer – it depends on each country's priorities around innovation, consumer protection, and financial stability.

As of 2024, 52 countries have some form of crypto regulation; 10 have outright bans.

The Regulatory Landscape

Blockchain regulation varies dramatically across the world. Three broad approaches have emerged:

1. **Comprehensive frameworks:**
   - EU: MiCA (Markets in Crypto-Assets) – full licensing regime
   - Switzerland: "Crypto Valley" friendly regulation since 2018
2. **Evolving / fragmented:**
   - USA: SEC vs CFTC jurisdictional battles
   - UK: FCA registration required for crypto firms
3. **Restrictive / banned:**
   - China: all crypto trading and mining banned since 2021
   - India: heavy taxation (30% on gains, 1% TDS on transfers)



- **What you see:** A world map or bar chart showing regulatory stance by region.
- **Key pattern:** Regulatory clarity correlates with higher institutional adoption.
- **Takeaway:** Projects must consider regulatory risk as a first-class design constraint, not an afterthought.

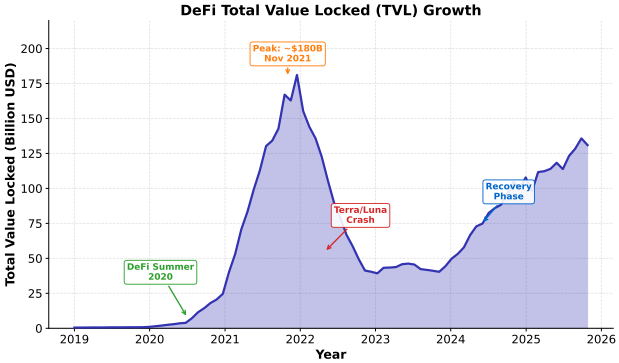
DeFi: Value Running on Smart Contracts

DeFi (Decentralized Finance) recreates traditional financial services – lending, borrowing, trading, insurance – using smart contracts instead of banks.

Key milestones:

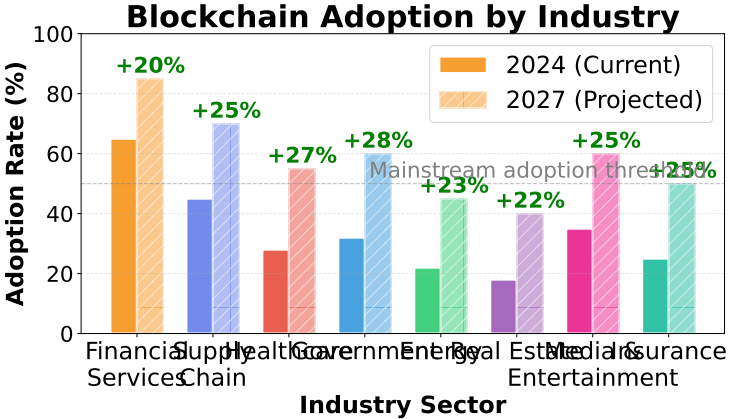
- **2020 ("DeFi Summer"):** Total Value Locked (TVL) grew from $1B to $15B in six months
- **2021 peak:** TVL exceeded $180B
- **2022 crash:** Terra/Luna collapse wiped out $40B
- **2024 recovery:** TVL stabilized around $90–100B

Why it matters: DeFi operates 24/7, requires no identity check, and is accessible to anyone with an internet connection. It is the largest real-world application of smart contracts.



- **What you see:** DeFi TVL over time, showing explosive growth and subsequent corrections.
- **Key pattern:** Boom-bust cycles, but each trough is higher than the previous one.
- **Takeaway:** DeFi is volatile but growing structurally – each cycle brings more resilient protocols.

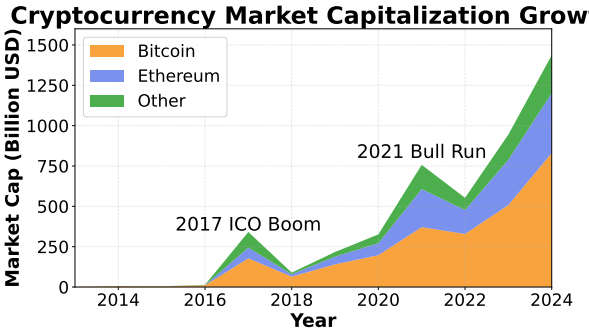
Adoption Across Industries



- **Financial services** lead adoption: cross-border payments, trade finance, asset tokenization (turning real-world assets into blockchain tokens)
- **Supply chain** is the leading enterprise use case: Walmart uses blockchain to trace food origins in seconds instead of days
- **Healthcare** and **real estate** are emerging sectors: medical records, property title registration, credential verification

Crypto Market Capitalization: From Millions to Trillions

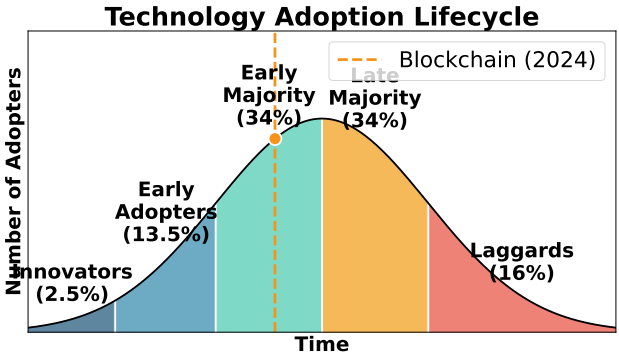
- **Bitcoin dominated early** – near 100% market share in 2013, now roughly 50% as Ethereum and other assets have grown
- **Two boom-bust cycles** stand out: the 2017 ICO boom (total market cap reached $800B) and the 2021 bull run (exceeded $2.5T at peak)
- **Structural growth** persists through crashes – each cycle's trough sits higher than the previous cycle's peak, reflecting genuine adoption gains



Market cap = price × circulating supply. It measures investor sentiment, not economic activity – treat it as a rough adoption proxy.

Where Is Blockchain on the Technology Adoption Curve?

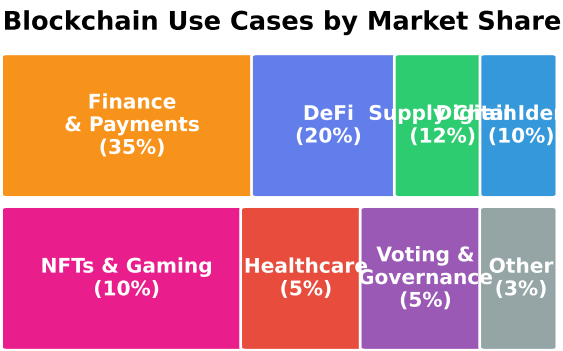
- **Rogers' adoption model** divides technology uptake into five groups: Innovators (2.5%), Early Adopters (13.5%), Early and Late Majority (34% each), and Laggards (16%)
- **Blockchain in 2024** sits at the Early Majority boundary – past the speculative fringe, not yet mainstream – mirroring the internet circa 1998
- **Crossing the chasm** requires solving the key friction points: wallet complexity, transaction fees, and regulatory uncertainty that still deter ordinary users



The internet reached 50% global adoption roughly 25 years after its commercial launch (1993–2018). Blockchain launched commercially in 2009.

Blockchain Use Cases by Market Share

- **Finance and payments** lead with 35% share – cross-border transfers, stablecoins, and asset tokenization are the clearest product-market fits
- **DeFi (20%) and supply chain (12%)** are the next largest sectors, followed by digital identity and NFTs/gaming at 10% each
- **Healthcare and governance** remain small (5% each) – high regulatory barriers slow adoption even where the technology fits well



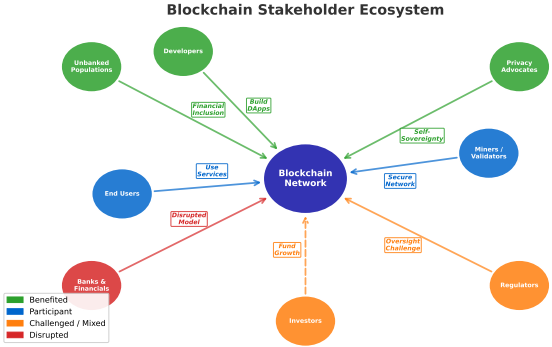
Treemap area is proportional to market share. Finance dominates because the cost of trust failures (fraud, settlement delays) is highest there.

Who Wins and Loses When Trust Moves to Code?

Blockchain does not create value from nothing – it **redistributes** who captures value and who loses it.

Stakeholder	Impact
End users	+ Lower fees, 24/7 access
Developers	+ New business models
Banks	– Disintermediation risk
Regulators	+/– New tools, new risks
Miners/Validators	+ Revenue from securing
Fraudsters	– Transparent audit trail
Unbanked	+ Financial inclusion

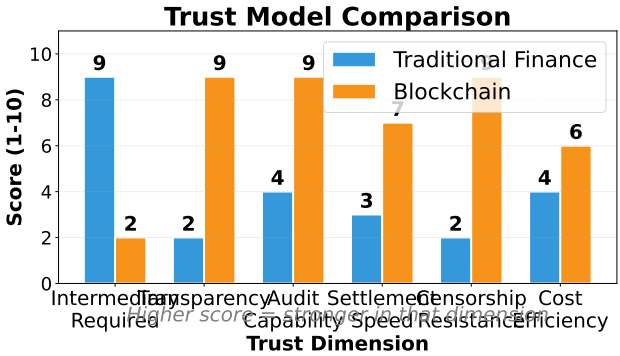
The paradox: Banks are both threatened by and investing in blockchain. JPMorgan runs its own blockchain (Onyx) while warning customers about crypto volatility.



- **What you see:** A stakeholder map plotting impact (positive/negative) against influence (high/low).
- **Key pattern:** High-influence incumbents (banks, regulators) face mixed impact – they shape adoption pace.
- **Takeaway:** Adoption speed depends more on incumbent response than on technology readiness.

Blockchain vs Traditional Finance: A Trust Dimension Comparison

- **Blockchain dominates** on transparency (9/10), audit capability (9/10), and censorship resistance (9/10) – dimensions where traditional finance scores 2–4/10
- **Traditional finance leads** on intermediary reliance (9/10) – this is intentional: banks, clearinghouses, and regulators are the trust anchors in the current system
- **The core trade-off**: blockchain removes intermediaries at the cost of requiring users to manage their own security – a shift of responsibility, not an elimination of risk



Higher score = stronger in that dimension. Note that "Intermediary Required" scoring 9 for traditional finance is descriptive, not a flaw – it reflects the existing system's design.

The Blockchain Generation Gap

Two groups approach blockchain from fundamentally different starting points. Understanding this divide helps explain why adoption is uneven.

Dimension	Digital Natives (Gen Z, Millennials)	Institutions (Banks, Governments)
Default trust	Trust code and community	Trust licenses and regulation
Self-custody	Comfortable holding own keys	Prefer insured custodians
Risk appetite	High – "number go up" culture	Low – fiduciary duty
Entry point	Meme coins, NFTs, gaming	Bitcoin ETFs, tokenized bonds
Regulatory view	Regulation = barrier	Regulation = enabler
Time horizon	Often short-term, speculative	Long-term, strategic

Key insight: Neither group is "right." Digital natives drive innovation and find new use cases. Institutions bring capital, compliance, and scale. The most impactful blockchain projects will bridge both worlds – retail accessibility with institutional robustness.

Example: Bitcoin ETFs (approved January 2024) let institutions invest in Bitcoin through familiar brokerage accounts – no wallets or private keys required. Over $50 billion flowed in within the first year.

A 2024 survey found 55% of 18–25 year-olds owned crypto, compared to 8% of those over 65.

Five Questions for Any Blockchain Project

Use this evaluation framework whenever someone proposes a blockchain solution. If you cannot answer "yes" to at least four of five, the project probably does not need a blockchain.

The Five Questions:

1. **Multiple writers?** Do several independent parties need to write data – not just read it?
2. **Trust deficit?** Is there a genuine lack of trust among these parties that a shared database with access controls cannot solve?
3. **Immutability value?** Would tamper-proof records provide regulatory, legal, or operational value?
4. **Disintermediation benefit?** Would removing a central authority reduce cost, increase speed, or improve access?
5. **Acceptable trade-offs?** Can the project tolerate lower throughput, higher latency, and public transparency (or the cost of privacy solutions)?

Scoring: 5/5 = strong blockchain candidate. 4/5 = possible, investigate further. 3/5 or below = a traditional database is likely sufficient.

This framework is adapted from the Wuest (2018) blockchain decision model used by the World Economic Forum.

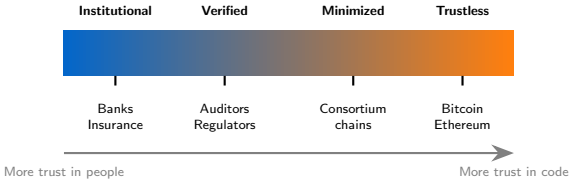
The Trust Spectrum

Trust is not binary – it exists on a spectrum. Different systems occupy different positions, and the "right" position depends on context.

Moving left to right:

- **Full institutional trust:** You trust a bank to hold your money. If something goes wrong, courts and insurance protect you.
- **Verified trust:** You use a third-party auditor or regulator to verify claims. Trust, but verify.
- **Minimized trust:** A consortium blockchain where known participants follow shared rules. Some trust required, but less.
- **Trustless:** A public blockchain where you verify everything yourself. No trust in any single party needed.

"Trustless" does not mean "no trust." It means trust is placed in mathematics and open-source code rather than in people or institutions.



Key insight: The right position on this spectrum depends on your use case. Buying a coffee does not need trustless settlement. Sending $10,000 across borders to a stranger might.

Even "trustless" systems require trust in the protocol developers, hardware manufacturers, and internet infrastructure.

What Comes Next: Cryptographic Foundations

Today you learned *what* blockchain is and *why* it works at a high level. In Lesson 2, we zoom into the *how* – the cryptographic primitives that make all of this possible.

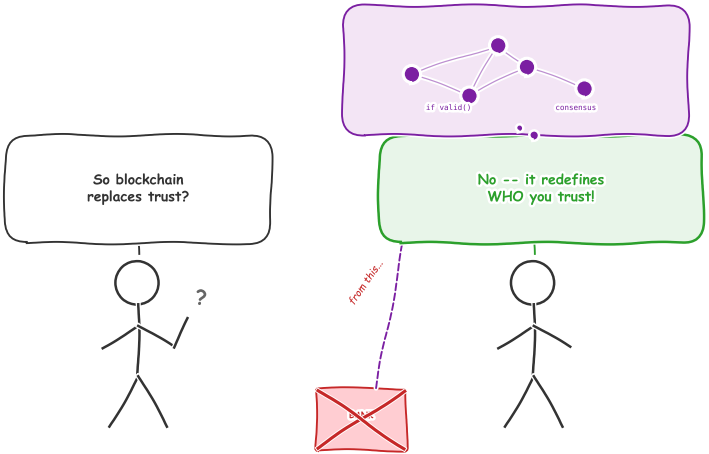
Lesson 2 will cover:

- **Hash functions:** How SHA-256 and Keccak-256 produce the fingerprints that chain blocks together (we introduced these today – next time we go deeper)
- **Public-key cryptography:** How a pair of mathematically linked numbers (public key and private key) enables digital signatures without sharing secrets
- **Merkle trees:** How a single hash can summarize thousands of transactions, enabling efficient verification without downloading the entire blockchain
- **Digital signatures:** The mechanism behind "sign" in our five-stage transaction flow – proving you authorized a transfer without revealing your private key

Preparation: Think about how a lock-and-key system works in the physical world. A public-key system is similar – except anyone can make a lock, but only one person has the key.

Lesson 2 builds directly on today's transaction flow and hash chaining concepts.

One Last Thought...



Trust the code, trust the network, verify for yourself.

Now you understand why "just put it on the blockchain" is not always the answer – and when it genuinely is. The technology is powerful

Key Takeaways

1. **Blockchain defined:** An append-only, cryptographically linked, distributed ledger that replaces trust in institutions with trust in mathematics.
2. **Transaction lifecycle:** Create, Sign, Broadcast, Validate, Confirm – five stages, zero intermediaries.
3. **Consensus trade-offs:** Proof of Work prioritizes security at the cost of energy; Proof of Stake prioritizes efficiency at the cost of wealth concentration risk.
4. **The trilemma:** Decentralization, security, and scalability cannot all be maximized simultaneously – every blockchain makes a trade-off.
5. **Decision framework:** Four "yes" answers (multiple writers, trust deficit, immutability value, disintermediation benefit) before choosing blockchain over a database.
6. **Adoption reality:** Financial services lead, DeFi demonstrates the potential, but scalability, energy, and regulation remain open challenges.

Review question: Name one scenario where a database is better than a blockchain, and explain why using the decision framework.

Summary / Next Lesson Preview

Blockchain is not a single invention but a combination of existing technologies – hashing, digital signatures, peer-to-peer networking, and consensus protocols – arranged in a way that eliminates the need for trusted intermediaries. It excels when multiple distrusting parties need a shared, tamper-evident record. It struggles when speed, privacy, or centralized control is the priority.

Key Vocabulary:

- Blockchain
- Decentralization
- Consensus mechanism
- Proof of Work (PoW)
- Proof of Stake (PoS)
- Hash function
- Immutability
- Smart contract
- DeFi (Decentralized Finance)
- 51% attack

Next lesson: *Cryptographic Foundations* – the math behind the "magic." How do hash functions, digital signatures, and Merkle trees actually secure a blockchain?

Try this before Lesson 2: look up the SHA-256 hash of the word "blockchain" – then change one letter and see how the output changes completely.