

L48: Course Synthesis

Blockchain & Cryptocurrency: The Complete Journey

Prof. Dr. Jörg Osterrieder

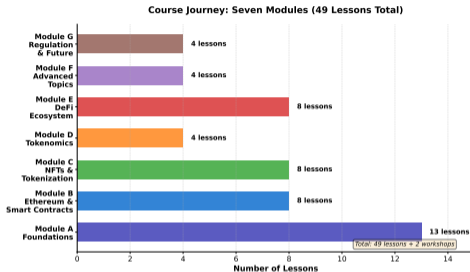
BSc Blockchain, Crypto Economy & NFTs

Spring 2026

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

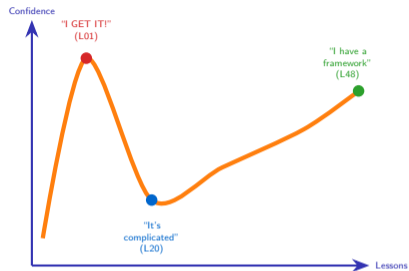
Building on L47: CBDCs and Future Trends



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



The Dunning-Kruger effect in crypto education: true confidence comes from understanding the complexity

The Problem: How do all the pieces fit together?

Part 4/4: Course Synthesis (Integration)

The Challenge

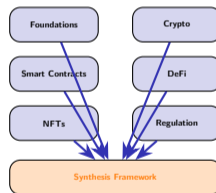
After studying 49 lessons across blockchain, DeFi, NFTs, and regulation, how do we synthesize this knowledge into a coherent framework for evaluating any crypto project or protocol?

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



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

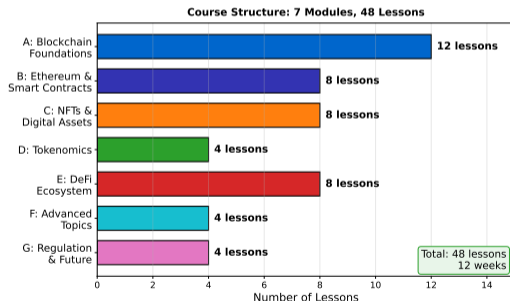
NFT standards, marketplaces, tokenomics, DAOs

Module F: Advanced Topics

Layer 2 scaling, flash loans, security

Module G: Regulation & Future

Global frameworks, CBDCs, 2025+ trends



Course Journey: Seven modules provide a unified framework—from foundational cryptography to advanced DeFi to regulation, all viewed through The Cryptoeconomics Lens

Recall Our Problem

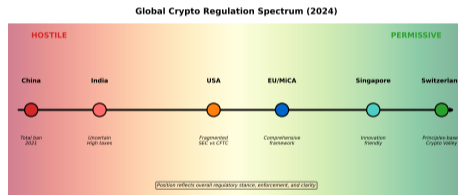
How should governments regulate crypto?

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)

Still to Address

- 2024-2025 milestones (Bitcoin ETFs, MiCA, Dencun upgrade), realistic 2030 scenarios
- Will crypto transform global finance or remain a parallel system?



Pause and reflect: How does what we've learned so far address "How should governments regulate crypto?"

Incentive Structure

- Managing systemic and idiosyncratic risks
- Risk-adjusted returns, insurance mechanisms
- Users bear risk for higher returns

Economic Security

- Attack cost must exceed potential gain
- Honest behavior = Nash equilibrium

Key Economic Question

Who Pays, Who Earns?

Users bear risk for higher returns

Design Principle

Attack Cost $>$ Potential Gain



Cryptoeconomic security: Honest behavior must be the Nash equilibrium

Alternatives Considered

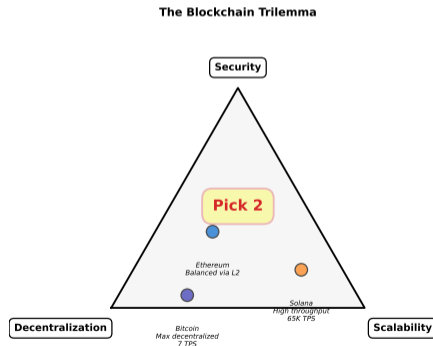
1. **Chosen Design:** Risk parameters, circuit breakers
2. **Alternative:** Traditional risk management approaches

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?



Every design is a trade-off. Understanding alternatives reveals the “why” behind choices.

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?

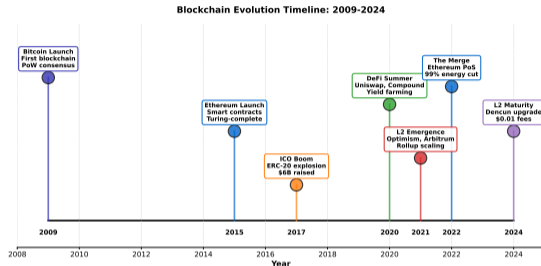
What Are the Key Blockchain Fundamentals?

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

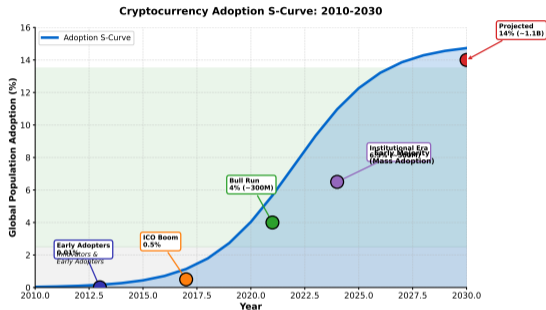
How Do Cryptocurrencies Actually Work?

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

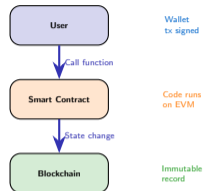
What Makes Smart Contracts Revolutionary?

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 → PoS (99% energy cut)
- **ERC Standards:** ERC-20, ERC-721, ERC-1155



Paradigm Shift: From “code is code” to “code is law”

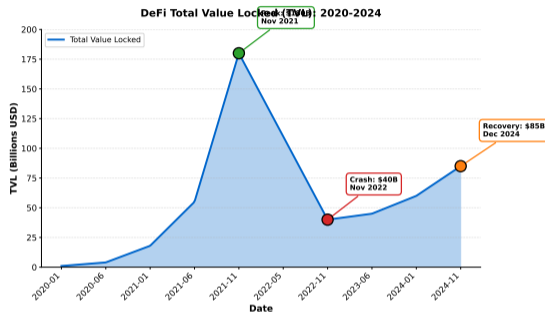
How Does DeFi Reconstruct Finance?

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



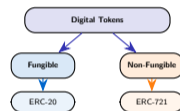
Innovation vs Risk: Composability enables innovation but also cascading failures

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 → 90%+ correction



Lasting Impact: Digital ownership infrastructure, beyond speculative JPEGs

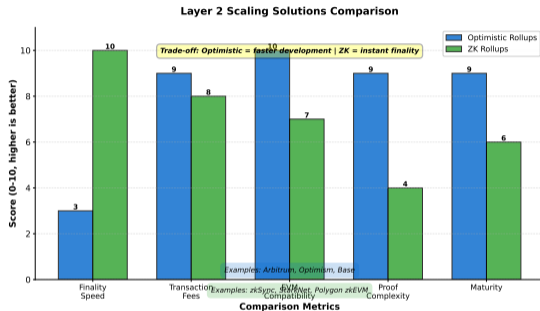
How Do We Scale and Secure Blockchains?

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

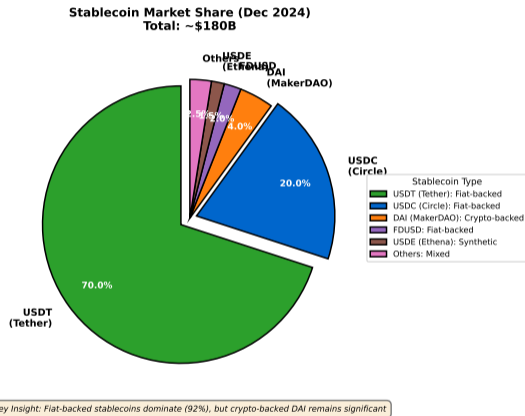
How Will Regulation Shape Crypto's Future?

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?

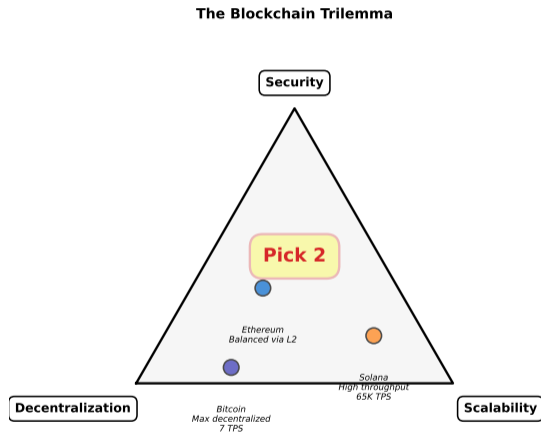
The Blockchain Trilemma:

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 collapse, Nov 2022)
- **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

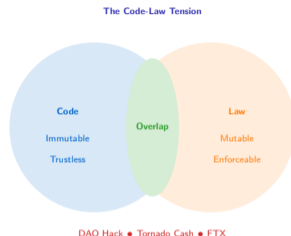
When Does “Code is Law” Actually Apply?

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

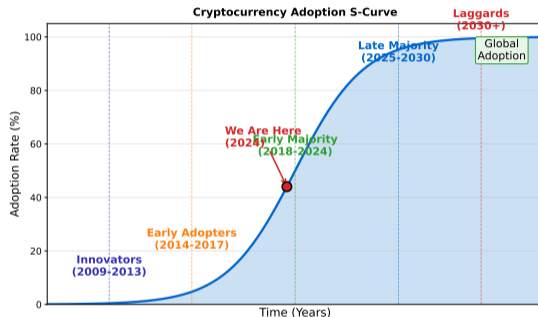
Will Crypto Ever Move Beyond Speculation?

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 and utility-driven

TradFi (Traditional Finance, i.e., banks, brokers, exchanges) vs DeFi:

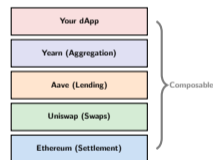
- TradFi: Licenses, capital, compliance
- DeFi: Deploy contract, anyone can use

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



“Move fast and break things” applied to finance — permissionless innovation with real trade-offs

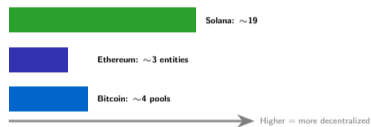
Why Does Centralization Keep Emerging?

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)



Reality:
Decentralization is a spectrum, not binary

The centralization paradox: convenience and efficiency naturally concentrate power, even in decentralized systems

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:

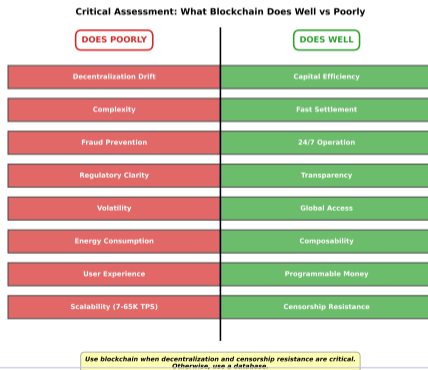
- AML/CFT requirements
- Tax enforcement needs
- Human right to privacy
- Dissident/activist protection



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



These 8 strengths represent blockchain's genuine competitive advantages over traditional systems

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



Honest assessment: blockchain is a tool, not a solution—context determines whether strengths outweigh weaknesses

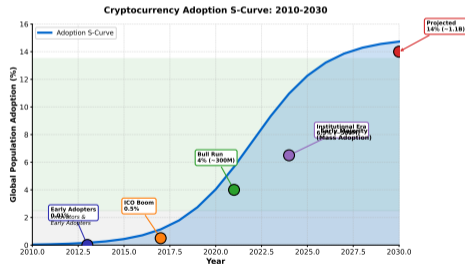
When Does Blockchain Actually Add Value?

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

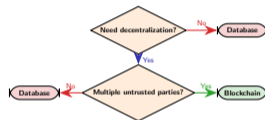
When is Blockchain Just Marketing Hype?

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



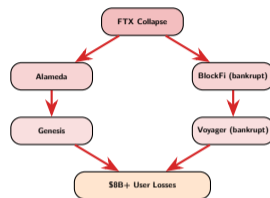
Heuristic: If you can use a database, use a database. Blockchain only when decentralization is critical.

What Happened (Nov 2022):

- FTX commingled funds with Alameda
- Alameda lost billions (Luna collapse May 2022, 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

FTX proved that centralized intermediaries in crypto face the same risks as traditional finance—plus less oversight

What Made 2024 Transformative for Crypto?

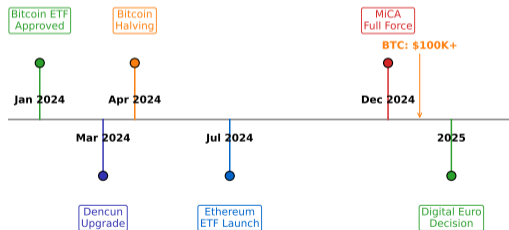
Q1 2024:

- **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 → \$0.01

Q2-Q4 2024:

- **Apr:** Bitcoin 4th halving
- **Jul:** Ethereum ETFs approved
- **Nov:** Pro-crypto US administration
- **Dec:** MiCA full EU implementation

2024-2025 Crypto Industry Milestones



2024: The year crypto went institutional—ETFs, regulatory frameworks, and political engagement converged

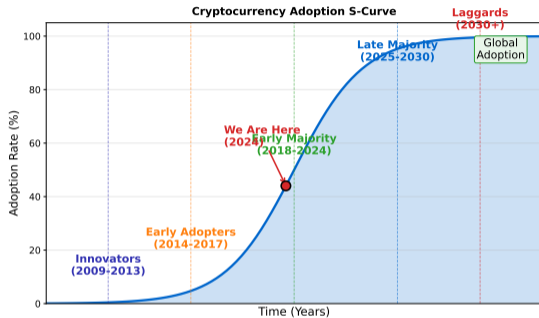
What's Changing in the 2025 Landscape?

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:

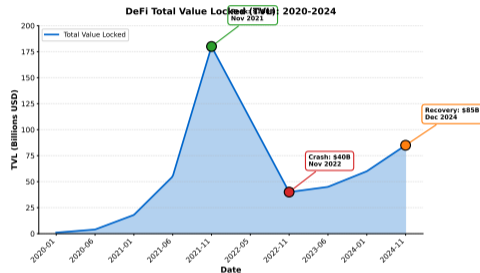
- L2 thriving: Base, Arbitrum, Optimism
- Restaking (EigenLayer) as new primitive
- Account abstraction accelerating
- Post-halving bull market dynamics



2025 marks a shift: institutional infrastructure, regulatory clarity, and L2 maturity converge

How Has Reality Evolved Since Course Design?

Topic	When 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 admin
Layer 2 fees	\$0.50-2.00	\$0.01-0.10
DeFi TVL	Recovery phase	\$80B+ TVL
Restaking	Emerging	\$15B+ EigenLayer
CBDCs	Racing ahead	US paused, EU prep



Takeaway: Industry moves fast; stay current with primary sources

Every row in this table changed between course design and delivery—this is why frameworks matter more than facts

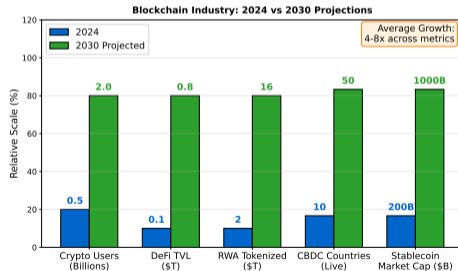
What Are the Critical Questions for 2025-2030?

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

2030 Scenarios: Three Possible Futures

Optimistic	Realistic	Pessimistic
Institutional 5-10% allocation	Hybrid: CeFi + DeFi coexist	Regulatory: DeFi banned, privacy outlawed
Stablecoins: \$1T+ market	Stablecoins: \$500B regulated	CBDC: Monopoly, crypto marginalized
Tokenization: \$10T+ assets	Institutional: Compliant on-ramps	Centralization: Mega-platforms dominate
L2 Success: 100K+ TPS, <\$0.01 fees	L2 Mobility: 50K TPS, \$0.10 fees	Scaling: L2 fragmentation, fees remain high
Regulatory: Global convergence	Regulation: Retail KYC, protocols exempt	Security: Major exploit destroys trust
UX: Social recovery, gas abstraction	Privacy: Limited, KYC mandatory	Quantum: ECDSA broken before migration
Privacy: ZK proofs solve compliance	CBDCs: Launched but limited adoption	Environmental: PoW globally banned
Impact: 1B+ users, transformed finance	Users: 750M (50% growth), parallel systems	Outcome: Niche survival like 1%r

Most likely: Realistic scenario with elements from both optimistic and pessimistic paths

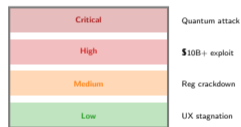
Best case: Financial system fundamentally transformed — more inclusive and efficient

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

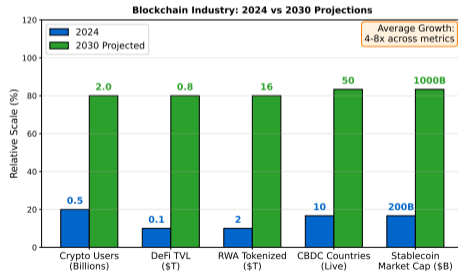
What's the Most Likely Scenario for 2030?

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

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



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



The course gave you frameworks; the real learning continues as you apply them

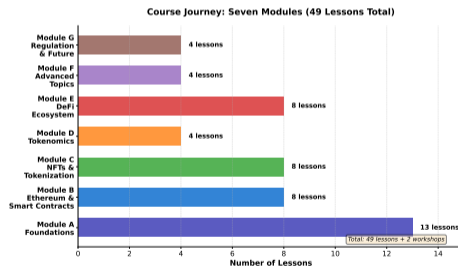
What Are the Core Lessons from This Course?

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

Don't Trust, Verify:

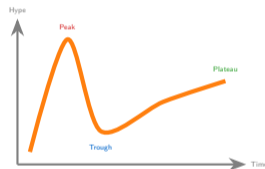
- Verify token contracts before investing
- Audit smart contracts before depositing
- Check proof of reserves (exchanges, stablecoins)

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

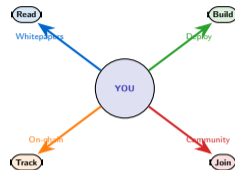
How Can You Keep Learning About Crypto?

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

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

Critical Assessment: What Blockchain Does Well vs Poorly

DOES POORLY	DOES WELL
Decentralization Drift	Capital Efficiency
Complexity	Fast Settlement
Fraud Prevention	24/7 Operation
Regulatory Clarity	Transparency
Volatility	Global Access
Energy Consumption	Composability
User Experience	Programmable Money
Scalability (7-65K TPS)	Censorship Resistance

Use blockchain when decentralization and censorship resistance are critical. Otherwise, use a database.

Blockchain is a tool, not a solution—its value depends on thoughtful application to real problems

“The best way to predict the future is to invent it.”

– Alan Kay

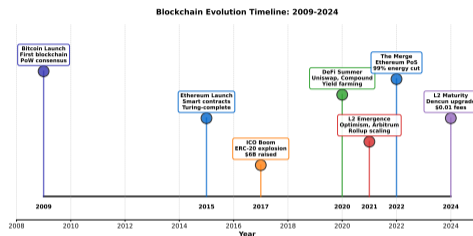
“In the long run, the most important thing is not to make money, but to build systems that are more fair, more open, and more free.”

– Crypto Ethos

“Stay curious. Stay skeptical. Stay building.”

– Course Conclusion

Three principles for your crypto journey: verify everything, question incentives, build something

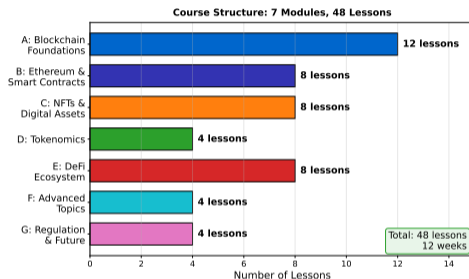


Thank you for completing this course!

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]

49 lessons, 7 modules, 1 framework — The Cryptoeconomics Lens is your tool for lifelong learning

Q1 (Module A). What is the minimum number of nodes needed to tolerate 2 Byzantine faults?

A) 5 B) 6 C) 7 D) 9

Answer: C – $n \geq 3f + 1 = 7$.

Q2 (Module A). Which property of cryptographic hashes makes the chain tamper-evident?

A) Encryption strength B) Pre-image + collision resistance C) Symmetric keys D) Random number generation

Answer: B – both properties together prevent forging or finding alternate blocks with the same hash.

Q3 (Module B). Under EIP-1559, where does the base fee go?

A) Validator B) Burned C) Treasury D) Gas refund pool

Answer: B – base fee is burned; only the priority fee (tip) goes to the validator.

Q4 (Module B). Which standard underlies fungible tokens like USDC and DAI?

A) ERC-721 B) ERC-1155 C) ERC-20 D) ERC-4337

Answer: C – ERC-20 is the canonical fungible-token interface.

Q5 (Module C). Which standard supports both fungible and non-fungible tokens in one contract?

- A) ERC-20 B) ERC-721 C) ERC-1155 D) ERC-3525

Answer: C – ERC-1155 multi-token standard supports both types and batched transfers.

Q6 (Module C). What is the primary purpose of IPFS in NFT design?

- A) Faster transactions B) Decentralised storage of metadata + assets C) Smart contract auditing D) Identity verification

Answer: B – IPFS provides content-addressed storage so the asset persists even if a centralised host disappears.

Q7 (Module D). What incentive property does linear vesting create for a project team?

- A) Short-term price floor B) Long-term alignment with protocol value C) Burns supply automatically D) Lowers gas fees

Answer: B – vesting locks the team's wealth to long-term protocol success.

Q8 (Module D). A token with no team allocation and no pre-mine is called...

- A) Premium launch B) Fair launch C) Bonding curve launch D) Vested launch

Answer: B – fair launches forgo pre-allocation; trade-off is no funded treasury.

Q9 (Module E). Constant-product AMMs (Uniswap V2) maintain which invariant?

- A) $x + y = k$ B) $x \cdot y = k$ C) $x^2 + y^2 = k$ D) $x/y = k$

Answer: B – $x \cdot y = k$ is the constant-product formula.

Q10 (Module E). Flash loans require...

- A) 150% collateral B) Atomic repayment in the same transaction or full revert C) Whitelist approval D) 30-day repayment

Answer: B – flash loans are atomic; repayment is enforced by the EVM transaction model.

Q11 (Module F). What did Ethereum's Dencun upgrade (March 2024) introduce?

- A) Proof of Work B) Proto-danksharding (EIP-4844 blobs) C) Account abstraction D) ZK-EVM

Answer: B – Dencun shipped EIP-4844 blobs, lowering L2 data costs by 10-100x.

Q12 (Module F). The Checks-Effects-Interactions pattern protects against which vulnerability?

- A) Integer overflow B) Reentrancy C) Front-running D) Oracle manipulation

Answer: B – updating state BEFORE external calls prevents reentrant withdrawals.

Q13 (Module G). When did MiCA reach full implementation across the EU?

- A) January 2024 B) July 2024 C) December 30, 2024 D) January 2025

Answer: C – MiCA full implementation date is 30 December 2024 with an 18-month grandfathering period.

Q14 (Module G). What did Trump's January 23, 2025 Executive Order do regarding US CBDCs?

- A) Mandated CBDC issuance B) Banned Federal Reserve CBDCs C) Required CBDC pilots in 5 states D) Created Strategic CBDC Reserve

Answer: B – the EO explicitly banned Federal Reserve CBDCs; it also created a Strategic Bitcoin Reserve study group.

Q15 (Module H). Which workshop deploys an ERC-20 token to Sepolia?

- A) W01 First Smart Contract B) W02 Create Cryptocurrency C) W03 Mint Your First NFT D) W04 Create Your DAO

Answer: B – W02 Create Cryptocurrency walks through deploying a custom ERC-20.

Q16 (Module H). Which workshop teaches deploying an NFT with IPFS-hosted metadata?

- A) W01 B) W02 C) W03 D) W04

Answer: C – W03 Mint Your First NFT covers ERC-721 deployment + IPFS metadata.