Lesson 13: What is Blockchain?

Module 2: Blockchain and Cryptocurrencies

Digital Finance

December 12, 2025

The Trust Problem in Digital Transactions

Traditional Digital Payments:

- Require trusted intermediary (bank)
- Centralized ledger control
- Single point of failure
- Gatekeeping and censorship risk
- High transaction fees

The Double-Spending Problem:

- Digital files can be copied
- Same money spent twice
- Who determines truth?
- Intermediaries solve this... at a cost

"How can strangers transact without trusting each other or a central authority?"

Digital transactions require trust mechanisms—blockchain removes the need for intermediaries.

The Evolution of Digital Cash

Year	Innovation	Limitation
1983	DigiCash (Chaum)	Required central bank
1997	Hashcash (Back)	No transfer mechanism
1998	b-money (Dai)	Theoretical only
2005	Bit Gold (Szabo)	No implementation
2008	**Bitcoin (Nakamoto)**	**First working solution**

Key Insight: All prior attempts failed to solve Byzantine Generals Problem in decentralized networks

Understanding history helps predict future developments in the technology.

Satoshi Nakamoto's Breakthrough (October 2008)

Bitcoin Whitepaper:

- "Bitcoin: A Peer-to-Peer Electronic Cash System"
- 9 pages, published on cryptography mailing list
- Combined existing cryptographic primitives in novel way
- Genesis block mined January 3, 2009

Core Innovations:

- Proof-of-Work consensus
- Decentralized timestamp server
- Longest chain rule
- Economic incentives (mining rewards)

Mystery Identity:

- Unknown person/group
- Disappeared April 2011
- Owns 1M BTC (never moved)
- Multiple theories, no proof

Genesis block message:
"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"

Bitcoin combined existing cryptographic primitives in a novel way to solve double-spending.

What is a Blockchain? Core Definition

Blockchain: A distributed, immutable ledger of transactions organized in cryptographically linked blocks

Key Components:

1. **Blocks:** Batches of transactions
2. **Chain:** Cryptographic links between blocks
3. **Network:** Distributed nodes maintaining copies
4. **Consensus:** Agreement mechanism (PoW/PoS)
5. **Cryptography:** Hash functions + digital signatures

Essential Properties:

- **Decentralization:** No single controller
- **Transparency:** All transactions visible
- **Immutability:** Cannot alter history
- **Security:** Cryptographic protection
- **Pseudonymity:** Addresses, not names

Clear definitions are essential for understanding complex technical concepts.

Centralized vs Decentralized Systems

Centralized (Traditional):

- Single authority controls ledger
- Fast transaction processing
- Easy to upgrade/modify
- Single point of failure
- Requires trust in intermediary
- Examples: Banks, PayPal, Visa

Advantages:

- Efficiency and speed
- Clear governance
- Customer support

Decentralized (Blockchain):

- Multiple nodes maintain ledger
- Slower (consensus overhead)
- Difficult to change rules
- No single point of failure
- Trustless operation
- Examples: Bitcoin, Ethereum

Advantages:

- Censorship resistance
- Transparency
- No intermediary needed

Centralized systems trade trust for efficiency; decentralized systems trade efficiency for trustlessness.

The Blockchain Trilemma

Impossible to maximize all three simultaneously:

DECENTRALIZATION
Number of independent validators
Resistance to control

SECURITY
Cost to attack network
Immutability guarantees

SCALABILITY
Transactions per second
Low fees

Network	Decentralization	Security	Scalability
Bitcoin	High	High	Low (7 TPS)
Ethereum	High	High	Medium (15-30 TPS)
BSC	Low	Medium	High (100+ TPS)
Solana	Medium	Medium	Very High (3000+ TPS)

The blockchain trilemma forces trade-offs between decentralization, security, and scalability.

How Blockchain Works: Simplified Flow

Transaction Lifecycle (6 Steps):

1. **Initiation:** User broadcasts transaction to network
2. **Validation:** Nodes verify signature and sufficient balance
3. **Mempool:** Valid transactions wait in memory pool
4. **Block Creation:** Miner/validator selects transactions for new block
5. **Consensus:** Network agrees on new block (PoW/PoS)
6. **Finalization:** Block added to chain, transaction confirmed

Typical Confirmation Times:

- Bitcoin: 10 minutes per block (6 blocks for finality = 1 hour)
- Ethereum: 12 seconds per block (32 blocks for finality = 6-7 minutes)
- Solana: 400ms per block (instant practical finality)

Understanding the process flow is key to identifying optimization opportunities.

Public vs Private Blockchains

Feature	Public (Permissionless)	Private (Permissioned)
Access	Anyone can join	Invited participants only
Validators	Anyone can become validator	Pre-approved validators
Transparency	Fully transparent	Controlled visibility
Speed	Slower (global consensus)	Faster (known validators)
Energy	High (PoW) or Medium (PoS)	Low (simple consensus)
Use Cases	Cryptocurrencies, DeFi	Enterprise, supply chain
Examples	Bitcoin, Ethereum	Hyperledger, R3 Corda
Trust Model	Trustless	Trust in consortium

Hybrid Models: Some networks (e.g., VeChain) combine public chain with private enterprise features

Public and private blockchains serve different use cases with different trust models.

Blockchain Use Cases Beyond Cryptocurrency

Financial Services:

- Cross-border payments (Ripple)
- Securities settlement (ASX)
- Trade finance (we.trade)
- Insurance claims (Etherisc)

Supply Chain:

- Food traceability (Walmart + IBM)
- Pharmaceutical tracking
- Luxury goods authentication
- Carbon credit tracking

Digital Identity:

- Self-sovereign identity (DID)
- Academic credentials
- Government IDs (Estonia)

Other Applications:

- Voting systems
- Real estate registries
- Intellectual property
- Healthcare records (HIPAA-compliant)
- Energy grid management

Real-world applications demonstrate the practical value of blockchain technology.

Real-World Example: Walmart Food Traceability

Problem: 2018 E. coli outbreak in romaine lettuce took weeks to trace source

Solution: Walmart + IBM Food Trust (Hyperledger Fabric)

Before Blockchain:

- Manual record keeping
- 7 days to trace mango origin
- Paper-based documentation
- Information silos
- Difficult recalls

After Blockchain:

- Digital immutable records
- 2.2 seconds to trace origin
- Real-time visibility
- Shared data access
- Precise, fast recalls

Impact: Reduced food waste, improved consumer safety, lower liability costs

---

Case studies provide concrete evidence of technology impact and adoption patterns.

Limitations and Challenges

Technical Limitations:

- Scalability: Low TPS vs Visa (24,000 TPS)
- Energy: Bitcoin uses 150 TWh/year
- Storage: Bitcoin blockchain ¿ 500 GB
- Finality: Long confirmation times
- Irreversibility: No undo for mistakes

Adoption Barriers:

- Regulatory uncertainty
- User experience complexity
- Integration with legacy systems
- Lack of interoperability
- Environmental concerns (PoW)
- Volatility (for crypto)

Key Insight: Blockchain is not a universal solution - use only when decentralization and immutability are critical requirements

---

Understanding limitations helps identify appropriate use cases and avoid over-engineering.

Blockchain vs Traditional Database

Criterion	Traditional Database	Blockchain
Control	Centralized administrator	Distributed consensus
CRUD Operations	Create, Read, Update, Delete	Create, Read only (append)
Performance	Very fast (ms latency)	Slow (seconds to minutes)
Data Integrity	Trust in administrator	Cryptographic guarantees
Transparency	Opaque to external parties	Transparent to all participants
Cost	Low operational cost	High (consensus overhead)
Failure Tolerance	Backup/replication needed	Inherently redundant
Auditability	Depends on logging	Complete audit trail
Best For	Most business applications	Multi-party distrust scenarios

Decision Rule: Use blockchain ONLY if multiple parties need shared write access without mutual trust

Comparative analysis helps identify the right tool for specific requirements.

The Hype Cycle: Where Are We?

Gartner Hype Cycle for Blockchain (2015-2024):

- **2015-2017:** Peak of Inflated Expectations - "Blockchain will change everything"
- **2018-2020:** Trough of Disillusionment - ICO crash, failed enterprise pilots
- **2021-2022:** Slope of Enlightenment - Real use cases emerge (DeFi, NFTs, CBDCs)
- **2023-2024:** Plateau of Productivity - Mature applications in specific domains

Current Reality (2024):

- Cryptocurrencies: Established asset class (total market cap $2T)
- DeFi: $50B+ total value locked, real financial infrastructure
- Enterprise: Selective adoption where justified (supply chain, trade finance)
- CBDCs: 130+ countries exploring, 11 launched (e.g., Nigeria eNaira, Bahamas Sand Dollar)

Technology adoption follows predictable patterns—timing matters for investment decisions.

Bitcoin Network Statistics (2024)

Network Metrics:

- **Hash Rate:** 600 EH/s
- **Active Addresses:** 1M/day
- **Transactions:** 400k/day
- **Block Size:** 1-2 MB average
- **Nodes:** 17,000 reachable
- **Mining Difficulty:** Adjusts every 2016 blocks

Next halving: April 2024 (reward drops to 3.125 BTC)

Economic Metrics:

- **Market Cap:** $850B
- **Circulating Supply:** 19.5M BTC
- **Max Supply:** 21M (hard cap)
- **Block Reward:** 6.25 BTC (halves every 4 years)
- **Fees:** $2-50 per transaction
- **Energy:** 150 TWh/year (0.5% global)

Network metrics provide objective measures of adoption and ecosystem health.

Ethereum Network Statistics (2024)

Post-Merge Metrics:

- **Consensus:** Proof-of-Stake (Sept 2022)
- **Validators:** 950,000
- **Staked ETH:** 32M (27% of supply)
- **Transactions:** 1.2M/day
- **Smart Contracts:** 50M deployed
- **Energy:** 99.95% reduction vs PoW

EIP-4844 (Proto-Danksharding) expected 2024 - major scalability upgrade

DeFi Ecosystem:

- **TVL:** $25B
- **DEX Volume:** $50B/month
- **NFT Sales:** $500M/month
- **Gas Fees:** $1-20 (varies)
- **ERC-20 Tokens:** 500k
- **Layer 2 Adoption:** Growing (Arbitrum, Optimism)

Network metrics provide objective measures of adoption and ecosystem health.

Key Terminology Summary

Block: Batch of transactions

Blockchain: Chain of cryptographically linked blocks

Node: Computer maintaining blockchain copy

Miner: Node creating new blocks (PoW)

Validator: Node validating blocks (PoS)

Consensus: Agreement mechanism

Hash: Cryptographic fingerprint

Nonce: Number used once (PoW)

Difficulty: Mining puzzle hardness

Mempool: Pending transactions pool

UTXO: Unspent transaction output

Gas: Transaction fee unit (Ethereum)

Smart Contract: Self-executing code

DeFi: Decentralized finance

Layer 1: Base blockchain

Layer 2: Scaling solution on top

Fork: Protocol rule change

51% Attack: Majority control threat

Lesson 14: Blocks and Cryptographic Hashing

What We'll Cover:

- Block structure and anatomy
- SHA-256 hash function in depth
- Avalanche effect demonstration
- Hash pointers and Merkle trees
- Why blockchain is immutable
- Practical examples and calculations

Prepare:

- Review basic binary and hexadecimal notation
- Understand exponential growth (important for hash space)
- Install Bitcoin Core or blockchain explorer for hands-on exploration

Summary: Key Takeaways

1. **Trust Problem:** Blockchain solves double-spending without intermediaries
2. **Satoshi's Innovation:** Combined existing cryptography with economic incentives
3. **Core Properties:** Decentralization, transparency, immutability, security
4. **Trilemma:** Cannot maximize decentralization, security, and scalability simultaneously
5. **Not a Panacea:** Use only when multiple parties need shared, tamper-proof records
6. **Real Adoption:** Cryptocurrencies, DeFi, supply chain, identity - but still early stage
7. **Public vs Private:** Different trust models and use cases
8. **Evolution:** From hype (2017) to practical applications (2024)

"Blockchain is a solution looking for the right problems - choose wisely."