L01: Introduction to Blockchain

Extended Slides – BSc Blockchain Course

Digital Finance

2026

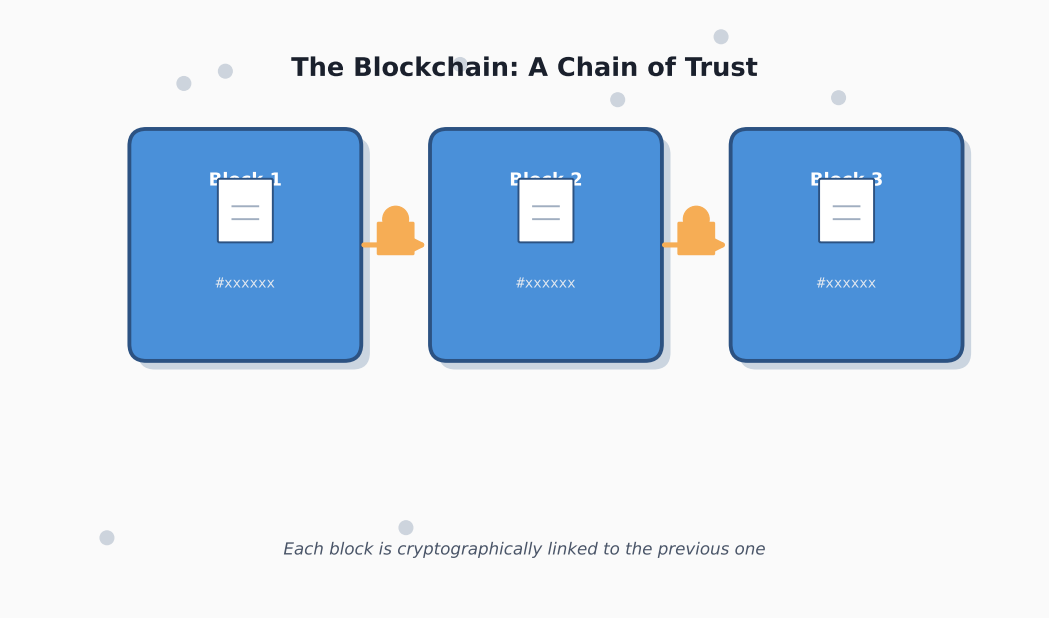
Learning Objectives

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

1. Define blockchain and explain its core properties
2. Distinguish between centralized, distributed, and decentralized systems
3. Identify key milestones in blockchain history
4. Explain the trust model shift from institutions to cryptography
5. Compare blockchain with traditional database systems

Prerequisites: Python programming and basic statistics.

Why Blockchain Matters



Purpose: Blockchain removes the need for trusted intermediaries in digital transactions. Understanding this technology is essential as it reshapes finance, supply chains, and digital identity.

From Bitcoin to CBDCs, blockchain is transforming how value moves globally.

What is Blockchain?

Formal Definition
A blockchain is a **distributed ledger** that:

- Records transactions in chronologically ordered **blocks**
- Links blocks using **cryptographic hashes**
- Is replicated across a **peer-to-peer network**
- Uses **consensus mechanisms** to agree on state

Key Insight: Blockchain is not a single technology, but a combination of existing technologies (hashing, digital signatures, P2P networks, consensus protocols) arranged in a novel way.

The term "blockchain" was coined after Bitcoin, not by Satoshi Nakamoto.

Core Properties of Blockchain

The Four Pillars

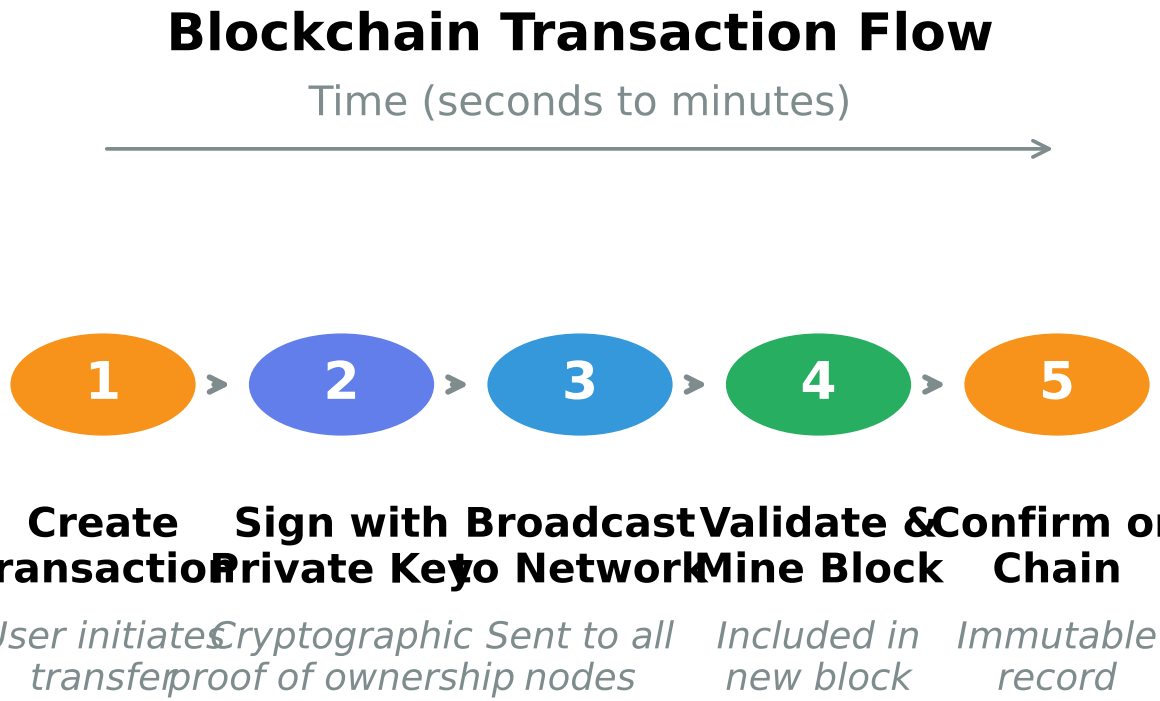
1. **Decentralization:** No single entity controls the network
2. **Immutability:** Once written, data cannot be altered
3. **Transparency:** All transactions are publicly verifiable
4. **Security:** Cryptography ensures data integrity

Trade-off Triangle (Blockchain Trilemma):

- Decentralization vs Scalability vs Security
- No blockchain optimizes all three simultaneously

Vitalik Buterin popularized the "trilemma" framing circa 2017.

How a Transaction Works



Each step involves cryptographic verification – no trust required.

Transaction Flow – Step by Step

Five Stages of a Blockchain Transaction

1. **Create:** User specifies recipient, amount, and data
2. **Sign:** Private key generates digital signature
3. **Broadcast:** Transaction propagates to all nodes
4. **Validate:** Miners/validators check signature and balance
5. **Confirm:** Transaction included in a block and finalized

Confirmation Times:

- Bitcoin: 10 minutes average (6 confirmations = 1 hour)
- Ethereum: 12 seconds (finality in $\sim$12.8 min / 2 epochs)

Finality = irreversible confirmation.

History: Origins (1980s-2008)

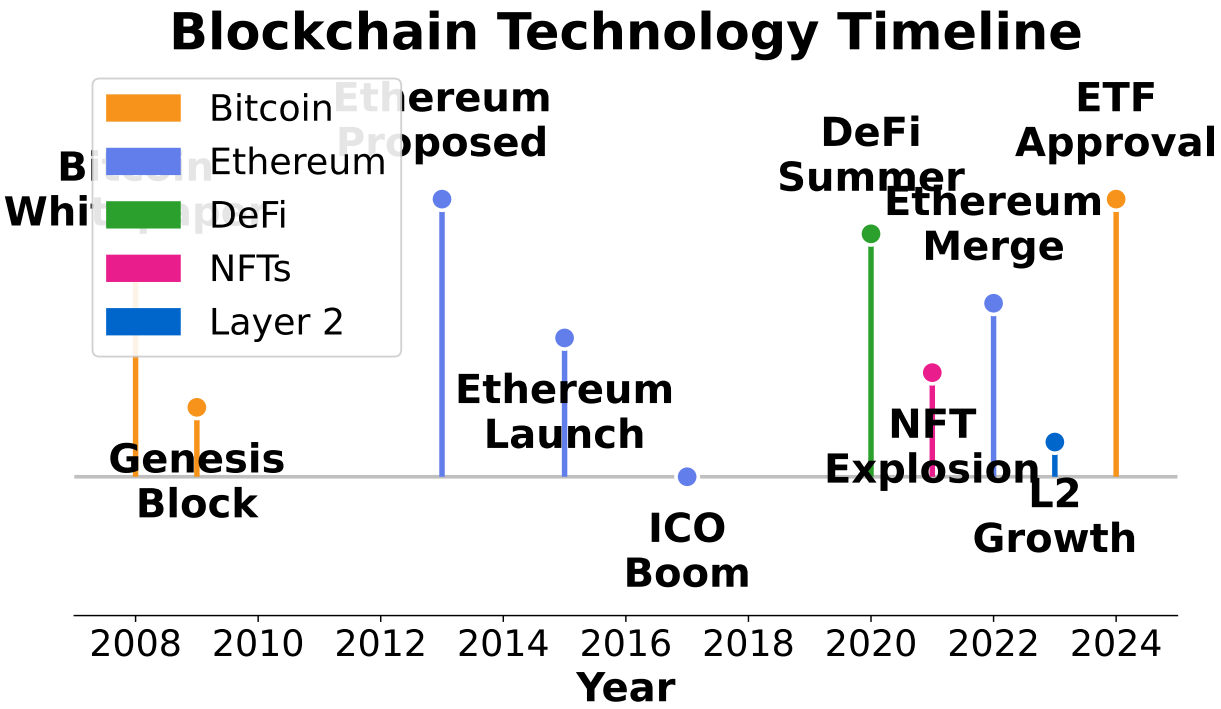
Pre-Bitcoin Innovations

- **1982:** David Chaum – digital cash concepts
- **1991:** Haber & Stornetta – timestamped documents
- **1997:** Adam Back – Hashcash (proof-of-work)
- **1998:** Wei Dai – b-money proposal
- **2004:** Hal Finney – reusable proof-of-work

2008 Financial Crisis: Provided motivation for trustless money.

Bitcoin combined many existing ideas into a working system.

Blockchain Timeline



From academic curiosity to mainstream financial infrastructure.

History: Bitcoin Era (2009-2014)

Key Events

- **Jan 2009:** Genesis block mined
- **May 2010:** First real-world purchase (10,000 BTC for pizza)
- **2011:** Altcoins emerge (Litecoin, Namecoin)
- **2013:** Bitcoin reaches $1,000 for first time
- **2014:** Mt. Gox collapse – $\sim$650,000 BTC lost

Lessons Learned:

- Centralized exchanges are single points of failure
- "Not your keys, not your coins"

Mt. Gox handled 70% of all Bitcoin trades before collapse.

History: Ethereum Era (2015-2019)

Smart Contract Revolution

- **2013:** Vitalik Buterin proposes Ethereum
- **2015:** Ethereum mainnet launches
- **2016:** The DAO hack – $60M stolen, hard fork
- **2017:** ICO boom – $6B raised
- **2018:** ICO bust – 90% of tokens fail

Key Innovation: Turing-complete programmability enabled DApps.

The DAO hack led to Ethereum Classic fork – "code is law" debate.

History: Modern Era (2020-Present)

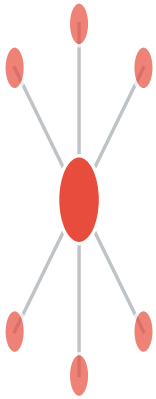
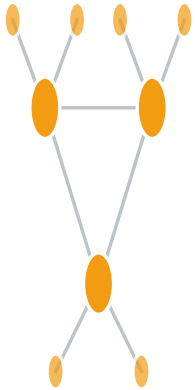
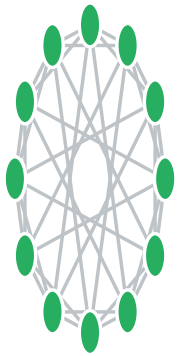
Institutional Adoption

- **2020:** DeFi Summer – TVL grows from $1B to $15B
- **2021:** NFT explosion, Bitcoin ATH $69K
- **2022:** Ethereum Merge (PoW to PoS)
- **2023:** Layer 2 adoption accelerates
- **2024:** Bitcoin ETF approval, institutional flows

Current Phase: Infrastructure maturation and regulatory clarity.

BlackRock, Fidelity, and major banks now offer crypto products.

Network Topology Comparison

Centralized	Distributed	Decentralized (P2P)
		
Single point of failure	*Multiple hubs*	*No central authority*

Each topology has different failure modes and trust assumptions.

Centralized Systems

Characteristics

- Single authority controls data and rules
- High efficiency and throughput
- Easy to update and maintain
- Single point of failure

Examples:

- Traditional banks
- Cloud services (AWS, Google)
- Social media platforms

Risk: Central party can censor, modify, or lose data.

Most of the internet today runs on centralized infrastructure.

Decentralized Systems

Characteristics

- No single point of control
- Censorship resistant
- Requires consensus mechanism
- Lower throughput (trade-off)

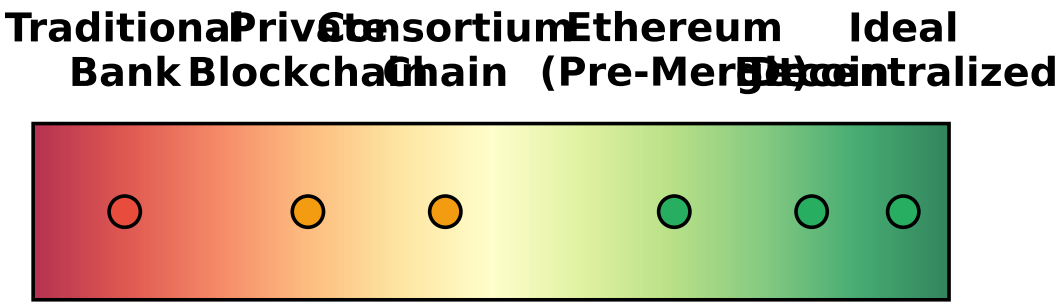
Benefits:

- No permission needed to participate
- Rules enforced by code, not authority
- Resistant to shutdown

Examples: Bitcoin, Ethereum, BitTorrent

Decentralization is a spectrum, not binary.

Decentralization Spectrum



Centralized

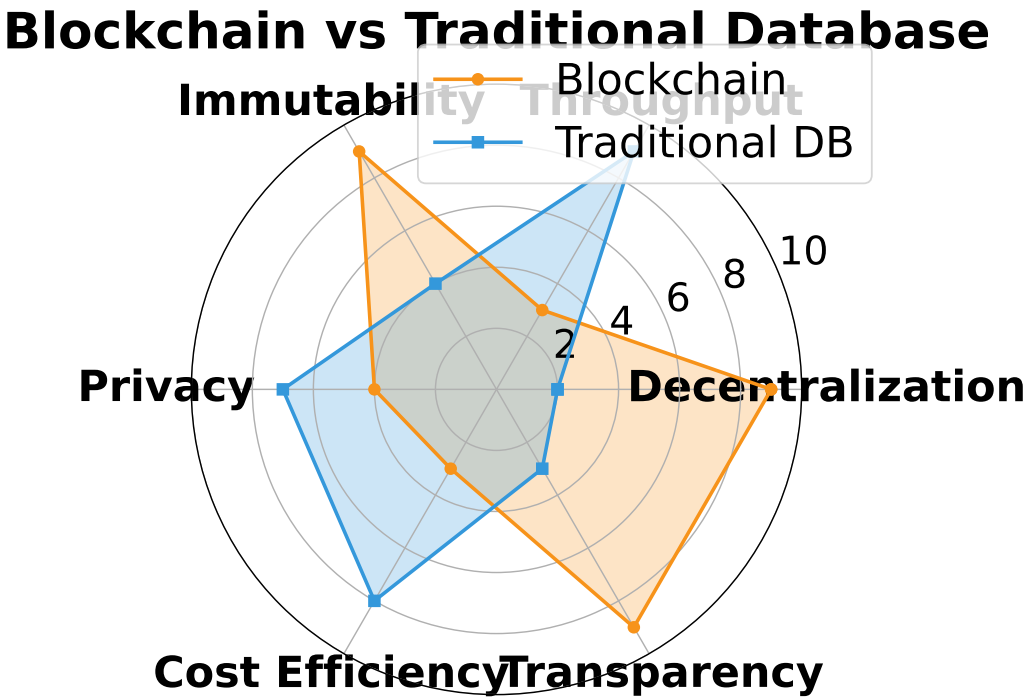
- Single authority
- High throughput
- Easy to update

Decentralized

- No single authority
- Censorship resistant
- Immutable

Private and consortium chains sacrifice decentralization for control.

Blockchain vs Traditional Database



Choose blockchain when you need trustless coordination among adversaries.

When to Use Blockchain

Blockchain is Appropriate When:

- Multiple parties need shared truth
- Trust between parties is low
- Intermediary removal provides value
- Immutability is required
- Transparency is beneficial

Blockchain is NOT Appropriate When:

- Single organization controls data
- High throughput is required
- Data needs to be deletable
- Privacy is paramount

Most enterprise "blockchain" projects would be better as databases.

Traditional Trust Model

How Traditional Finance Works

- Trust in institutions (banks, governments)
- Trust in legal systems for enforcement
- Identity verified by third parties
- Settlement through intermediaries

Problems:

- Counterparty risk
- Censorship potential
- Slow cross-border transfers
- Exclusion of unbanked populations

As of 2021, 1.4 billion adults remained unbanked globally (World Bank Global Findex); this number has since decreased.

Blockchain Trust Model

How Blockchain Changes Trust

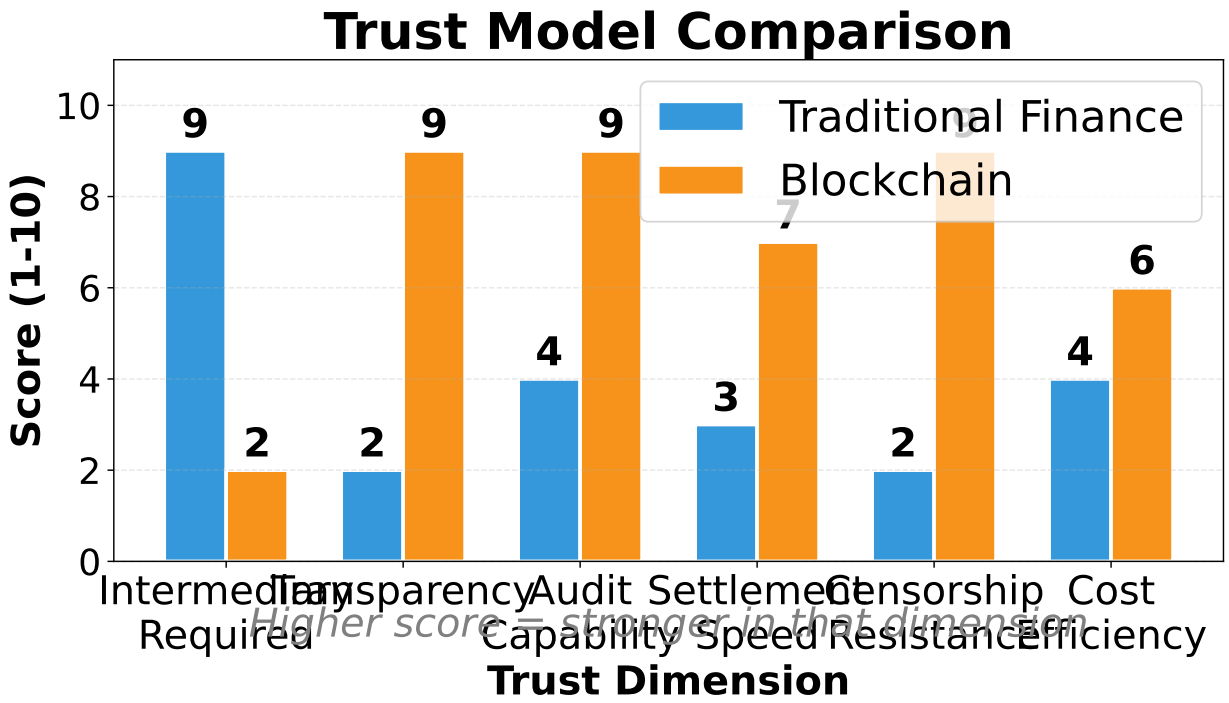
- Trust in mathematics and code
- Verification replaces trust
- Self-custody of assets
- Permissionless participation

Benefits:

- No counterparty risk (for on-chain assets)
- Censorship resistance
- 24/7 global access
- Financial inclusion

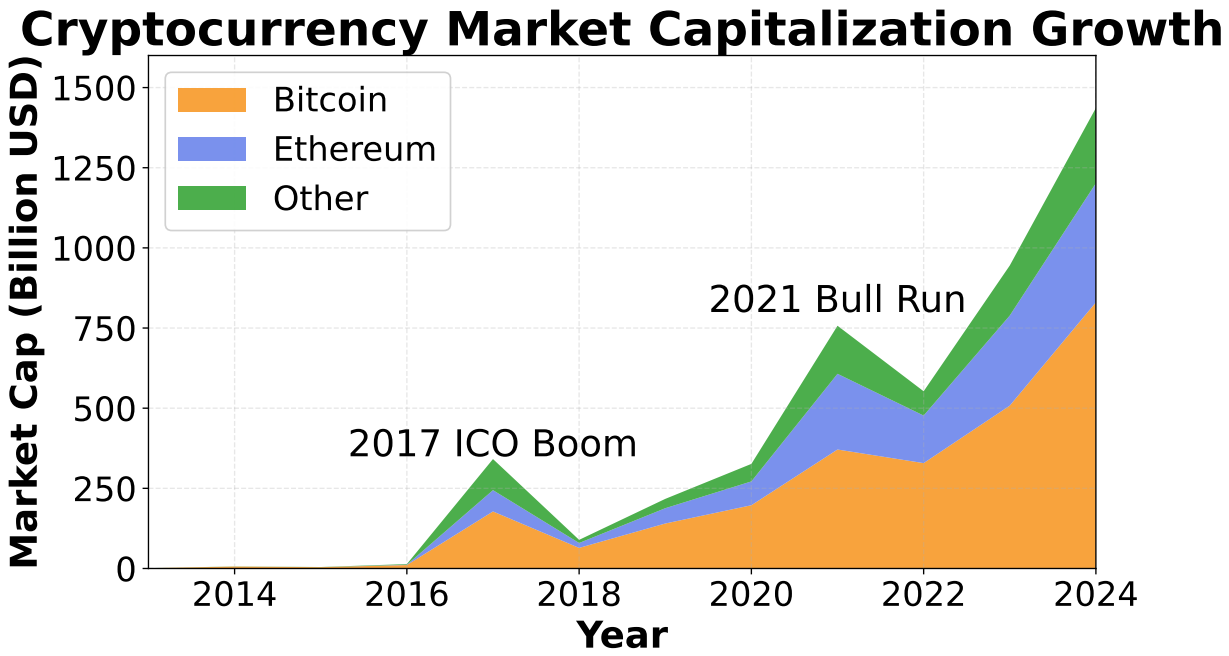
"Don't trust, verify" – Bitcoin community mantra.

Trust Model Comparison



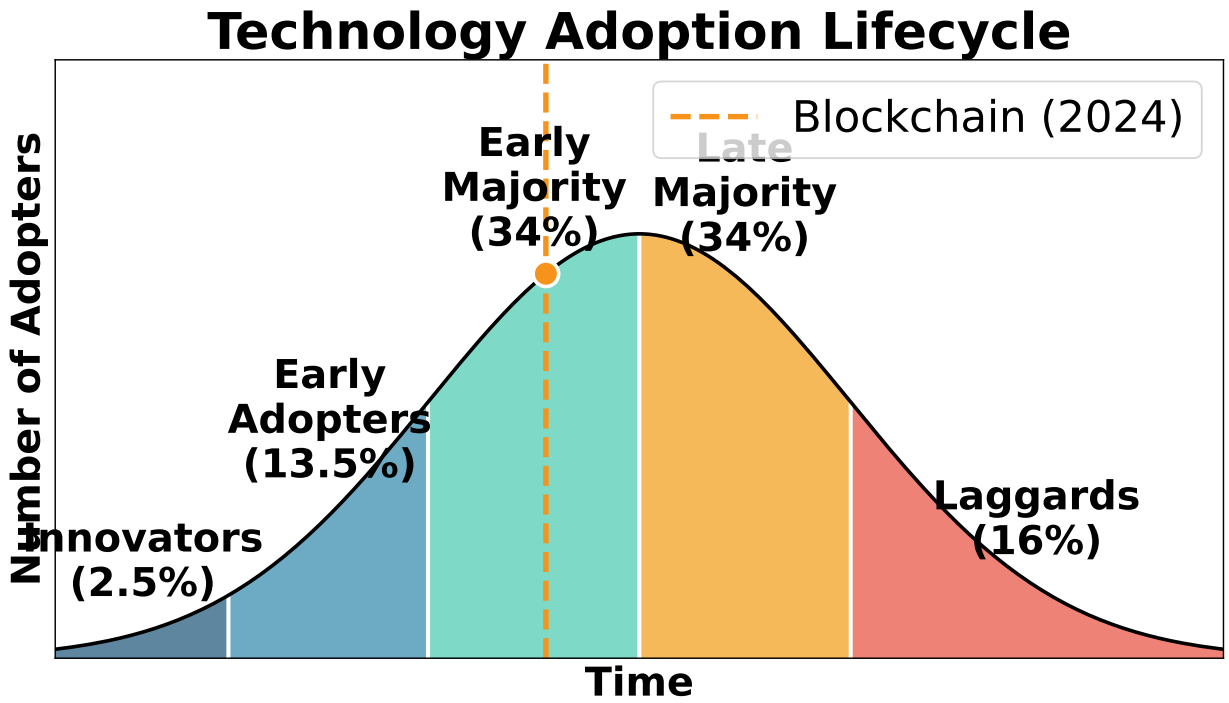
Neither model is universally superior – context determines optimal choice.

Market Capitalization Growth



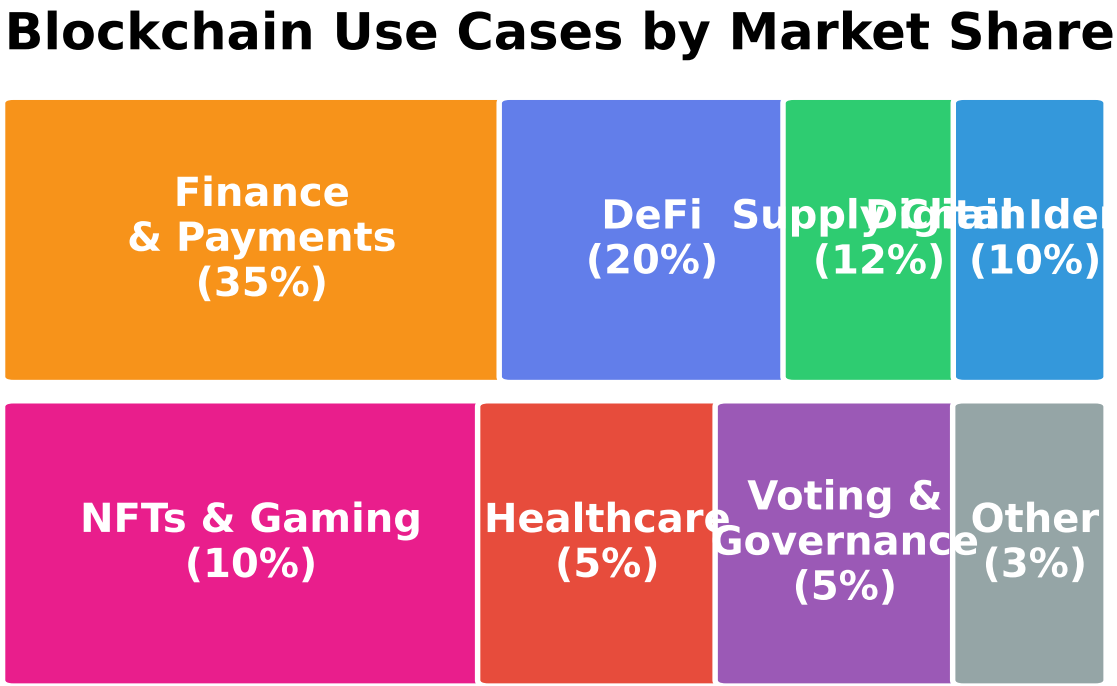
Crypto is now larger than many traditional asset classes.

Technology Adoption Lifecycle



Blockchain is transitioning from early adopters to early majority.

Blockchain Use Cases



Finance leads adoption, but other sectors are catching up.

Use Case: Finance and Payments

Applications

- Cross-border remittances
- Decentralized lending/borrowing (DeFi)
- Asset tokenization (real estate, securities)
- Stablecoins for commerce

Benefits:

- Lower fees than traditional rails
- 24/7 operation
- Programmable money

Stablecoin settlement volume has at times exceeded Visa (by some metrics).

Use Case: Supply Chain

Applications

- Product provenance tracking
- Anti-counterfeiting
- Compliance documentation
- Automated payments on delivery

Examples:

- IBM Food Trust (Walmart, Nestle)
- De Beers diamond tracking
- Pharmaceutical supply chains

Supply chain is the leading enterprise blockchain use case.

Use Case: Digital Identity

Applications

- Self-sovereign identity (SSI)
- Verifiable credentials
- KYC/AML compliance
- Voting systems

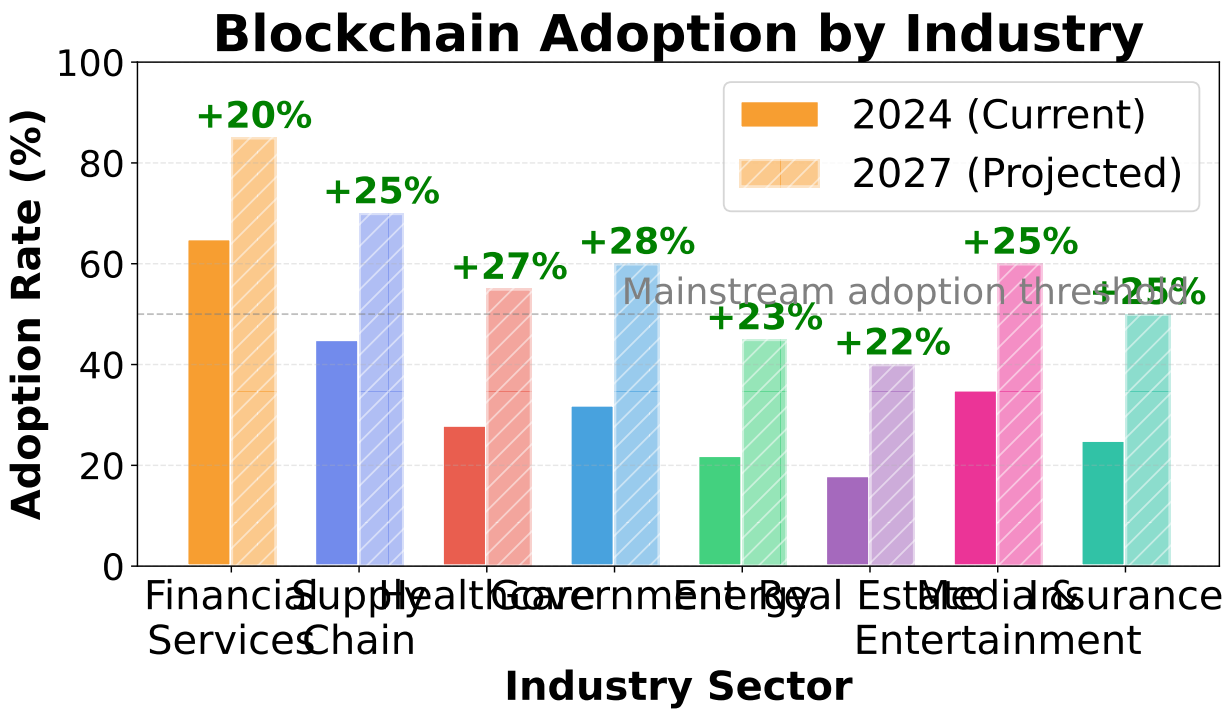
Key Innovation: Users control their own identity data.

Examples:

- Microsoft ION (Bitcoin-based identity)
- World ID (biometric proof of personhood)

Privacy-preserving identity is an active research area.

Industry Adoption Rates



Financial services lead; healthcare and real estate are emerging.

Key Blockchain Platforms

Public Blockchains

- **Bitcoin:** Store of value, digital gold
- **Ethereum:** Smart contracts, DeFi, NFTs
- **Solana:** High throughput, low fees
- **Polygon:** Ethereum scaling solution

Enterprise/Permissioned

- **Hyperledger Fabric:** IBM-backed, supply chain
- **R3 Corda:** Financial institutions
- **Quorum:** JPMorgan-developed (now ConsenSys)

Public chains dominate innovation; enterprise chains focus on specific use cases.

Challenges and Risks

Technical Challenges

- Scalability limitations
- Energy consumption (PoW)
- User experience complexity

Adoption Challenges

- Regulatory uncertainty
- Integration with existing systems
- Skills gap

Security Risks

- Smart contract bugs
- Private key management
- Exchange hacks

These challenges are being addressed but remain significant.

Key Takeaways

Remember These Points

1. Blockchain is a distributed, immutable ledger
2. Decentralization eliminates single points of failure
3. Trust shifts from institutions to cryptography
4. Trade-offs: throughput vs decentralization vs security
5. Use blockchain when parties don't trust each other

Next Lesson: Cryptographic Foundations – hash functions, digital signatures, and Merkle trees.

Lesson 2 will explain the math that makes blockchain secure.