

# Lesson 1: What is Blockchain?

## History, Motivation & Core Concepts

BSc Blockchain, Crypto Economy & NFTs

FHGR School of Management

Winter Semester 2025

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

1. Define blockchain and identify its core components
2. Trace the historical evolution from 1991 to present day
3. Understand the double spending problem and how blockchain solves it
4. Identify real-world applications across industries

**Duration:** 45 minutes

---

This lesson establishes the foundation for understanding distributed ledger technology

## Part 1: Foundation (20 min)

- Historical timeline 1991-2025
- The double spending problem
- Why previous digital cash failed

## Part 2: Core Concepts (25 min)

- Block structure and chain linking
- Distributed ledger architecture
- Immutability and decentralization
- Real-world applications

**Format:** Interactive lecture with visual demonstrations

---

**Questions welcome throughout the session**

[5.5cm]

Chart: Timeline visualization 1991-2008

## 1991: Cryptographic Foundations

- Haber & Stornetta: timestamping
- First blockchain-like structure
- Published in *Journal of Cryptology*  
Foundation concepts existed decades before Bitcoin

## 2004: Reusable Proof-of-Work

- Hal Finney introduces RPOW
- Attempt at digital scarcity
- Required trusted servers

# Historical Timeline: The Bitcoin Revolution

[5.5cm]

Chart: Timeline visualization 2008-2015

**October 31, 2008**

Satoshi whitepaper:

"Bitcoin: A Peer-to-Peer Electronic  
Cash System"

~~Bitcoin solved the double spending problem without trusted third parties~~

**January 3, 2009**

Genesis block mined

Network goes live

~~Block reward: 50 BTC~~

**July 30, 2015**

Ethereum launches

Smart contracts enabled

Blockchain 2.0 era begins

[5.5cm]

Chart: Timeline visualization 2020-2025 with major milestones

## 2020-2024: Corporate Entry

- PayPal adds crypto support (2020)
- Tesla invests \$1.5B in Bitcoin (2021)
- El Salvador adopts Bitcoin as legal tender (2021)

## 2024-2025: Mainstream Integration

- Bitcoin ETF approvals (Jan 2024)
- Institutional custody solutions
- Central bank digital currencies (CBDCs)

# The Problem: Double Spending

## Physical Cash: No Problem

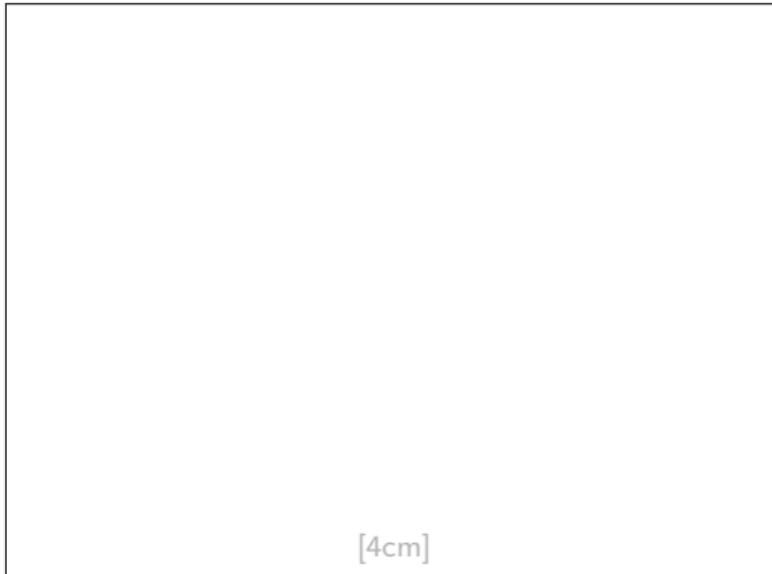


Chart: Physical money exchange diagram

- Alice gives \$10 bill to Bob
- Alice no longer has the bill
- ~~Physical scarcity prevents duplication~~  
~~Double spending was the fundamental barrier to digital currency~~

## Digital Cash: Major Problem

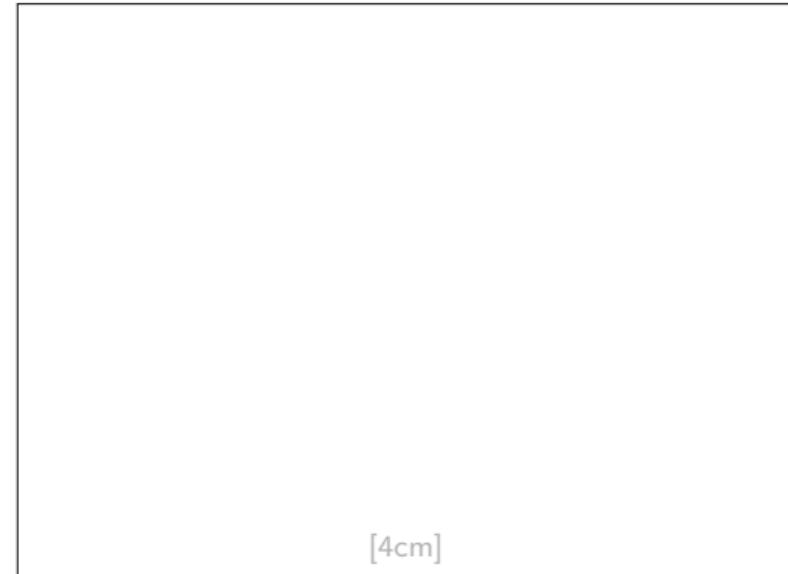
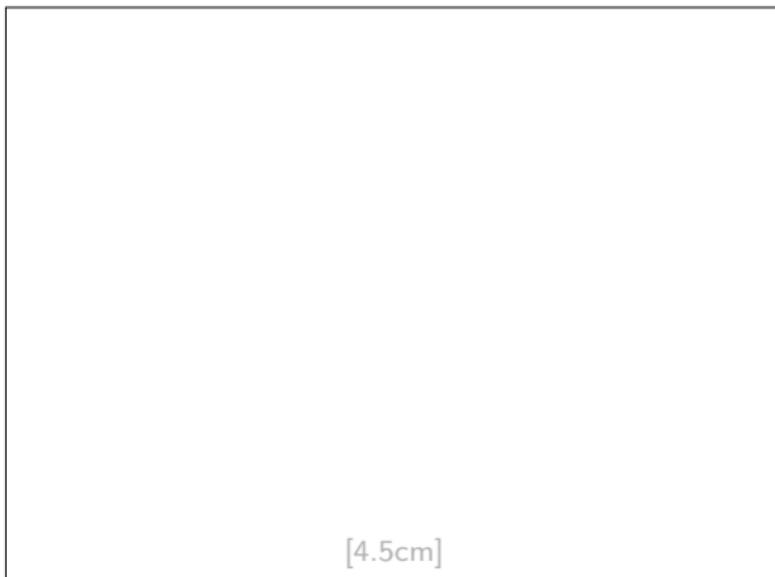


Chart: Digital file duplication diagram

- Digital files are easily copied
- Alice could send same \$10 to Bob and Carol
- No inherent scarcity in digital format

# Traditional Solution vs. Blockchain Solution

## Centralized Solution (Banks)

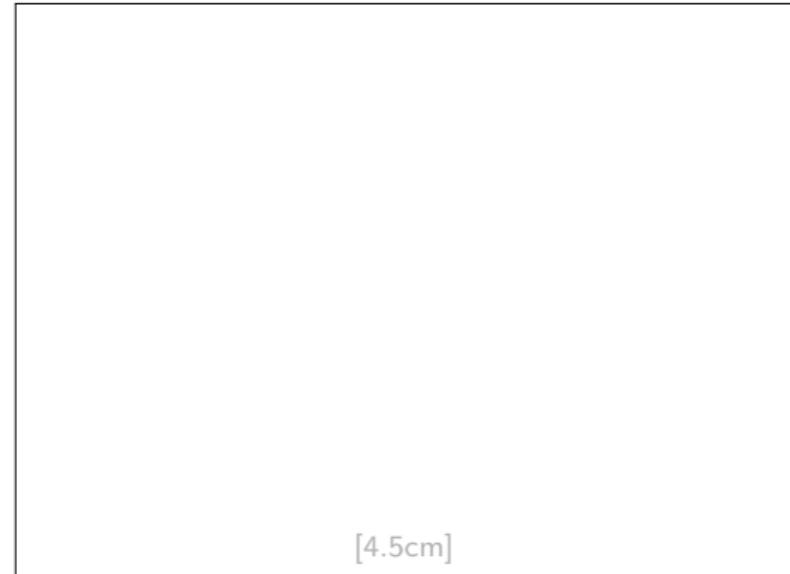


[4.5cm]

Chart: Centralized ledger with bank as middleman

- + Prevents double spending
- + Familiar and trusted
- Single point of failure

## Blockchain Solution



[4.5cm]

Chart: Distributed ledger with multiple nodes

- + Prevents double spending
- + No intermediary needed
- + 24/7 global access

[5cm]

Chart: Detailed block anatomy showing header and body

### Block Header

- Previous block hash (link to chain)
- Timestamp
- Nonce (for proof-of-work)

### Block Body

- List of verified transactions
- Bitcoin: avg 2,000-3,000 transactions
- Block size: 1-4 MB (Bitcoin)

[5.5cm]

Chart: Chain of blocks showing hash connections

### How Blocks Link Together:

- Each block contains the hash of the previous block
- Hash functions create unique digital fingerprints
- Changing any data changes the hash
- Broken hash link = invalid chain

[5cm]

Chart: Network diagram showing multiple nodes with identical ledgers

### Key Characteristics

- Thousands of identical copies
- Bitcoin: 15,000+ full nodes
- Each node validates independently

### Benefits

- No single point of failure
- High availability (99.99%+)
- Transparent and auditable

### Why Changes are Impossible

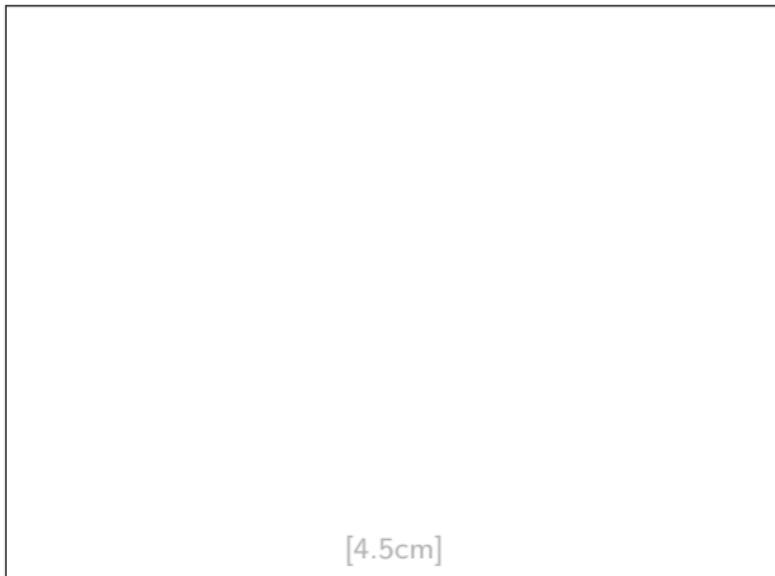


Chart: Cascade effect of changing one block

1. Attacker changes Block 100
2. Hash of Block 100 changes
3. Block 101 now points to wrong hash

### Mathematical Security

- Bitcoin network: 400+ EH/s
- Would need 51% of computing power
- Cost: billions of dollars in hardware
- Economically irrational for attacker
- Deeper blocks = more secure

**Best Practice:** Wait 6 confirmations (60 min) for large transactions

[5cm]

Chart: Centralized vs Decentralized vs Distributed network topology

### Centralized

- Single authority
- Fast decisions
- ~~Single point of failure~~

~~True blockchain systems are distributed, not just decentralized~~

### Decentralized

- Multiple authorities
- Federated control
- Resilient to attacks

### Distributed (Blockchain)

- No authorities
- Peer-to-peer consensus
- Maximum resilience

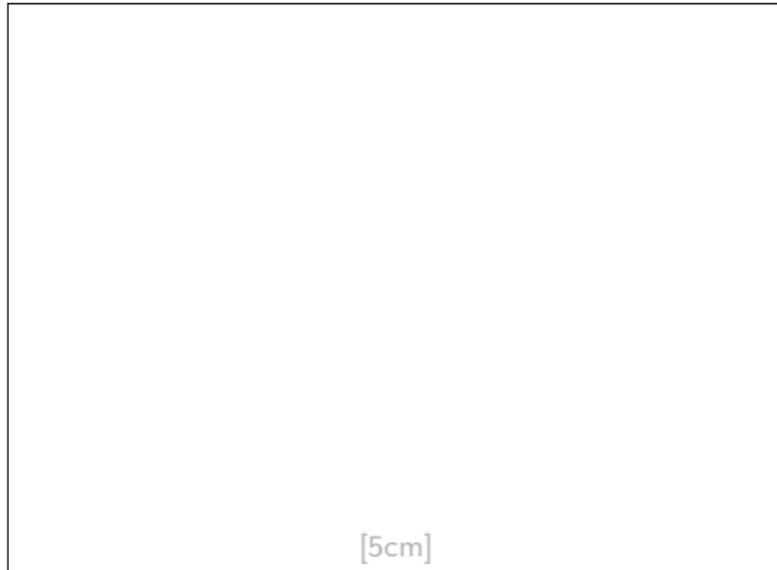


Chart: Market statistics visualization

**From zero to mainstream adoption in 15 years**

## Market Size (2024-2025)

- Bitcoin market cap: \$1.79 trillion
- Total crypto market cap: \$3+ trillion
- Daily trading volume: \$100+ billion

## User Adoption

- Global crypto users: 559-617 million
- 28% of US adults own cryptocurrency
- Growth rate: 34% year-over-year

## Network Activity

- Bitcoin transactions: 300,000-400,000/day
- Ethereum transactions: 1.2 million/day
- Combined: 2,000+ blockchain networks

## Financial Services

- Cross-border payments (Ripple, Stellar)
- Decentralized finance (Uniswap, Aave)
- Tokenized assets (real estate, stocks)
- Stablecoins (USDC, USDT)

## Supply Chain

- Walmart: food traceability
- Maersk: shipping logistics
- De Beers: diamond provenance
- Pharmaceutical authentication

## Digital Identity

- Self-sovereign identity (SSI)
- Credential verification
- Healthcare records
- Academic diplomas

## Government & Public Sector

- Land registries (Georgia, Sweden)
- Voting systems (pilot projects)
- Public benefit distribution
- Tax collection and auditing

---

Blockchain is transitioning from cryptocurrency to enterprise infrastructure

[5cm]

Chart: Job market and salary data visualization

## Technical Roles

- Blockchain developer: \$100k-\$180k
- Smart contract auditor: \$120k-\$200k
- Protocol engineer: \$150k-\$250k

## Business Roles

- Blockchain consultant: \$90k-\$150k
- Product manager: \$110k-\$180k
- Legal and compliance specialist

# Summary: Key Takeaways

## What We Learned

1. Blockchain evolved from 1991 research to \$3T market
2. Solves double spending without intermediaries
3. Core components: blocks, chain, distribution, immutability
4. Applications span finance, supply chain, identity

**Preparation:** Review Satoshi Nakamoto whitepaper (provided in course materials)

## Next Lesson Preview

- L02: Distributed Ledger Technology Deep Dive
- Consensus mechanisms
- Byzantine Fault Tolerance
- Network architecture

---

Questions? Office hours: Thursdays 14:00-16:00

Thank you

Questions?

Next: Lesson 2 – Distributed Ledger Technology