Lesson 1: What is Blockchain?

Module A: Blockchain Foundations

BSc Blockchain & Cryptocurrency

University Course

2025

Learning Objectives

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

1. Explain what blockchain technology is and how it works
2. Describe the historical evolution from 1991 to 2025
3. Understand the double-spending problem and how blockchain solves it
4. Identify key properties that make blockchain unique
5. Compare centralized vs. decentralized systems
6. Recognize real-world blockchain use cases across industries

Prerequisites: Basic understanding of databases and networks

What is Blockchain? A First Definition

Blockchain Definition

A **blockchain** is a distributed, immutable ledger that records transactions in a chain of blocks, secured by cryptography and maintained by a decentralized network of nodes.

Key Components:

- **Distributed**: No single point of control or failure
- **Immutable**: Once recorded, data cannot be altered retroactively
- **Chain of Blocks**: Data organized in sequential, linked blocks
- **Cryptography**: Mathematical techniques ensure security and integrity
- **Consensus**: Network agrees on the state of the ledger

Think of it as a shared spreadsheet that everyone can read, but no one can cheat.

How Does a Blockchain Work?

Traditional Database

- Central server stores all data
- Single administrator controls access
- Users trust the central authority
- Fast but vulnerable to attacks
- Single point of failure

Example: Your bank's database

Blockchain System

- Data replicated across many nodes
- No single controller (decentralized)
- Users verify through consensus
- More resilient, slower transactions
- No single point of failure

Example: Bitcoin network

Key Insight: Blockchain trades speed for trust and security

Timeline: 1991-2008 (Pre-Bitcoin)

The Building Blocks

- **1991**: Stuart Haber & Scott Stornetta propose cryptographically secured chain of blocks
- **1992**: Merkle trees incorporated to improve efficiency
- **1998**: Nick Szabo designs "Bit Gold" (precursor to Bitcoin)
- **2004**: Hal Finney creates "Reusable Proof of Work" (RPOW)
- **2008**: **Satoshi Nakamoto** publishes Bitcoin whitepaper (Oct 31)

Key Innovation

Bitcoin solved the **double-spending problem** without a trusted third party by combining cryptographic techniques with economic incentives (proof-of-work mining).

Timeline: 2009-2015 (Bitcoin Era)

The First Cryptocurrency

- **2009 Jan**: Bitcoin network launches (Genesis Block mined)
- **2010 May**: First real-world transaction (10,000 BTC for 2 pizzas)
- **2011**: Alternative cryptocurrencies emerge (Litecoin, Namecoin)
- **2013**: Bitcoin price exceeds $1,000 for first time
- **2014**: Ethereum whitepaper published by Vitalik Buterin
- **2015**: Ethereum mainnet launches (introducing smart contracts)

Key Development: Shift from "blockchain as currency" to "blockchain as platform"

Timeline: 2016-2020 (Enterprise Adoption)

Blockchain Goes Mainstream

- **2016**: Enterprise blockchain platforms (Hyperledger Fabric)
- **2017**: ICO boom (Initial Coin Offerings raise $5.6 billion)
- **2018**: Security Token Offerings (STOs) emerge
- **2019**: Facebook announces Libra (later Diem, now defunct)
- **2020**: DeFi (Decentralized Finance) explosion ($15B to $100B+ TVL)
- **2020**: Central banks explore CBDCs (Digital currencies)

Trend: From public cryptocurrencies to private enterprise blockchains

Timeline: 2021-2025 (Maturity & Regulation)

Current State of Blockchain

- **2021**: NFT boom ($25 billion in sales)
- **2022**: Ethereum transitions to Proof-of-Stake ("The Merge")
- **2022**: FTX collapse highlights need for regulation
- **2023**: EU's MiCA regulation passes (Markets in Crypto-Assets)
- **2024**: Bitcoin ETFs approved in major markets
- **2025**: Institutional adoption accelerates (BlackRock, Fidelity)

Current Focus: Scalability, sustainability, regulatory compliance

What is Double-Spending?

Physical Cash

- You have a $10 bill
- You give it to Alice
- Now Alice has the bill
- You **cannot** give the same bill to Bob
- Physical scarcity prevents double-spending

Digital Money (Without Blockchain)

- You have a digital file: "10 coins"
- You send it to Alice
- You **still have** a copy of the file
- You **can** send the same file to Bob
- Problem: Digital files are easily copied

The Challenge

How do we create digital scarcity without a trusted central authority (like a bank)?

Traditional Solution: Trusted Third Party

Banks Prevent Double-Spending

1. Alice wants to send $10 to Bob
2. Alice's bank checks: Does Alice have $10?
3. If YES: Bank deducts $10 from Alice's account
4. Bank adds $10 to Bob's account
5. Bank updates its central ledger

Advantages:

- Fast transactions
- Easy to reverse errors
- Regulatory oversight

Disadvantages:

- Must trust the bank
- Single point of failure
- Censorship possible
- High fees for international transfers

Blockchain Solution: Distributed Consensus

How Bitcoin Prevents Double-Spending

1. Alice broadcasts: "Send 1 BTC to Bob" to the entire network
2. Thousands of nodes receive and verify the transaction
3. Miners collect transactions into a new block
4. Miners compete to solve a cryptographic puzzle (Proof-of-Work)
5. First miner to solve puzzle broadcasts the block
6. Other nodes verify and add block to their chain
7. Bob's wallet shows 1 BTC after 6 confirmations ($\approx$ 60 minutes)

Key Insight: The longest chain (most computational work) represents the true history. Rewriting history requires more computing power than the entire network combined.

Property 1: Decentralization

What It Means:

- No central authority controls the network
- Thousands of nodes maintain copies
- Decisions made by consensus
- Anyone can join the network

Benefits:

- Censorship resistance
- No single point of failure
- Transparent governance

Decentralization is a spectrum, not a binary choice

Trade-offs:

- Slower decision-making
- Harder to upgrade
- More energy-intensive
- Lower transaction throughput

Example: Bitcoin has $\approx$ 15,000 full nodes worldwide

Property 2: Immutability

Immutability Definition

Once data is written to a blockchain and confirmed, it becomes **extremely difficult** (practically impossible) to alter or delete.

How It Works:

1. Each block contains a cryptographic hash of the previous block
2. Changing data in Block N would change its hash
3. This breaks the link to Block N+1
4. Attacker must recalculate hashes for ALL subsequent blocks
5. Attacker must do this faster than the honest network

Practical Implications:

- Permanent audit trail
- Cannot "cook the books"
- Mistakes are difficult to fix
- Requires careful design of smart contracts

Property 3: Transparency

Public Blockchains:

- All transactions visible to everyone
- Anyone can verify the entire history
- Pseudonymous (addresses, not names)
- Full auditability

Example: You can view every Bitcoin transaction ever made on blockchain explorers

Private/Permissioned Blockchains:

- Restricted read/write access
- Known participants only
- Selective transparency
- Enterprise use cases

Example: Hyperledger Fabric for supply chain tracking

Privacy Paradox: Transparent ledger + pseudonymous addresses = partial privacy

Property 4: Security

Multi-Layered Security

1. **Cryptographic Hashing**: SHA-256 ensures data integrity
2. **Digital Signatures**: ECDSA proves ownership of assets
3. **Consensus Mechanisms**: Proof-of-Work/Proof-of-Stake prevent attacks
4. **Network Distribution**: No single point to attack
5. **Economic Incentives**: Attacking costs more than potential gain

Common Attack Vectors:

- **51% Attack**: Attacker controls majority of mining power
- **Smart Contract Bugs**: Coding errors (e.g., DAO hack 2016)
- **Private Key Theft**: Wallet compromise
- **Exchange Hacks**: Centralized weak points

The blockchain itself is secure; the ecosystem around it may not be

System Architecture Comparison

Centralized Systems

- Single entity controls data
- Fast decision-making
- Efficient resource use
- Easy to upgrade
- Clear accountability
- User-friendly interfaces

Examples:

- Traditional banks
- Facebook, Google
- Amazon AWS

Neither is inherently better; it depends on the use case

Decentralized Systems

- Distributed control
- Slower consensus required
- Resource-intensive
- Difficult upgrades
- Shared responsibility
- Often technical UX

Examples:

- Bitcoin, Ethereum
- IPFS (file storage)
- Tor network

When to Use Blockchain vs. Traditional Database

Use Blockchain When:

- Multiple parties need to write data
- Parties don't fully trust each other
- Immutable audit trail required
- Removing intermediaries adds value
- Transparency is critical
- Censorship resistance needed

Good fit: Supply chain tracking, land registries, cross-border payments

Use Traditional Database When:

- Single organization controls data
- High transaction throughput needed
- Data updates/deletions required
- Strong privacy is essential
- Existing solutions work well
- Energy efficiency matters

Poor fit: Social media posts, personal files, high-frequency trading

Blockchain is not a solution looking for a problem; it solves specific trust challenges

Finance & Banking

Cryptocurrency & Payments

- **Bitcoin**: Peer-to-peer electronic cash system (market cap $800B+)
- **Stablecoins**: USDC, USDT (pegged to fiat currencies)
- **Cross-border Payments**: Ripple/XRP for banks
- **Remittances**: Stellar for low-cost international transfers

Decentralized Finance (DeFi)

- **Lending/Borrowing**: Aave, Compound (no credit checks)
- **Decentralized Exchanges**: Uniswap, PancakeSwap
- **Yield Farming**: Earn interest on crypto holdings
- **Derivatives**: Perpetual swaps, options trading

DeFi Total Value Locked (TVL): $50B+ as of 2025

Supply Chain & Logistics

Transparency & Traceability

- **Walmart + IBM Food Trust**: Track produce from farm to store
  - Reduced food recall time from 7 days to 2.2 seconds
- **Maersk + TradeLens**: Shipping container tracking
  - 150+ organizations, 1.5B shipping events logged
- **De Beers**: Diamond provenance on blockchain (Tracr platform)
- **VeChain**: Luxury goods authentication (Louis Vuitton)

Benefits:

- Reduce counterfeiting
- Improve food safety
- Streamline customs processes
- Verify ethical sourcing

Healthcare

Patient Data Management

- **Electronic Health Records**: Patients control access to medical data
- **Drug Traceability**: Combat counterfeit pharmaceuticals
- **Clinical Trials**: Transparent, tamper-proof trial data
- **Insurance Claims**: Automated, fraud-resistant processing

Example Projects:

- **MedRec** (MIT): Patient-centered EHR system
- **Chronicled**: Pharmaceutical supply chain verification
- **Guardtime**: Estonian national health records on blockchain

Challenges: GDPR compliance (right to be forgotten vs. immutability)

Government & Public Services

Digital Identity & Voting

- **Estonia e-Residency**: Digital identity for 100,000+ global citizens
- **Dubai Land Registry**: All real estate on blockchain by 2025
- **Georgia**: Land titles recorded on blockchain since 2016
- **Voatz**: Mobile blockchain voting (limited pilots in West Virginia)

Central Bank Digital Currencies (CBDCs):

- **China**: Digital Yuan (e-CNY) in widespread use
- **European Union**: Digital Euro pilot programs
- **Bahamas**: Sand Dollar (fully launched 2020)

90+ countries exploring CBDCs as of 2025

Other Emerging Use Cases

Energy & Sustainability

- Peer-to-peer energy trading
- Carbon credit tracking
- Renewable energy certificates
- Electric vehicle charging networks

Media & Entertainment

- NFTs (art, music, gaming)
- Royalty distribution
- Content licensing
- Anti-piracy measures

Education

- Academic credential verification
- Lifelong learning records
- Decentralized universities
- Micro-credentialing

Internet of Things (IoT)

- Device identity management
- Secure firmware updates
- Machine-to-machine payments
- Data marketplace

Key Takeaways

What You Should Remember:

1. **Blockchain** is a distributed, immutable ledger secured by cryptography
2. **Historical Evolution**: From 1991 research to 2025 institutional adoption
3. **Double-Spending Solution**: Consensus eliminates need for trusted intermediaries
4. **Core Properties**: Decentralization, immutability, transparency, security
5. **Architecture Choice**: Centralized for speed/efficiency, decentralized for trust
6. **Use Cases**: Finance, supply chain, healthcare, government, and beyond

Critical Insight

Blockchain is not a universal solution. It trades computational efficiency for trust and resilience. The key question is: *Does your problem require decentralized trust?*

Discussion Questions

Consider and discuss:

1. **Trust vs. Efficiency**: In what scenarios is the trade-off worth it?
   - Example: International remittances vs. buying coffee
2. **Privacy Paradox**: How can we balance transparency with user privacy?
   - Explore: Zero-knowledge proofs, private transactions
3. **Environmental Impact**: Is Proof-of-Work's energy consumption justified?
   - Compare: PoW vs. PoS vs. traditional banking infrastructure

Prepare your thoughts for next session's discussion

References & Resources

Foundational Papers

- Nakamoto (2008): *Bitcoin Whitepaper*
- Buterin (2014): *Ethereum Whitepaper*
- Haber & Stornetta (1991): *Timestamping Digital Documents*

Books

- Antonopoulos (2023): *Mastering Bitcoin*
- Narayanan et al. (2016): *Bitcoin and Cryptocurrency Technologies*

Online Resources

- Blockchain.com Explorer
- Ethereum.org Documentation
- CoinDesk Research
- MIT OpenCourseWare: Blockchain

Industry Reports

- Gartner Blockchain Trends
- PwC Blockchain Survey
- CB Insights: Crypto Trends

Next Lesson Preview

L02: Distributed Ledger Technology (DLT)

We will explore:

- Deep dive into DLT concepts and architectures
- The Byzantine Generals Problem and consensus challenges
- Network topologies (centralized, decentralized, distributed)
- Anatomy of a block (headers, transactions, Merkle trees)
- Types of nodes (full nodes, light nodes, miners)
- Permissioned vs. permissionless blockchains

Preparation: Review basic networking concepts and data structures (hash tables, trees)

Thank you

Questions?

See you in Lesson 2: DLT Concepts