

## Lesson 16: Proof of Work

### Module 2: Blockchain Fundamentals

Digital Finance

# The Double-Spending Problem

## Digital Money Challenge:

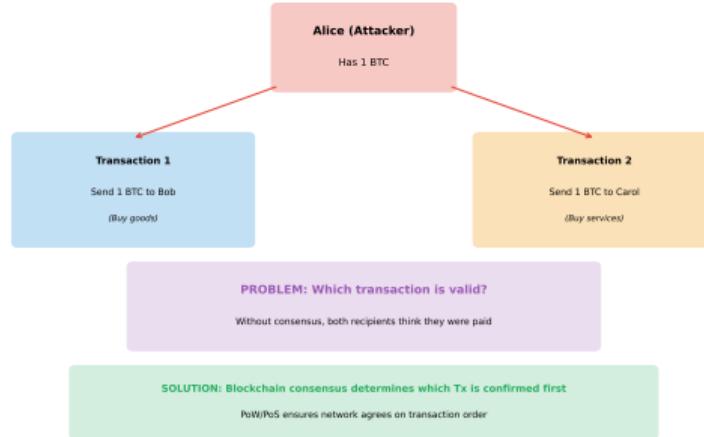
- Digital files are copyable
- How to prevent spending same coin twice?
- Traditional solution: Central authority (bank)

## Decentralized Challenge:

- No central ledger
- Network latency
- Conflicting transactions
- Malicious actors

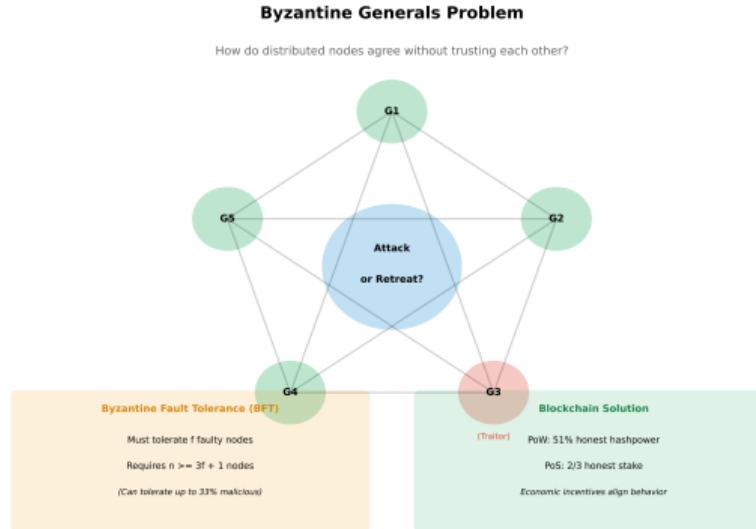
## The Double Spending Problem

Why digital cash needs blockchain consensus



Key concepts from this slide inform practical applications in finance.

# Consensus Problem: Agreeing on Transaction Order



Source: Lamport et al., "The Byzantine Generals Problem" (1982)

## Key Questions:

- Which transaction came first?
- Who decides the canonical order?
- How to prevent censorship or manipulation?
- How to incentivize honest behavior?

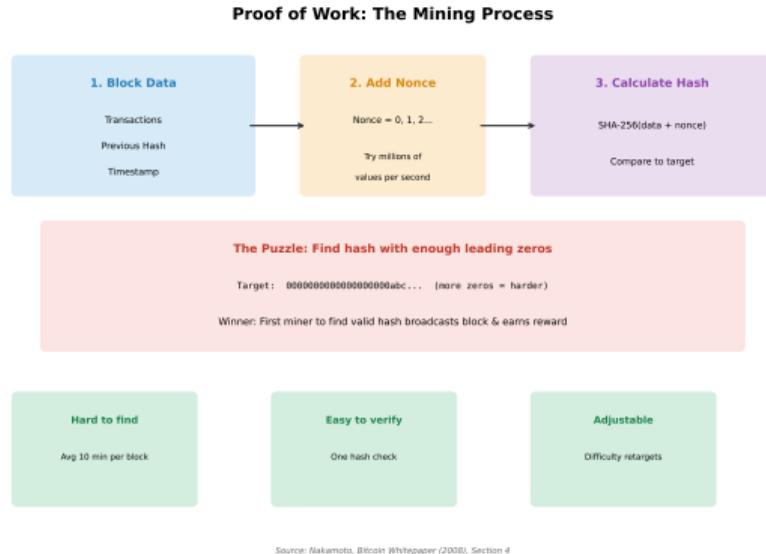
# Proof of Work: The Solution

## Core Idea:

- Make block creation expensive
- Require computational work
- Probability-based selection
- Longest chain wins

## Properties:

- Sybil resistance (one CPU = one vote)
- Objective chain selection rule
- Economic security
- No coordination needed



**Proof-of-Work provides security through computational cost but has energy concerns.**

# Hash Puzzle: Finding theNonce

**Mining Goal:** Find nonce such that block hash is below target

$$\text{SHA256(Block Header)} < \text{Target}$$

**Block Header Contains:**

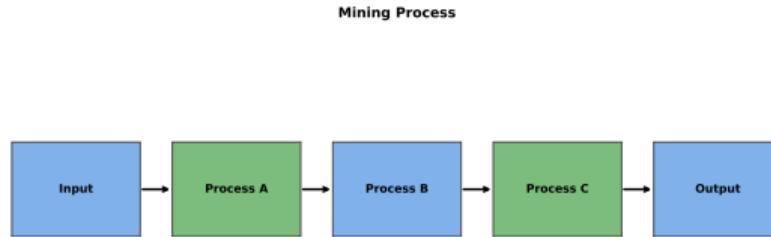
- Previous block hash
- Merkle root (transaction summary)
- Timestamp
- Difficulty target
- **Nonce** (number to vary)

**Example:**

Target: 00000000000000000000f1a2b3c4d...

Hash attempt 1: 8a3f2e1d9c... (too high)

Hash attempt 2: 00000000000000000000a1b2c3d... (success!)



[SYNTHETIC DATA]

## Steps:

- ① Collect transactions from mempool
- ② Build Merkle tree, create block header
- ③ Try different nonces (brute force search)
- ④ Hash until target reached
- ⑤ Broadcast valid block to network

---

Understanding the process flow is key to identifying optimization opportunities.

# Difficulty Target: Controlling Block Time

Target Representation:

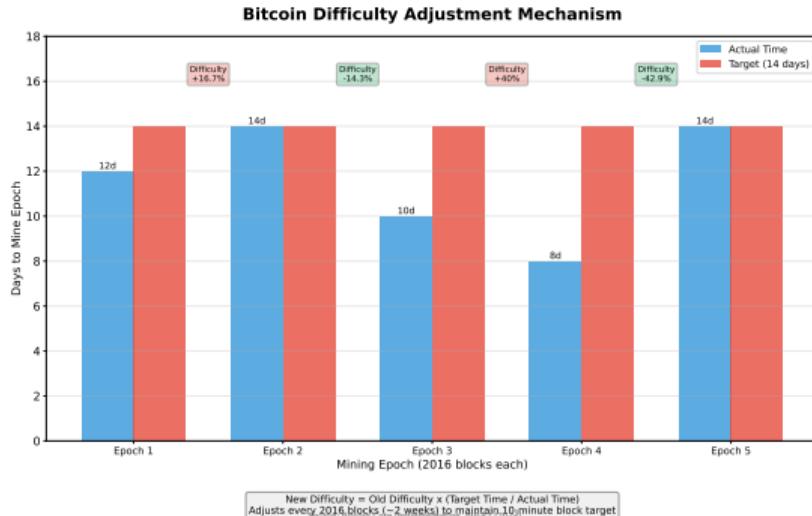
$$\text{Target} = \text{coefficient} \times 2^{8(\text{exponent} - 3)}$$

Difficulty:

$$\text{Difficulty} = \frac{\text{Max Target}}{\text{Current Target}}$$

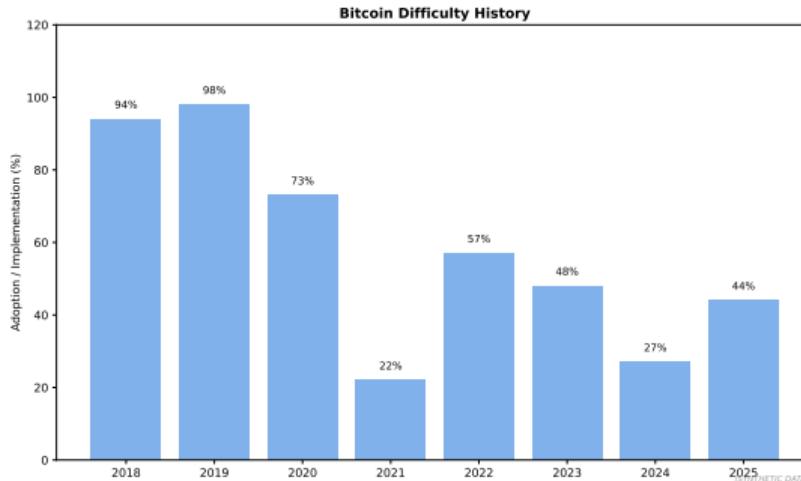
Bitcoin:

- Target block time: 10 minutes
- Adjusts every 2016 blocks (2 weeks)
- Difficulty  $\propto$  total hashrate



Key concepts from this slide inform practical applications in finance.

## Difficulty Over Time: Bitcoin Example



### Observations:

- Exponential growth from 2009 to 2024
- Difficulty in 2024:  $\sim 10^{13}$  times harder than 2009
- Hashrate: From CPU mining to specialized ASICs

---

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

# Mining Probability and Expected Time

**Probability of Success per Hash:**

$$P(\text{success}) = \frac{\text{Target}}{2^{256}}$$

**Expected Number of Hashes:**

$$E[\text{hashes}] = \frac{2^{256}}{\text{Target}} = \text{Difficulty} \times 2^{32}$$

**Expected Time to Find Block:**

$$T = \frac{\text{Difficulty} \times 2^{32}}{\text{Hashrate}}$$

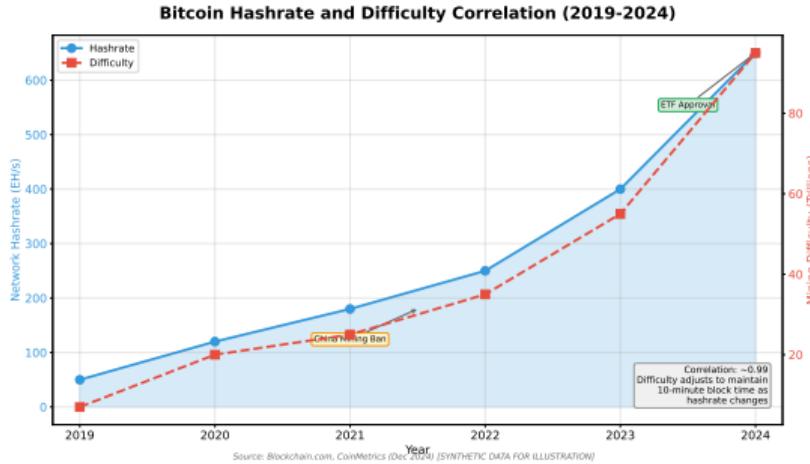
**Example:** Difficulty = 50 trillion, Hashrate = 100 TH/s

$$T = \frac{50 \times 10^{12} \times 2^{32}}{100 \times 10^{12}} \approx 2147 \text{ seconds} \approx 36 \text{ minutes}$$

---

Key concepts from this slide inform practical applications in finance.

# Mining Difficulty vs Hashrate



## Relationship:

- Hashrate increases → blocks found faster
- Difficulty adjusts upward → restores 10-min average
- Self-regulating system maintains predictable issuance

Comparative analysis helps identify the right tool for specific requirements.

# Blockchain Security: The 51% Attack

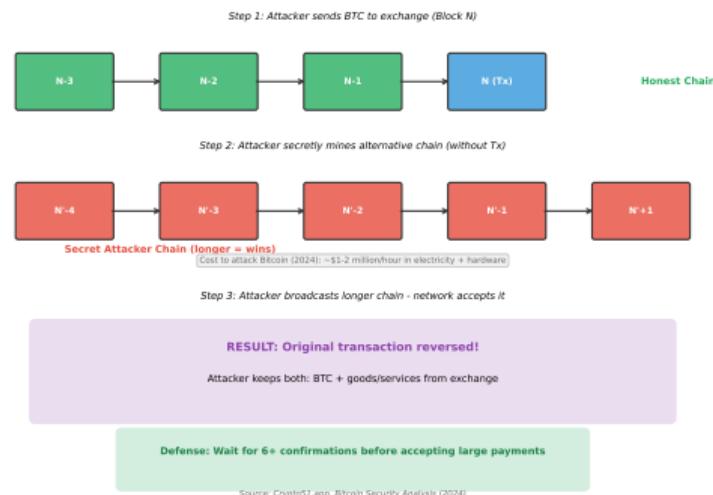
## Attack Scenario:

- Attacker controls >50% hashrate
- Can create longest chain
- Rewrite transaction history
- Double-spend attack

## Limitations:

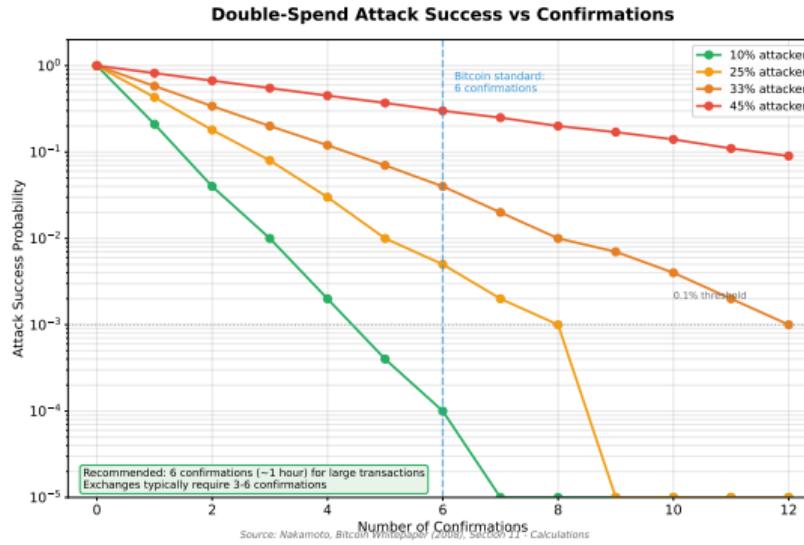
- Cannot steal others' coins
- Cannot create coins from nothing
- Cannot change protocol rules

## 51% Attack: Double Spending via Chain Reorg



Security analysis identifies vulnerabilities and helps design robust systems.

# Confirmation Depth: Security Over Time



## Probability of Reversal:

$$P(\text{reorg after } z \text{ blocks}) \approx \left( \frac{q}{p} \right)^z$$

where  $p$  = honest hashrate fraction,  $q$  = attacker hashrate fraction

**Bitcoin Standard:** 6 confirmations ( $\sim 1$  hour) for high-value transactions

---

Security analysis identifies vulnerabilities and helps design robust systems.

# Mining Economics: Costs and Rewards

## Revenue:

- Block reward: 3.125 BTC (as of 2024, halves every 4 years)
- Transaction fees: Variable (0.1–2 BTC per block)

## Costs:

- Hardware (ASICs): \$3,000–\$15,000 per unit
- Electricity: 3–6 cents per kWh (industrial rates)
- Cooling, maintenance, facility

## Profitability Equation:

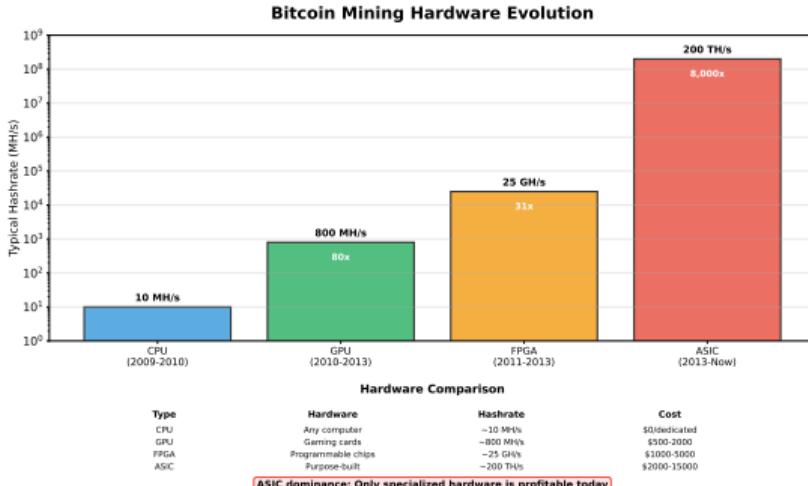
$$\text{Profit} = (\text{Block Reward} + \text{Fees}) \times \text{BTC Price} - \text{Electricity Cost}$$

**Break-even:** Electricity cost  $\approx$  40–60% of revenue at scale

---

Key concepts from this slide inform practical applications in finance.

# Mining Hardware Evolution



- 2009–2010: CPU mining (1–10 MH/s)
- 2010–2012: GPU mining (100–500 MH/s)
- 2013+: ASIC mining (1–200+ TH/s)
- Modern ASICs: Antminer S19 Pro (110 TH/s, 3250W)

Understanding history helps predict future developments in the technology.

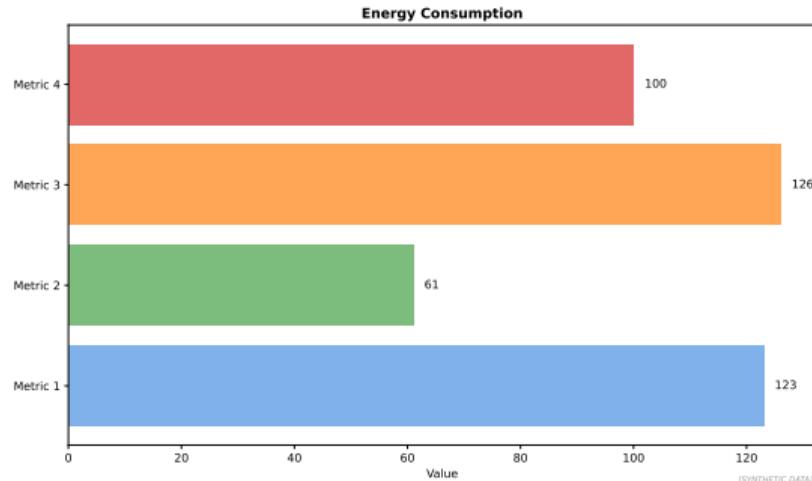
# Energy Consumption: The Elephant in the Room

## Bitcoin Network (2024):

- Total hashrate:  $\sim 600 \text{ EH/s}$
- Power consumption:  $\sim 150 \text{ TWh/year}$
- Comparable to Argentina or Netherlands

## Per Transaction:

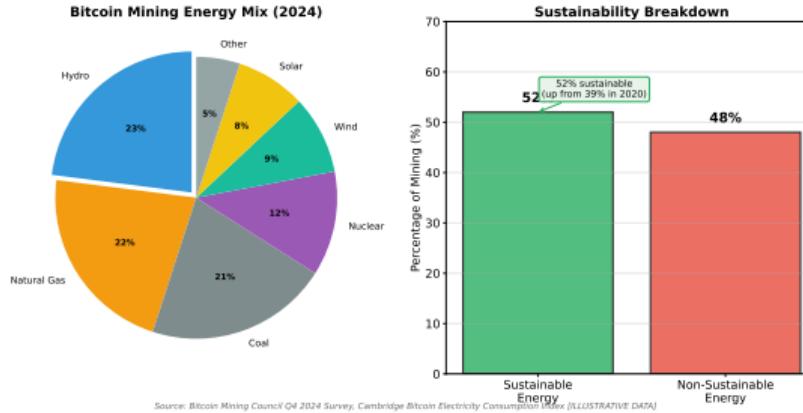
- $\sim 700 \text{ kWh}$  per transaction
- vs Visa:  $\sim 0.001 \text{ kWh}$
- But: Bitcoin = settlement layer



---

Key concepts from this slide inform practical applications in finance.

# Energy Sources: Renewable Debate



## Estimates (2024):

- Renewable energy: 40–60% (hydroelectric, wind, solar)
- Natural gas: 20–30%
- Coal: 10–20%
- Nuclear: 5–10%

**Trend:** Miners seek cheap, stranded renewable energy (e.g., flare gas, curtailed hydro)

---

Key concepts from this slide inform practical applications in finance.

# Environmental Criticisms and Counterarguments

## Criticisms:

- Massive carbon footprint
- E-waste from obsolete ASICs
- Inefficient compared to databases
- Competes with useful computing

## Counterarguments:

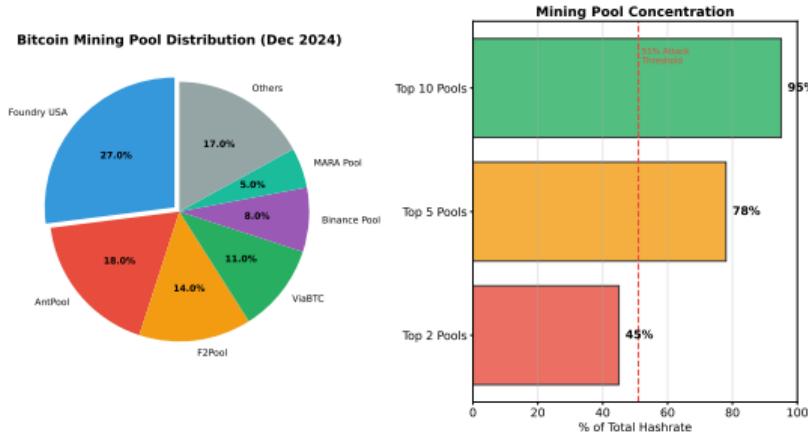
- Energy = security (makes attacks expensive)
- Incentivizes renewable buildup
- Banking system also energy-intensive
- Enables censorship-resistant money

**Trade-off:** Security vs energy efficiency (Proof of Stake addresses this)

---

Key concepts from this slide inform practical applications in finance.

# Mining Centralization Risks



## Concerns:

- Top 5 pools control >70% hashrate
- Geographic concentration (China historically dominant, now US/Kazakhstan)
- Pool operators could censor transactions

**Mitigation:** Miners can switch pools, Stratum V2 protocol improves decentralization

---

Risk management is essential for financial stability and profitability.

# Selfish Mining Attack

## Strategy:

- ① Miner finds block, keeps secret
- ② Continues mining on private chain
- ③ Reveals when ahead by 2+ blocks
- ④ Honest chain orphaned



## Result:

- Unfair revenue (more than hashrate share)
- Effective with >25% hashrate
- Wastes other miners' work

---

Security analysis identifies vulnerabilities and helps design robust systems.

# Alternatives to Proof of Work

Mechanism	Selection	Pros	Cons
Proof of Work	Computational power	Proven security	Energy intensive
Proof of Stake	Staked capital	Energy efficient	Rich get richer
Proof of Authority	Approved validators	Fast, low energy	Centralized
Proof of Space	Disk storage	Lower energy	Unproven security

**Note:** Ethereum switched from PoW to PoS in 2022 (The Merge)

---

**Proof-of-Work provides security through computational cost but has energy concerns.**

- **Double-Spending Problem:** Solved by probabilistic consensus via PoW
- **Mining:** Find nonce making block hash < target (SHA256 puzzle)
- **Difficulty:** Auto-adjusts to maintain constant block time (10 min for Bitcoin)
- **Security:** 51% attack possible but expensive; confirmation depth increases safety
- **Economics:** Revenue (block reward + fees) vs costs (hardware + electricity)
- **Energy Debate:** ~150 TWh/year, trade-off between security and efficiency

**Next Lesson:** Proof of Stake – energy-efficient alternative consensus