

Proof of Work Consensus

BSc Blockchain, Crypto Economy & NFTs

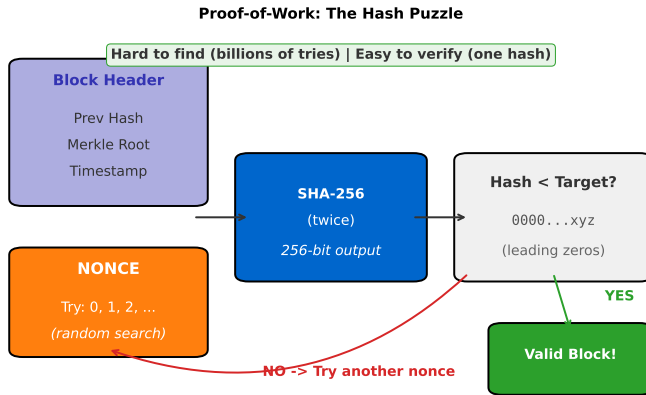
Course Instructor

Module A: Blockchain Foundations

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

- Explain the proof-of-work consensus mechanism
- Describe the mining process and nonce searching
- Understand difficulty adjustment and its purpose
- Calculate mining profitability and hash rate economics
- Recognize the security guarantees and vulnerabilities of PoW
- Evaluate the 51% attack threat model
- Discuss energy consumption and environmental impact

What is Proof of Work?



Core Concept: Find a nonce such that the hash of block header is below the target. No shortcut: must try nonces randomly until one works.

Key Properties:

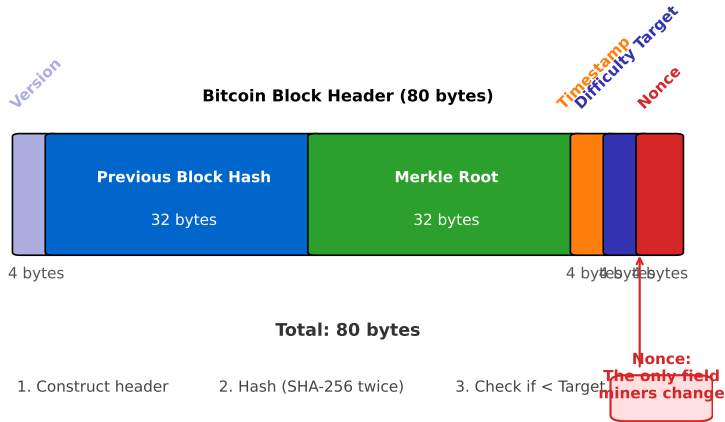
- ① **Asymmetry:** Hard to find, easy to verify
- ② **Probabilistic:** Expected time to find solution, no guarantee
- ③ **Adjustable difficulty:** Target changes to maintain block time
- ④ **Progress-free:** Past attempts do not help future attempts

Mathematical Formulation:

$$\text{SHA-256}(\text{SHA-256}(\text{BlockHeader})) < \text{Target}$$

Analogy: Rolling dice until you get 10 sixes in a row. Each roll is independent. Expected number of attempts: 6^{10} .
Verification: just look at the result.

Bitcoin Block Header Structure



Mining Process: Construct block → Set timestamp/difficulty → Try nonces → If hash $<$ target: success, else repeat.

Nonce Space Exhaustion:

- 4 bytes = 2^{32} = 4.3 billion possible nonces
- Modern ASICs exceed this in milliseconds
- Solution: modify coinbase transaction (extra nonce), recompute Merkle root

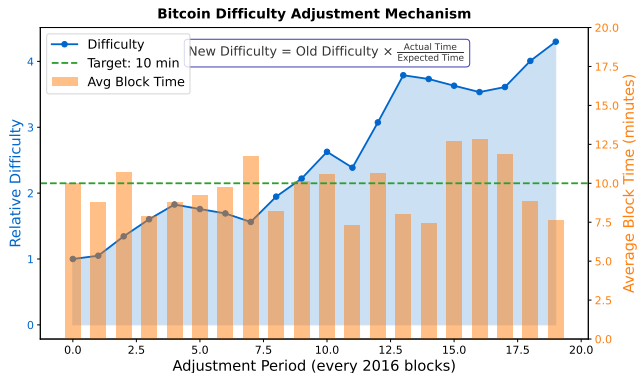
Merkle Trees:

- Commit to all transactions with single 32-byte hash
- Tree height: $\log_2(n)$ for n transactions
- Proof size: $\log_2(n)$ hashes to prove inclusion
- Example: 1000 transactions \rightarrow 10 hashes (\sim 320 bytes proof)

Extra Nonce Trick:

- Miners modify coinbase transaction (includes extra nonce field)
- Recompute Merkle root (different root for each extra nonce)
- Expands search space beyond 2^{32} nonces

Difficulty Adjustment



Adjustment Rule (Every 2016 Blocks):

$$\text{New Target} = \text{Old Target} \times \frac{\text{Actual Time}}{\text{Expected Time (20,160 min)}}$$

Clamped to $[T/4, T \times 4]$ to prevent extreme changes.

Hash Rate and Mining Probability

Hash Rate:

- Number of hashes computed per second
- Units: H/s, KH/s, MH/s, GH/s, TH/s, PH/s, EH/s
- Bitcoin network (late 2024): ~ 700 EH/s (all-time high)

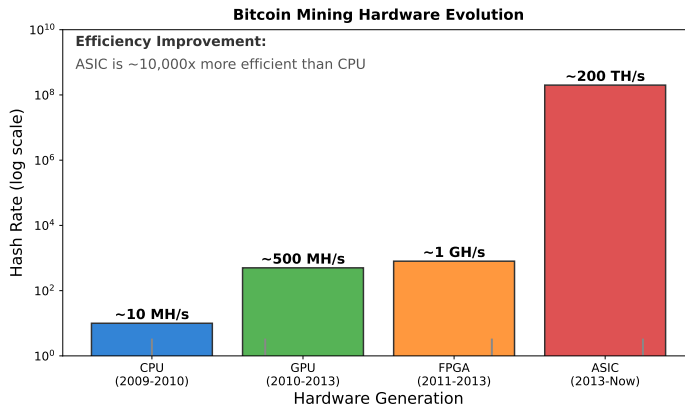
Mining Probability:

$$P(\text{find block}) = \frac{\text{Your Hash Rate}}{\text{Network Hash Rate}}$$

Example:

- Miner: 100 TH/s, Network: 500 EH/s
- Probability: $0.0000002 = 0.00002\%$
- Expected time to find block: ~ 100 years solo mining
- Solution: Join mining pools for steady income

Mining Hardware Evolution



Implications: Mining centralization, high barrier to entry, geographic concentration in low-electricity regions.

Revenue:

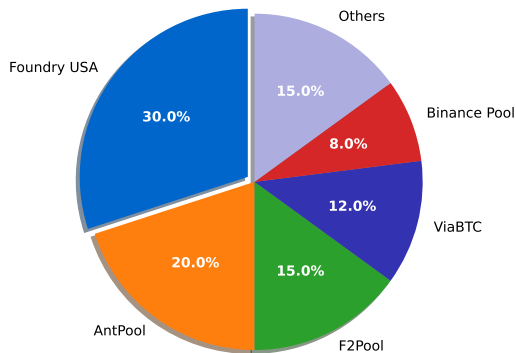
$$\text{Daily Revenue} = \frac{\text{Hash Rate}}{\text{Network Hash Rate}} \times 144 \times (\text{Reward} + \text{Fees})$$

Example (Antminer S19 Pro):

- Hash rate: 110 TH/s, Power: 3250 W = 78 kWh/day
- Electricity: $\$0.05/\text{kWh} \times 78 = \$3.90/\text{day}$
- Revenue (@\$40k BTC): $\sim \$7.92/\text{day}$
- Profit: $\$4.02/\text{day}$, Payback: ~ 2 years

Risk Factors: BTC price volatility, difficulty increases, hardware obsolescence, electricity cost changes.

Bitcoin Mining Pool Distribution (2024)



Top 5 pools control ~85% of hash rate

(Miners can switch pools - pools do not own hardware)

Payout Schemes: PPS (fixed/share), PPLNS (share recent blocks), FPPS (PPS + fees).

Why Pools Exist:

- Solo mining: high variance (might wait years for block)
- Pooled mining: steady income (proportional to hash rate)

Pool Operation:

- 1 Pool coordinator distributes mining tasks (shares)
- 2 Miners submit partial solutions (lower difficulty)
- 3 Pool tracks contribution of each miner
- 4 When pool finds block, reward distributed proportionally
- 5 Pool takes fee (1-3%)

Centralization Concern:

- Pools do not own hardware (miners can switch pools)
- Mitigation: decentralized pool protocols (P2Pool, Stratum V2)

Block Reward Components:

$$\text{Total Reward} = \text{Block Subsidy} + \text{Transaction Fees}$$

Period	Reward	Cumulative Supply
2009-2012	50 BTC	10.5M BTC
2012-2016	25 BTC	15.75M BTC
2016-2020	12.5 BTC	18.375M BTC
2020-2024	6.25 BTC	19.6875M BTC
2024-2028 (current)	3.125 BTC	20.34M BTC

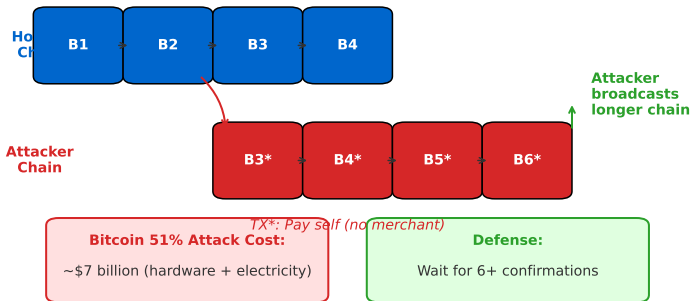
Future: Transaction fees must eventually sustain mining as block subsidy approaches zero (~2140).

The 51% Attack

51% Attack: Double-Spend Mechanism

Double-Spend Attack Timeline

TX: Pay merchant



CAN do: Double-spend, censor transactions.

CANNOT do: Steal coins without keys, create coins out of thin air.

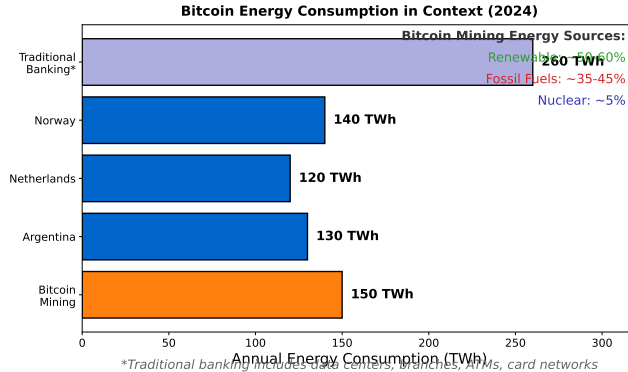
Cost of Attack (Bitcoin):

- Need 255 EH/s (>50% of network)
- Hardware: ~ 2.3 million ASICs = \$6.9 billion
- Electricity (1 week): \sim \$63 million
- Total: \sim \$7 billion

Consequences:

- Attack becomes public immediately
- Bitcoin price crashes (attacker's hardware worthless)
- Community may hard fork (bricks attacker's ASICs)

Vulnerable Chains: Small PoW chains, shared mining algorithms. Historical: Bitcoin Gold, Ethereum Classic, Verge.



Counterarguments: Incentivizes renewable development, facilitates grid balancing, security proportional to value.

ASIC-Resistant Algorithms:

- **Scrypt (Litecoin):** Memory-hard hashing (ASICs developed 2014)
- **Ethash (Ethereum pre-merge):** Memory-hard with large DAG
- **RandomX (Monero):** CPU-optimized, frequently updated

Trade-offs:

- ASIC resistance → lower security per watt
- Easier for botnets to attack (commodity hardware)
- Algorithm changes create hard fork risks
- Debate: specialization increases security investment

- Proof-of-work provides Sybil resistance via computational cost
- Mining searches for nonces to produce valid block hashes
- Difficulty adjusts every 2016 blocks to maintain 10-minute block time
- Mining profitability depends on hash rate, electricity cost, and BTC price
- 51% attacks are economically infeasible for large PoW chains
- Block rewards halve every 4 years, shifting incentives toward fees
- Energy consumption is significant but incentivizes renewable energy

Core Insight: Proof-of-work converts energy into cryptographic security. The cost of attacking equals cumulative computational work by honest miners.

- 1 Why is proof-of-work described as “progress-free”?
- 2 How does difficulty adjustment make Bitcoin resilient to hash rate fluctuations?
- 3 What would happen if block rewards fell to zero but fees remained low?
- 4 Is ASIC mining centralization a threat to Bitcoin’s decentralization?
- 5 How does mining pool concentration differ from miner concentration?
- 6 Can proof-of-work be justified from an environmental perspective?

Lab activities:

- Install and configure MetaMask wallet
- Understand seed phrase security and backup
- Connect to Ethereum testnet (Sepolia)
- Obtain testnet ETH from faucets
- Execute first testnet transaction

Preparation:

- Install a modern web browser (Chrome, Firefox, Brave)
- Review public-private key concepts from Lesson 5
- Prepare a secure location for seed phrase backup