L03: Bitcoin Deep Dive

Extended Slides – BSc Blockchain Course

Digital Finance

2026

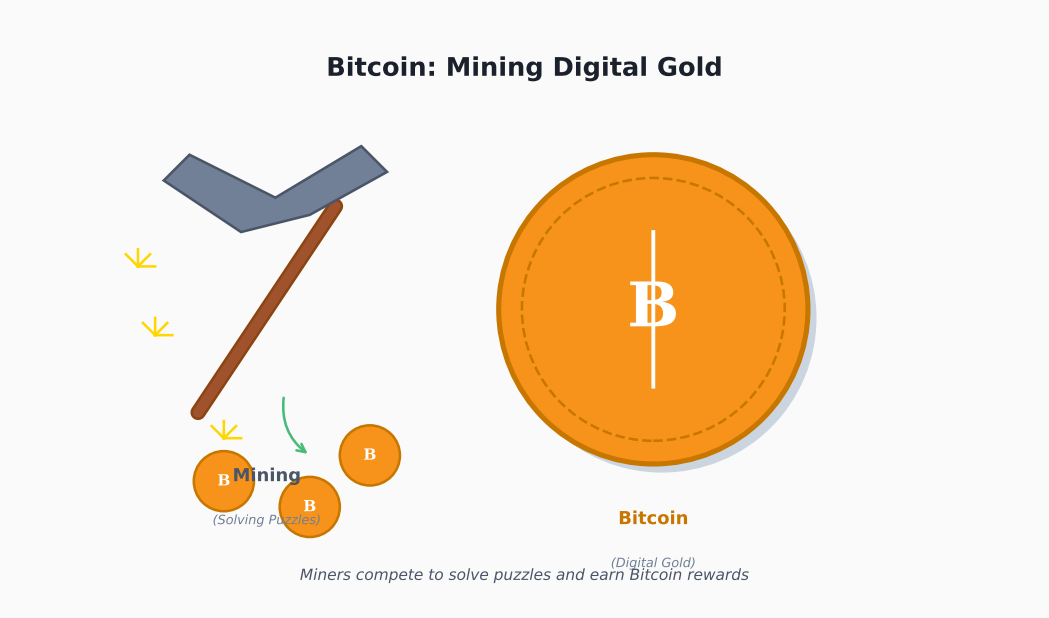
Learning Objectives

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

1. Explain the UTXO model and transaction structure
2. Describe Bitcoin block structure and mining process
3. Understand difficulty adjustment and reward schedule
4. Analyze the fee market and mempool dynamics
5. Explain chain selection rules and fork resolution

Prerequisites: L02 Cryptographic Foundations.

The First Cryptocurrency



Purpose: Bitcoin introduced the world to decentralized digital money. Understanding its design reveals the core principles that all cryptocurrencies build upon.

A $1 trillion asset class built on elegant computer science.

Bitcoin Architecture Overview

Core Components

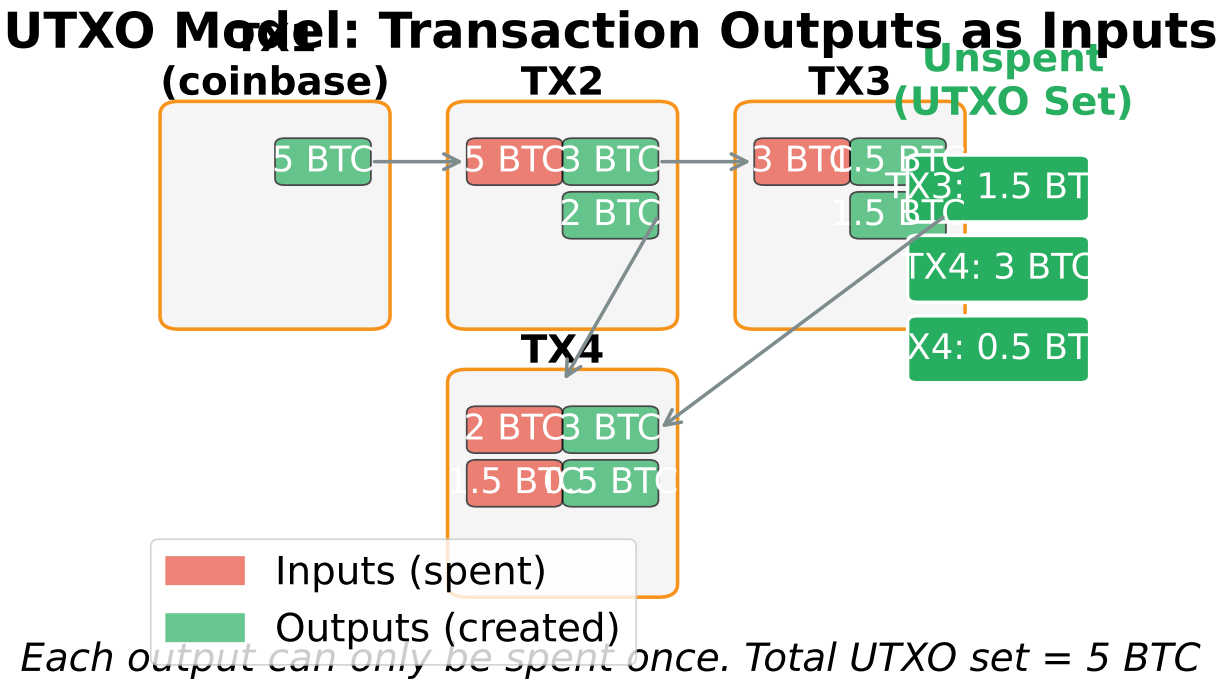
- **Transactions:** Transfer value between addresses
- **Blocks:** Bundle transactions with proof-of-work
- **Chain:** Linked blocks forming immutable history
- **Network:** P2P nodes validating and relaying
- **Miners:** Create new blocks, earn rewards

Design Philosophy:

- Simple, conservative, secure
- Prioritize decentralization over features
- Slow, deliberate upgrades

"Be your own bank" – Bitcoin enables self-custody.

UTXO Model Explained



Each output can only be spent once. Total UTXO set = 5 BTC

UTXO = Unspent Transaction Output. Each can only be spent once.

UTXO vs Account Model

UTXO Model (Bitcoin):

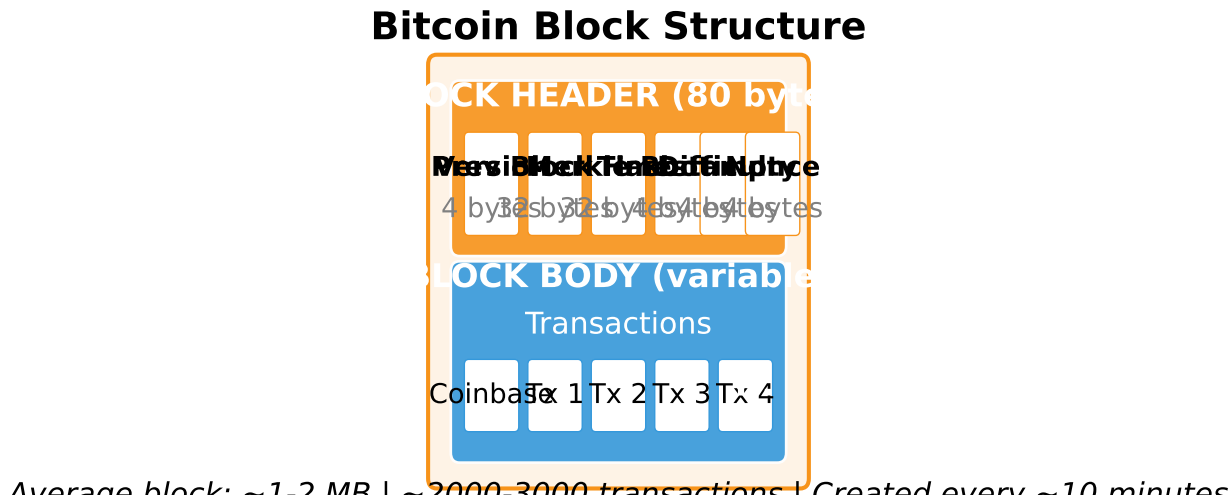
- Track individual outputs
- Better privacy (new address per tx)
- Parallel transaction validation
- More complex wallet logic

Account Model (Ethereum):

- Track balances per address
- Simpler mental model
- Sequential nonce required
- Easier smart contract state

Neither is objectively better – different trade-offs.

Bitcoin Block Structure



Average block: ~1-2 MB | ~2000-3000 transactions | Created every ~10 minutes

Block header is always 80 bytes; body size varies with transaction count.

Block Header Fields

80-byte Header Contains:

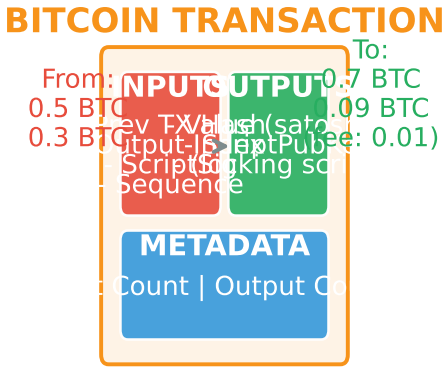
1. **Version (4B):** Protocol version
2. **Previous Block Hash (32B):** Links to parent
3. **Merkle Root (32B):** Summarizes all transactions
4. **Timestamp (4B):** Block creation time
5. **Difficulty Target (4B):** PoW requirement
6. **Nonce (4B):** Mining solution

Block Hash: SHA256(SHA256(header))

Only the header is hashed for proof-of-work.

Transaction Anatomy

Bitcoin Transaction Structure



Inputs unlock funds | Outputs create new UTXOs | Fee = Sum(inputs) - Sum(outputs)

Inputs reference previous outputs; outputs create new UTXOs.

Transaction Components

Inputs (spending UTXOs):

- Previous transaction hash
- Output index (which output)
- ScriptSig (unlocking script)
- Sequence number

Outputs (creating UTXOs):

- Value (in satoshis)
- ScriptPubKey (locking script)

Transaction Fee:

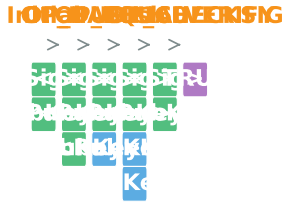
$$\text{Fee} = \sum \text{Input Values} - \sum \text{Output Values}$$

1 BTC = 100,000,000 satoshis.

Bitcoin Script

P2PKH Script Execution (Pay-to-Public-Key-Hash)

ScriptPubKey (Locking): OP_DUP OP_HASH160 <PubKeyHash> OP_EQUALVERIFY OP_CHECKSIG
ScriptSig (Unlocking): <Signature> <PublicKey>



Common Opcodes:

OP_DUP Duplicate top stack item
OP_HASH160 SHA256 then RIPEMD160
OP_EQUALVERIFY Verify equality
OP_CHECKSIG Verify ECDSA signature

Stack-based, intentionally NOT Turing-complete for security.

Script Types

Common Script Patterns:

- **P2PKH:** Pay to Public Key Hash (starts with 1)
- **P2SH:** Pay to Script Hash (starts with 3)
- **P2WPKH:** Native SegWit (starts with bc1q)
- **P2TR:** Taproot (starts with bc1p)

Why Not Turing-Complete?

- Prevents infinite loops
- Deterministic execution
- Simpler security analysis
- Lower attack surface

Bitcoin Script has 100 opcodes, many disabled for safety.

Mining Process

Proof-of-Work Algorithm:

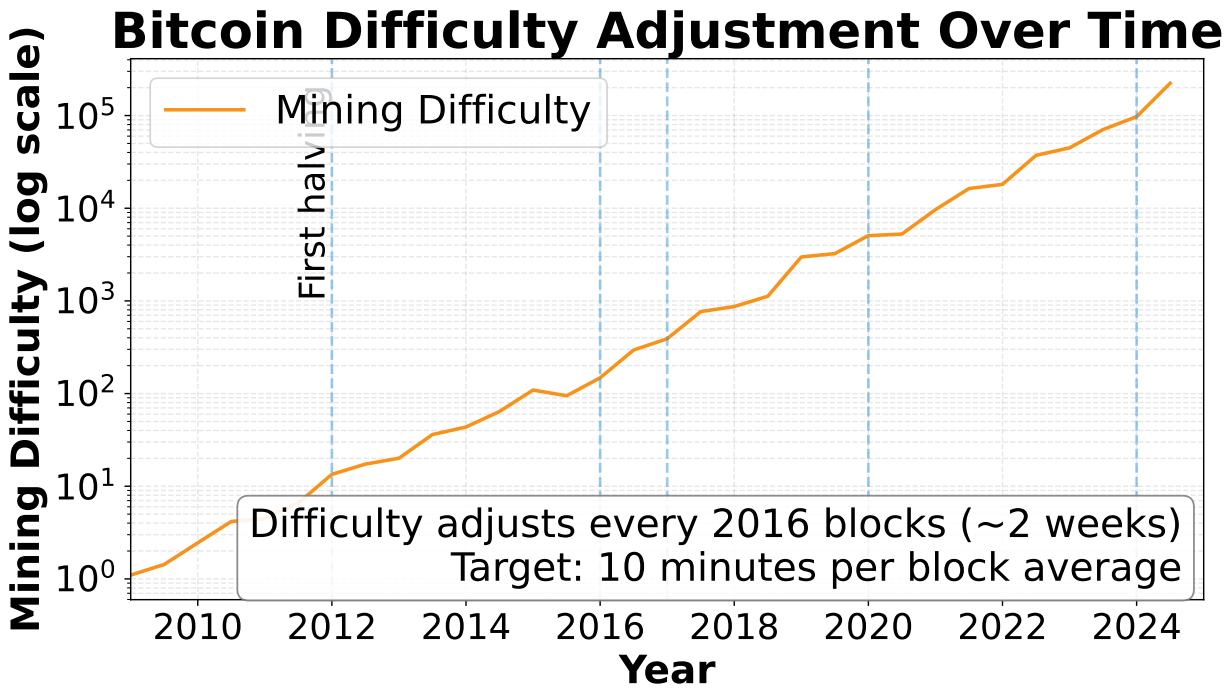
1. Collect transactions from mempool
2. Build block with coinbase transaction
3. Hash header: $H = \text{SHA256}^2(\text{header})$
4. Check if $H < \text{target}$
5. If not, increment nonce and repeat
6. If found, broadcast block to network

Current Statistics (2025):

- Hash rate: ~ 1 ZH/s (zettahash per second, or 1000+ EH/s)
- Energy: ~ 170 TWh/year
- Block time: 10 minutes average

Mining is a lottery – more hashes = more tickets.

Difficulty Adjustment



Adjusts every 2016 blocks (∼2 weeks) to maintain 10-minute target.

Difficulty Algorithm

Adjustment Formula:

$$D_{new} = D_{old} \times \frac{T_{actual}}{T_{target}}$$

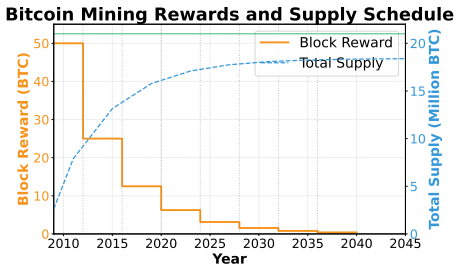
- $T_{target} = 2016 \times 10$ minutes $= 20160$ minutes
- Capped at 4x increase or 0.25x decrease per period

Example:

- If last 2016 blocks took 10080 min (7 days)
- Blocks are too fast (should be 14 days)
- Difficulty doubles to slow things down

Self-adjusting system maintains stability as hash rate changes.

Mining Reward Schedule



21M Cap

Block reward halves every 210,000 blocks (∼4 years).

Bitcoin Supply Schedule

Halving Events:

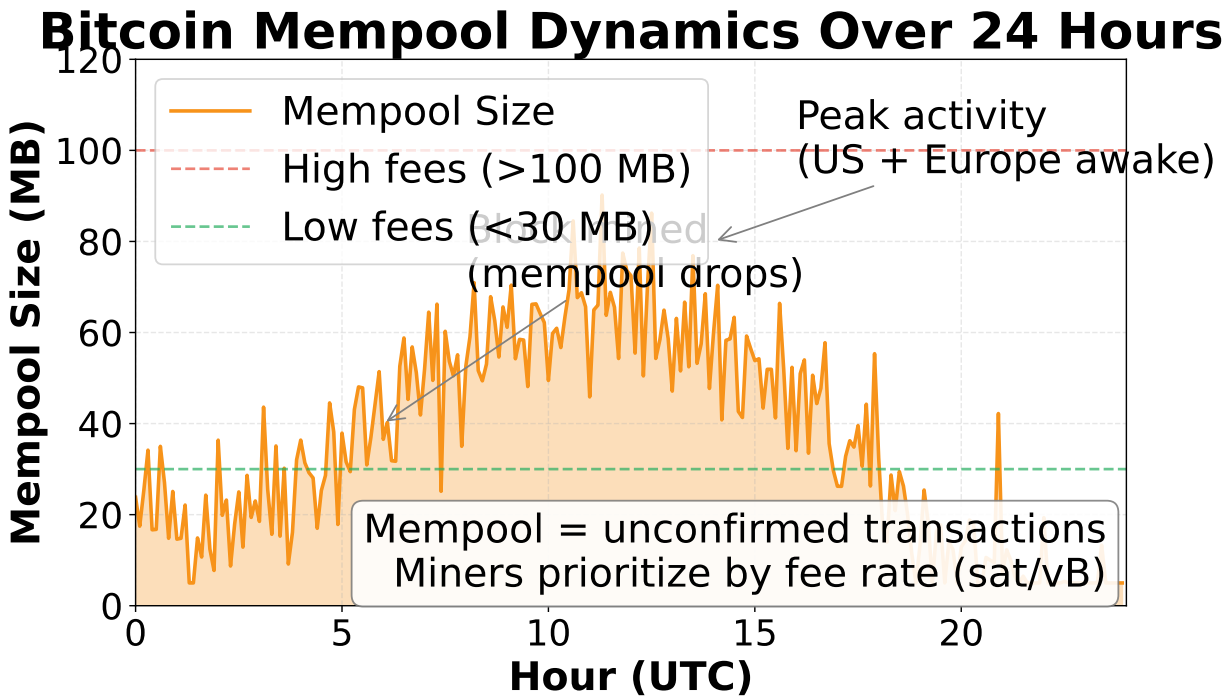
Year	Block Reward	Supply (%)
2009-2012	50 BTC	50%
2012-2016	25 BTC	75%
2016-2020	12.5 BTC	87.5%
2020-2024	6.25 BTC	93.75%
2024-2028	3.125 BTC	96.875%

Key Facts:

- Total supply: 21,000,000 BTC
- Current supply: ∼20M BTC (95%)
- Last bitcoin: ∼year 2140

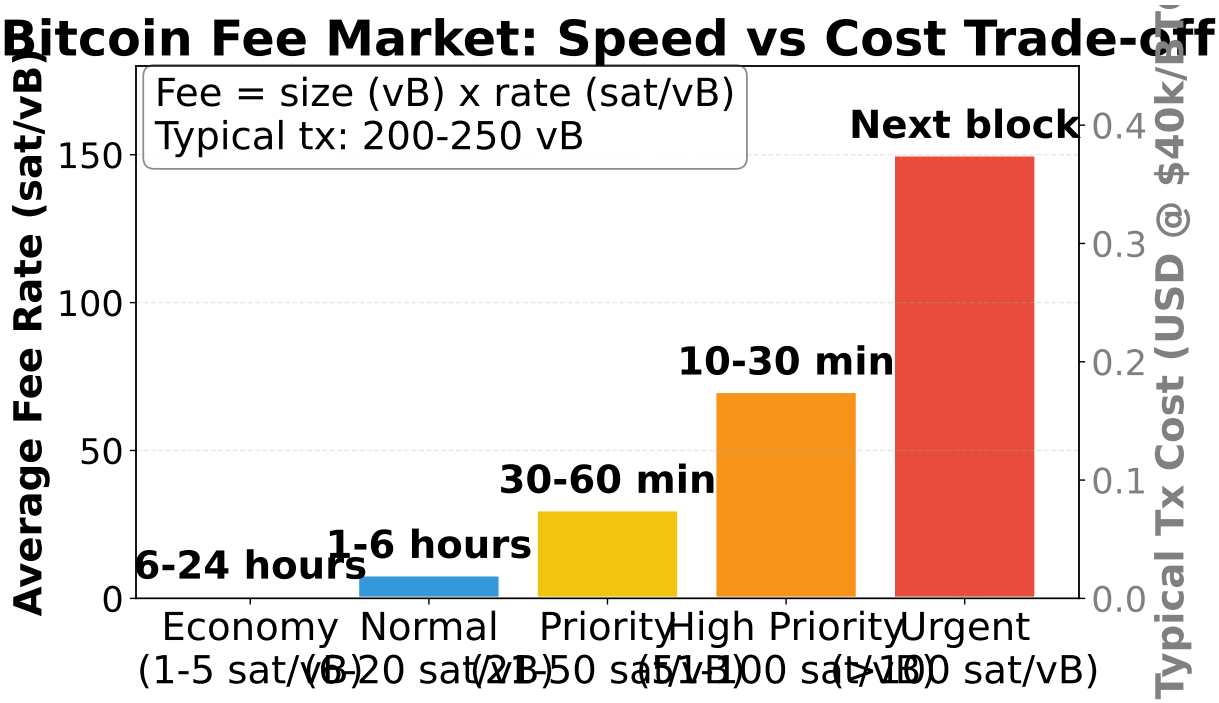
Predictable monetary policy – no central bank discretion.

Mempool Dynamics



Mempool = unconfirmed transactions waiting to be mined.

Fee Market



Fee rate (sat/vB) determines priority, not absolute fee.

Transaction Priority

How Miners Select Transactions:

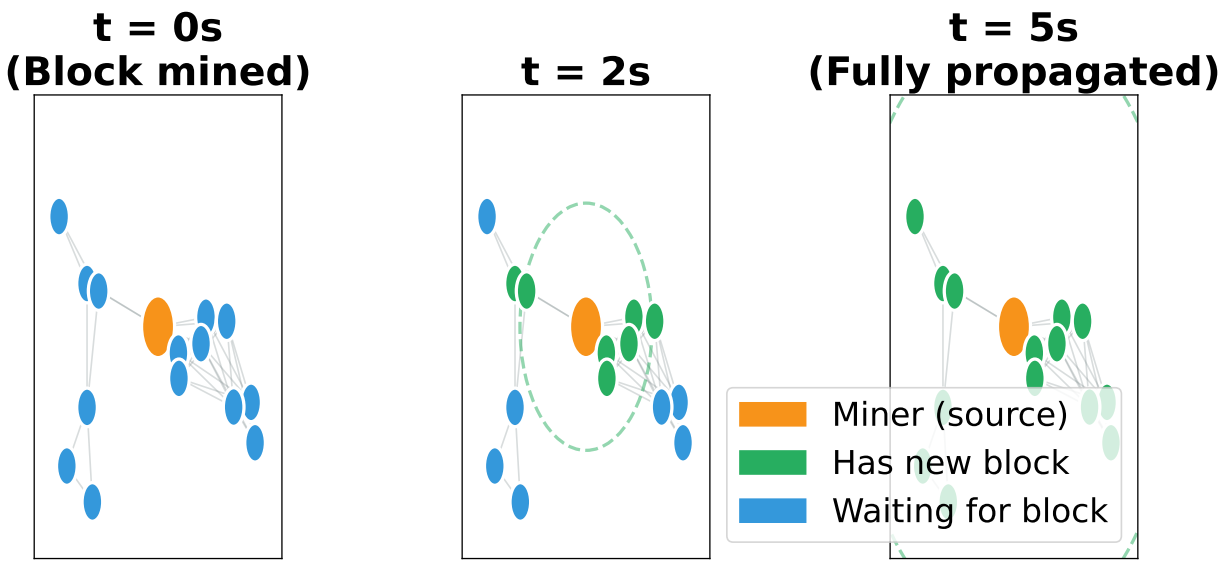
1. Sort mempool by fee rate (sat/vB)
2. Fill block with highest-paying transactions
3. Stop when block is full (1 MB / 4 MW)

Fee Estimation:

- Wallets estimate based on recent blocks
- APIs: mempool.space, blockchain.info
- RBF (Replace-By-Fee) allows fee bumping

SegWit and batching reduce effective transaction size.

Block Propagation



Blocks propagate globally in 2-5 seconds via P2P network.

Network Topology

Node Types:

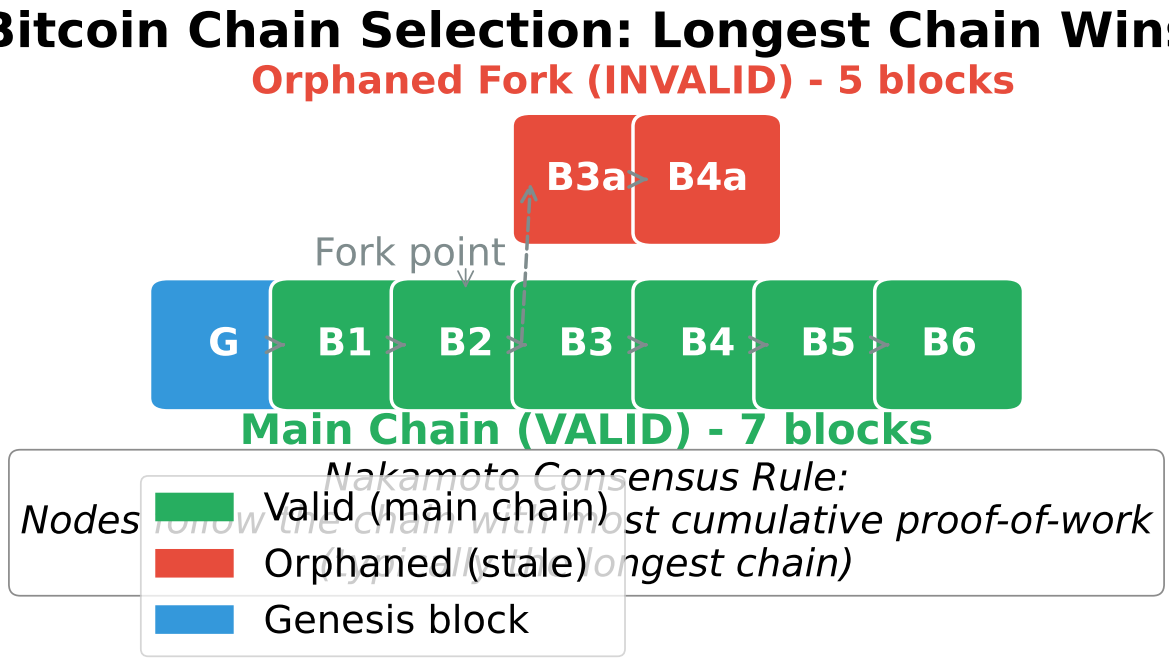
- **Full nodes:** Validate everything, store full chain
- **Mining nodes:** Full nodes that create blocks
- **SPV clients:** Light clients, trust headers only
- **Archive nodes:** Store all historical states

Current Network (2025):

- $\sim$20,000–25,000 reachable full nodes
- $\sim$50,000+ total nodes
- Majority run Bitcoin Core

Anyone can run a full node – this is decentralization.

Chain Selection



Nakamoto consensus: follow the chain with most proof-of-work.

Fork Resolution

Types of Forks:

- **Temporary:** Two miners find blocks simultaneously
- **Soft fork:** Backward-compatible rule tightening
- **Hard fork:** Non-backward-compatible change

Resolution Process:

1. Nodes see competing chains
2. Each builds on the chain they saw first
3. Once one chain gets ahead, others switch
4. Orphaned blocks are discarded

Confirmations reduce reorganization risk exponentially.

Confirmation Security

Probability of Reorganization:

Confirmations	Attacker Needs	Risk Level
1	51% hashrate	High
2	26% (with luck)	Moderate
6	Extremely unlikely	Low
12	Near zero	Very low

Common

Standards:

- Small tx: 1-2 confirmations
- Medium tx: 3-4 confirmations
- Large tx: 6+ confirmations
- Exchanges: Often 3-6 confirmations

"6 confirmations" became standard from Satoshi's analysis.

SegWit (Segregated Witness)

What Changed (2017):

- Witness data moved outside main block
- New weight metric: 4 MW limit (was 1 MB)
- Fixes transaction malleability
- Enables Lightning Network

Benefits:

- $\sim$40% more transactions per block
- Lower fees for SegWit transactions
- Better script versioning

SegWit was a soft fork – old nodes still validate.

Taproot (2021)

Latest Major Upgrade:

- Schnorr signatures (more efficient than ECDSA)
- MAST (Merkelized Abstract Syntax Trees)
- Better privacy for complex scripts
- Key aggregation for multisig

Benefits:

- All transactions look similar on-chain
- Cheaper multisig and complex contracts
- Foundation for future upgrades

Adoption growing steadily – check mempool.space for current statistics.

Key Takeaways

Remember These Points

1. UTXO model: track outputs, not balances
2. Blocks: 80-byte header + variable body
3. Mining: SHA256 lottery with difficulty adjustment
4. Supply: 21M cap via halving schedule
5. Fees: market-based priority system
6. Chain: longest (most work) wins

Next Lesson: Consensus Mechanisms – PoW, PoS, and alternatives.

Bitcoin's design choices prioritize security and decentralization.