Bitcoin Deep Dive

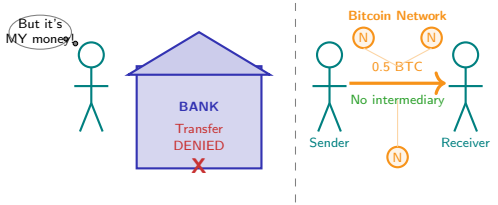
A Five-Minute Overview

BSc Blockchain Course

What If Money Had No Central Controller?

Every digital payment you make passes through a gatekeeper: a bank, a card network, a payment processor. That gatekeeper can freeze your account, reverse your transaction, or simply say "no" – and you have no recourse. **The problem with centralised money:**

- **Permission required:** every transfer needs approval from an intermediary who can refuse.
- **Single point of failure:** one server outage, one policy change, one court order stops everyone.
- **Reversibility:** chargebacks protect buyers but let institutions rewrite history.



Left: permission required. Right: permission impossible to deny.

Bitcoin replaces institutional trust with cryptographic proof – but trustless money means no password resets, no customer support, and no reversals.

Key insight: Bitcoin is not faster or cheaper than banks – it is uncensorable. No single entity can block a valid transaction.

How Does Bitcoin Track Value Without a Bank?

Two fundamentally different ways to represent money:

Property	Account Model (Banks, Ethereum)	UTXO Model (Bitcoin)
Balance stored as	Single number	Set of unspent outputs
Analogy	Bank statement	Pile of coins in a jar
Partial spending	Yes (debit any)	No (must spend whole UTXO)
Change returned	Not needed	New UTXO to sender
Privacy	One address	Fresh address per tx
Parallelism	Sequential	Naturally parallel
Double-spend check	Check nonce	Check if UTXO exists

Why Bitcoin chose UTXOs:

Each UTXO is a discrete, independently verifiable unit of value. Nodes do not need to know your total balance – they only check whether a specific output has been spent. This makes validation massively parallelisable across thousands of nodes.

You do not have a Bitcoin "balance." You have a collection of unspent outputs whose sum is your balance – like coins in a jar, not a number on a screen.

A UTXO transaction step by step:

1. **Select inputs:** Alice owns two UTXOs worth 0.3 and 0.5 BTC. She wants to send 0.6 BTC to Bob.
2. **Consume both:** The transaction destroys both UTXOs entirely (0.8 BTC total input).
3. **Create outputs:** Two new UTXOs are created – 0.6 BTC locked to Bob's key, 0.19 BTC returned to Alice as change.
4. **Fee is implicit:** The gap between inputs and outputs (0.01 BTC) goes to the miner. No fee field exists.

Every BTC in circulation can be traced back through an unbroken chain of UTXOs to the coinbase transaction that created it.

UTXO = Unspent Transaction Output. Bitcoin's entire state is the set of all UTXOs – currently about 80 million entries.

How Does Mining Secure the Network Without a Boss?

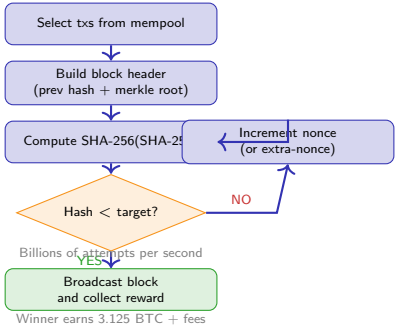
Miners compete to find a **nonce** – a 32-bit number appended to the block header – such that the double hash falls below a target threshold:

$$\text{SHA-256}(\text{SHA-256}(\text{header})) < \text{target}$$

The only strategy is brute-force guessing. SHA-256 has no shortcut, no pattern, and no memory of previous attempts. **Self-regulating parameters:**

- **Difficulty adjusts** every 2,016 blocks (about 2 weeks) to maintain an average 10-minute block time.
- **Reward halves** every 210,000 blocks (about 4 years): 50 BTC in 2009, 3.125 BTC today.
- **Energy cost** is the security deposit – reversing history means redoing all that computational work.

Mining is a lottery where the ticket price is electricity and the winning probability equals your share of global hash power.



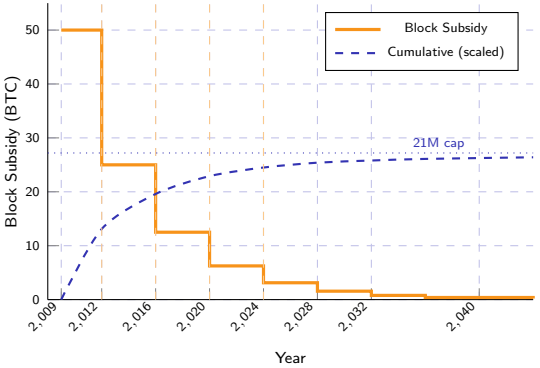
Difficulty formula: new_target = old_target × (actual_time / 1,209,600 s). If blocks arrive too fast, difficulty rises; too slow, it falls.

Why Will There Never Be More Than 21 Million BTC?

Bitcoin's monetary policy is hard-coded: the block subsidy halves every **210,000 blocks** (roughly 4 years). Total supply converges to exactly **21 million BTC** – no committee, no vote, no exception. **Halving milestones:**

- **2009:** 50 BTC per block (genesis)
- **2012:** 25 BTC (halving 1)
- **2016:** 12.5 BTC (halving 2)
- **2020:** 6.25 BTC (halving 3)
- **2024:** 3.125 BTC (halving 4)

Over 93% of all BTC has already been mined. The last satoshi will be created around the year 2140. After that, miners earn transaction fees only.



Supply formula: $S = \sum_{n=0}^{32}(50/2^n) \times 210{,}000 = 21{,}000{,}000$ **BTC. Halvings create a geometric series that converges exactly.**

Five Pillars of Bitcoin's Design

How Bitcoin Works

1. **UTXOs replace balances.** Your wealth is a collection of discrete, unspent outputs – like digital coins in a jar. No central database stores your "balance."
2. **Mining is a fair lottery.** Your probability of finding the next block equals your fraction of global hash power. The prize: new BTC plus all transaction fees.
3. **Difficulty self-adjusts.** Whether hash power doubles or halves, the network retargets every 2,016 blocks to maintain one block per 10 minutes.
4. **Supply is fixed at 21M.** The halving schedule is hard-coded consensus rules, not a policy decision. No person or committee can change it.
5. **Fees are market-priced.** When demand for block space exceeds supply, users bid for inclusion. No authority sets the fee – it emerges from competition.

What You Now Know

- → Why Bitcoin needs no central controller: cryptographic proof replaces institutional trust, making censorship structurally impossible.
- → How UTXOs differ from account balances: discrete outputs enable parallel validation and per-transaction privacy.
- → Why mining works: SHA-256 brute-force ensures anyone can verify the winner instantly, but no one can predict or shortcut the outcome.
- → Why the 21M cap is credible: halving is enforced by every node, not promised by a central bank.

The Trade-Off

Trustless money means no password resets, no chargebacks, and no customer support. Self-sovereignty requires self-responsibility.

UTXO = discrete — Mining = lottery — Difficulty = self-adjusting — Supply = fixed — Fees = market. Next: L04 Consensus Mechanisms.