Bitcoin Deep Dive

A Standalone Mini-Course

BSc Blockchain Course

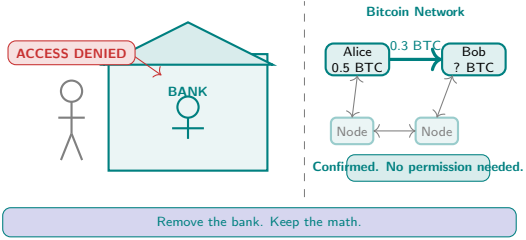
What If Money Had No Central Controller?

In 2008, governments bailed out banks with public money while ordinary depositors lost savings. Satoshi Nakamoto asked: *what if no single institution could freeze your money, inflate your savings, or demand your identity?*

Three problems Bitcoin was designed to solve:

- **Censorship:** A bank can block any transaction. Bitcoin transactions cannot be stopped if they pay a sufficient fee.
- **Inflation:** Central banks print money, diluting holders. Bitcoin's supply is capped at 21 million coins.
- **Custody:** Banks hold your funds; if they fail, you lose them. Bitcoin enables true self-custody – your keys, your coins.

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



Nakamoto S. (2008). "Bitcoin: A Peer-to-Peer Electronic Cash System." bitcoin.org/bitcoin.pdf

Pizza for 10,000 BTC: The First Real Transaction

On 22 May 2010, Laszlo Hanyecz paid 10,000 BTC for two pizzas – approximately $41 at the time. At Bitcoin's 2021 peak, those coins were worth over $600 million. Every year, the Bitcoin community celebrates **Bitcoin Pizza Day** on that date.

Think Before We Continue – Three Prompts

1. **If you had owned 10,000 BTC in 2010, would you have spent them?** At the time, Bitcoin had no clear value – it was an experiment. Hanyecz wanted to prove the system worked for commerce. When does a new technology become "real money"? Write down the conditions that would convince *you* that a new asset has lasting value.

2. **Mt. Gox collapsed in 2014 – 850,000 BTC vanished.** The exchange held customer funds in a custodial wallet. A security breach drained the reserves. Customers received cents on the dollar after a decade of court proceedings. What is the difference between holding Bitcoin on an exchange versus holding your own private keys?

3. **In November 2021, Bitcoin's market cap crossed $1 trillion for the first time.** At that moment, Bitcoin was larger than most national stock markets. Does size equal legitimacy? What would it take for your country's central bank to hold Bitcoin as a reserve asset?

Keep these stakes in mind. By the end of this lecture, you will understand exactly why Laszlo's transaction worked – and why it was revolutionary.

Bitcoin Pizza Day: 22 May 2010. Mt. Gox hack: Feb 2014. Bitcoin $1T market cap: Nov 2021. El Salvador BTC legal tender: Sep 2021.

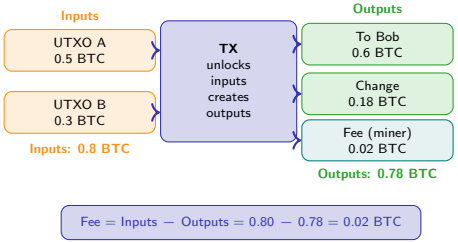
The UTXO Model: Not Your Bank Account

Your bank stores one number per account. Bitcoin stores a set of **Unspent Transaction Outputs (UTXOs)** – discrete chunks of value, each locked to an owner's public key.

Rules of the UTXO model:

- A UTXO can only be spent *in full*. Like a banknote: you spend the whole thing and receive change.
- Each input references a prior UTXO by transaction ID and output index.
- Each output creates a **new UTXO**, locked to a recipient address. The difference between inputs and outputs is the miner's fee.
- Your "balance" is simply the sum of all UTXOs your wallet can unlock.

Privacy implication: every UTXO has a traceable history. Blockchain analytics can often link UTXOs to real identities.



Every unspent output traces back to a coinbase transaction. Full nodes track the UTXO set (approx. 5 GB) for fast validation without scanning the full chain.

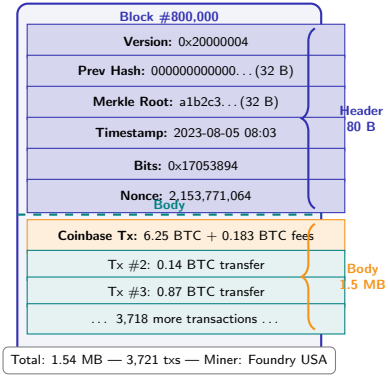
Anatomy of Block #800,000

Block 800,000 was mined on 5 August 2023 by Foundry USA. It contained **3,721 transactions** and a block reward of 6.25 BTC plus fees.

Header fields (80 bytes total):

- **Version (4 B):** Protocol version and soft-fork signalling bits.
- **Prev Block Hash (32 B):** SHA-256d of previous header – the "chain" in blockchain.
- **Merkle Root (32 B):** Root of a hash tree of all transaction IDs.
- **Timestamp (4 B):** Unix time, within 2 hours of network median.
- **Bits (4 B):** Compact difficulty target.
- **Nonce (4 B):** The number miners vary to find a valid hash.

The entire 80-byte header – not the block body – is what miners hash billions of times per second.



Block 800,000: mined 2023-08-05, 3,721 transactions, 1.54 MB, fee revenue 0.183 BTC. Source: mempool.space

The Mining Loop: Hash Until You Win

Mining is a probabilistic race. Every miner independently runs the same loop, trying to be first to find a valid block hash.

Why SHA-256 makes this a fair lottery:

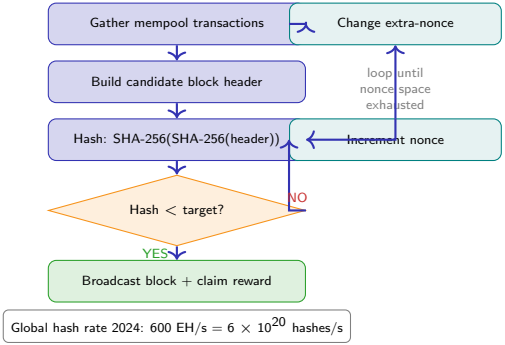
- SHA-256 is a one-way function. There is no shortcut to predict which nonce produces a hash below the target.
- Changing the nonce by 1 completely changes the hash (avalanche effect). No gradient to follow.
- If p is the success probability per hash and you compute H hashes per second, expected time to a block is $1/(p \cdot H)$.

Difficulty adjustment:

$$T_{\text{new}} = T_{\text{old}} \times \frac{\text{actual time (2 weeks)}}{1{,}209{,}600 \text{ s}}$$

Capped at 4x change per period. Target: one block every 10 minutes.

The 4-byte nonce is exhausted in seconds by modern ASICs. Miners also vary the coinbase transaction (extra-nonce) to extend the search space.



Expected hashes per block: 2^{256}/target. A solo miner at 100 TH/s would wait approx. 190,000 years on average at 2024 difficulty.

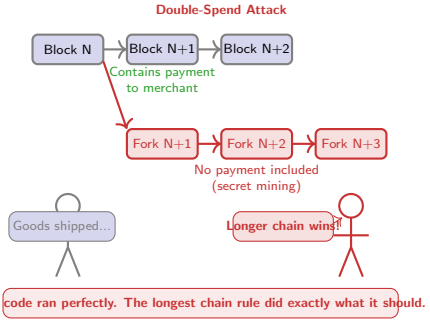
What Happens When the Code Runs Perfectly – But the Attacker Wins?

Bitcoin's security assumes no single entity controls more than half the network's hash power. If an attacker reaches 51%, the protocol still runs correctly – but the attacker can rewrite recent history.

The 51% attack – a double-spend scenario:

1. Attacker sends 100 BTC to a merchant (public chain).
2. Merchant sees confirmations and ships goods.
3. Attacker secretly mines a longer fork *without* that transaction.
4. Attacker releases the secret chain. Network accepts it as the longest chain.
5. Original payment vanishes. Attacker keeps goods and BTC.

At 600 EH/s, acquiring 51% would cost billions in hardware and electricity. The attack is theoretically possible but economically irrational for Bitcoin – though smaller chains have been attacked successfully (Ethereum Classic, 2019).



51% attacks: Ethereum Classic lost $1.1M (Jan 2019). Bitcoin's hash rate makes such attacks economically prohibitive – but not mathematically impossible.

21 Million BTC: The Fixed Supply Schedule

Bitcoin has two automatic governance mechanisms encoded in its protocol – no committee, no vote required.

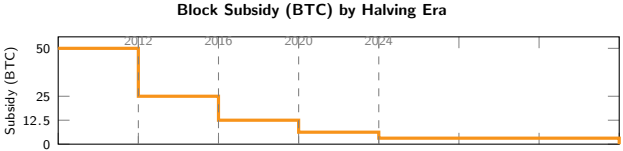
Clock 1 – Halving schedule:

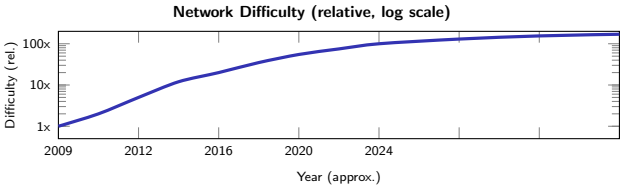
- Every **210,000 blocks** (approx. 4 years), the block subsidy halves.
- Supply converges to exactly 21,000,000 BTC.
- Each halving is a supply shock – historically followed by a price rally 12–18 months later.

Clock 2 – Difficulty adjustment:

- Every **2,016 blocks** (approx. 2 weeks), the target adjusts to maintain 10-minute blocks.
- Difficulty has risen by a factor of more than 10^{14} since genesis.

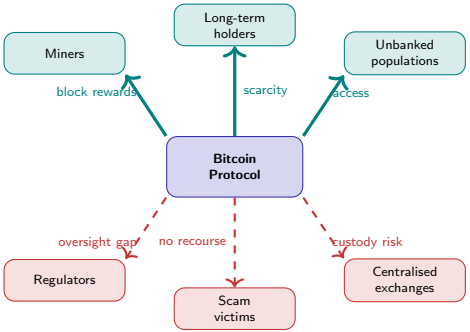
These two clocks are independent: difficulty adjusts to hash rate; halving adjusts to block count. Together they govern Bitcoin's monetary policy with zero human intervention.





Halving every 210,000 blocks; difficulty adjusts every 2,016 blocks. Last BTC will be mined around the year 2140.

Who Wins and Who Loses in Bitcoin's Design?



The same design – opposite effects:

Miners:	Earn block rewards and fees for securing the network. Hardware investment creates a de facto oligopoly among large pools.
Holders:	Fixed supply means no inflation dilution. Scarcity is baked into the protocol.
Unbanked:	A phone and internet are sufficient to store and transfer value. No bank account needed.
Regulators:	Pseudonymous, cross-border, 24/7 transactions challenge frameworks built around national institutions.
Scam victims:	No central authority can reverse a confirmed transaction. Lost keys mean lost coins forever.
Exchanges:	Custodial risk – when exchanges fail (Mt. Gox, FTX), users lose funds they thought were safe.

Irreversibility is liberation for the self-sovereign and impunity for the fraudster. Bitcoin's design is neutral; outcomes depend on who uses it.

Mt. Gox (2014): 850K BTC lost. FTX (2022): $8B customer shortfall. Irreversibility is a feature – until it is a catastrophe.

Five Questions That Reveal Any Cryptocurrency's True Design

Apply these five questions to any cryptocurrency – including Bitcoin:

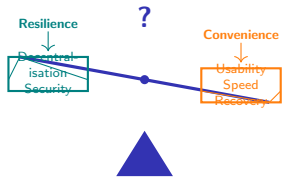
Q1 **Who can censor a transaction?** If anyone can block a valid transaction, the system is not fully decentralised. Bitcoin: only a 51% coalition can censor.

Q2 **Who controls the money supply?** If a committee can change emission rules, the scarcity promise is political, not mathematical. Bitcoin: hard-coded halving schedule.

Q3 **What happens when you lose your keys?** If there is a recovery mechanism, someone else has access. Bitcoin: no recovery – total self-sovereignty.

Q4 **How many transactions per second can the base layer handle?** Higher throughput often requires centralisation trade-offs. Bitcoin: approx. 7 TPS on-chain.

Q5 **Who can change the protocol rules?** If a foundation or company controls upgrades, decentralisation is an illusion. Bitcoin: rough consensus among miners, node operators, and developers.



Every cryptocurrency tips this balance differently.
Q1–Q5 reveal exactly where.

Quick diagnostic:

- Q1–Q3 answers point left? Maximally decentralised (Bitcoin model).
- Q4–Q5 answers point right? Optimised for usability (Solana, Ripple model).
- No cryptocurrency can maximise both sides simultaneously.

These five questions form a universal audit framework. Apply them to any cryptocurrency to reveal the real design philosophy behind the marketing.

Apply Q1–Q5 to every cryptocurrency you encounter. The answers reveal the true design philosophy – not the marketing.

Your Challenge

Apply the five-question framework from the previous slide to compare two real cryptocurrencies.

Activity: Cryptocurrency Design Audit (20 minutes)

Choose two cryptocurrencies (e.g., Bitcoin vs. Ethereum, Bitcoin vs. Solana, or any pair).

Fill in the evaluation table below for each:

Question	Crypto A	Crypto B
Q1: Who can censor a transaction?	.....	.....
Q2: Who controls the money supply?	.....	.....
Q3: What happens when you lose keys?	.....	.....
Q4: Base-layer TPS?	.....	.....
Q5: Who can change protocol rules?	.....	.....
Overall: left or right on the scale?	.....	.....

Discuss with your neighbour (5 min): Where do your two cryptocurrencies sit on the decentralisation–usability scale? Which design choices explain the difference? Is one "better," or do they serve different users?

There is no universally "best" cryptocurrency – only designs optimised for different trade-offs. Q1–Q5 makes those trade-offs visible.