Bitcoin and Cryptocurrency Technologies
Lecture 7: Bitcoin Protocol

Yuri Zhykin

Mar 20, 2025

Bitcoin Protocol

- **Bitcoin Protocol** is a distributed protocol for producing a **limited amount** of **digital tokens (currency)**, **provably assigning ownership** of the tokens to certain entities, giving those entities the ability to **irreversibly transfer (spend)** the ownership of the tokens to other entities and **preventing double transfer**.
- Previous attempts at digital currencies were unable to resolve the problem of **double spending** without central authority.

Bitcoin Network Roles 1/2

- Members of the Bitcoin Network are divided into the following classes:
  - **full nodes** (validating nodes) - members that run Bitcoin Node software, propagating and validating blocks and transactions; these guarantee the *strength-in-numbers* policy of the distributed Bitcoin protocol;
  - **miners** (full nodes with mining hardware) - members that compute blocks and provide the *computational security* of the network;
  - **light nodes** - nodes that are only interested in particular parts of Bitcoin protocol, e.g. transactions and their corresponding blocks (Simplified Payment Verification nodes, mobile wallet software).

Bitcoin Network Roles 2/2

- **Full nodes** ensure that miners do not mine invalid blocks (i.e. low chainwork blocks or blocks with invalid transactions);
- **Miners**
  - cannot mine invalid blocks because these will immediately be rejected by the full nodes, which results in immediate loss of all resources spent on computing PoW,
  - heavily invested in hardware and their only income is block rewards, so if the network is compromised, their investment loses value;
- **Light nodes** only keep a chain of block headers (68 MiB of data as of March 2025) and validate only specific transactions.

Limited Supply 1/4

- Bitcoin Protocol incentivises miners to spend resources on PoW computation by allowing them to generate new bitcoin in the **coinbase** transactions.
- Additionally, miner claims fee of all transactions that were included in the block.
- Bitcoin is designed to have a **strictly limited supply** of the bitcoin tokens, so the amount of bitcoin generated in each new block is reduced over time.
- As block reward becomes smaller, miners rely more on transaction fees.

Limited Supply 2/4

- Every 210,000 blocks the reward is halved:
  - 50 BTC (5,000,000,000 satoshis) in 2009-2012,
  - 25 BTC (2,500,000,000 satoshis) in 2012-2016,
  - 12.5 BTC (1,250,000,000 satoshis) in 2016-2020,
  - 6.25 BTC (625,000,000 satoshis) in 2020-2024.
  - 3.125 BTC (312,500,000 satoshis) since 2024.
- Bitcoin block reward follows a geometric progression

$$a_n = ar^n,\ a = 50,\ r = \frac{1}{2}$$

the sum of which is the total amount of bitcoin to ever exist:

$$210000 \times \sum_{n=1}^{n:a_n \geq 1} a_n = 210000 \times \frac{a(1 - r^n)}{1 - r} = 21000000$$

Limited Supply 3/4

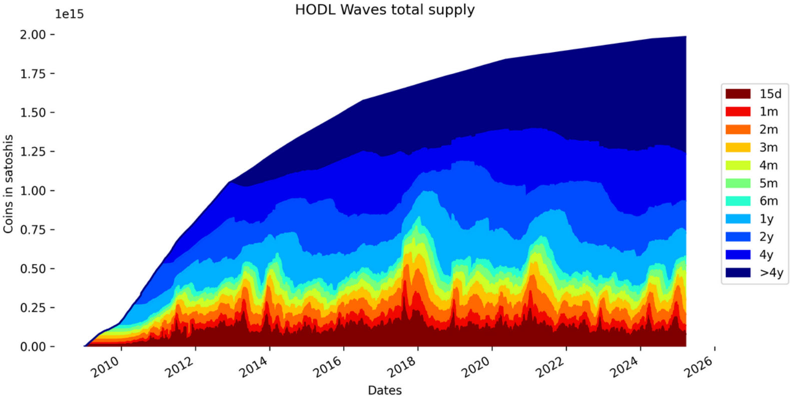
- Bitcoins can be accidentally “lost” (the owner loses access to the key needed to unlock the lock script).
- Bitcoin can also be intentionally “destroyed” by sending coins to an address with an unknown key, for example

$$1BitcoinEaterAddressDontSendf59kuE$$

- According to some studies, around 600,000-1,100,000 bitcoins may belong to Satoshi Nakamoto from the early network period.

Limited Supply 4/4

- bitcoinisdata.com: 4-6 million bitcoins are likely lost forever



Forks 1/2

- **Soft fork** is a Bitcoin Protocol change that **restricts** the set of rules applied to blocks and transactions.
- **Some** of the blocks or transactions considered **valid** by the **old (non-upgraded) nodes** are considered **invalid** by the **new (upgraded) nodes**.
- Soft fork does not drop any nodes from consensus, but requires majority of the nodes to upgrade for the new rule to be enforced.
- Old nodes can still “play by the old rules”.

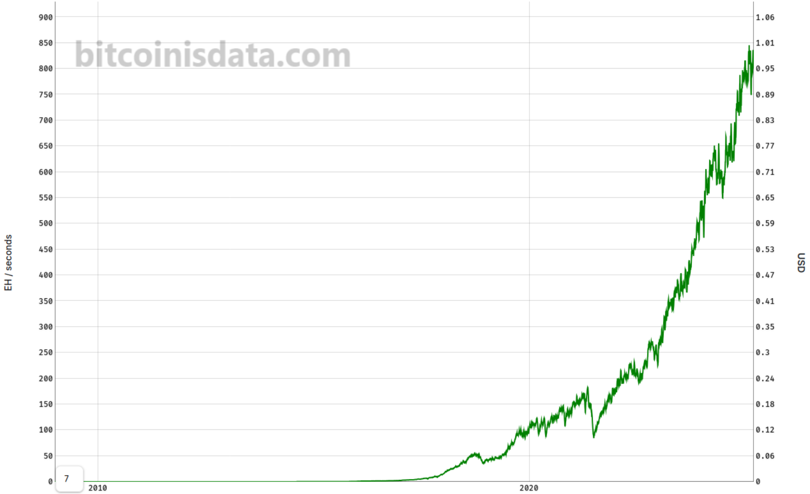
Forks 2/2

- **Hard fork** is a Bitcoin Protocol change that **relaxes** the set of rules applied to blocks and transactions:
- **Some** of the blocks or transactions considered **valid** by the **new (upgraded) nodes** are considered **invalid** by the **old (non-upgraded) nodes**.
- Hard fork effectively drops old nodes from consensus, so it requires all nodes to upgrade to avoid the network split.
- Nodes that "play by the old rules" are separated from the main network into a separate network.

Network Hashrate 1/2

- For **hash-based Proof-of-Work systems**, the computing power can be conveniently measured by **hashrate - hashes computed per second** (H/s).
- Current total **hashrate** of the Bitcoin network is approximately 804 Eh/s ($804 \times 10^{18} = 804{,}000{,}000{,}000{,}000{,}000$ H/s), compared to 375 Eh/s in 2022.
- As block rewards attract more miners, the total computing power of Bitcoin network increases.

Network Hashrate 2/2



Difficulty Adjustment

- In order to accomodate to the increasing computing power of the network, Bitcoin Protocol includes the **difficulty adjustment process**.
- Every 2,016 blocks (approximately 2 weeks), the difficulty of the PoW task is recalculated based on the last 2,016 blocks:
  - if the averate time between last 2,016 blocks is *more than 600 seconds*, the *difficulty is decreased* (the *PoW target is increased*), otherwise the *difficulty is increased* (the *PoW target is decreased*).
- The PoW difficulty is represented as the **PoW target** 256-bit number, which is in turn encoded as **bits** value and included in the block header, so the PoW solution can be verified independently.

The End

Thank you!