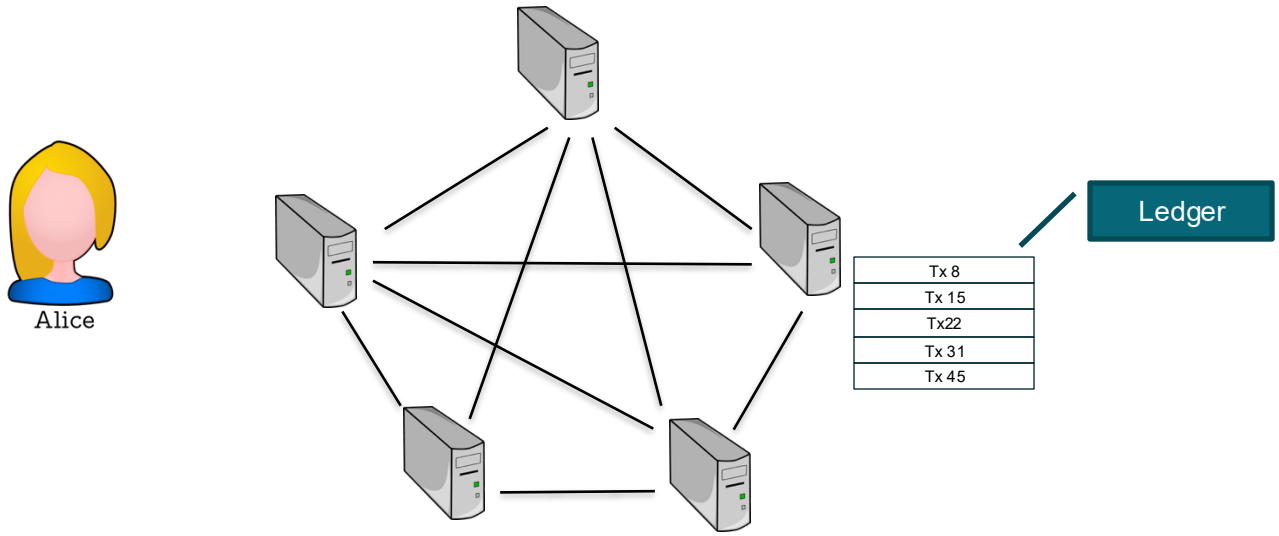
Consensus - #04

Blockchain and Distributed Ledger technologies

SAPIENZA
UNIVERSITÀ DI ROMA

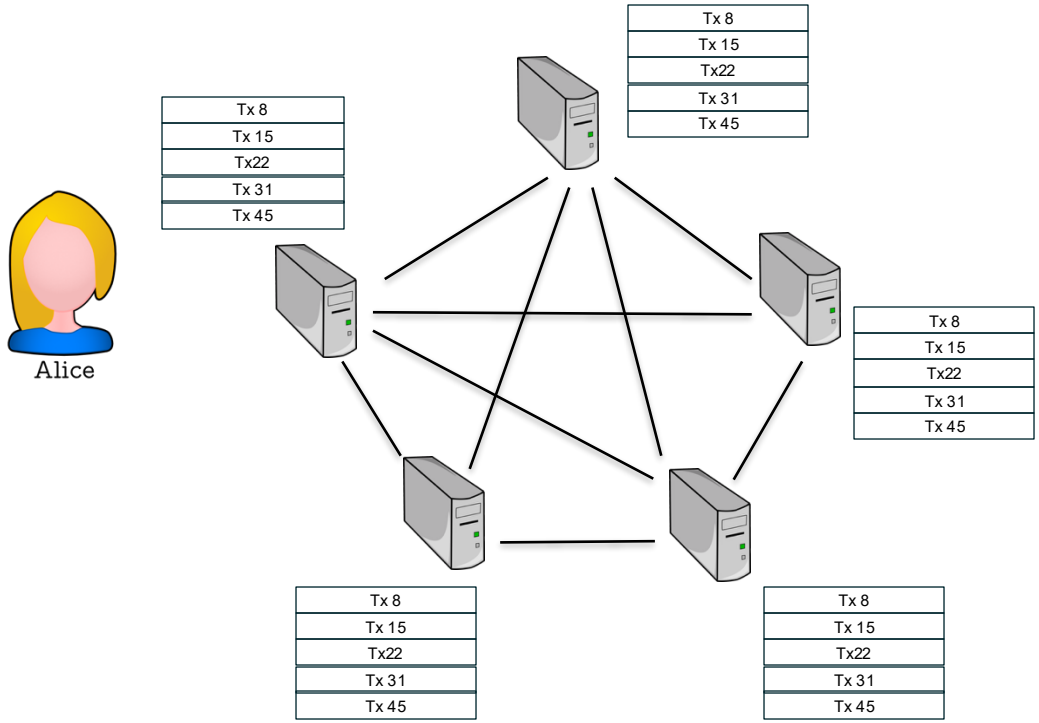
Massimo La Morgia
massimo.lamorgia@uniroma1.it

How Bitcoin Works



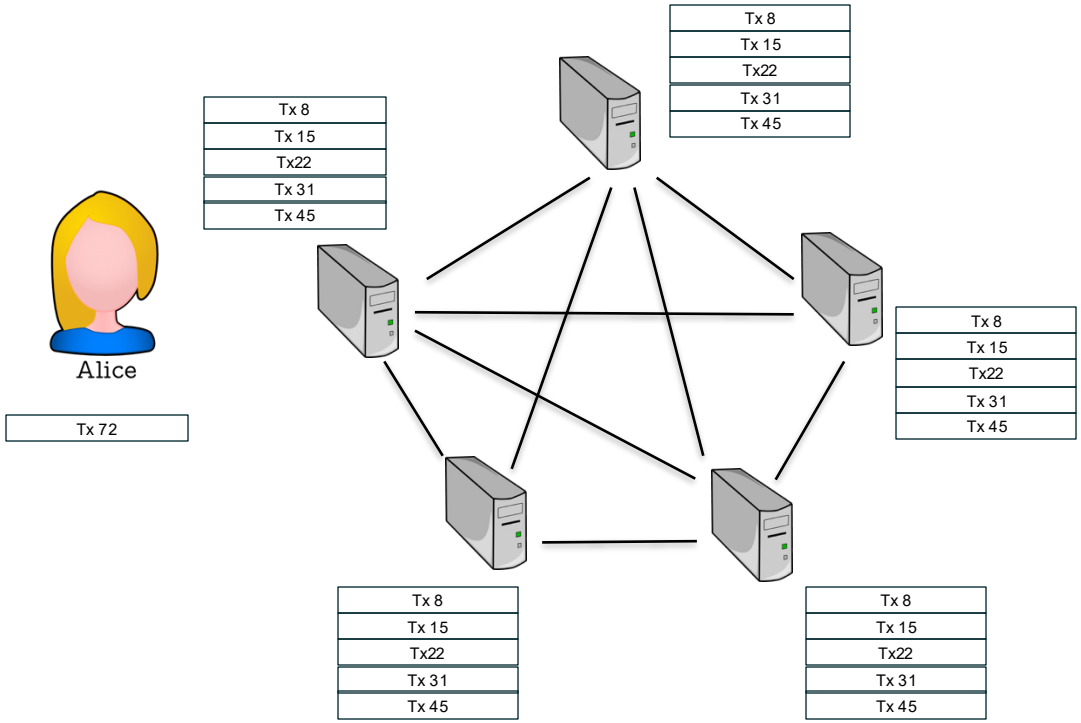
It is a network of nodes that aim to maintain the exact same copy of data, which is the ledger.

How Bitcoin Works



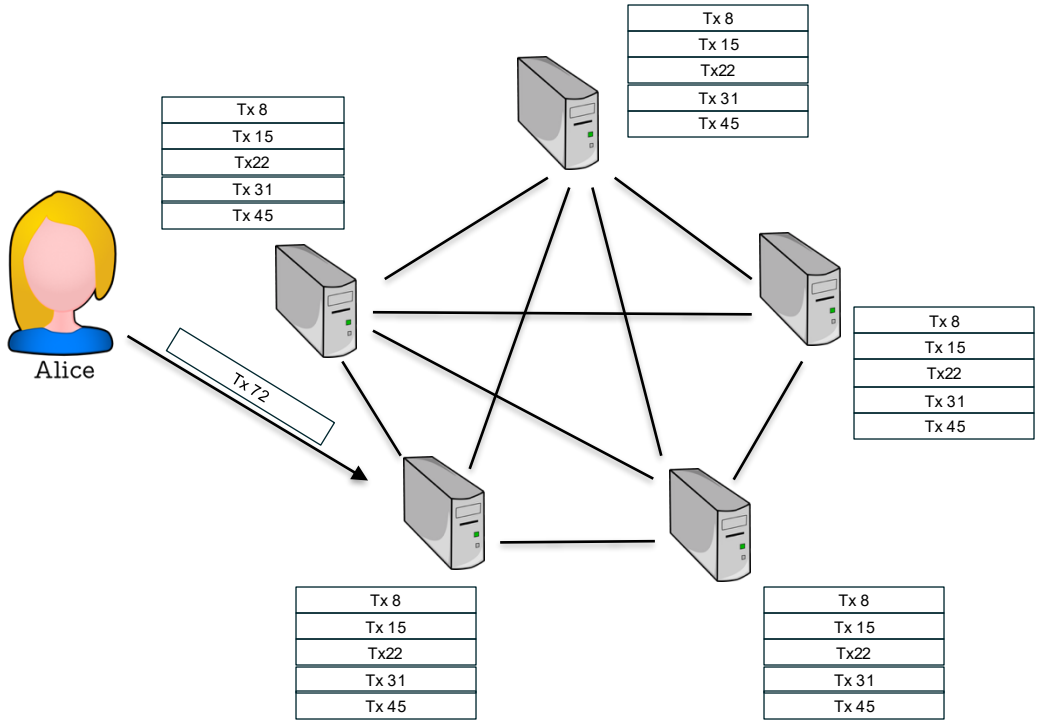
We want a guarantee that everyone can add entries to the ledger, but no one can modify existing data.

How Bitcoin Works



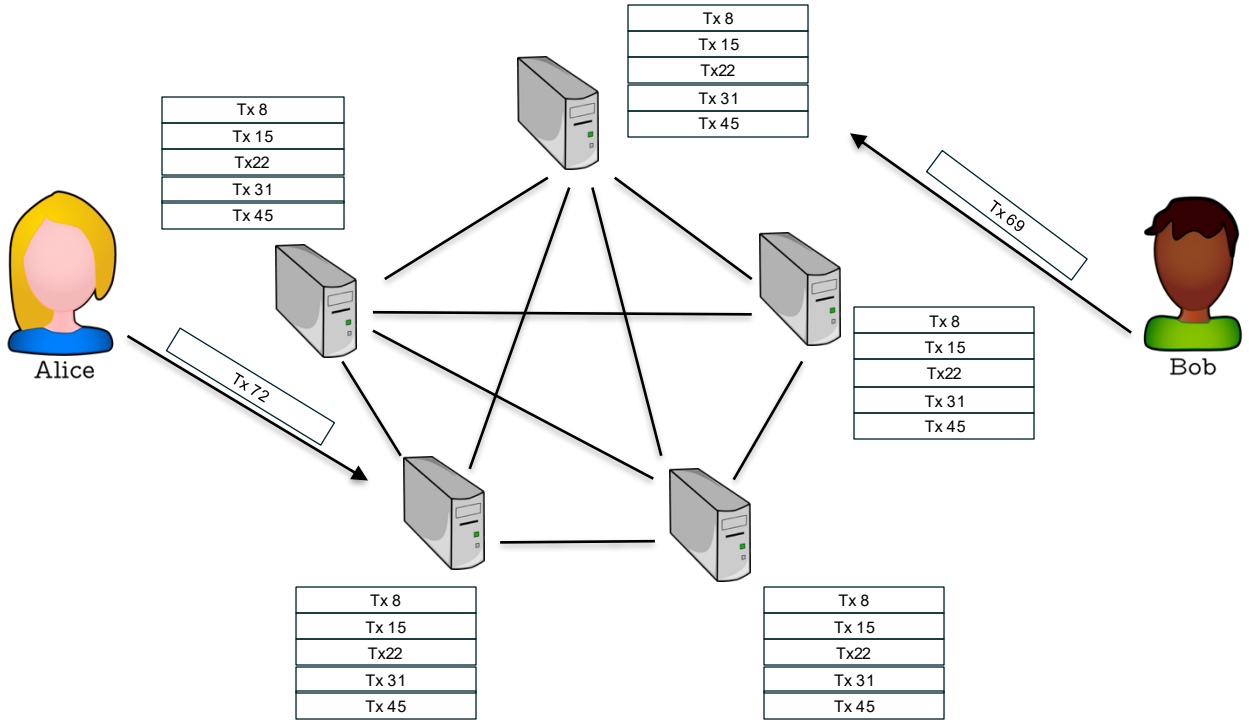
Transaction is the kind of data recorded into the ledger.

How Bitcoin Works



A user forwards a new transaction to a node, this last broadcast the transaction to all the other node in Peer-2-Peer.

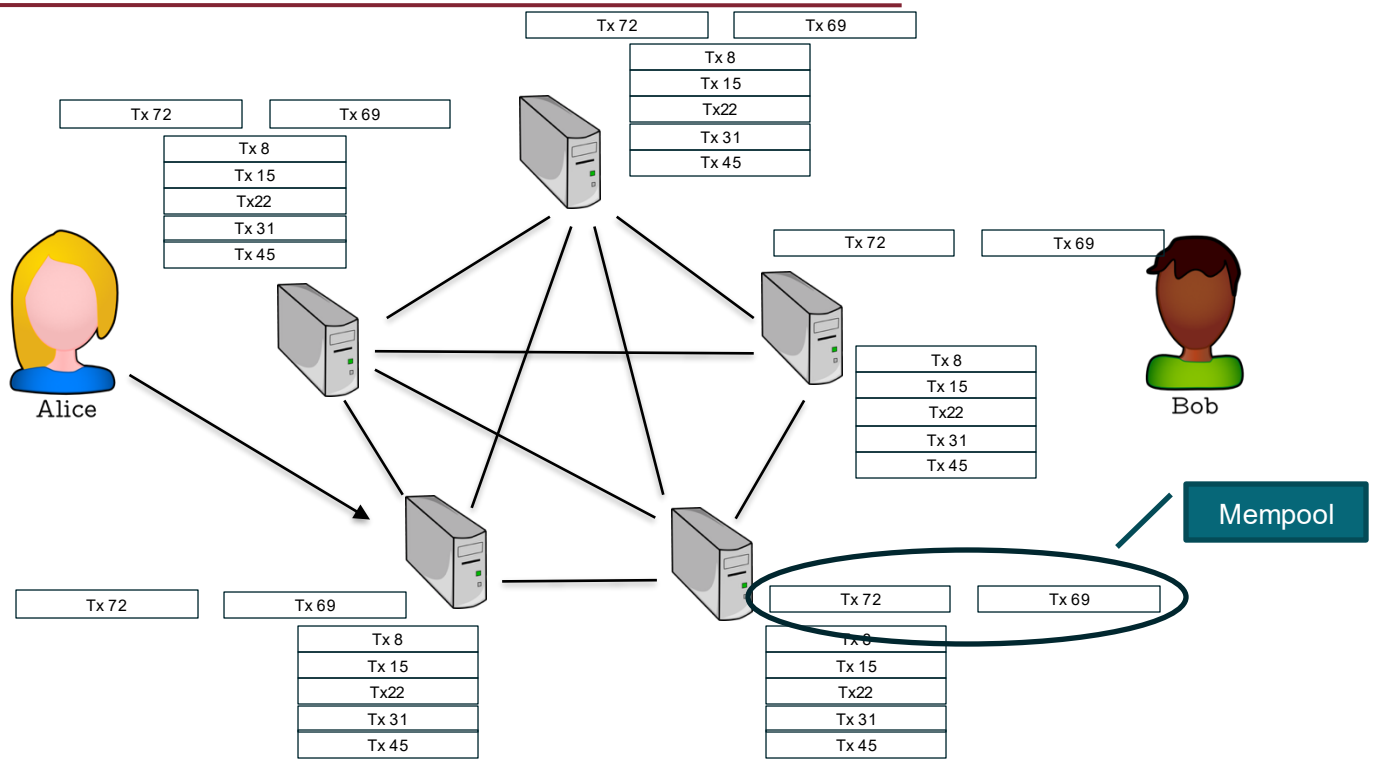
How Bitcoin Works



A user forwards a new transaction to a node, this last broadcast the transaction to all the other node in p2p.

However, there could be multiple users in the systems.

How Bitcoin Works



A mempool is a collection of unconfirmed Bitcoin transactions that are waiting to be included in a **block** and added to the blockchain. Each node on the Bitcoin network has its own mempool.

How we can decide what is the order of the transactions?

Who decides which transactions can be inserted and which cannot?

Distributed system – Recall that

“A distributed system is one in which the failure of a computer you didn't even know existed can render your own computer unusable.” [Laslie Lamport]

In a distributed systems you can make no assumption about:

- **Timing** – messages can be delayed, reordered, or lost.
- **Network reliability** – links can fail or recover unpredictably.
- **Node availability** – any process or machine may crash or restart at any moment.
- **Global state** – no single node ever has a perfectly up-to-date view of the whole system.
- **Clocks** – physical clocks drift; you can’t assume perfectly synchronized time.

Distributed consensus

In a network of n nodes, each node has an input value. Some nodes may be faulty or malicious.

A distributed consensus protocol must satisfy two key properties:

- All honest nodes must reach agreement on the same value.
- The agreed-upon value must originate from an honest node.

Simplified bitcoin consensus

1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block by including its hash in the next block they create

Proof - of – Work (PoW)

The early idea

The concept of **Proof of Work (PoW)** has its roots in early research on combating spam and preventing denial-of-service attacks.

It was designed as an anti-spam mechanism that required email senders to perform a small computational task, effectively proving that they expended resources (in the form of CPU time) before sending an email.

In Bitcoin

To propose a new block miners have to solve a puzzle.

$$H(\text{nonce} \,||\, \text{prev\_hash} \,||\, \text{tx} \,||\, \text{tx} \,||\, \ldots \,||\, \text{tx}) < \text{target}$$

Miner that solves the puzzle have the right to propose the next block and broadcast it.

Other nodes in the network, once received the new block, validate the information contained and if there are no error, insert the new block on the head of their blockchain.

A round

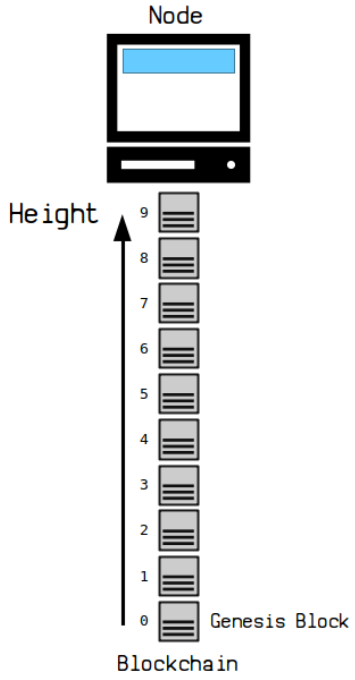
In a distributed system, a "round" refers to a discrete step or iteration in which processes communicate, perform actions, and update their states.

A block is the time unit of the blockchain.

A block should be produced every 10 minutes, however new miners can join the network while other can left.

So the target change over time, it is updated every 2016 blocks, in such a way that the time to find a new block needs on average 10 minutes.

(2016 blocks * 10 minutes)/24 hours = 14 days (2 weeks)



Target coefficient

Block headers contain the target in a notations called “target bits”.

Target bits = 0x1903a30c

The first two hexadecimal digits for the exponent and the next six hex digits as the coefficient

Exponent = 0x19
Coefficient = 0x03a30c

$$\text{target} = \text{coefficient} \times 2^{(8 \times (\text{exponent} - 3))}$$

$$\text{target} = 0\text{x}03\text{a}30\text{c} \times 2^{(8 \times (0\text{x}19 - 3))}$$

Target = 22,829,202,948,393,929,850,749,706,076,701,368,331,072,452,018,388,575,715,328

Target = 0x00000000000003A30C0000000000000000000000000000000000000000

This means that a valid block is one that has a block header hash less than the target. In binary that number must have more than 60 leading bits set to zero

Target adjustment

Target adjustment formula

```
New Target = Old Target * (Actual Time of Last 2015 Blocks/ 20,160 minutes)
```

(MTP) Median Type Past

The timestamps set in block headers are set by the miners.
There is no global clock

- If a miner sets their time in the future, they can lower difficulty, allowing them to mine more blocks and claim some of the block subsidy reserved for future miners.
- If a miner set their times in the past for some blocks, they can use the current time for some other blocks, and so make it look like there's a long time between blocks for the purpose of manipulating difficulty.

Rules:

- no node will accept any block with a time further in the future than two hours.
- no node will accept a block with a time less than or equal to the median time of the last 11 blocks, called median time past (MTP).

**Please note that the target adjustment formula in the Mastering Bitcoin book contains an error. Please refer to reported correct version*

Validating a new block

Valid block

- The block data structure is syntactically valid.
- The block header hash is less than the target (enforces the proof of work).
- The block timestamp is between the MTP and two hours in the future (allowing for time errors).
- The block weight is within acceptable limits.
- The first transaction (and only the first) is a coinbase transaction.
- All transactions within the block are valid.

Valid transaction

- The transaction's syntax and data structure must be correct.
- Neither lists of inputs nor outputs are empty.
- The transaction weight is low enough to allow it to fit in a block.
- The outputs being spent match outputs in the mempool or unspent outputs in a block in the main branch.
- Reject if the sum of input values is less than sum of output values.
- The scripts for each input must validate against the corresponding output scripts.

Incentives – mining reward

The miner that proposes the new block can collect the block reward and the fees.

The miner that proposes the new block can forge a transaction that mint new Bitcoins, this transaction is called **coinbase transaction**.

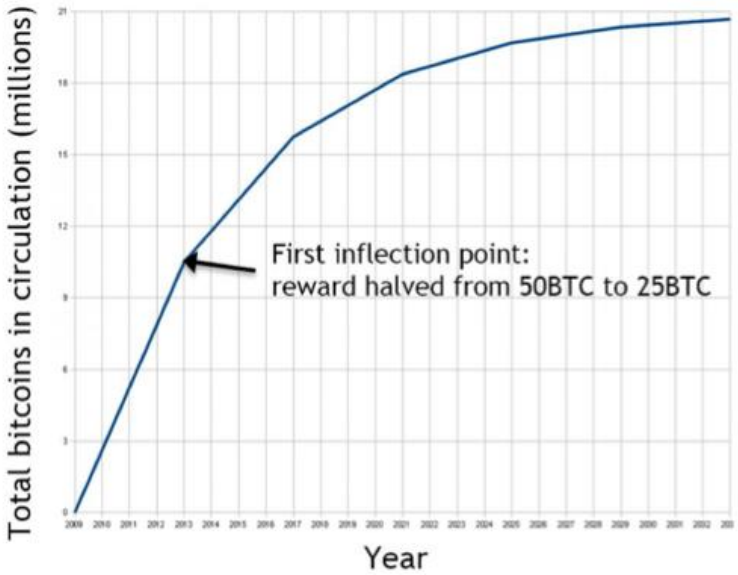
Actual block reward is of 3.125 bitcoins

Bitcoin total supply limit is of 21'000.

Halving

Every 210,000 blocks, or approximately every **four years**, the currency issuance rate is decreased by 50%. For the first four years of operation of the network, each block contained 50 new bitcoins.

Approximately in 2140 no new Bitcoins will be mined.



Incentives -fees

Each transaction only pays a single fee—it doesn't matter how large the transaction is.

The fee rate for a transaction's size divided by weight (Sat/byte)

The fee rate is established in a kind of virtual auction.

When network demand increases and more users seek rapid confirmation of their transactions, they tend to offer higher fees, causing the overall fee rate to rise.

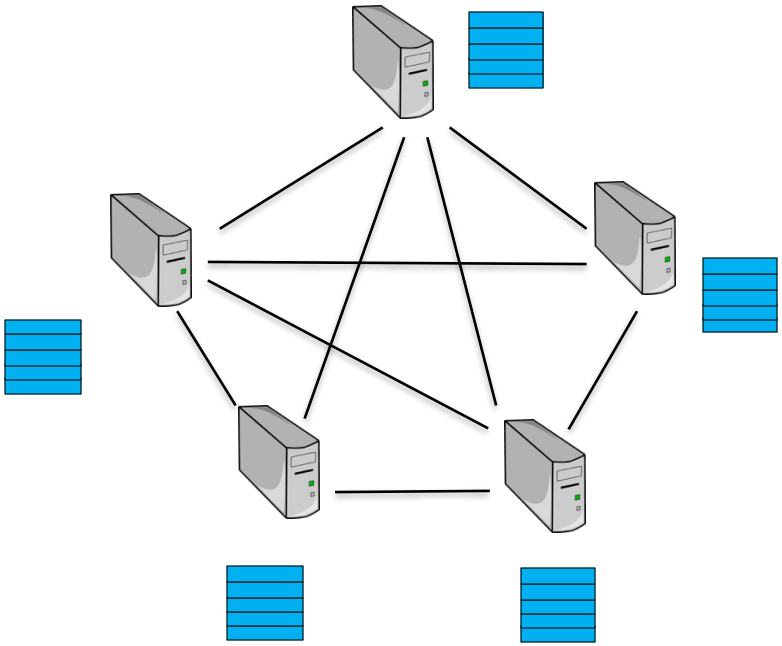
The data structure of transactions does not have a field for fees. Instead, fees are implied as the difference between the sum of inputs and the sum of outputs. Any excess amount that remains after all outputs have been deducted from all inputs is the fee that is collected by the miners.

Replace by fee (RBF): creating a conflicting version of the transaction that pays a higher fee. Two or more transactions are considered to be conflicting transactions if only one of them can be included in a valid blockchain, forcing a miner to choose only one of them.

Child Pays for Parent (CPFP) : Anyone who receives the output of an unconfirmed transaction can incentivize miners to confirm that transaction by spending that output. The transaction you want to get confirmed is called the parent transaction. A transaction that spends an output of the parent transaction is called a child transaction

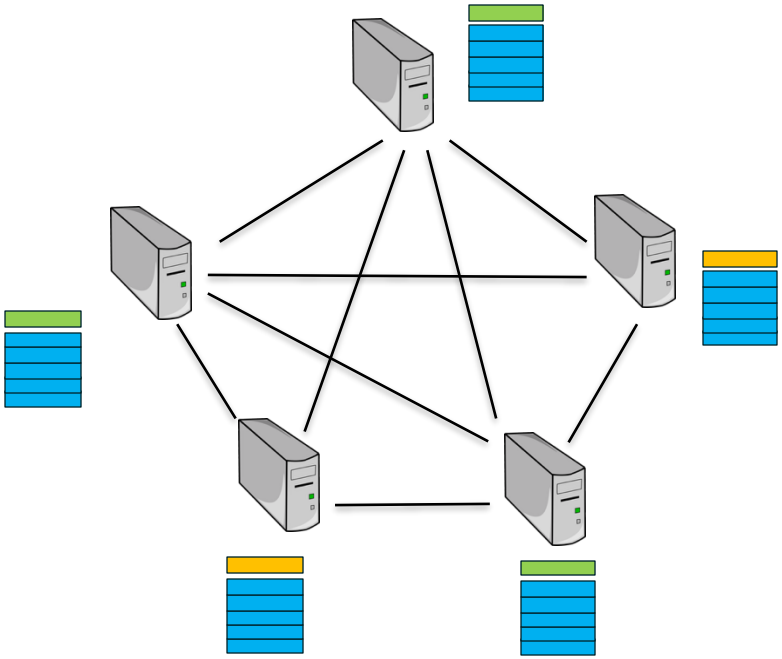
Fork

What happen if 2 or more miners solve the puzzle at the same time.



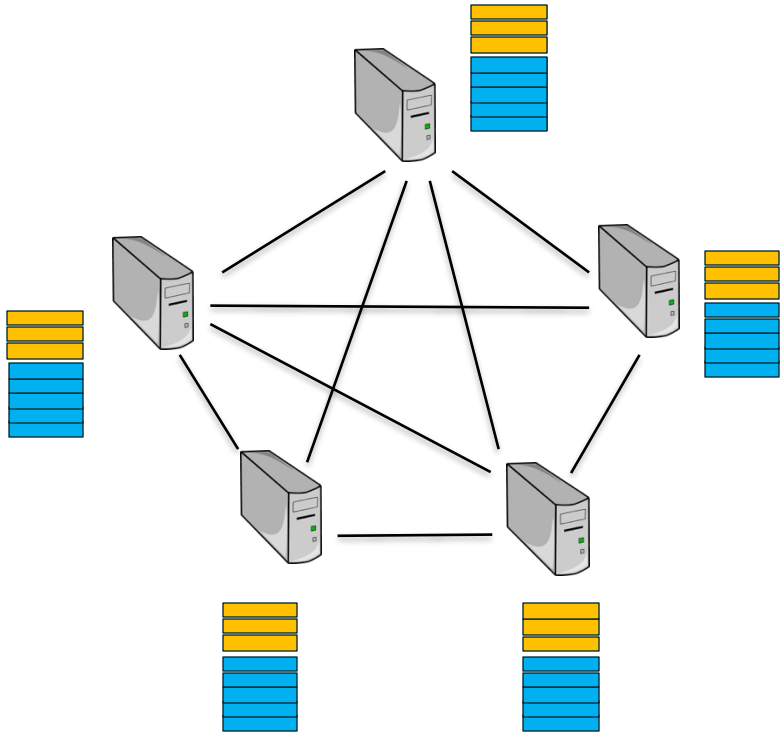
Fork

Nodes into the systems start to have different version of the blockchain. So, exist a fork of the blockchain.



Longest chain rule

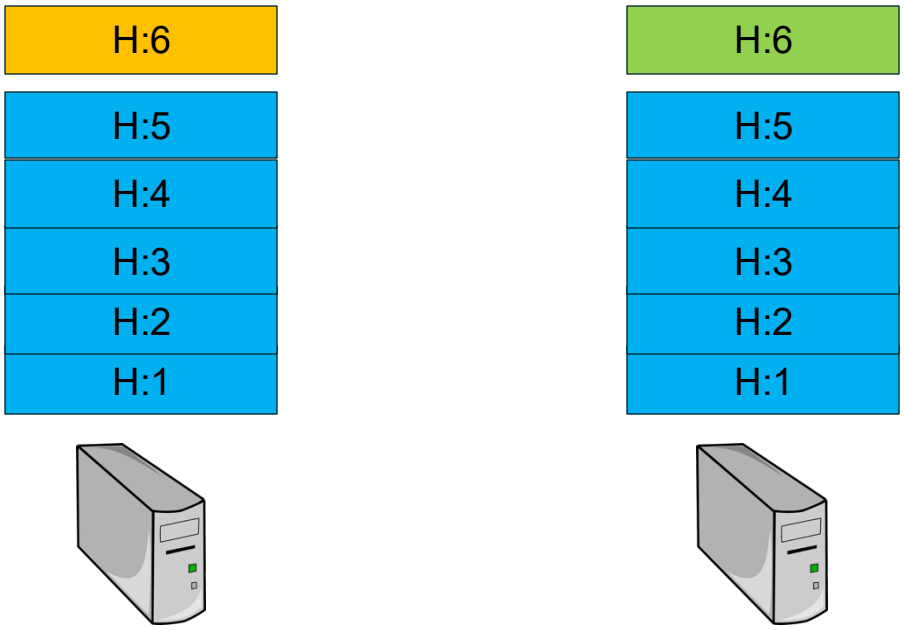
Longest fork will be selected as canonical blockchain (actually it is selected the chain with most cumulative work) and eventually all nodes will agree on the canonical blockchain. The blocks belonging to the other fork will be discarded and lost forever. (Yes, some transactions can be lost forever)



Longest chain rule

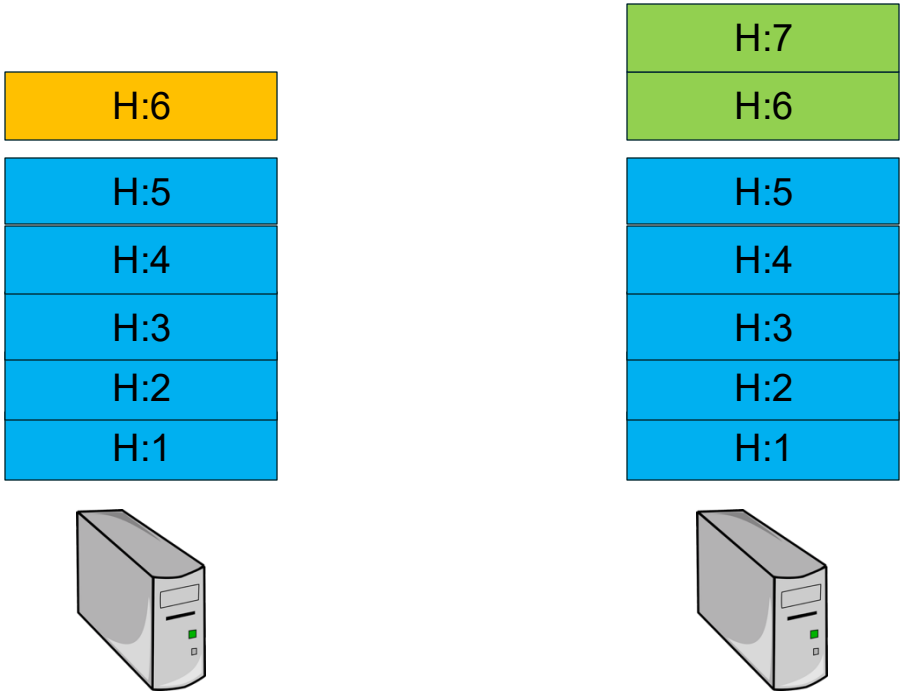
Node 0x0A and 0x0B have a different vision of the actual blockchain. Indeed, they have different block at height 6.

Both the yellow and the green blocks are valid, these two blocks are siblings.



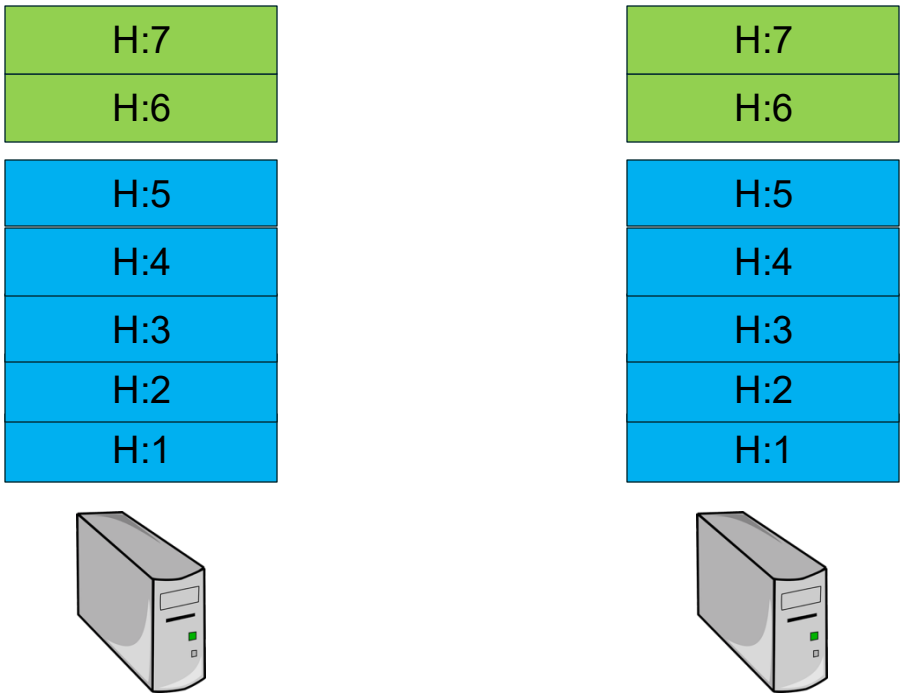
Longest chain rule

A new green block H:7 confirmed the green block H:6 green, making the blockchain of the node 0x0B the longest one and those with more cumulative PoW associated with it and thus the new canonical chain. The yellow block H:6 become **stale**.



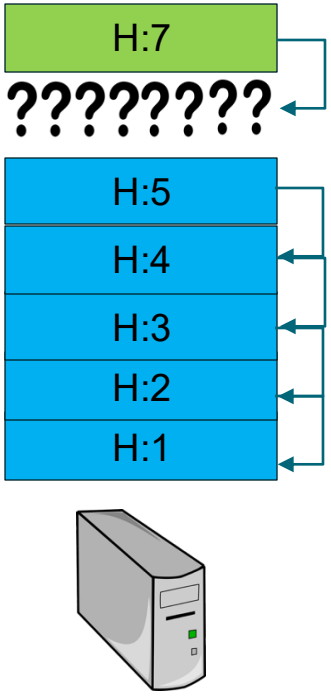
Longest chain rule

According with the chain selection criteria the node 0x0A updates its block and reorganizes its view of confirmed transactions.



Orphan blocks

An orphan block is a legitimate block with a nonexistent or unknown parent block. It is also known as an orphan, detached block, or extinct block. They were common in the early versions of bitcoins (no more possible since 2015). Nowadays it is also used for referring to stale block, because the client denotes their block rewards as “orphaned”.

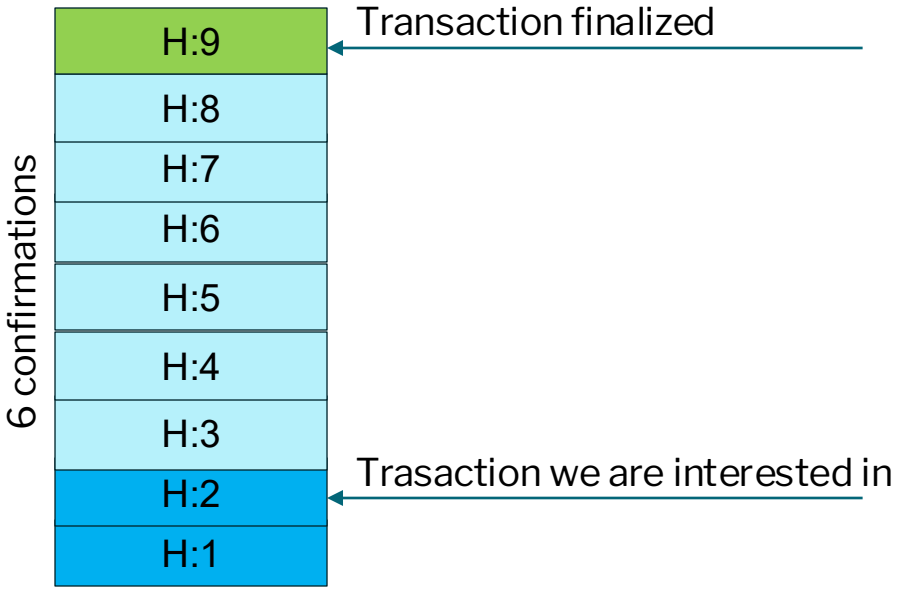


Confirmations and finality

Confirmations: Once a transaction is included in a block, it has one confirmation. As soon as another block is mined on the same blockchain, the transaction has two confirmations, and so on. Six or more confirmations is considered sufficient proof that a transaction cannot be reversed.

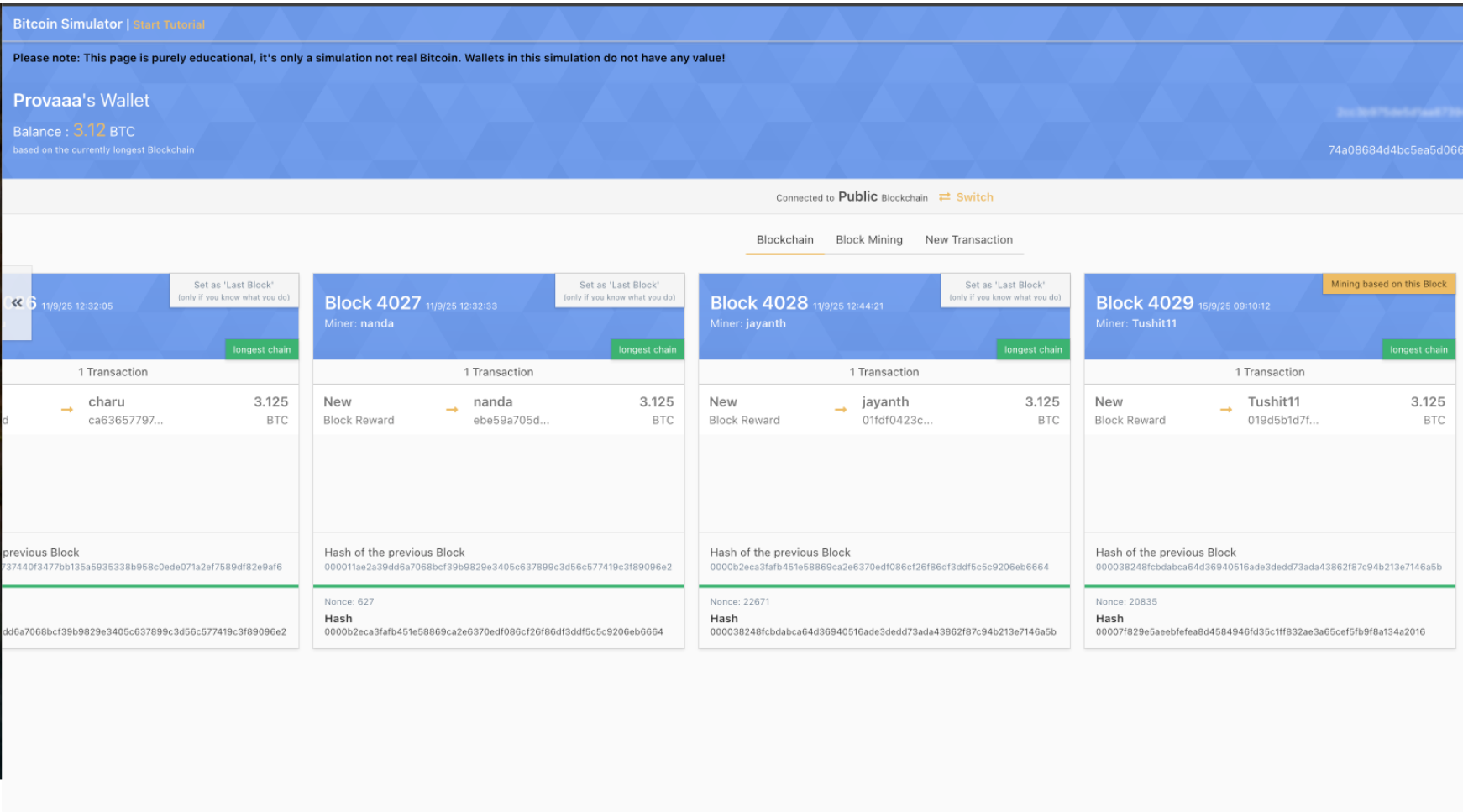
Finality: Finality is metric that measure the amount of time one has to wait for a reasonable guarantee that crypto transactions executed on the blockchain will not be reversed or changed.

Bitcoin finality : 6 block confirmations X 10 minutes = 60 minutes



Let’s play with consensus

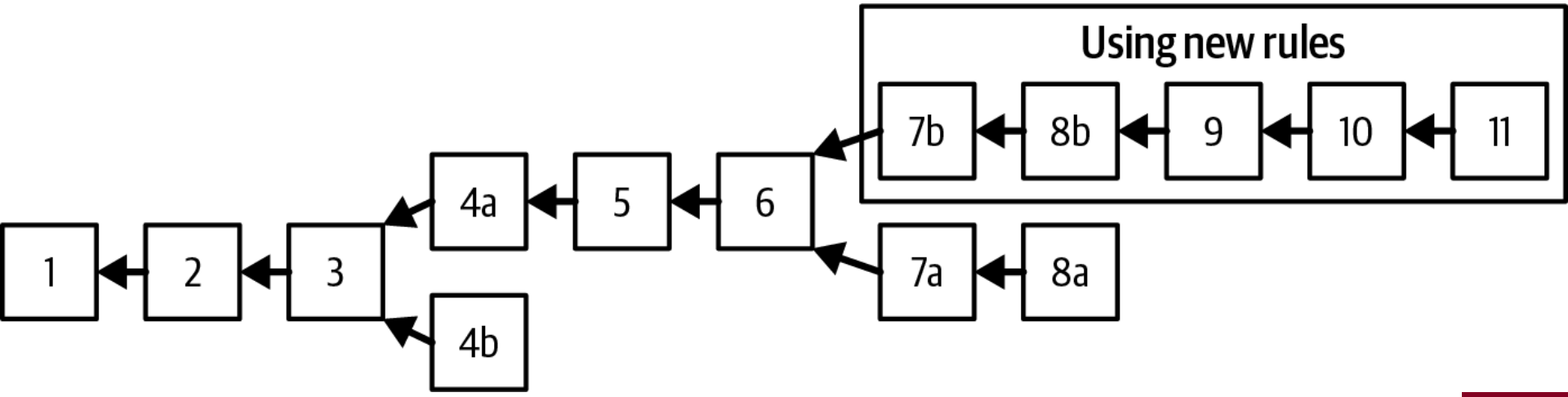
https://bitcoinsimulator.duckdns.org/



Upgrading the protocol - Soft and Hard fork

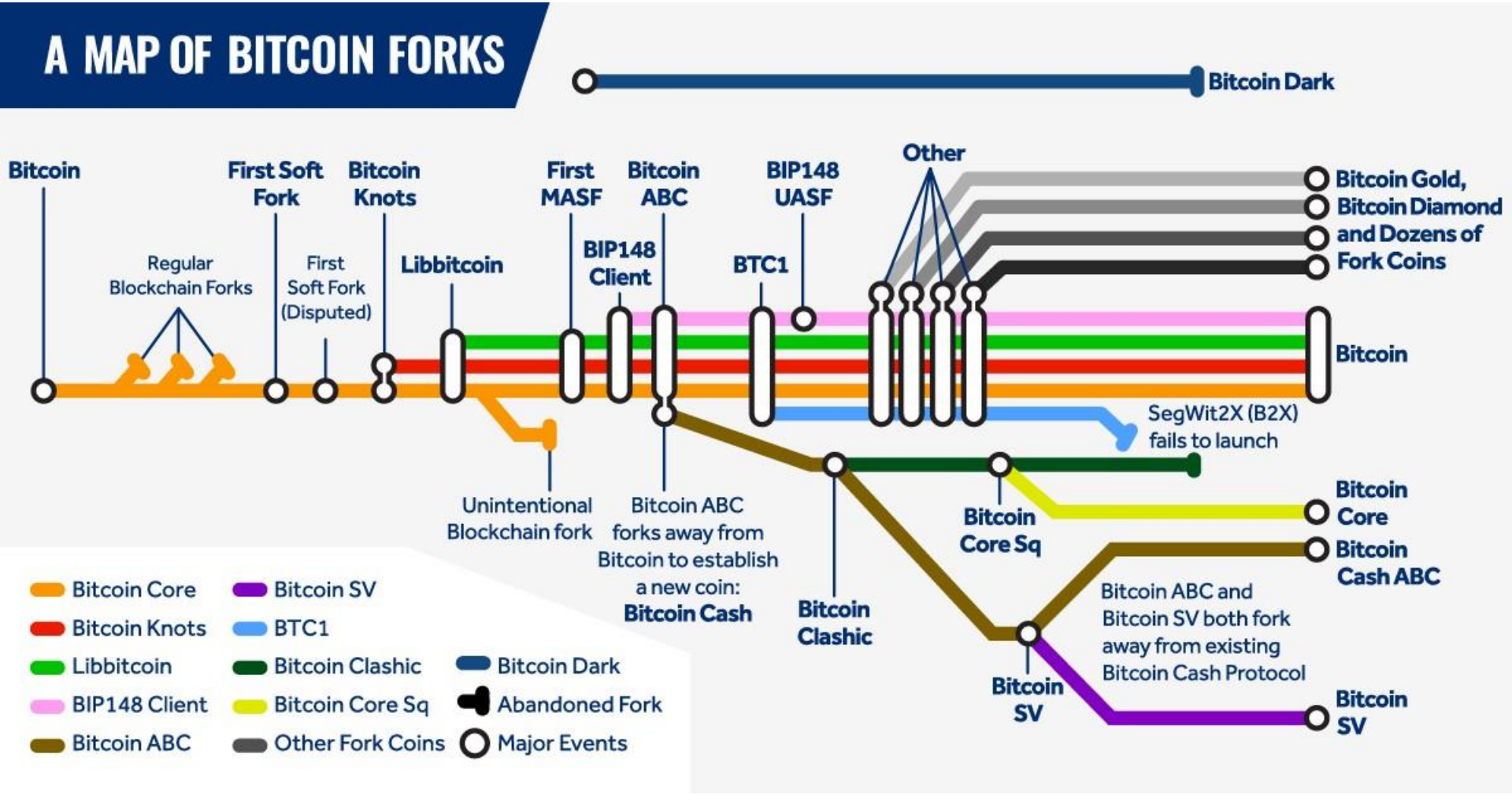
Hard fork: Hard forks occur when part of the network is operating under a different set of consensus rules than the rest of the network. This may occur because of a bug or because of a deliberate change in the implementation of the consensus rules.
Thus, the new version of the software would recognize blocks as valid that the old software would reject.

Soft fork: Soft forks occur when new features are added to Bitcoin that make the validation rules stricter. That is, they restrict the set of valid transactions or valid blocks so that the old version would accept all blocks, whereas the new version would reject some.
A soft fork avoids the permanent split that a hard fork introduces. This is because blocks considered valid by new miners are also considered valid by old miners.
Old miners risk to mine block that are considered invalid by new miners.
Does a soft fork really generate a fork?



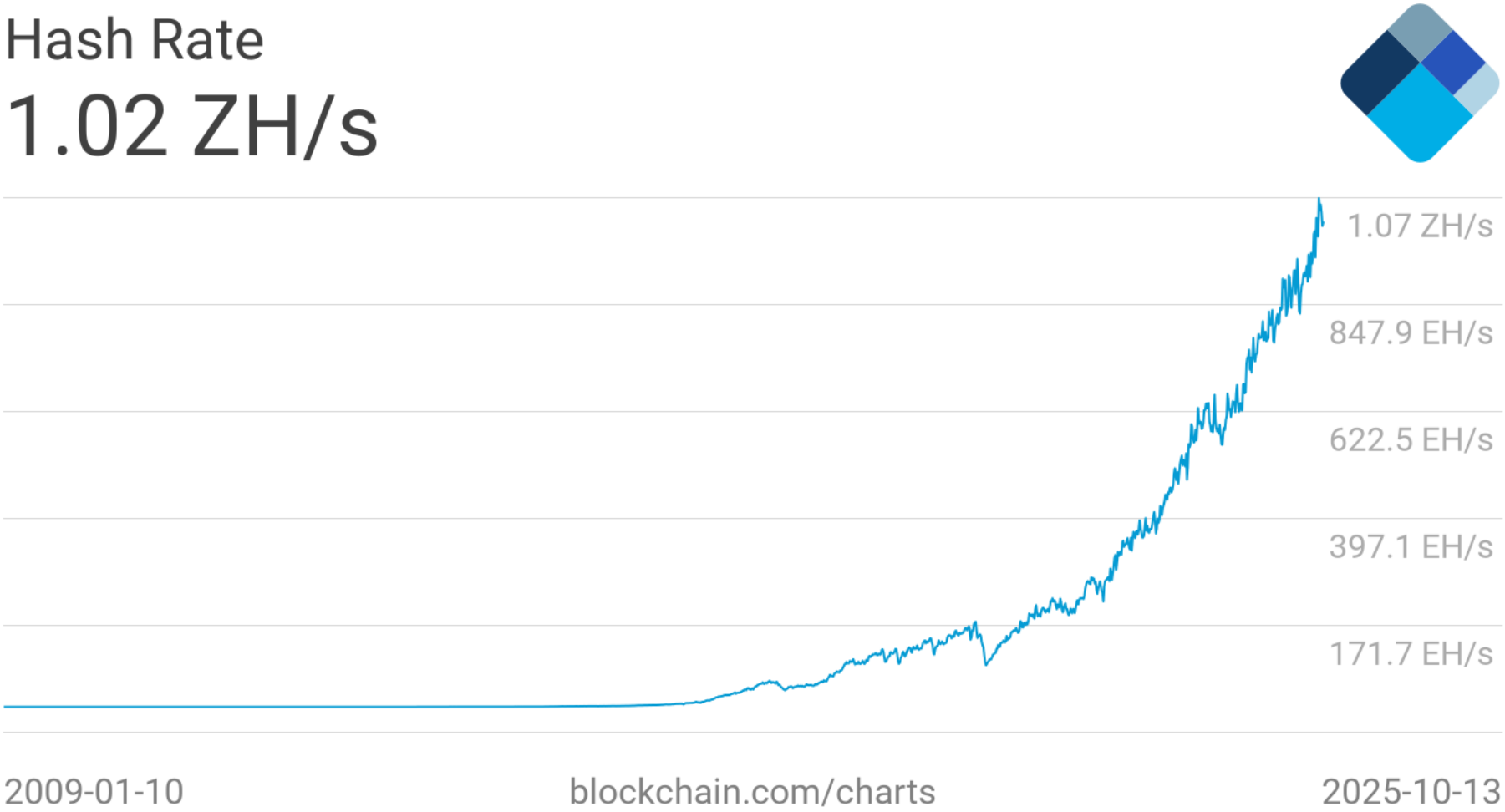
Upgrading the protocol - Soft and Hard fork

What will happen if there is a hard fork and the miners split between the two forks? Let's say 60%-40%?



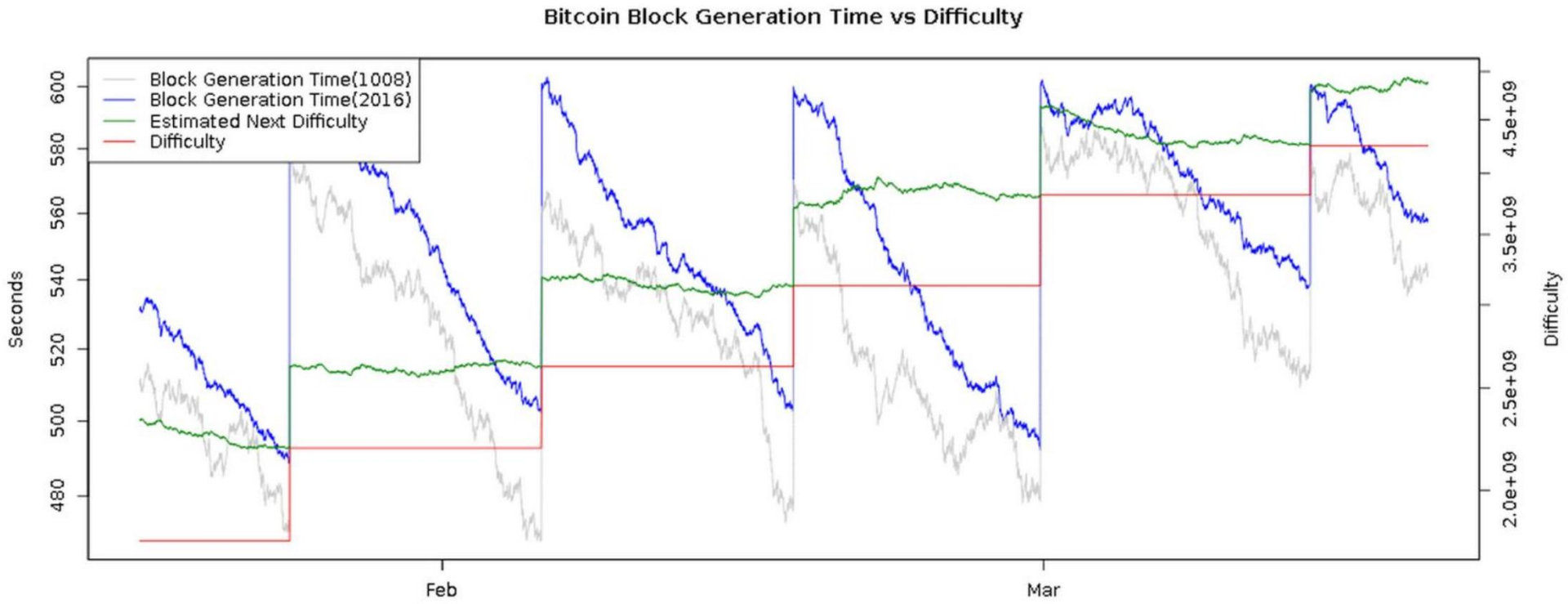
https://bitcoinmagazine.com/technical/infographic-map-bitcoin-forks

HashRate



https://bitcoinmagazine.com/technical/infographic-map-bitcoin-forks

HashRate


Bitcoin Block Generation Time vs Difficulty
Block Generation Time(1008)
Block Generation Time(2016)
Estimated Next Difficulty
Difficulty
Seconds
480
500
520
540
560
580
600
Feb
Mar
2.0e+09
2.5e+09
3.5e+09
4.5e+09
Difficulty

Mining

CPU : In the beginning (2009), Bitcoin was mined using regular computer processors, or CPUs. Not efficient.

GPU: (2010) A single video card can be dozens of times more efficient than one CPU, and up to 4 video cards could be installed on a single cheap motherboard. The price of GPU skyrocket.
However, GPUs are not energy efficient, need a lot of maintainece

Field-programmable gate array FPGA: (2011) is a type of configurable integrated circuit that can be repeatedly programmed after manufacturing. They consist of a grid-connected array of programmable logic blocks that can be configured "in the field" to interconnect with other logic blocks to perform various digital functions. It's faster and more energy-efficient than GPU.

Application Specific Integrated Circuits (ASICs): Entered into market in 2013, s a computer chip designed specifically for mining a particular cryptocurrency, such as Bitcoin. Unlike general-purpose hardware, it performs one type of calculation (the mining algorithm) extremely efficiently. It's faster and more energy-efficient than FPGA

Mining pool

- Mining alone is no more convenient.
- The likelihood of finding a block is so low .
- Even the most powerful last just released ASIC represent a negligible share of the total hash power. Thus, there is the chance that the hardware become old before it mines the first block.

Many miners now collaborate to form mining pools, pooling their hashing power and sharing the reward among thousands of participants. By participating in a pool, miners get a smaller share of the overall reward, but typically get rewarded every day, reducing uncertainty.

How it works:

- A group of miners form a mining pool to work together on finding blocks.
- The pool manager run a bitcoin node collect transactions, ensemble them into a block and send the block to the pool particpiants
- All miners in the pool try to mine a block with a designated coinbase recipient (the pool manager).
- Regardless of who finds the block, the pool manager receives the mining reward.
- The pool manager then distributes the rewards among participants based on each miner's contribution (amount of work done).
- The pool manager takes a small fee for managing the pool.
- Miners trust the pool manager

Mining pool

Mining shares: Miners can prove probabilistically how much work they're doing by outputting shares , or near-valid blocks. In the process of searching for such a block, miners will find some blocks with hashes beginning with a lot of zeros, but less then those needed by the target.

```
4AA087F0A52ED2093FA816E53B9B6317F9B8C1227A61F9481AFED67301F2E3FB
D3E51477DCAB108750A5BC9093F6510759CC880BB171A5B77FB4A34ACA27DEDD
00000000008534FF68B98935D090DF5669E3403BD16F1CDFD41CF17D6B474255
BB34ECA3DBB52EFF4B104EBBC0974841EF2F3A59EBBC4474A12F9F595EB81F4B
00000000002F891C1E232F687E41515637F7699EA0F462C2564233FE082BB0AF
0090488133779E7E98177AF1C765CF02D01AB4848DF555533B6C4CFCA201CBA1
460BEFA43B7083E502D36D9D08D64AFB99A100B3B80D4EA4F7B38E18174A0BFB
000000000000000078FB7E1F7E2E4854B8BC71412197EB1448911FA77BAE808A
652F374601D149AC47E01E777613845618 1FA4F9D0EEDD8C4FDE3BEF6B1B7ECE
785526402143A291CFD60DA09CC80DD066BC723FD5FD20F9B50D614313529AF3
000000000041EE593434686000AF77F54CDE839A6CE30957B14EDEC10B15C9E5
9C20B06B01A0136F192BD48E0F372A4B9E6BA6ABC36F02FCED22FD9780026A8F
```

Mining pool

Pay per shares: In the pay per share model, the pool manager pays a flat fee for every share above a certain difficulty for the block that the pool is working on. In this model, miners can send their shares to the pool manager right away and get paid without waiting for the pool to find a block.

Proportional: Every time a valid block is found the rewards from that block are distributed to the members proportional to how much work they actually did.

Summary of Mined Blocks

Miner / Pool	Percent	Blocks Mined
Unknown	53.254%	90
AntPool	17.160%	29
ViaBTC	12.426%	21
F2Pool	11.243%	19
SBI Crypto	2.367%	4
Braiins Pool	1.775%	3
BTC.com	1.183%	2
Ultimus	0.592%	1

https://www.blockchain.com/explorer/charts/pools

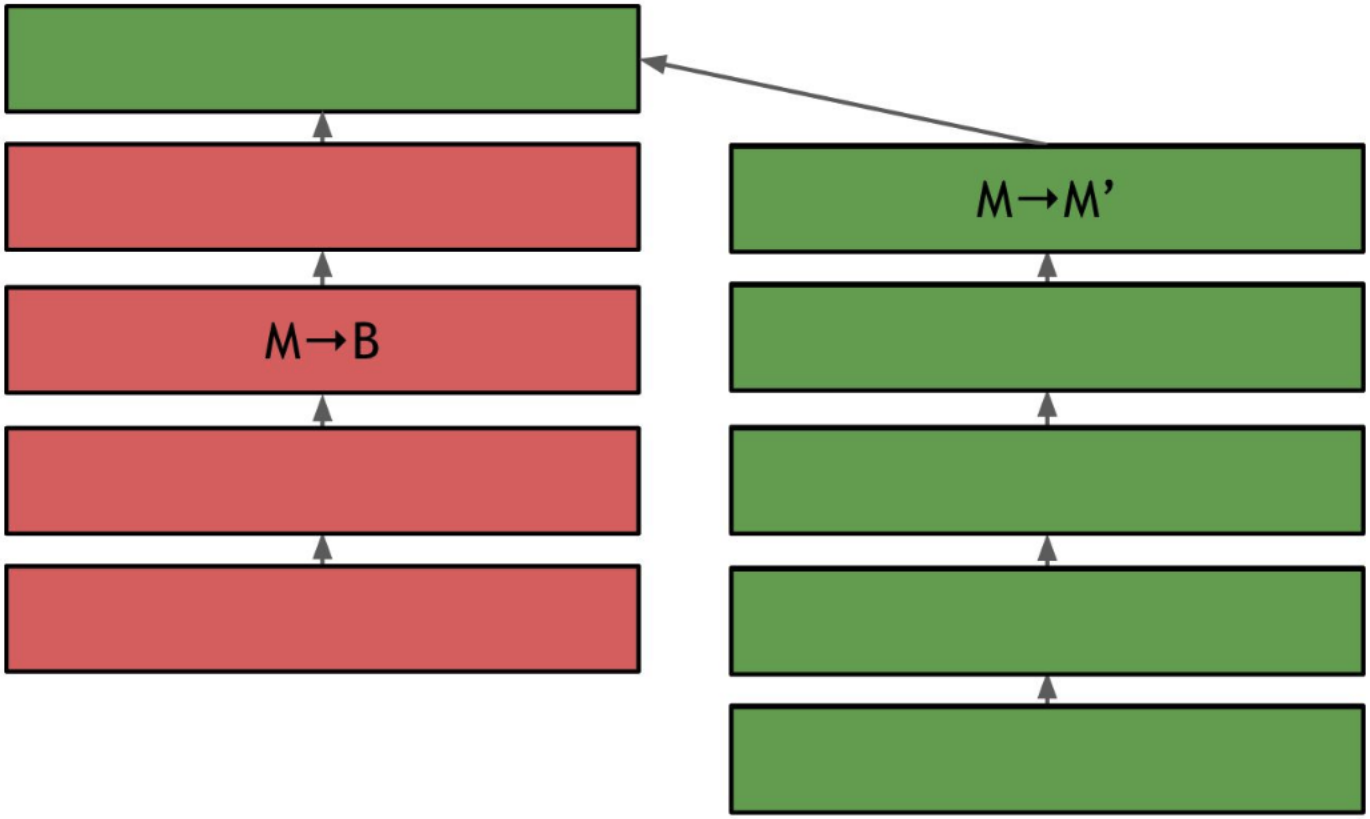
Hash rate attacks

51% attack: in a 51% attack, one miner or mining group gains or purchases enough hash power to take control of 51% or more of a blockchain network and double-spend the cryptocurrency involved.

In June 2014, the mining pool GHash.IO reached a level of about 55% of Bitcoin's hashrate over a 24-hour period.

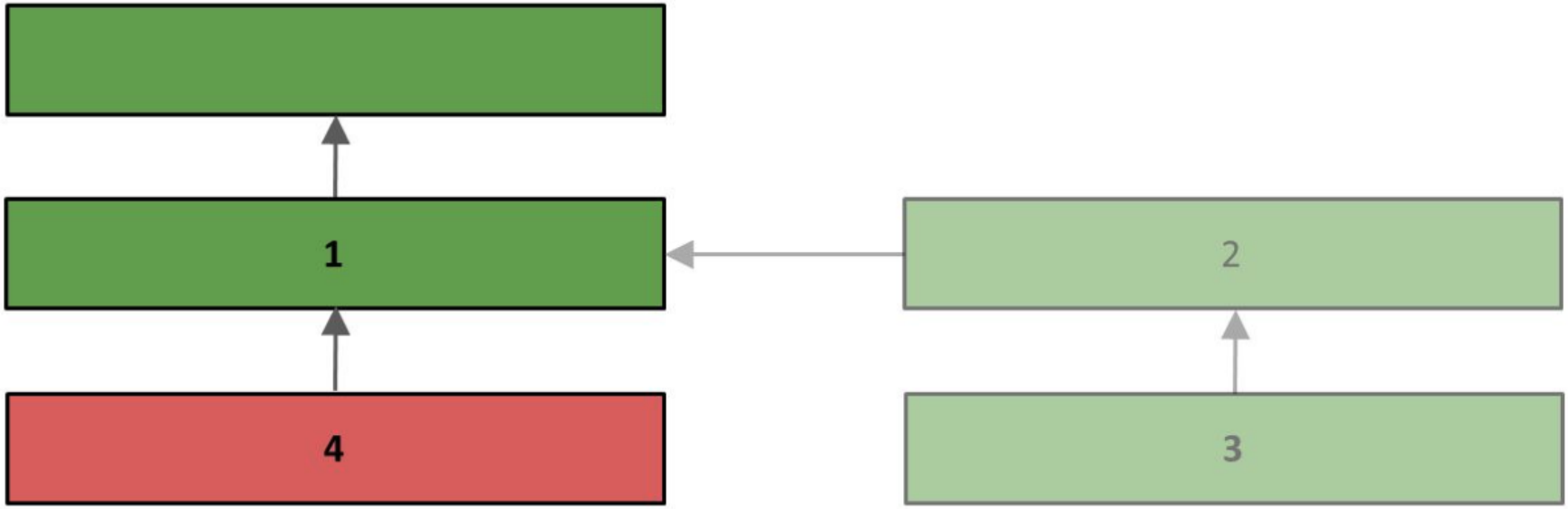
Hash rate attacks

Forking attack ($\alpha > 50\%$): The miner sent a transaction to B (M->B). Then, the miner goes ahead and begins working on an earlier block — before the block that contains the transaction to B. In this forked chain, the miner inserts an alternate transaction (M->M') — or a double spend — which sends the coins paid to B on the main chain back to one of the miner's own addresses M'.



Hash rate attacks

Temporary block-withholding attacks ($\alpha > 25 - 33\%$): : When a new block is mined, instead of follow the default behavior and immediately announce it to the network, you don't announce it right away. Instead you try to get ahead by doing some more mining on top of this block (**selfish mining**) in hopes of finding two blocks in a row before the rest of network finds even one, keeping your blocks secret the whole time.



Hash rate attacks

Blacklisting and punitive forking ($\alpha > 50\%$) : In punitive forking, miners agree to reject any chain that includes transactions from a blacklisted address. By refusing to mine on such chains, and if they control a majority of the hash power, they can effectively prevent those transactions from ever being confirmed. Other miners eventually stop including the blacklisted transactions, since their blocks would be repeatedly orphaned and yield no rewards.

Blacklisting and punitive forking : Instead of announcing that you're going to fork forever as soon as you see a transaction originating from address X , you announce that you'll attempt to fork if you see a block that has a transaction from address X , but you will give up after a while. For example, you might announced that after k blocks confirm the transaction from address X, you'll go back to the longest chain.