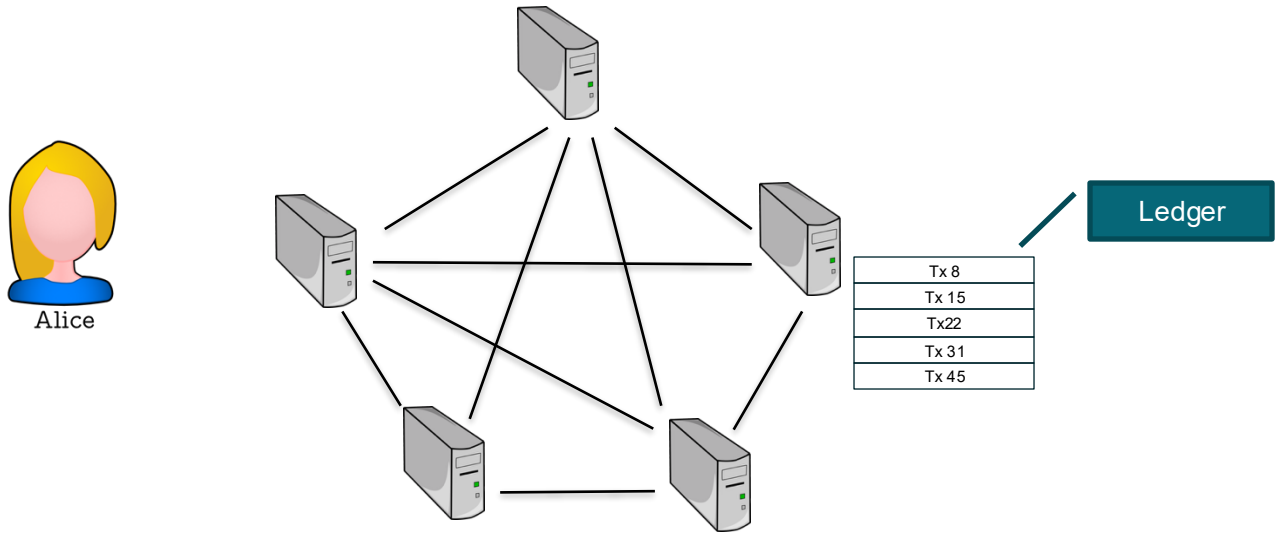
Bitcoin in 2 hours (or less) - #01

Blockchain and Distributed Ledger technologies

SAPIENZA
UNIVERSITÀ DI ROMA

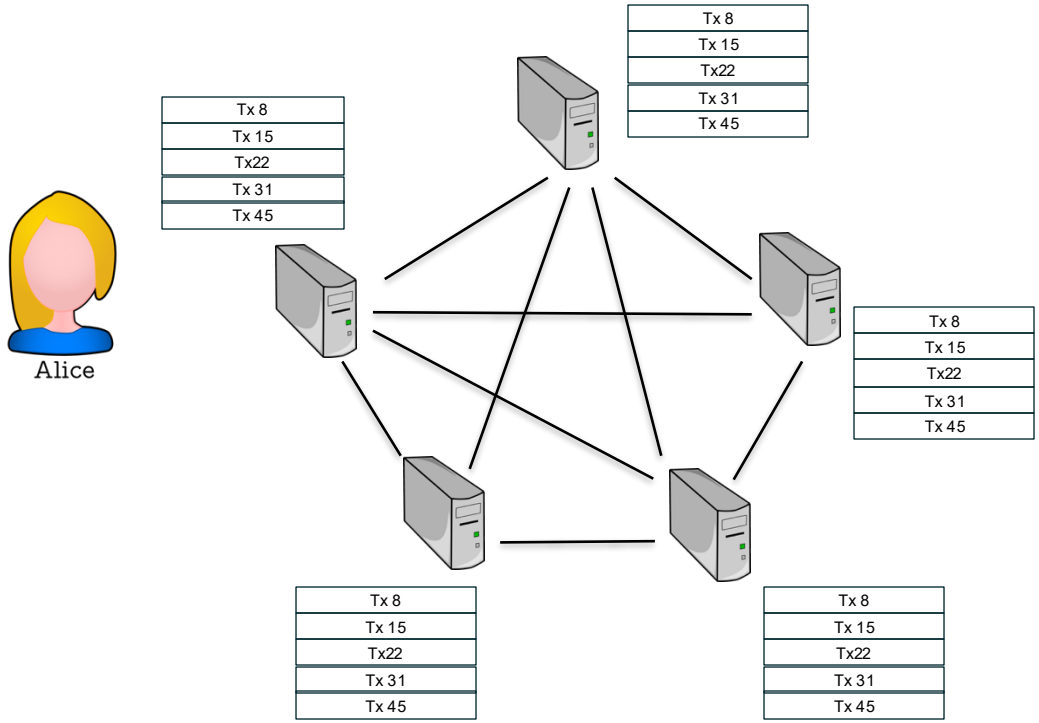
Massimo La Morgia
massimo.lamorgia@uniroma1.it

How Bitcoin Works



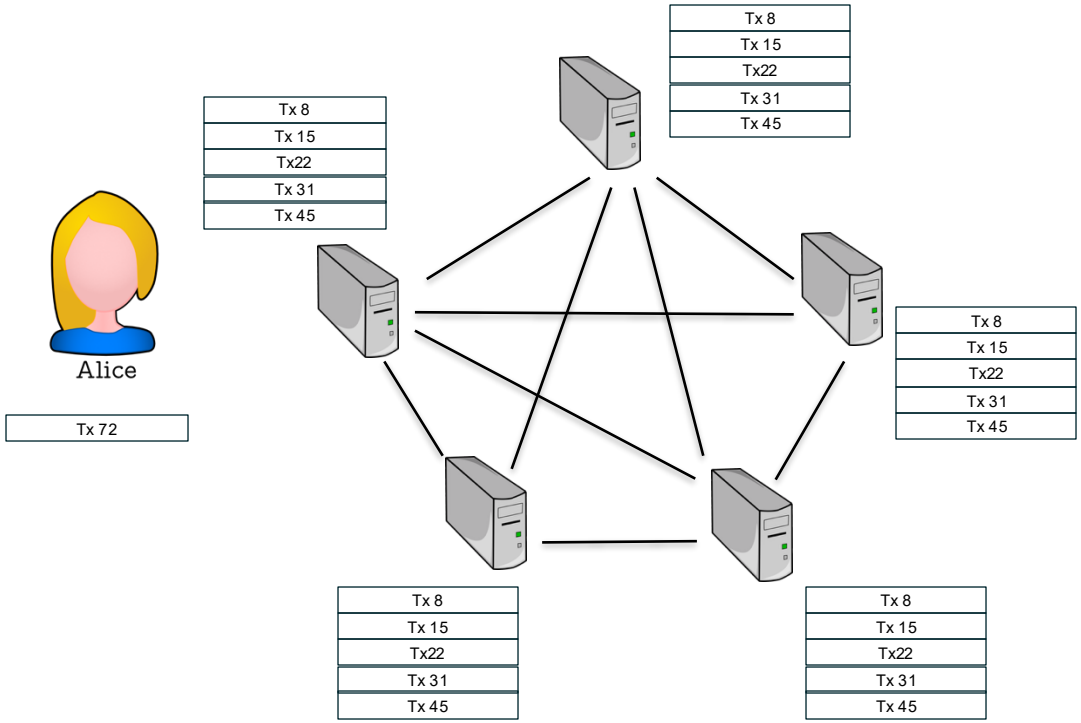
It is a network of nodes that aim to maintain the exact same copy of data, which is the ledger.

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.

Transactions

A **transaction** is the transfer of **X** coins from an account **A** to an account **B**.

Transactions are recorded into the ledger.

Each transaction must be **signed** by the owner of the funds (the sender of the transaction).

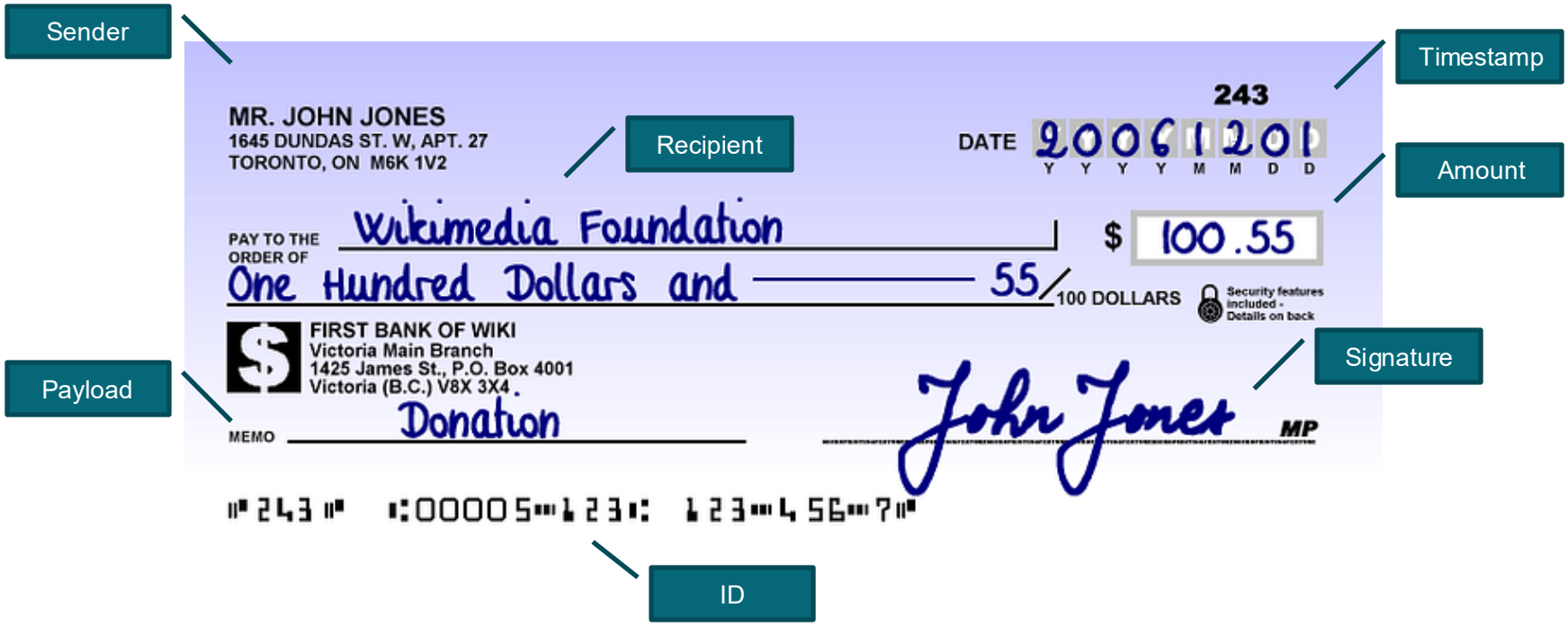
Digital signature

We can think to the digital signature as the digital analog to a handwritten signature on paper.

We desire two properties from digital signatures:

- only you can make your signature, but anyone who sees it can verify that it's valid.
- The signature have to be tied to a particular document so that the signature cannot be used to indicate your agreement or endorsement of a different document.

Metaphor: the paper check



No money exchanges hands until:

a) the person/company you gave the check to deposits it into their bank

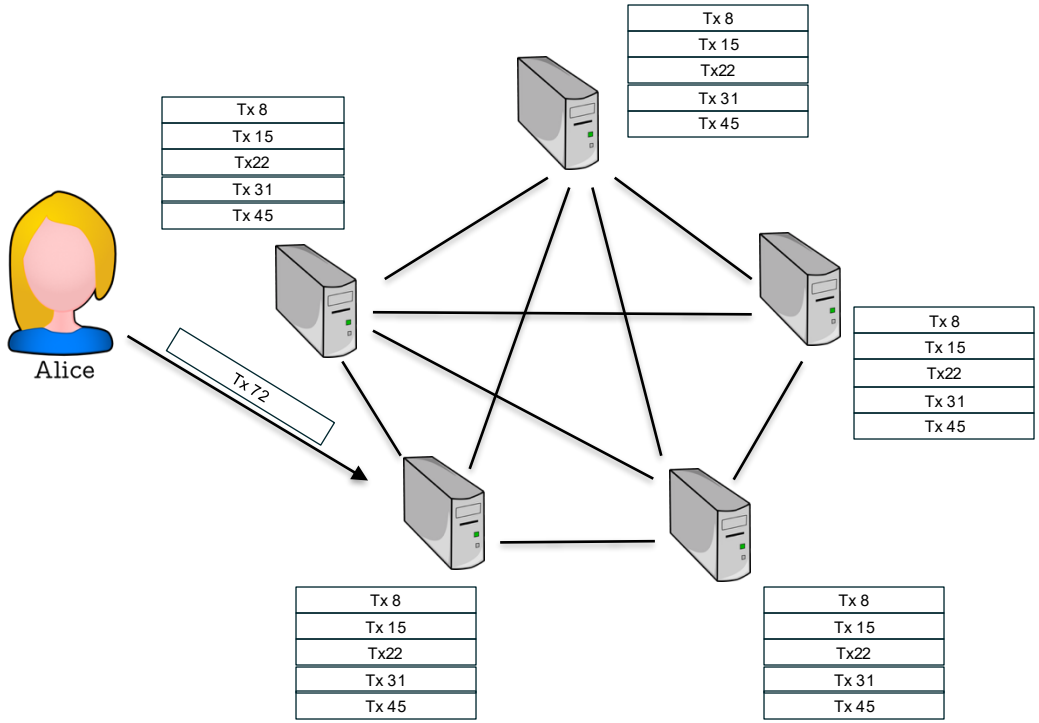
b) their bank then asks your bank for the money using the check as proof

c) if your bank account has enough money to cover it, the amount is subtracted from your account and sent to the recipients bank — if your account doesn't have enough money it is rejected (bounced check)

d) the recipients bank adds the amount to their account

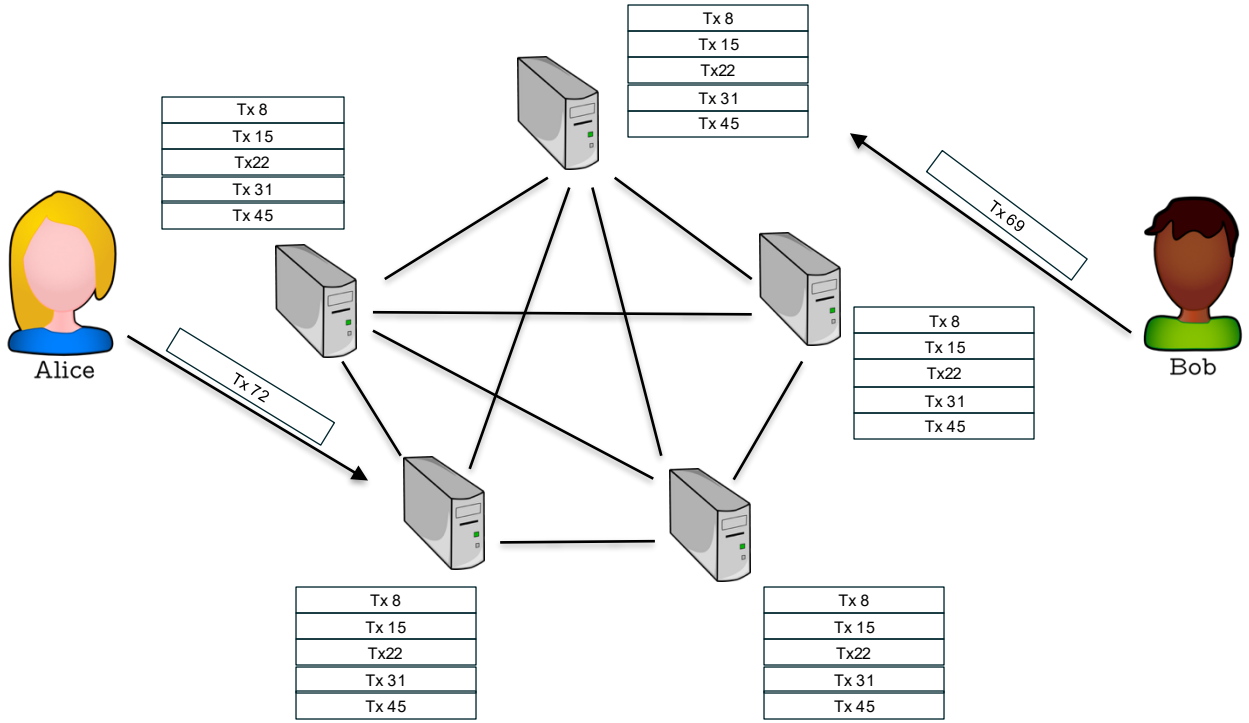
https://medium.com/gochain/a-cryptocurrency-transaction-is-almost-the-same-as-a-check-cheque-b169b08a20d6

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.

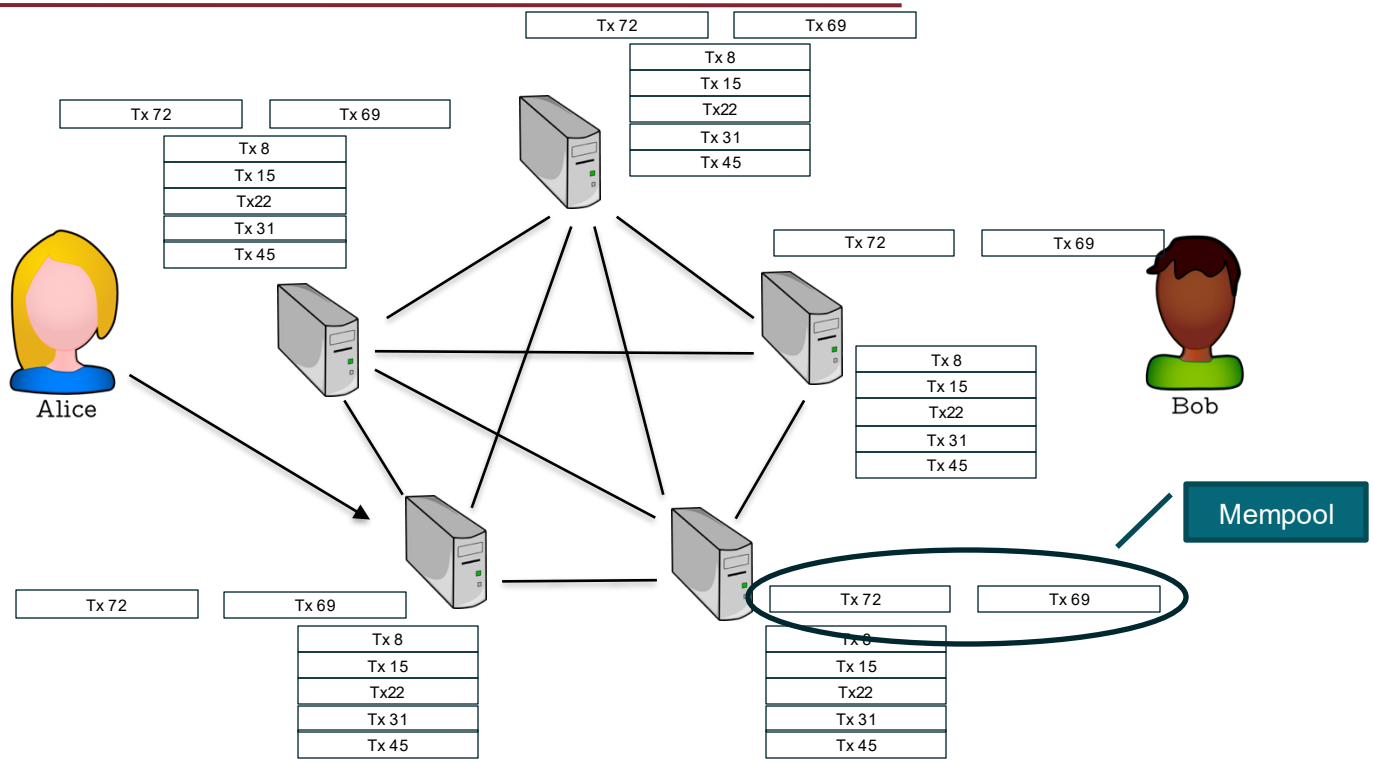
How Bitcoin Works



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 ùyou 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.

Are transactions f(r)ee?

No, transactions are not free. To record a transaction on the blockchain, users must pay a fee.

The fee is not based on the amount of Bitcoin being transferred but on the transaction's size in bytes.

The fee rate (sat/B, or Satoshis per byte) is determined through a competitive auction process.

During network congestion, users must pay higher fees to get their transactions prioritized.

The higher the sat/byte paid, the faster the transaction will be confirmed and added to the blockchain.

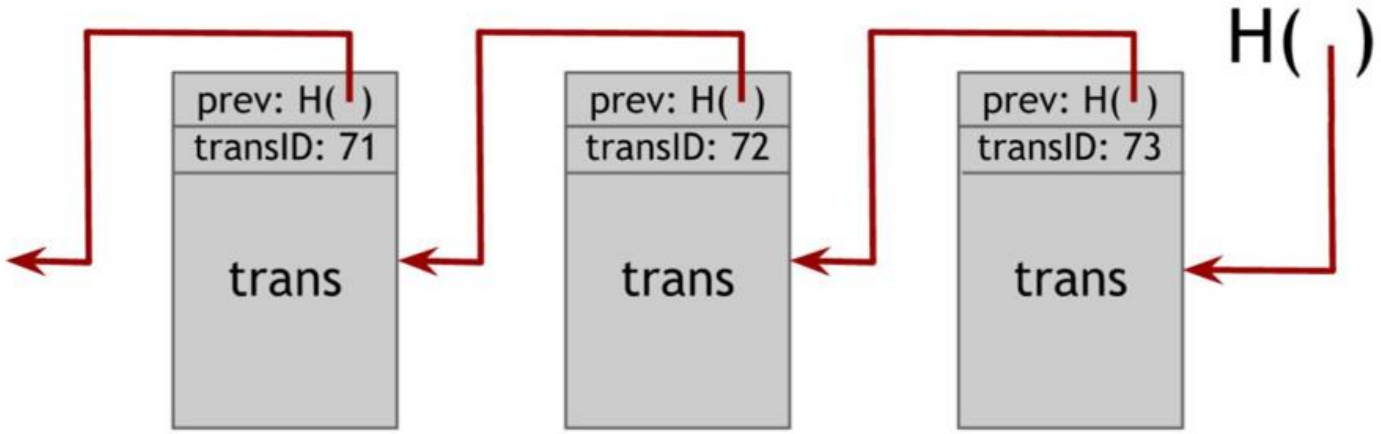
If the fee is too low, the transaction may remain stuck in the **mempool** indefinitely

A block

Transactions are packed into a block.

A block have a fixed size.

A blockchain is a sequence of block linked each other.



Bitcoin nodes

There are two main kind of nodes in Bitcoin:

Client nodes: These nodes store a complete copy of the Bitcoin blockchain and validate transactions independently.

- Verify all transactions and blocks according to Bitcoin's consensus rules.
- Help propagate valid transactions and blocks across the network.
- Increase decentralization and security by ensuring no single point of failure.

Mining nodes: Special client nodes that participate in Bitcoin mining by solving cryptographic puzzles (Proof-of-Work).

- Create new blocks by competing to solve complex mathematical problems.
- Receive Bitcoin block rewards and transaction fees as incentives.
- Require high computational power (ASIC miners are commonly used).

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

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

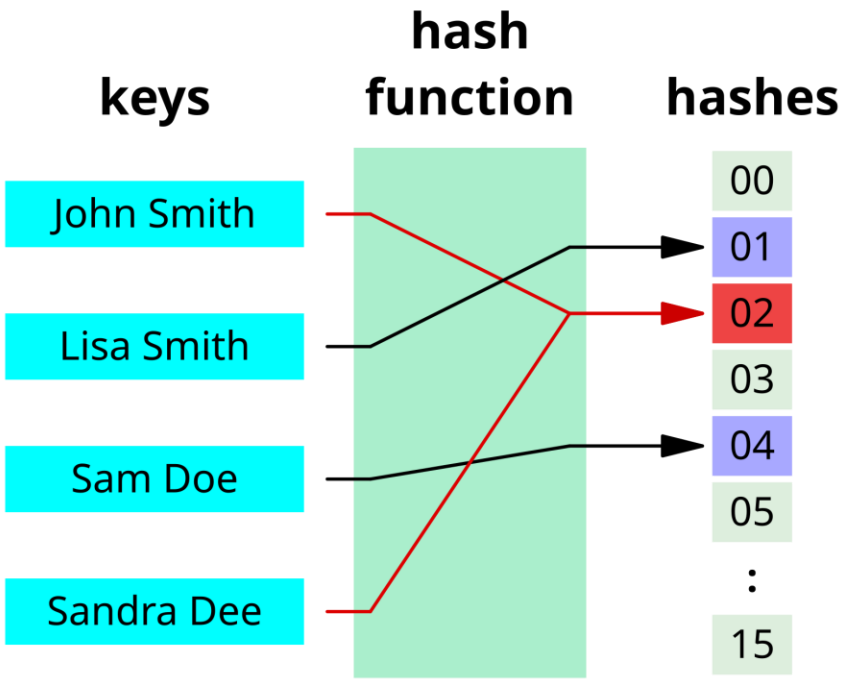
1. New transactions are broadcast to all nodes
2. Each node collects new transactions into a block
3. In each round a random node gets to broadcast its block
4. Other nodes accept the block only if all transactions in it are valid (unspent, valid signatures)
5. Nodes express their acceptance of the block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

Hash

Definition

A hash function is a computationally efficient function mapping binary strings of arbitrary length to binary strings of some fixed length, called hash-values.

Hashing is a method of applying a cryptographic hash function to data, which calculates a relatively unique output (called a message digest, or just digest) for an input of nearly any size



Images from Wikipedia and definition from NISTIR 8202 and "Handbook of Applied Cryptography" (Menez, Van Oorschot, Vanstone)

Hash

H(“Bitcoin”) = b4056df6691f8dc72e56302ddad345d65fead3ead9299609a826e2344eb63aa4

H(”bitcoin”) = 6b88c087247aa2f07ee1c5956b8e1a9f4c7f892a70e324f1bb3d161e05ca107b

H(“1”) = 6b86b273ff34fce19d6b804eff5a3f5747ada4eaa22f1d49c01e52ddb7875b4b

H(“2”) = d4735e3a265e16eee03f59718b9b5d03019c07d8b6c51f90da3a666eec13ab35

H() is the SHA-256

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

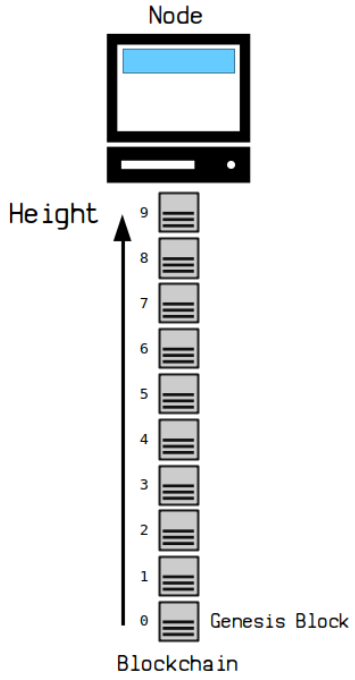
In a distributed system, a "round" refers to a discrete step or iteration in which processes communicate, perform actions, and update their states.

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)



Incentives

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

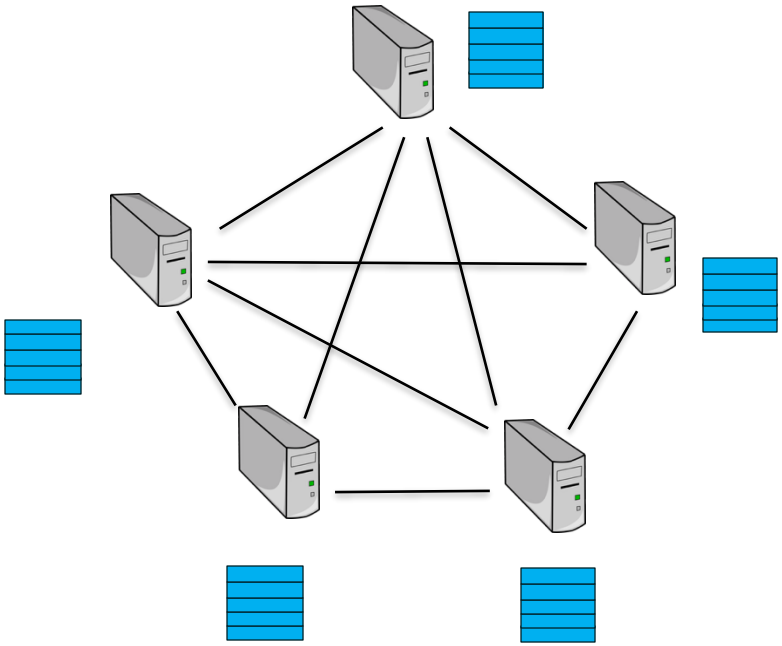
The miner that proposes the new block can forge a transaction that mint new Bitcoins, this transaction is called **coinbase transaction**.

Actual block reward 3.125 bitcoins

Bitcoin total supply limit 21’000’000

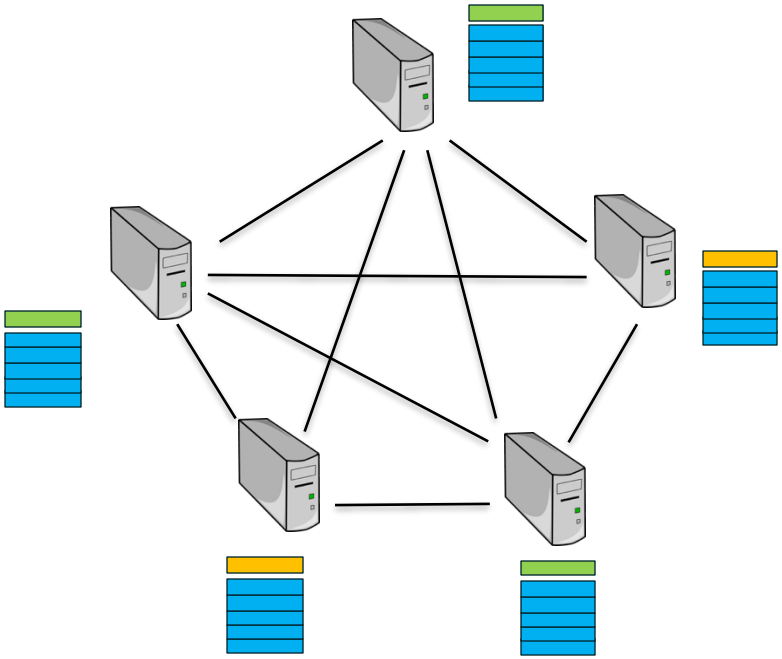
Fork

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 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)