LimeChain

A Survey of Blockchain Consensus Algorithms and attacks

By Ognyan Chikov

Senior Blockchain Developer @LimeChain

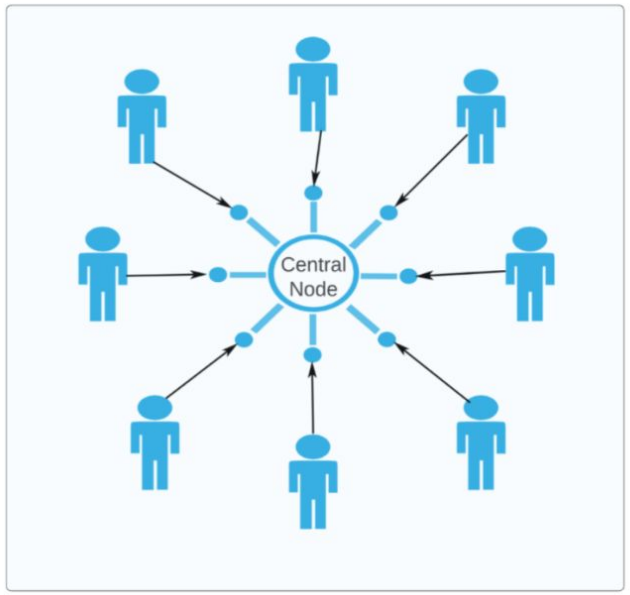
limechain.tech

Table of contents

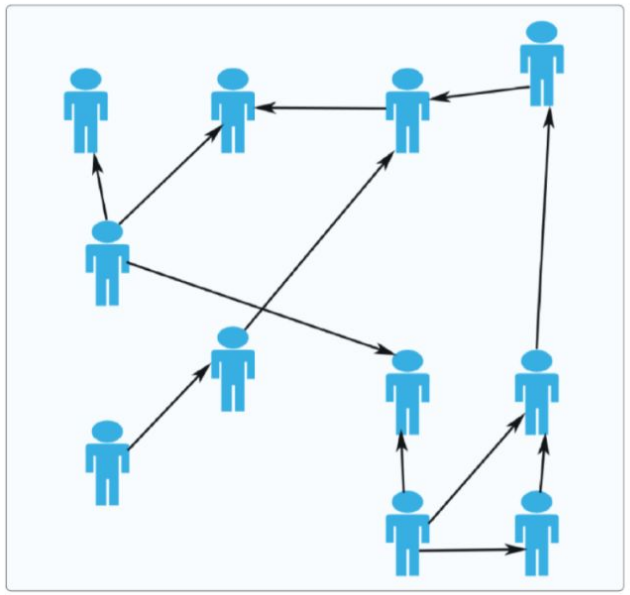
What is a Blockchain?

You can add a short description or leave it blank. It’s up to you.

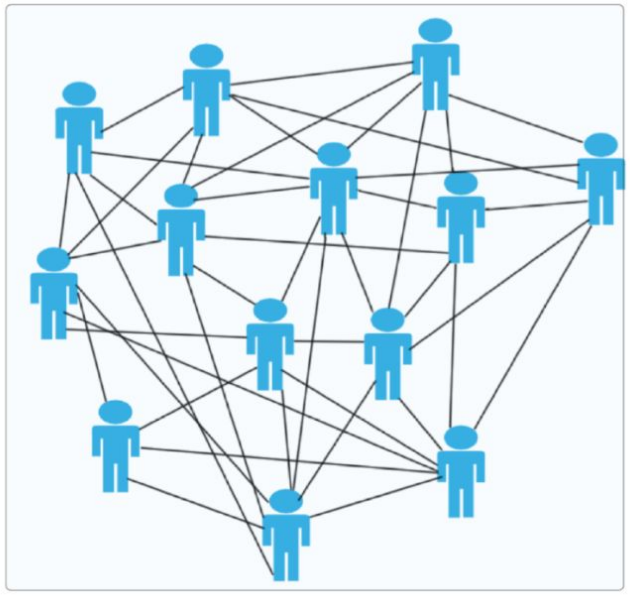
Centralized Network



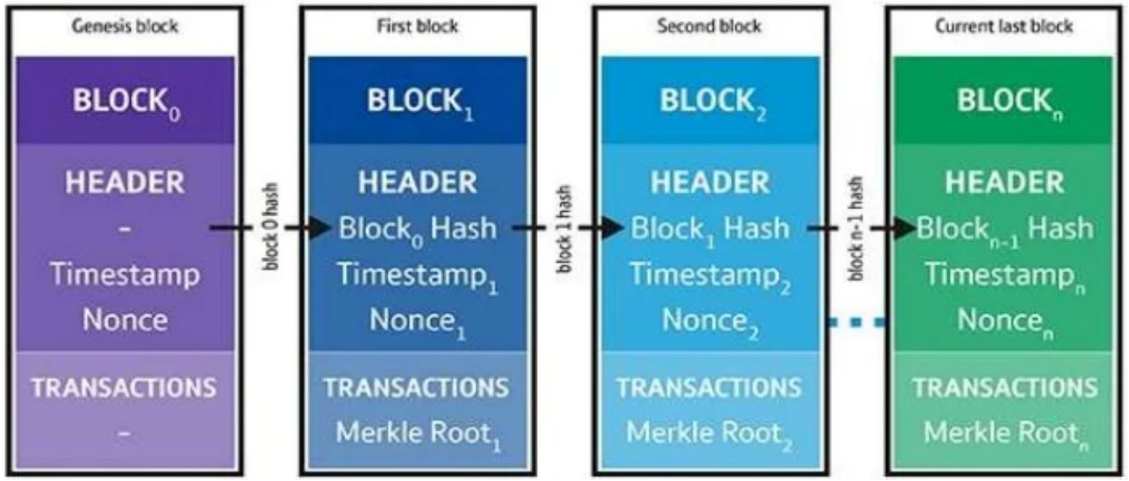
Decentralized Network



Distributed Network



Blockchain - Decentralized Ledger Technology

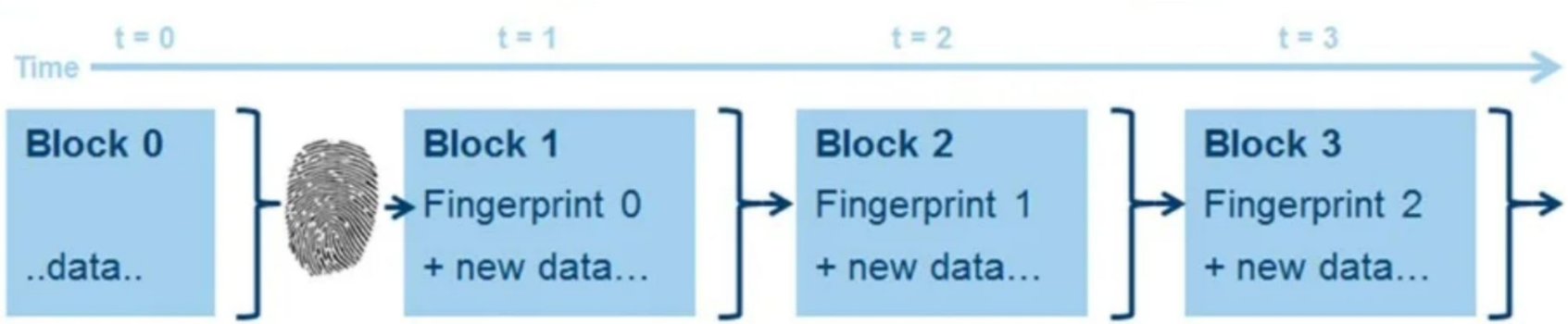


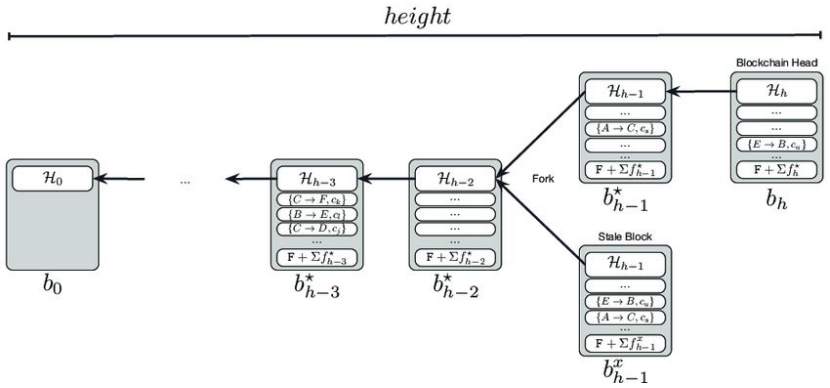
How does a Blockchain work?

You can add a short description or leave it blank. It’s up to you.

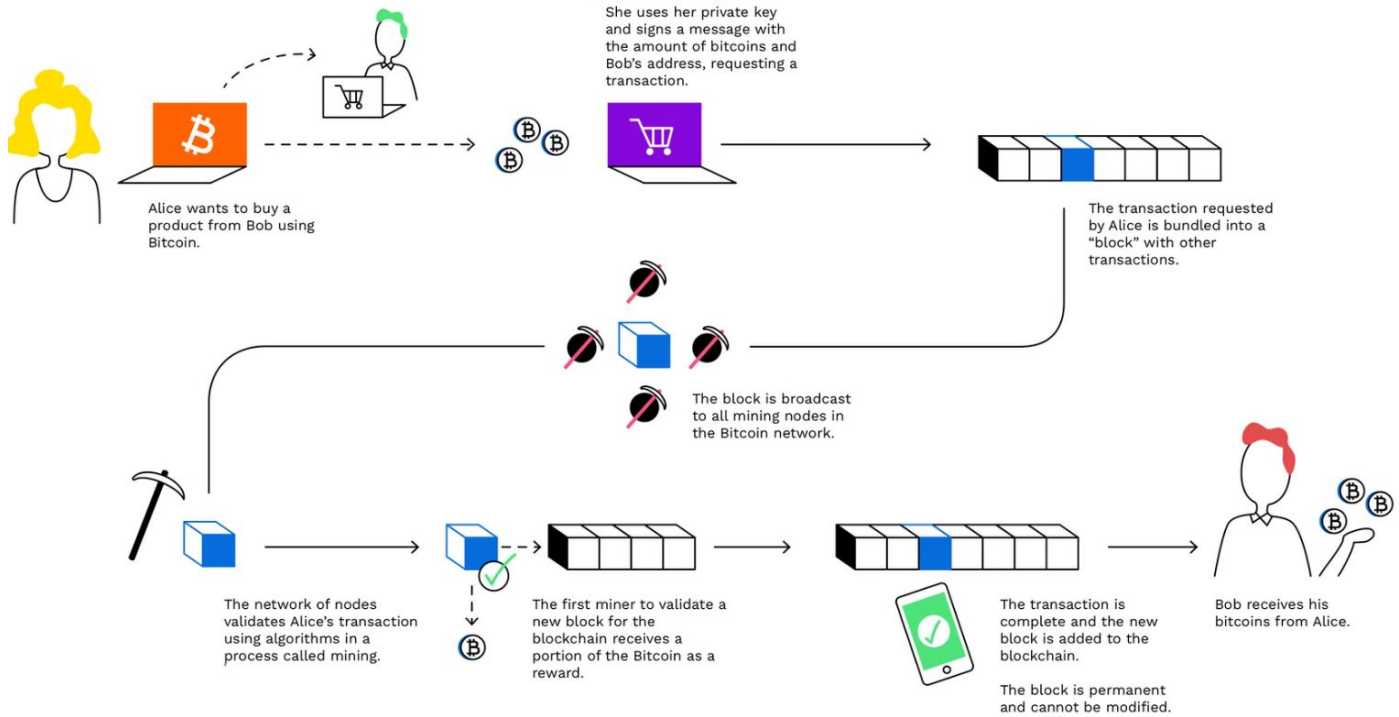
Blockchain == chain of data blocks

You can ad





Mining the next block


Alice wants to buy a product from Bob using Bitcoin.
She uses her private key and signs a message with the amount of bitcoins and Bob's address, requesting a transaction.
The transaction requested by Alice is bundled into a "block" with other transactions.
The block is broadcast to all mining nodes in the Bitcoin network.
The network of nodes validates Alice's transaction using algorithms in a process called mining.
The first miner to validate a new block for the blockchain receives a portion of the Bitcoin as a reward.
The transaction is complete and the new block is added to the blockchain.
The block is permanent and cannot be modified.
Bob receives his bitcoins from Alice.

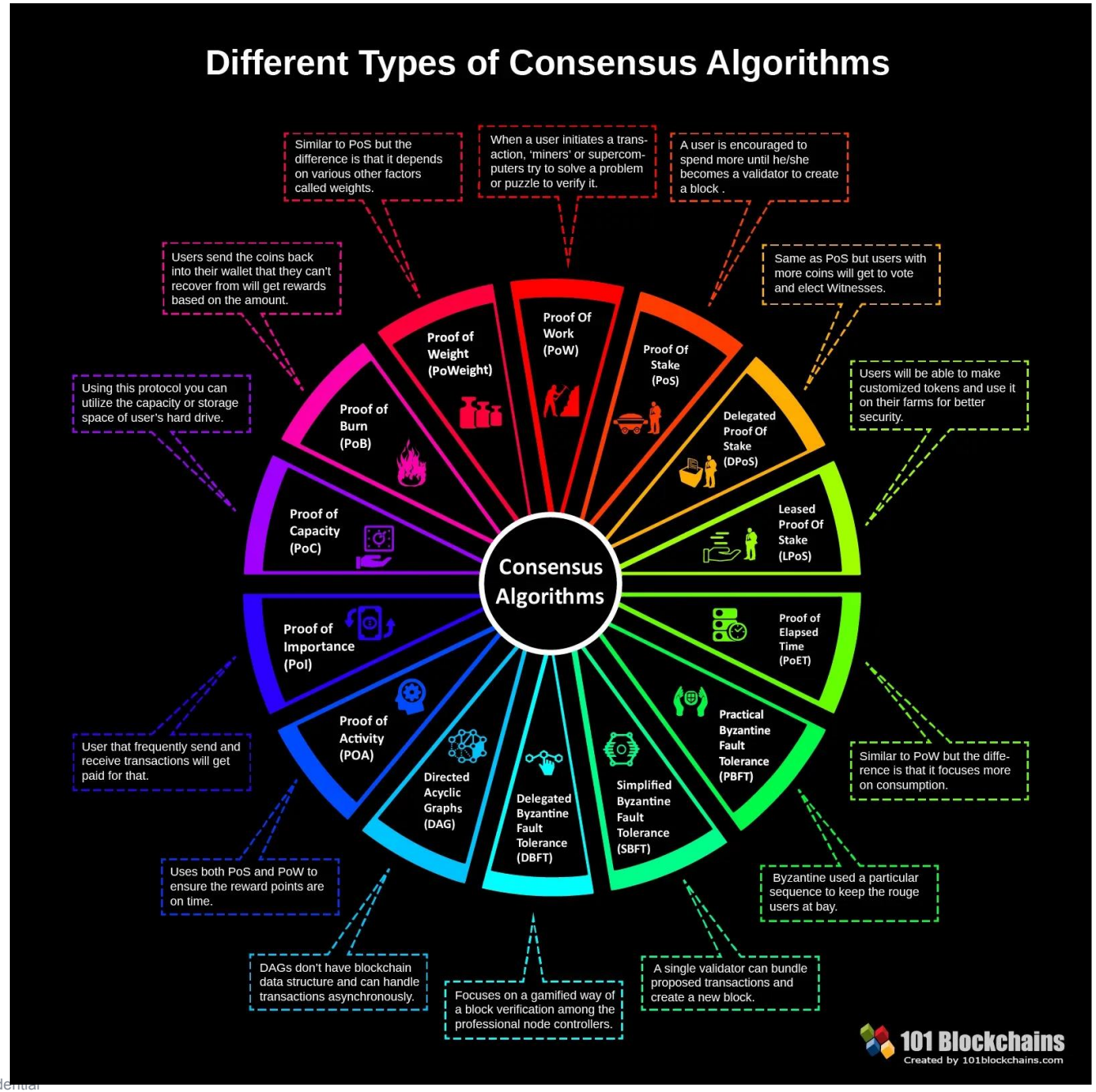
What is a Consensus Algorithm?

You can add a short description or leave it blank. It’s up to you.

- **Consensus Algorithm / Consensus Protocol / Consensus Mechanism**
- **Algorithm to reach agreement among the blockchain nodes**
- **All nodes should agree about the changes in the distributed ledger**
- **Proof of Work (PoW) / Proof of Stake (PoS) / Others**

Consensus Algorithms

You can add a short description or leave it blank. It’s up to you.


Different Types of Consensus Algorithms
Consensus Algorithms
Proof Of Work (PoW)
When a user initiates a transaction, 'miners' or supercomputers try to solve a problem or puzzle to verify it.
Proof Of Stake (PoS)
A user is encouraged to spend more until he/she becomes a validator to create a block .
Delegated Proof Of Stake (DPoS)
Same as PoS but users with more coins will get to vote and elect Witnesses.
Leased Proof Of Stake (LPoS)
Users will be able to make customized tokens and use it on their farms for better security.
Proof of Elapsed Time (PoET)
Similar to PoW but the difference is that it focuses more on consumption.
Practical Byzantine Fault Tolerance (PBFT)
Byzantine used a particular sequence to keep the rouge users at bay.
Simplified Byzantine Fault Tolerance (SBFT)
A single validator can bundle proposed transactions and create a new block.
Delegated Byzantine Fault Tolerance (DBFT)
Focuses on a gamified way of a block verification among the professional node controllers.
Directed Acyclic Graphs (DAG)
DAGs don't have blockchain data structure and can handle transactions asynchronously.
Proof of Activity (POA)
Uses both PoS and PoW to ensure the reward points are on time.
Proof of Importance (PoI)
User that frequently send and receive transactions will get paid for that.
Proof of Capacity (PoC)
Using this protocol you can utilize the capacity or storage space of user's hard drive.
Proof of Burn (PoB)
Users send the coins back into their wallet that they can't recover from will get rewards based on the amount.
Proof of Weight (PoWeight)
Similar to PoS but the difference is that it depends on various other factors called weights.
101 Blockchains
Created by 101blockchains.com

Consensus Algorithm - Requirements

- Fault tolerance
  - Some nodes will be unavailable when the ledger is changes
  - Consensus should be reached by part of the nodes (e.g MAJORITY)
- Attack-resistance
  - Some nodes will intentionally behave incorrectly
  - Honest nodes should win in the consensus process
  - Everyone in the network can verify the correctness of next block
  - Too much resources should be required for successful attack

Proof of Work (PoW)

A “proof of work” is a piece of data which:

- Difficult to produce
- Easy for others to verify
- Producing proof of work can be a random guessing process
- Can be organized in mining pools

Example:

- Find a number X such that SHA256(text + x) has 10 leading zeros
- 10 zeros == network difficulty

Proof of Work Problems

Needs computing power

- Computationally expensive
- Energy expensive

51% Attack:

- Attackers holding more than 50% of the power could potentially reverse-back transactions (double spend money / deny service)

Hashing Algorithm Types:

- ASIC minable (CPU Mineable)
- GPU mineable

Proof of Work Problems (2)

Transaction Speed - Average Wait Time

- Bitcoin - every new block is mined ~9 min
- Ethereum - every new block is mined ~10 sec
- Business needs real-time transactions (milliseconds)

Transactions Throughput - Transactions per second (tps)

- Bitcoin 2000 - 3000 transactions per block 3-5 tps
- Ethereum 200 - 300 transactions per block 10-15 tps
- Business needs thousands of tps (VISA performs 2000 tps)

Proof of Capacity (PoC)

Similar to PoW but based on HDD, not CPU/GPU

- Pay for mining with Hard drive space
- More Hard drive space -> better chance to mine the next block

Calculating hashes is slow, so hashes are stored into HDD for faster access

- Plots - large data files holding of precomputed hashes
- More plots -> better your chance finding the next block
- Plot size is similar to hash rate in PoW

Proof of Stake (PoS)

PoS is designed to increase network security and reduce resource wasting

The creator of the next block is chosen in:

- Combination of random selection and wealth
- E.g Holding 1% of the coins gives the chance to verify (mine) 1% of the “Proof of Stake blocks”

The Monopoly problem:

- A monopolist (holder of the most coins) could double spend or deny / filter others transactions.
- Executing a monopoly attack is much more expensive than in PoW

Delegated Proof-of-Stake (DPoS)

Stakeholders vote for delegates in democratic way

- Every wallet holding coins can vote for delegates
- Votes weight is proportional to the wallet's stake in the network

Delegates generate new blocks (like miners in PoW)

- Validate transactions and take the fees as profit
- Maintain the blockchain, e.g vote for changing the network parameters like block intervals, transaction fees, others
- Very fast confirmation of transactions (<1s)

Leased Proof-of-Stake (LPoS)

In Leased PoS users can choose:

- To be a full node or lease their stake
- Votes weight is proportional to the wallet’s stake in the network

Full nodes maintain the network

- Process transactions and generate new blocks
- PoS based on own stake + leased stake
- Serve as mining pool - collect fees and distribute profits
- Most users lease their stake to full nodes
- Users take a portion of the full node`s profits just like in the pool mining

Proof of Burn (PoB)

Pob is similar to PoS, where stakes are based on burned coins

Burning coins gives the privilege to mine

- Burn coins by sending them to a burning address (where they are irretrievable)
- More coins you burn = better chance to be selected to mine the next block
- Random selection process (weighted)

Like traditional mining -> invest money to get mining power:

- PoW -> invest in hardware; PoB -> invest in burning coins

Practical Byzantine Fault Tolerance (PBFT)

Nodes collecting transactions, selects a leader for the next block

- Can be random (deterministic) or random based on stake
- The leader orders the transaction + broadcast the ordered list
- Each nodes validates / executes the transactions + broadcast the calculated hash of the new block
- When ⅔ of the nodes has the same hash the new block is published (mined)
- Transactions are fast