Co**nsensus Mechanism**

What is Consensus?

Consensus means achieving a state of a decision on which all network participants agree. For example, a group of friends decides on a trip to Goa without conflicts. Here, reaching a decision to visit Goa together is a state of consensus or mutual agreement

What is Consensus Mechanism?

A consensus algorithm is a way to keep network members synchronized under democracy. With decentralization, each network member has equal power to make decisions in the system. Hence, rules need to be established for network members (or nodes) to implement new changes to the system with a global agreement.

"The purpose of the Consensus mechanism in a decentralized network is to allow a group of independent nodes to distribute the right to update as well as validate the change in the network equally. Therefore, decide on the next update of a decentralized network."

In a blockchain, each participant shares the exact same copy of the network transactions, which helps them stay synchronized and connected.

How Does Consensus Work?

There is a number of consensus mechanisms to operate on a decentralized network. **Each algorithm has its own way of reaching a global agreement on a network update.**

Generally, consensus protocols form at least 51% of participants in the network to agree on the upcoming change. If they agree, the network system gets updated with the new change. Else, it rejects the change by mutual agreement.

Types of Consensus Mechanisms

Following are the consensus mechanisms used in various blockchain networks:-

SNS COLLEGE OF ENGINEERING
Kurumbapalayam (Po), Coimbatore – 641 107
AN AUTONOMOUS INSTITUTION
Accredited by NAAC-UGC with 'A' Grade, Accredited by NBA
Approved by AICTE & Affiliated to Anna University, Chennai.

DIFFERENT TYPES OF CONSENSUS MECHANISMS

PROOF OF WORK (PoW)

- PoW lets miners add a new block to the network based on the computation done to find the correct block hash.

PROOF OF STAKE (PoS)

- PoS uses a staking mechanism where participants lock up some of their coins to get selected for block addition.

DELEGATED PROOF OF STAKE (DPoS)

- In DPoS mechanism, the block delegates' selection is based on voting. It's an additional layer to PoS.

PROOF OF IMPORTANCE (PoI)

- PoI rewards users with importance scores which eventually helps them to become block harvesters.

PROOF OF CAPACITY (PoC)

- PoC uses the storage capacity for mining a block in a decentralized network.

PROOF OF ELAPSED TIME (PoET)

- PoET uses a time-lottery-based consensus mechanism, distributing wait time to each participating node.

PROOF OF ACTIVITY (PoA)

- Proof of Activity (PoA) combines the capabilities of proof of work (PoW) and Proof of Stake (PoS) algorithms.

PROOF OF AUTHORITY (PoA)

- Proof of Authority (PoA) relies on the validator's reputation to make the blockchain work properly.

PROOF OF BURN (PoB)

- PoB allows miners to add their block by sending some of their coins to an unspendable account.

BYZANTINE FAULT TOLERANCE (BFT)

- BFT works on system to stay intact even if one of the nodes fails with constant communication among nodes.

Proof of Work (PoW)

PoW is a popular consensus algorithm used by Bitcoin and Ethereum networks. Here, miners (or block adders) have to do **heavy mathematical computations** to find a **right hash** by changing the nonce of the block. The miner who finds the **hash below the difficulty level** gets the chance to add his block to the network. Hence, takes the reward.It's a **puzzle-friendly** way to reach consensus by using high computational power. Afterward, already present network participants valid transactions in the block added by the miner.

Blockchains using PoW algorithm: Bitcoin, Ethereum, Dogecoin, Litecoin, Zcash, Horizon, and many more.

Proof of Stake (PoS)

PoS consensus **eliminates the high energy consumption** by PoW. PoS uses a **staking mechanism** in which **miners (or validators) hold some of their earned coins** in the network to get selected for adding a block.It's not an initial consensus algorithm for a network. It can only be implemented after a network gets a good amount of participants (or nodes).

Blockchains using PoS algorithm: Polkadot, EOSIO, Cardano, Ethereum 2.0, and
Blockchains using the DPoS algorithm: EOS, Lisk, Ark y Tron
Blockchains using BFT algorithm: Hyperledger Fabric and Zilliqa

1. **Proof of Work (PoW):** Used by Bitcoin and other cryptocurrencies, this model requires participants (miners) to solve complex mathematical problems. The first to solve the problem gets to add a new block to the blockchain and is rewarded. The difficulty of the problem ensures that it's hard to manipulate the system.
2. **Proof of Stake (PoS):** Instead of solving computational problems, participants (validators) are chosen based on the number of coins they hold and are willing to "stake" as collateral. This model aims to be more energy-efficient compared to PoW.

3. **Delegated Proof of Stake (DPoS):** A variation of PoS, where stakeholders elect a smaller number of delegates who are responsible for validating transactions and maintaining the blockchain. This model can improve scalability and speed.
4. **Practical Byzantine Fault Tolerance (PBFT):** Used in some permissioned blockchain systems, this model can handle a certain number of faulty or malicious nodes (up to one-third) while still reaching consensus.
5. **Proof of Authority (PoA):** In this model, a limited number of trusted nodes (authorities) are responsible for validating transactions. It is often used in private or consortium blockchains.
6. **Raft:** A consensus algorithm used in distributed systems to ensure that a group of computers (nodes) agree on changes to a shared state. Raft is designed to be more understandable and practical than some other consensus algorithms.

Each model has its trade-offs in terms of security, performance, and energy consumption, and the choice of model depends on the specific needs and goals of the system.

Key Consensus Models

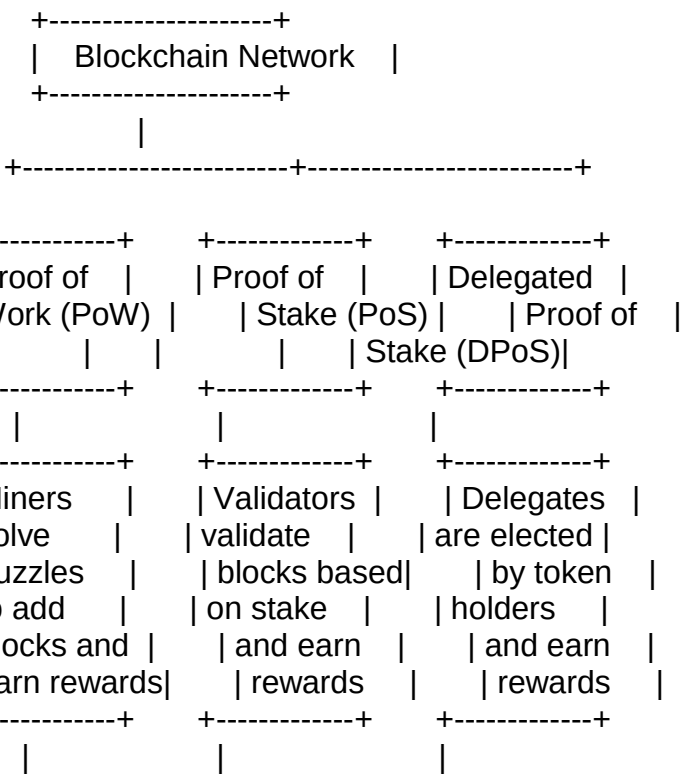
1. **Proof of Work (PoW)**
   - **Mechanism:** Miners compete to solve complex cryptographic puzzles. The first to solve the puzzle gets to add a new block to the blockchain and is rewarded.
   - **Example:** Bitcoin, Ethereum (pre-ETH 2.0).
2. **Proof of Stake (PoS)**
   - **Mechanism:** Validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral. Validators receive transaction fees and possibly rewards.
   - **Example:** Ethereum 2.0, Cardano.
3. **Delegated Proof of Stake (DPoS)**
   - **Mechanism:** Token holders elect a small number of delegates who are responsible for validating transactions and creating blocks. Delegates are rewarded, and may share rewards with voters.
   - **Example:** EOS, TRON.
4. **Proof of Authority (PoA)**
   - **Mechanism:** A limited number of trusted nodes (authorities) validate transactions and create blocks. Authority nodes are chosen based on reputation or stake, and they earn rewards for their participation.
   - **Example:** VeChain, Private blockchains.
5. **Proof of Elapsed Time (PoET)**

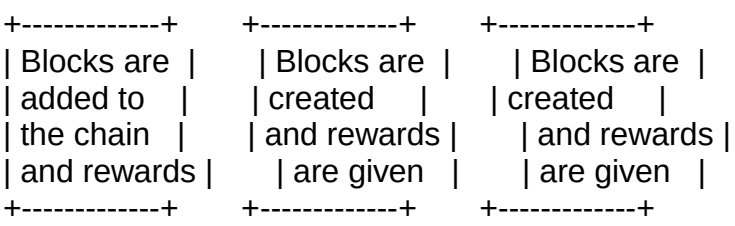
- **Mechanism:** Validators are selected based on random waiting times enforced by a trusted execution environment (TEE). The selection process is designed to be fair and efficient.
- **Example:** Hyperledger Sawtooth.

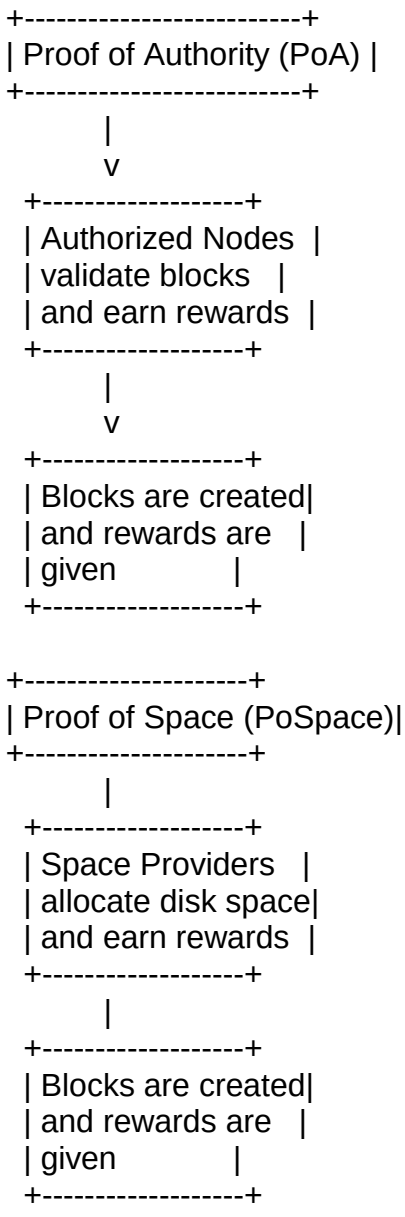
6. **Proof of Space (PoSpace)**
   - **Mechanism:** Participants allocate disk space for storing cryptographic data. The more space allocated, the higher the chance of being selected to create new blocks and receive rewards.
   - **Example:** Chia Network.
7. **Hybrid Models**
   - **Mechanism:** Combine elements from multiple consensus mechanisms to balance security, scalability, and decentralization. For example, combining PoW and PoS.
   - **Example:** Decred.

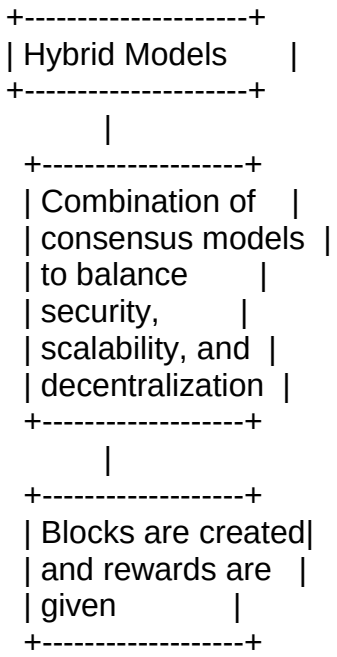
Diagram

Here's a conceptual diagram illustrating how various consensus models work:




Blocks are added to the chain and rewards
Blocks are created and rewards are given
Blocks are created and rewards are given


Proof of Authority (PoA)
Authorized Nodes validate blocks and earn rewards
Blocks are created and rewards are given
Proof of Space (PoSpace)
Space Providers allocate disk space and earn rewards
Blocks are created and rewards are given



Explanation of the Diagram

- **Proof of Work (PoW):** Miners solve cryptographic puzzles to add blocks to the blockchain and receive rewards.
- **Proof of Stake (PoS):** Validators are chosen based on their stake and validate blocks to earn rewards.
- **Delegated Proof of Stake (DPoS):** Token holders elect delegates who validate blocks and earn rewards.
- **Proof of Authority (PoA):** Trusted nodes validate transactions and create blocks, earning rewards.
- **Proof of Space (PoSpace):** Participants provide disk space for cryptographic data and are selected to create blocks based on the space they provide.
- **Hybrid Models:** Combine elements from different consensus mechanisms to achieve desired network characteristics.

Each consensus model has its own trade-offs in terms of security, efficiency, and decentralization, and the choice of model depends on the specific goals and needs of the blockchain network.