Types of Consensus Algorithms

Proof of Work (PoW)

- Proof of Work is a consensus algorithm used in many blockchain networks **to validate transactions and add new blocks to the chain**.
- PoW was **first introduced by** Bitcoin's creator, **Satoshi Nakamoto**, as a way **to secure the network** and **prevent double-spending**.
- The PoW algorithm **requires miners to solve complex mathematical problems, known as hashes**.
- Hash function used in PoW algorithms is designed to be **computationally difficult to solve**, it requires a **significant amount of computational power** to solve the problem and add a block to the chain.
- **Miners compete with each other** to solve the problem, and the **first one to solve it is rewarded with newly minted cryptocurrency**.
- This **algorithm's security** comes from the fact that it is **difficult to solve** the hash problem, which means that it is **expensive for an attacker** to try to take over the network.
- The attacker would **need to have control** over a significant portion of the network's computational power, known as the **hash rate**, in order **to launch an attack**.
- This is **known as a 51% attack**, and it is difficult to pull off because it would **require a massive amount of resources**.

Types of Consensus Algorithms

Proof of Stake (PoS)

- Unlike PoW, which requires miners to solve complex mathematical problems, **PoS relies on validators** who **hold a certain amount of cryptocurrency** to validate transactions and add new blocks to the chain.
- In a PoS network, **validators are chosen** to add new blocks to the chain **based on the amount of cryptocurrency they hold**, which is known as **their stake**.
- The larger the stake, the **greater the chance of being selected** to add a block to the chain.
- Validators are incentivized to act honestly because **they risk losing their stake if they validate fraudulent transactions** or try to attack the network.

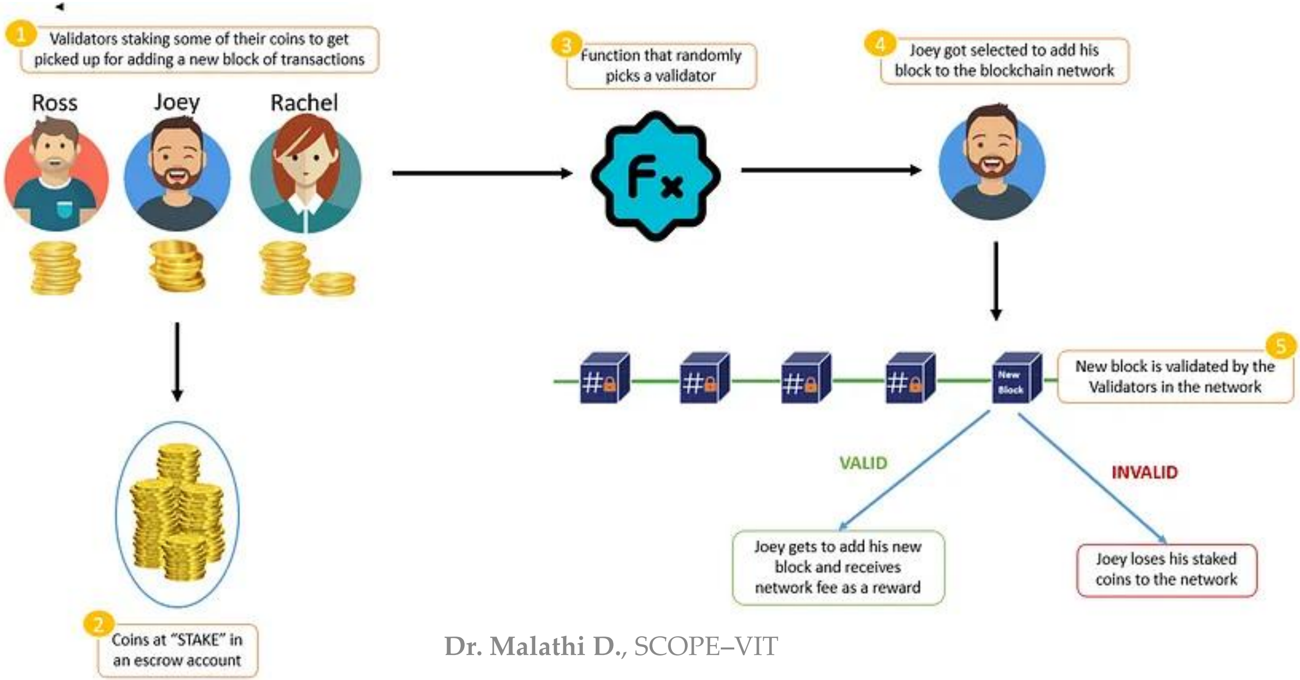
Advantages

- **Less energy-intensive**: PoW requires miners to use significant amounts of computational power to solve complex mathematical problems, while **PoS only requires validators to hold cryptocurrency**. This makes PoS more environmentally friendly and less costly to operate.
- **Promotes decentralization**: In a PoW network, **miners with the largest hash rate have more control** over the network, which can **lead to centralization**. In a PoS network, **validators with the largest stake have more control**, but it is **difficult for a single/group of validators** to gain control of the network because they would need to control a significant amount of cryptocurrency.

Types of Consensus Algorithms

Disadvantages

- **Rich-get-richer**: **Validators with the largest stake continue to earn more cryptocurrency**, making it more difficult for smaller validators to participate in the network.
- **Solution**: Random selection of validators or limiting the amount of cryptocurrency that a single validator can hold.



Types of Consensus Algorithms

Delegated Proof of Stake (DPoS)

- DPoS is a **variation** of Proof of Stake (PoS) that **relies on a smaller group of validators, known as delegates or witnesses**, to validate transactions and add new blocks to the chain.
- In a DPoS network, **token holders vote for delegates to represent them in the validation process**.
- The delegates are **incentivized to act honestly** because they risk losing their position and rewards if they validate fraudulent transactions or try to attack the network.

Advantages

- **Efficient**: **PoS requires all validators to participate** in the validation process, which can lead to inefficiencies if some **validators are not online or not actively participating**. In DPoS, only the **elected delegates participate** in the validation process, which makes it **faster and more efficient**.
- **Promotes decentralization:** In a PoS network, **validators with the largest stake have more control** over the network, which can lead to centralization. In a DPoS network, **token holders have a say in who gets to be a delegate**, which can lead to a more **decentralized network**.

Disadvantages

- It can lead to a **concentration of power in the hands of a small group of delegates.** If a small group of delegates controls a significant amount of voting power, they **could potentially collude to manipulate the network**.
- **Solution**: **Limiting the number of delegates** that any one entity can control.

Types of Consensus Algorithms

Leased Proof of Stake (LPoS)

- LPoS is a variation of Proof of Stake (PoS) that **allows smaller token holders to participate in the validation process by leasing their tokens to larger validators**.
- In a LPoS network, **token holders lease their tokens to a validator**, who uses those tokens to **increase their stake** and **improve their chances of being selected** to validate transactions and add new blocks to the chain.
- The **token holder** retains ownership of their tokens and **receives a share of the rewards** earned by the validator in **proportion to the amount of tokens they leased**.

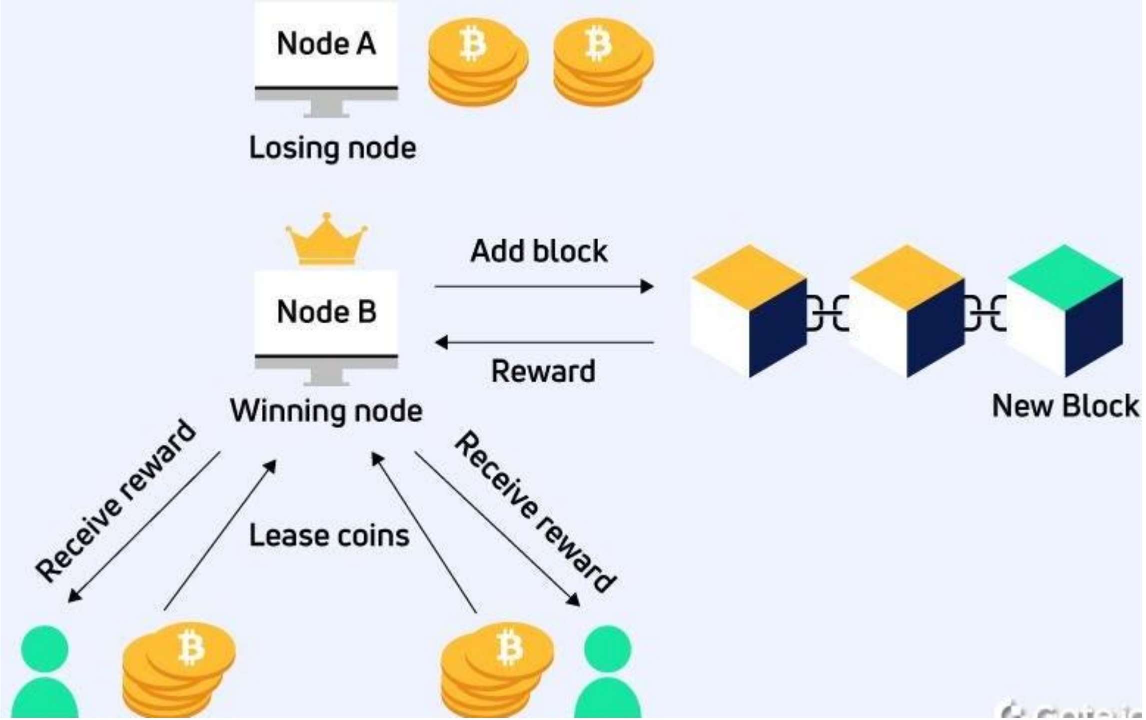
Advantages

- **Allows smaller token holders to participate** in the validation process and earn rewards without having to hold a significant amount of tokens. This **promotes decentralization** and allows for a more **diverse group of participants** in the network.
- **Increase the security**: By allowing more token holders to participate in the validation process, LPoS can **make it more difficult for a single validator or group of validators to gain control of the network and manipulate transactions**.

Types of Consensus Algorithms

Disdvantages

- **More complex** than other consensus algorithms. **Token holders** must understand the **risks and rewards of leasing their tokens** to a validator, and **validators** must **manage the tokens** they have leased in a responsible manner.



Types of Consensus Algorithms

Proof of Authority (PoA)

- Unlike other consensus algorithms such as PoW and PoS, **PoA relies on a group of trusted validators** instead of a decentralized network of nodes.
- In a PoA network, a **group of validators is designated as authoritative and responsible for validating transactions** and adding new blocks to the chain.
- Validators are typically **selected based on their reputation and expertise**, and they are incentivized to act honestly because their reputation is on the line.

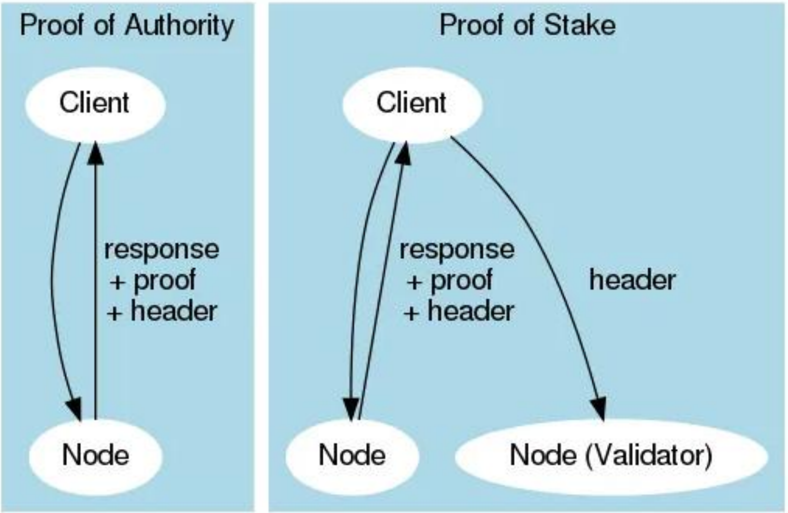
Advantages

- It is **more efficient** than other consensus algorithms.
- **PoW requires a significant amount of computational power** to validate transactions, which can be **costly and time-consuming**. **PoS requires a significant amount of stake** to participate in the validation process, which can **lead to centralization**. **PoA relies on a smaller group of trusted validators**, which makes it **faster and more efficient**.
- More suitable for **private or enterprise blockchain networks**. In these networks, it may **not be feasible** or desirable **to have a decentralized network** of nodes validating transactions. PoA **allows for a more controlled and centralized approach** to validation, which may be more appropriate in these contexts.

Types of Consensus Algorithms

Disadvantages

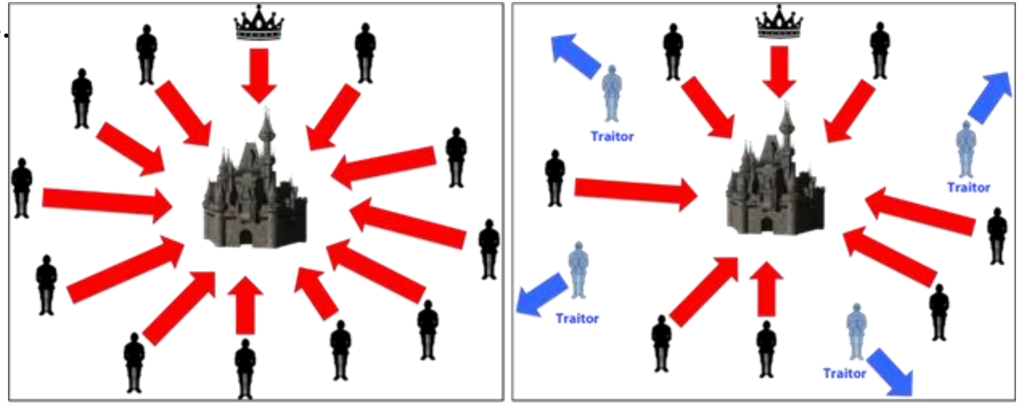
- It is **less secure** than other consensus algorithms.
- Because PoA **relies on a smaller group of validators**, the network is more **vulnerable to attacks** if one or more validators are compromised or act maliciously.
- Some PoA networks have implemented mechanisms **to address this issue**, such as **requiring multiple validators to sign off on transactions**.



Types of Consensus Algorithms

Byzantine Fault Tolerance (BFT)

- In general, it is the **System's ability to function correctly** and reach consensus **even if some of its components fail** or behave maliciously.
- In the context of blockchain technology, BFT is a consensus algorithm that **enables a distributed network of nodes to reach an agreement on the validity of transactions and maintain the integrity** of the blockchain even in the face of **malicious attacks or system failures**.
- BFT is designed **to prevent the "Byzantine Generals' Problem,"**: a scenario in which a group of generals must coordinate an attack on a city, but some of the generals are traitors who may send false information to others.



Coordinated Attack Leading to Victory   Uncoordinated Attack Leading to Defeat

Types of Consensus Algorithms

- In a blockchain network, the Byzantine Generals' Problem can manifest as **nodes** on the network that **behave maliciously or fail to communicate** correctly.
- BFT addresses this problem by **requiring a certain percentage of nodes to agree** on the validity of transactions before they are added to the blockchain.
- In a **traditional** BFT algorithm, this percentage is set at **two-thirds** of the total number of nodes. If two-thirds of the nodes agree on the validity of a transaction, then it is added to the blockchain. If less than two-thirds of the nodes agree, then the transaction is rejected.

Advantages

- It **does not require** a significant amount of **computational power or stake** to participate in the validation process, it **relies on a smaller group of nodes to reach agreement** on the validity of transactions, which makes it **more efficient and faster** than other consensus algorithms.

Disadvantages

- It **requires a higher level of trust** in the network participants.
- If a significant percentage of **nodes behave maliciously or fail to communicate** correctly, then the network may **not be able to reach a consensus and maintain the integrity** of the blockchain.
- BFT is often used in **private or enterprise blockchain networks** where participants are known and trusted.

Types of Consensus Algorithms

Practical Byzantine Fault Tolerance (PBFT)

- Extends the BFT algorithm **to provide a high level of fault tolerance** in distributed systems.
- PBFT is commonly used in **enterprise blockchain networks** and other distributed systems **where a high level of consensus is required**.
- PBFT works by **breaking down the consensus process into a series of steps** that are repeated for each transaction. Each step **involves a different node** in the network, and **each node is responsible for verifying** the validity of the transaction before passing it on to the next node.
- The PBFT algorithm **requires a certain number of nodes to reach a consensus** on the validity of a transaction before it can be added to the blockchain.
- This number is determined by the formula **f = (n-1)/3**, where f is the maximum number of faulty nodes that the system can tolerate, and n is the total number of nodes in the network.
- PBFT is **designed to be fault-tolerant**, meaning that it can **continue to function correctly** even if some nodes in the network **fail or behave maliciously**.
- If a node fails or behaves maliciously, the **other nodes can detect the problem and exclude the node** from the consensus process.

Types of Consensus Algorithms

Advantages

- It can achieve **high throughput and low latency**, even in networks with a large number of nodes.
- PBFT is also **known for its high level of security**, as it can tolerate up to f faulty nodes without compromising the integrity of the blockchain.

Disadvantages

- It **requires a certain number of nodes to reach consensus**, which means that it may **not be suitable for small networks**.
- PBFT **also requires a higher level of computational power** than some other consensus algorithms, which can make it **less energy-efficient**.

Types of Consensus Algorithms

Delegated Byzantine Fault Tolerance (dBFT)

- **Combines the advantages of both BFT and DPoS algorithms**.
- dBFT is commonly used in blockchain networks that **require a high level of consensus and throughput**.
- Like BFT and PBFT, dBFT is **designed to be fault-tolerant**.
- In dBFT, **consensus is reached through a process of voting**, where each node in the network can vote on the validity of a transaction.
- dBFT **uses a delegated model** where network **participants delegate their voting power to** a smaller number of trusted nodes, known as **validators**.
- Validators are responsible for verifying transactions and reaching a consensus on the validity of transactions.
- dBFT is **based on a round-robin system** where **validators take turns** validating transactions.
- Validators are **selected based on their reputation and stake** in the network.

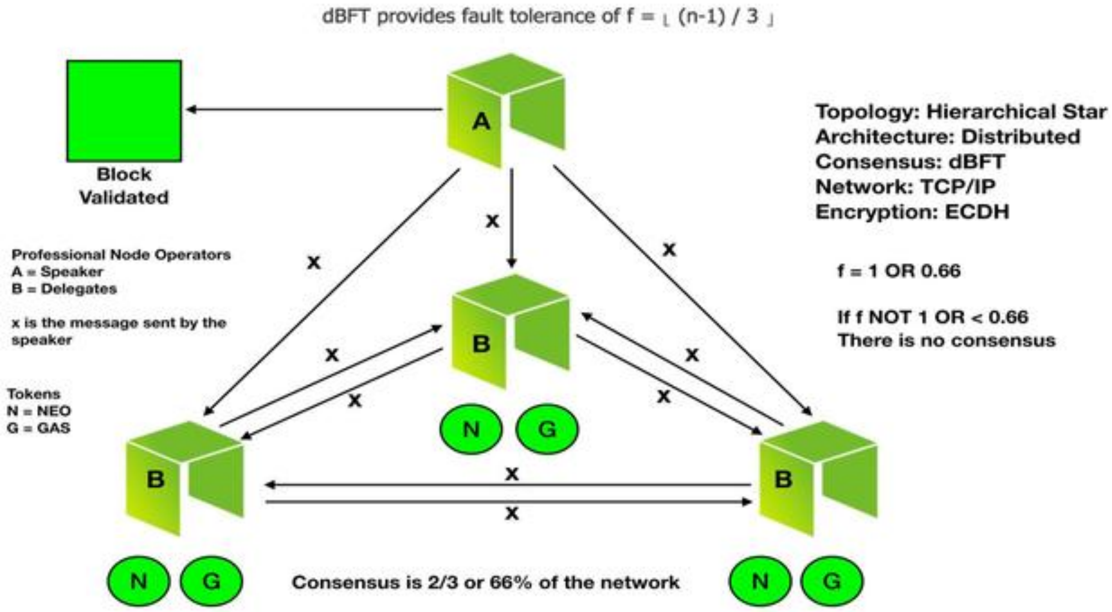
Advantages

- It can **achieve high throughput and low latency**, as only a **small number of validators are required** to reach a consensus, also **reduces the risk of centralization**, as **validators are selected based on their reputation and stake**, rather than their computational power.

Types of Consensus Algorithms

Disadvantages

- It **requires a high level of trust** in the selected validators, which can lead to potential vulnerabilities if a **large number of validators are controlled by a single entity**.
- dBFT is also **not suitable for all types** of blockchain networks, as it may **not be necessary to have such a high level of consensus** for some use cases.



Types of Consensus Algorithms

Directed Acyclic Graph (DAG)

- This type of data structure is **often used in distributed ledger technology** and blockchain systems.
- Unlike traditional blockchain architectures, which **organize data in a linear, chronological sequence of blocks**, DAGs allow for a **more flexible and efficient way to store and validate data**.
- **Each vertex represents a transaction and each edge represents a relationship between transactions**.
- In a DAG, **transactions are organized in a more complex structure** where each transaction is linked to multiple other transactions.

Types of Consensus Algorithms

Advantages

- They can **achieve high scalability and transaction throughput**.
  - Transactions can be **processed concurrently**, as long as there are no conflicts between them.
  - **Multiple transactions can be validated at the same time**, improving the overall efficiency of the system.
- **Ability to handle forks** in the network.
  - In a traditional blockchain, **when two blocks are created at the same time**, only one of them can be accepted into the chain, lead to a situation where a **block that was previously considered valid is suddenly rejected**, leading to a fork in the chain.
  - In a DAG-based system, **forks are resolved automatically**, as transactions are **validated based on their relationship to other transactions** in the graph.

Disadvantages

- **Need for a complex consensus mechanism** that can determine the **order of transactions** in the graph.
- DAGs may **not be suitable for all types of blockchain applications**, as they may **require a more complex architecture** than traditional blockchain systems.

Types of Consensus Algorithms

Proof of Capacity (PoC)

- **PoC is similar to Proof of Work (PoW)** in that it requires participants to **solve a computational puzzle** to add new blocks to the blockchain, but it differs in **how it utilizes computer storage** rather than computational power.
- In a PoC system, **participants allocate a portion of their computer's hard drive space to serve as a plot**, which is essentially a pre-computed segment of data that can be **used to generate a solution to the computational puzzle**.
- When a new block needs to be added to the blockchain, the **participant's plot is searched to find a solution to the puzzle**. The first participant to find a valid solution can add the new block to the blockchain and **receive a reward** in the form of cryptocurrency.

Disadvantages: Vulnerable to pre-computation and Sybil attacks.

- **Pre-computation attack**: an attacker could pre-compute a large number of plots and then use them to quickly solve the computational puzzle and add new blocks to the blockchain, giving them an unfair advantage over other participants.
- **Sybil attack**: an attacker could create **multiple identities to increase their chances of finding a solution** to the puzzle.

Types of Consensus Algorithms

Proof of Burn (PoB)

- PoB **requires participants to burn, or destroy, cryptocurrency tokens** to prove their commitment to the network, and **making a financial sacrifice**.
- User must **send a certain amount of cryptocurrency to an address** where it will be permanently destroyed - known as burning.
- Once it is burned, the **user is given the right to add new blocks** to the blockchain and receive rewards.
- **Reduces the likelihood of malicious actors attempting to attack the network**, as they would have to burn a significant amount of cryptocurrency to do so.

Advantages:

- Help to **reduce inflation**, Since tokens are being destroyed rather than created, the **overall supply of tokens decreases**, which can **help stabilize the value of the cryptocurrency**.

Disadvantages:

- **Difficult to determine the value of the burned tokens**, as they are permanently destroyed and cannot be recovered.
- This can make it **difficult to accurately measure the level of commitment and investment** in the network.

Types of Consensus Algorithms

Proof of Identity (PoI)

- It is a consensus mechanism **used to verify the identity of participants** in the network.
- Promote **trust, security, and authenticity** in blockchain transactions.
- PoI works by **requiring participants to provide a digital identity** that is linked to a real-world identity verification process, such as **government-issued IDs, biometric data**, or other forms of verifiable identity credentials.
- It ensures that each **participant is a real, identifiable** individual, which can help **prevent fraudulent or malicious activity** in the network.

Advantages:

- Help **prevent Sybil attacks**, where a single participant **creates multiple identities** in the network to gain control or manipulate the system, ensures each participant is a unique and identifiable entity.

Disadvantages:

- **Difficult to balance anonymity and privacy with identity verification**.
- Some participants may **not want to reveal their identities** to maintain their privacy, while others may **not have access to the necessary identity verification tools**.
- It is **time-consuming and costly**, which may discourage some participants from joining the network.