SESSION 11

Consensus Algorithms – 2

Learning Objectives

- Discuss different types of consensus algorithms

SESSION 11

Introduction

The consensus algorithm helps in reaching a common consensus in a distributed network. In a Bitcoin blockchain, reaching a common agreement is quite easy, which is achieved simply by sending and receiving bitcoins in a network. In other distributed networks, the consensus is reached by agreeing on various aspects such as the final state of smart contracts, or network information stored on the blockchain. Hence, it is important that the nodes store correct information and the incorrect data is ignored.

There has been a lot of research on consensus algorithms for decades, as the distributed network must resist various failures, message delays or invalid transactions. The blockchain that deals in finances can include nodes that are more interested in seeking profit rather than reaching a final decision.

Different consensus algorithms in a blockchain network ensure that the nodes present in a network must agree on a consistent global state of the blockchain. Different types of consensus algorithms used in a network are Proof of Work (PoW), Proof of Stake (PoS) and Proof of Elapsed time (PoET). The Proof of Authority (PoA) and Delegated Proof of Stake (DPoS) are the extended versions of PoS.

In this session, you will learn about different consensus algorithms used in blockchain networks such as Proof of Work (PoW), Proof of Stake (PoS) and Proof of Elapsed time (PoET) in detail.

Types of Consensus Algorithms

[LO - Discuss different types of consensus algorithms]

Apart from the Practical Byzantine Fault Tolerance algorithm, the distributed networks make use of other consensus algorithms. Some of the common consensus algorithms used in a network are:

- Proof of Work (PoW)
- Proof of Stake (PoS)
- Proof of Elapsed time (PoET)

The blockchain uses different types of consensus algorithms. Some of the reasons for selecting different consensus algorithms are listed as follows:

- **Business requirement**: Different business needs of an organization affect the type of consensus algorithm to be used.

- **Cryptocurrency requirement**: Not every business requires cryptocurrencies and might only want to use the blockchain technology with a consensus mechanism.
- **Performance requirement**: The nature of the blockchain also decides the consensus algorithm, as public blockchain needs more time to reach a consensus as compared to private blockchains. Depending on the performance requirements of an organization, a consensus algorithm is employed.
- **Security and privacy requirements**: Security and privacy requirements of every organization are different. Depending on the requirements, some organizations may prefer a public blockchain while others may opt for a private blockchain. This implies that different types of consensus algorithms will be employed for different organizations.
- **Robustness requirement:** Robustness refers to the level of security required by a business. The type of cryptography technique and consensus algorithm employed by an organization are some of the most important factors that determine robustness. For example, banking sector requires a high level of cryptographic and consensus algorithms as compared to other sectors.

Let's now discuss the different types of consensus algorithms.

Proof of Work (PoW)

The Proof of Work consensus algorithm is used by the Bitcoin and Ethereum networks to achieve consensus on a blockchain network. In PoW, the decisions of individual nodes are not required to achieve consensus in a network. The PoW algorithm uses a hash function for creating conditions. The individual nodes can broadcast their final decision about the submitted information, which is verified by all other participant nodes in a network. The hash function includes a parameter which ensures that the false information is not computed; thereby preventing the network from taking false decisions.

In the bitcoin network, some of the nodes authenticate the information on behalf of the network and these nodes are rewarded with bitcoins. The rewarding system for the nodes allows broader participation that helps in creating a robust and safe blockchain. It also helps in providing greater network stability and allows participant nodes to remain anonymous.

The major disadvantage of PoW is that the nodes require a lot of computation power and expensive hardware for reaching consensus in a network. Such requirements have made the mining activities an exclusive domain of a very closed group of miners. This is against the very idea of decentralization on which blockchain is based. Therefore, it may give rise to a 51% attack.

Proof of Stake (PoS)

PoS is used as a common alternative to PoW algorithm to verify and authenticate the transactions on the block. In the PoS algorithm, there is no requirement to mine the blocks. Instead, stakeholders invest in the underlying cryptocurrency. In PoS, the nodes are selected based on the proportional stake of each individual node in the network.

The selected nodes authenticate the validity of the newly submitted information.

In PoS, the selection of a node to create a new block depends on the fraction of cryptocurrency owned by it in a network. For instance, the node owning 600 bitcoins has six times more possibility to be chosen for new block creation, as compared to the node owning just 100 bitcoins.

The PoS algorithm faces the main problem of keeping nothing at stake. It does not penalize the nodes that authenticate more than one history; hence they can cause repudiation problem in the future. Even the nodes which vote for the correct block are not rewarded with any bitcoins. Hence, the nodes in a network can vote for multiple blocks, leading to the formation of a fork even though it is computationally economical.

Delegated Proof of Stake (DPoS)

DPoS is an extended version of PoS. In DPoS, the stakeholders do not perform the block validation, instead they use their cryptocurrency for selecting nodes that validate. The selected nodes are known as delegates or validators. Each delegate is allotted a specific time to publish a new block. In case, the delegates miss the creation time for a block or validate an invalid transaction, then they can be voted out by their stakeholders or can be replaced with other delegates.

The main disadvantage of the DPoS is that it is partially centralized and there is no financial punishment for betraying the network.

Proof of Authority (PoA)

PoA is an extended form of PoS consensus algorithm. In PoA algorithm, the node selection is performed based on the validator's identity, rather than the monetary value of a validator/stakeholder. The authentication of identity confirms that the validator is the same person whom he/she claims to be. PoA algorithm was first used by Gavin Wood of Parity Technologies that offered a different way of executing Ethereum- based blockchains.

For implementing the PoA algorithm, three main conditions that must be satisfied are listed as follows:

- The identity of a validator must be authenticated for ensuring that validators are undeniably whom they claim to be.
- The eligibility conditions for staking the identity should be difficult to make sure that only honest validator is rewarded and valued in a network.
- The procedure for authority establishment must be the same for all the validators. This is necessary to ensure that the network recognizes the process and can trust the integrity of the process.

Proof of Authority algorithm is used in a network where all the participant nodes are known and registered with the network. This type of blockchain is referred to as permissioned chain, as only the authorized nodes can forge the blocks in the blockchain. Hence, it is important that no node in a blockchain is compromised.

The main disadvantage of using the PoA algorithm is that the identity of every validator must be known, authenticated and trusted. In the global blockchains, the PoA algorithm is not preferred, as a blockchain's main feature is the ability to exchange value anonymously and PoA algorithm defies the same.

Proof of Elapsed time (PoET)

PoET algorithm uses a Trusted Execution Environment (TEE). It ensures that the blocks are generated in a random manner. In PoET, the time for achieving consensus in a network is based on a time rate provided through TEE. The PoET algorithm works with thousands of nodes effectively and can theoretically be processed on any processor which provides a TEE.

The limitation of using PoET algorithm is that you have to trust a third-party intermediary (the implementer of the TEE) while removing the third-party intermediary is the essential feature of a public blockchain.

SUMMARY

- In PoW, the decisions of individual nodes are not required to achieve consensus in a network. PoW algorithm uses a hash function for creating conditions.
- In the PoS algorithm, there is no requirement to mine the blocks. Instead, stakeholders invest in the underlying cryptocurrency.
- In DPoS, the stakeholders do not perform the block validation, instead they use their cryptocurrency for the selection of nodes which perform the function of validation.
- In PoA algorithm, the node selection is carried out based on the validator's identity, rather than the monetary value of a validator/stakeholder.
- PoET algorithm uses a Trusted Execution Environment (TEE) and ensures that the blocks are generated in a random manner.