Consensus Mechanism Overview

Publié le 13 septembre 2021

WisdomTree
Contributor

A decentralised system implies that no single participant has control over the system's rules, inputs and outputs. Security therefore becomes the biggest challenge to any decentralised system. This is especially true when participants don't trust each other, and the system provides a record of transactions that ascribe value (like on a public blockchain).

Without third-party verification, how can participants validate transactions and prevent malicious actors from imposing fake and fraudulent information?

Satoshi Nakamoto provided a solution to this question by combining various ideas to create a distributed, immutable, and cryptographic ledger of transactions .1 At its core is the proof-of-work consensus mechanism – a way to verify transactions by proving to others that considerable computing efforts were spent for the information to be appended to the ledger.

What's a Consensus Mechanism?

A consensus mechanism is an algorithm to approve transactions or records onto a decentralised ledger such that fake or fraudulent records are rejected.

The algorithm is run when new blocks are being appended to the existing chain of blocks, which is how the blockchain gets updated as an append-only ledger.

The idea is that by imposing a requirement of certain effort spent (or risk taken), malicious actors would refrain from tempering with the ledger as they deem the effort (or loss) to be unprofitable. The very first purpose of proof of work's invention was to filter email spam.

Hashcash, a proof-of-work system proposed by Adam Back in 1997, requires email senders to create and attach stamps on email headers to prove to receivers that they spent central processing unit (CPU) power to generate emails. These stamps are one-way encryption algorithms that are easy to verify by the receiver but hard (in computing terms) to generate by the sender. In this model, spammers would be reluctant to send out large quantities of email as it becomes unprofitable to use a large amount of CPU power to create stamps. However, the price of sending a single email is still affordable by regular users.

Since consensus mechanisms in the blockchain world are generally referred to as activities of "mining" and "staking," they are frequently regarded as methods to issue new coins. However, their primary purpose is to secure the decentralised network, whereas rewards in the form of coins are an added economic incentive for workers to maintain the network.

Source: Zhanga, Shijie and Lee, Jong-Hyouk. Analysis of the main consensus protocols of blockchain. Science Direct Vol. 6, Issue 2. June 2020.

Major consensus mechanisms include proof-of-work (PoW), proof-of-stake (PoS), delegated proof-of-stake (DPoS).

PoW is the oldest consensus mechanism. It accounts for more than 75% of the market cap of blockchain protocols. It is used by Bitcoin, Ethereum (up to Serenity), and Litecoin etc.2

In PoW, miners append new block with transaction information to existing blocks (called mining), via finding a random number (called nonce) that can be run through a universal encrypting function to the network (called hash) and can satisfy a difficulty requirement. This consists of the process of “solving” the mathematical task, which demands considerable energy and effort.

PoS, on the other hand, doesn’t require participants to use computing power to hash blocks and solve a mathematical requirement, but it requires them to stake ether. Participants are randomly selected to become block validators based on their wealth, and validators need to stake an amount of cryptocurrency that covers the transaction fee and their potential reward until the block is successfully appended. If inconsistent, absent, and abnormal behaviors are detected, dishonest participants could lose their stakes and be banned from the network.

DPoS is a variation of PoS. It changes the selection process in PoS from randomised algorithms to a more democratic approach, allowing stakers to vote for their representatives, who would carry out the validation act.

Besides PoW, PoS, and DPoS, there are many proof-of-X mechanisms that try to establish a decentralised and secure network. They include proof-of-capacity, proof-of-elapsed time, proof-of-importance, etc.

Another major family of consensus mechanisms is Byzantine Fault Tolerance; this is the feature of a distributed network to reach consensus(agreement on the same value) even when some of the nodes in the network fail to respond or respond with incorrect information. It has several variations such as practical Byzantine Fault Tolerance (pBFT), which is currently used by Hyperledger Fabric, and its improved version is used by the People’s Bank of China (PBoC) to develop its Central Bank Digital Currency (CBDC). Another variation is called delegated Byzantine Fault Tolerance (dBFT), which is used by Neo. The Stellar network’s model of consensus leverages a federated Byzantine agreement (FBA) model, and it seeks to build upon these models to build an open network for storing and moving money.

Source: Zhanga, Shijie and Lee, Jong-Hyouk. Analysis of the main consensus protocols of blockchain. Science Direct Vol. 6, Issue 2. June 2020. This chart summarizes the differences of discussed consensus mechanisms. Finality type refers to the model of how committed blocks are confirmed and irreversible. Probabilistic finality means that blocks are increasingly difficult to be reverted as the blockchain gets longer. Absolute finality means that blocks are finalized as soon as they are appended to the blockchain. Fault tolerance refers to a system's tolerance of malfunctioned or malicious components that would prevent it from operating. Power consumption refers to if the system consumes large amount of energy. Scalability

refers to how easy the system can grow and expand. Application refers to the ideal type of blockchain the consensus mechanism should be utilized in. Public refers to blockchains that can be accessed to everyone. Private refers to blockchains that require permissions to join.

Technical Comparison of Major Consensus Mechanisms				
	PoW	PoS	DPoS	pBFT
Type	Probabilistic-finality	Probabilistic-finality	Probabilistic-finality	Absolute-finality
Fault Tolerance	50%	50%	50%	33%
Power Consumption	Large	Less	Less	Negligible
Application	Public	Public	Public	Permissioned

Source: Zhanga, Shijie and Lee, Jong-Hyouk. Analysis of the main consensus protocols of blockchain. Science Direct Vol. 6, Issue 2. June 2020. This chart summarizes the differences of discussed consensus mechanisms. Finality type refers to the model of how committed blocks are confirmed and irreversible. Probabilistic finality means that blocks are increasingly difficult to be reverted as the blockchain gets longer. Absolute finality means that blocks are finalized as soon as they are appended to the blockchain. Fault tolerance refers to a system's tolerance of malfunctioned or malicious components that would prevent it from operating. Power consumption refers to if the system consumes large amount of energy. Scalability refers to how easy the system can grow and expand. Application refers to the ideal type of blockchain the consensus mechanism should be utilized in. Public refers to blockchains that can be accessed to everyone. Private refers to blockchains that require permissions to join.

Conclusion

The consensus mechanism is a key component to a decentralised network. It not only secures the system but also affects its efficiency and scalability.

Since Bitcoin's birth there have been many other consensus mechanisms created. Each of them has its own characteristics that determine the associated network's attributes. To learn more about them and how they differ, you can read morehere.

1 https://queue.acm.org/detail.cfm?id=3136559

2 As of 7/23/2021. Calculated using CoinMarketCap data.

Related blogs

+ Why Consider Ether As An Investment?

+ How Much Bitcoin Would That Be, Sir?

+ Ethereums History From Zero to 2 0

Important Risks Related to this Article

Informations importantes

Communications commerciales publiées dans l¼Espace économique européen (« EEE ») Ce document est publié et approuvé par WisdomTree Ireland Limited, une société autorisée et réglementée par la Central Bank of Ireland.

Communications commerciales émises dans des juridictions en dehors de l¼EEE Ce document est publié et approuvé par WisdomTree UK Limited, une société autorisée et réglementée par la Financial Conduct Authority du Royaume-Uni.

WisdomTree Ireland Limited et WisdomTree UK Limited sont toutes les deux désignées comme « WisdomTree » (le cas échéant). Notre Politique sur les conflits d¼intérêts et notre Inventaire sont disponibles sur demande.

Réservé aux clients professionnels uniquement. Les informations figurant dans ce document sont fournies à titre informatif et ne constituent pas une ore de vente, ou une sollicitation d¼ore d¼achat de titres ou d¼actions. Ce document ne doit pas être utilisé comme fondement d¼une décision d¼investissement. La valeur des investissements peut fluctuer et vous êtes susceptible de perte tout ou partie du montant investi. La performance passée ne constitue pas nécessairement une indication des performances futures. Toute décision d¼investissement doit être fondée sur les informations figurant dans le prospectus approprié et sur des conseils indépendants en matière d¼investissement, fiscaux et juridiques.

L¼application des réglementations et lois fiscales peut souvent conduire à des interprétations diérentes. Tous les points de vue ou opinions exprimés dans cette communication représentent les points de vue de WisdomTree et ne doivent pas être interprétés comme des conseils réglementaires, fiscaux ou juridiques. WisdomTree ne donne aucune garantie ou représentation quant à l'exactitude des vues ou opinions exprimées dans cette communication. Toute décision d'investissement doit être fondée sur les informations contenues dans le prospectus approprié et après avoir sollicité des conseils indépendants en matière d'investissement, fiscaux et juridiques. Ce document n¼est pas et ne doit en aucun cas être interprété comme une publicité ou une ore publique d¼actions ou de titres aux États-Unis ou dans toute province ou tout territoire des États-Unis. L¼introduction, la transmission et la distribution (directes ou indirectes) de l¼original ou d¼une copie de ce document sont interdites aux États-Unis.

Bien que WisdomTree s¼eorce d¼assurer l¼exactitude du contenu de ce document, WisdomTree ne peut en garantir l¼exactitude. Les fournisseurs de données tiers sollicités pour obtenir les informations contenues dans le présent document ne donnent aucune garantie ou représentation de quelque sorte en rapport avec ces données. Lorsque WisdomTree exprime ses propres opinions concernant le produit ou l¼activité du marché, ces opinions sont susceptibles de changer. WisdomTree, ses ailiés et leurs dirigeants, directeurs, partenaires ou employés respectifs déclinent toute responsabilité pour toute perte directe ou indirecte découlant de l¼utilisation de ce document ou de son contenu.