
CONSENSUS MECHANISM OVERVIEW

Wisdomtree EU
13 Sep 2021

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.

Comparison of Major Consensus Mechanisms					
	Invented Year	Nouns	Pros	Cons	Blockchain
Proof-of-Work (PoW)	1993	mining miners	<ul style="list-style-type: none"> • secure • simple • relatively long history 	<ul style="list-style-type: none"> • energy intensive • susceptible to be centralized 	Bitcoin, Litecoin, Ethereum (up to Serenity)
Proof-of-Stake (PoS)	2012	minting validators	<ul style="list-style-type: none"> • energy efficient • less centralized • better designed for attack recovery 	<ul style="list-style-type: none"> • shorter track record • nothing-at-stake problem • long-range attacks 	Ethereum (planned to be implemented in Serenity), Cardano
Delegated Proof-of-Stake (DPoS)	2014	minting witnesses, delegates	<ul style="list-style-type: none"> • same as PoS • but more democratic • faster 	<ul style="list-style-type: none"> • susceptible to be centralized 	Bitshares, Steemit, Ark, Lisk

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 more [here](#).

Sources

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](#)

Related products

- + [WisdomTree Ethereum](#)
- + [Wisdomtree Bitcoin](#)

View the online version of this article [here](#).

Important Information

Marketing communications issued in the European Economic Area (“EEA”): This document has been issued and approved by WisdomTree Ireland Limited, which is authorised and regulated by the Central Bank of Ireland.

Marketing communications issued in jurisdictions outside of the EEA: This document has been issued and approved by WisdomTree UK Limited, which is authorised and regulated by the United Kingdom Financial Conduct Authority.

WisdomTree Ireland Limited and WisdomTree UK Limited are each referred to as “WisdomTree” (as applicable). Our Conflicts of Interest Policy and Inventory are available on request.

For professional clients only. The information contained in this document is for your general information only and is neither an offer for sale nor a solicitation of an offer to buy securities or shares. This document should not be used as the basis for any investment decision. Investments may go up or down in value and you may lose some or all of the amount invested. Past performance is not necessarily a guide to future performance. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

The application of regulations and tax laws can often lead to a number of different interpretations. Any views or opinions expressed in this communication represent the views of WisdomTree and should not be construed as regulatory, tax or legal advice. WisdomTree makes no warranty or representation as to the accuracy of any of the views or opinions expressed in this communication. Any decision to invest should be based on the information contained in the appropriate prospectus and after seeking independent investment, tax and legal advice.

This document is not, and under no circumstances is to be construed as, an advertisement or any other step in furtherance of a public offering of shares or securities in the United States or any province or territory thereof. Neither this document nor any copy hereof should be taken, transmitted or distributed (directly or indirectly) into the United States.

Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Where WisdomTree has expressed its own opinions related to product or market activity, these views may change. Neither WisdomTree, nor any affiliate, nor any of their respective officers, directors, partners, or employees accepts any liability whatsoever for any direct or consequential loss arising from any use of this document or its contents.