CONSENSUS MECHANISM OVERVIEW

August 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.

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. In this article, we review several existing consensus mechanisms and provide an overview on how they differ.

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 tampering 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 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 for regular users.

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

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. They are a necessary component of any decentralised network because they secure the network and dictate the network's sustainability and scalability.

COMPARISON OF MAJOR CONSENSUS MECHANISMS

	Invented Year	Nouns	Pros	Cons	Blockchain
Proof-of-Work (PoW)	1993	mining I miners	• secure • simple • relatively long history	• energy intensive • susceptible to be centralized	Bitcoin, Litecoin, Ethereum (up to Serenity)
Proof-of-Stake (PoS)	2012	minting I validators	• energy efficient • less centralized • better designed for attack recovery	• 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 I witness, delegates	• same as PoS • but more democratic • faster	• 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.

PROOF-OF-WORK (POW)

Proof-of-work is the oldest and the most popular 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 race to generate a block of data containing three things: new transactions waiting for verification, a record of the previous block, and a new transaction (called the 'coinbase') paying themselves a reward (and in the process increasing the supply of currency).

This block must satisfy a certain mathematical requirement when the block of data is cryptographically 'hashed'. Miners are free to choose any transactions they want to verify from a pool of unverified transactions (i.e., not in a block already on the blockchain) maintained by the network. Before adding a transaction to their block, the miner checks the sending party's digital signature on each transaction, and that the party sending coins has previously received enough coins in a prior transaction recorded in a block on the blockchain.

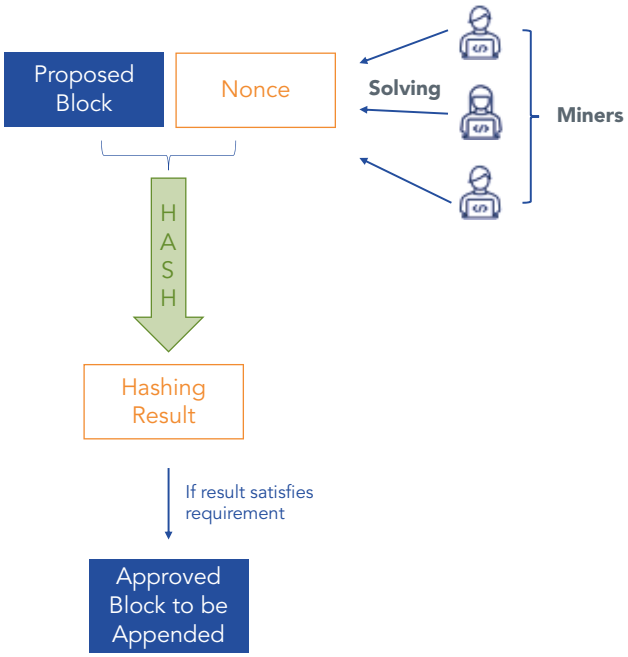
A **hash** function takes an arbitrary amount of input data and computes a fixed length numerical output that has several important properties: for the same input data, anyone using the same hash function will get the same hash output; the output is unpredictable and cannot be guessed; and there is no way to get from the hash output back to the inputs. Blockchains may use different hash functions (e.g., bitcoin uses the SHA256 function), but whichever they choose typically has these properties.

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

For a block to be valid the hash output must be a 256-bit long number that starts with a certain number of leading zeros (known as the **difficulty**). In binary notation, this number has 256 ones or zeros. A number this big can uniquely describe all of the atoms in the universe. Therefore, a valid hash output is usually a very small number relative to all possible numbers with 256-bits.

Since the cryptographic hash function generates this output in an unpredictable manner, the miner cannot know what the result will be, and chances are that the hash output won't start with enough zeros. The miner repeatedly changes and hashes the block by incrementing a number known as the **nonce** and adding the nonce to the block's data – thereby guaranteeing a different hash output each time.

When the miner finds a nonce and set of transactions that, when hashed, satisfy the difficulty requirement it broadcasts that block to other miners so they can verify and accept that block. Once other miners verify a block's validity, they add that block to their copy of the blockchain and start mining a new block including a hash of the previous block in their new block. There is no incentive to continue verifying transactions contained in a new block as other miners will only add to the longest chain of blocks.



The advantage of this mechanism is its security and long history, but the downside is that it is energy intensive as each miner uses computing power to hash blocks trillions of times a second. It also tends to be more centralised as the mechanism requires advanced machines to run the operation. Miners with aggregated advanced machines have an advantage in the number of hashes they can run and have more chance of producing a valid block.

PROOF-OF-STAKE (POS)

Proof-of-stake is the second most popular consensus mechanism.

Ethereum is currently transitioning from proof-of-work to proof-of-stake to be more efficient, scalable, and sustainable.

Unlike PoW, PoS doesn't require participants to use computing power to hash blocks and solve a mathematical requirement, but it requires them to stake ether. The participants are called **validators** as opposed to miners, and the action of appending is referred to as **minting**, instead of mining.

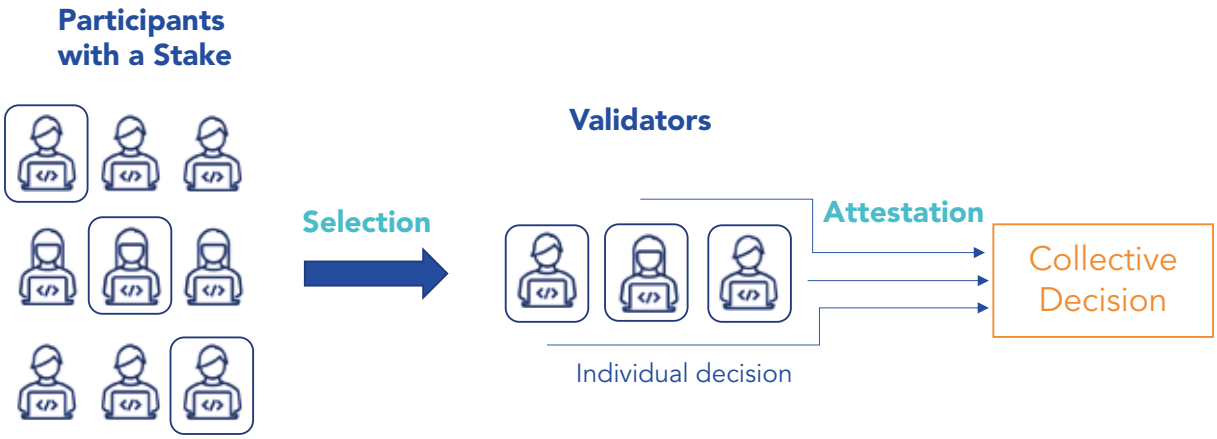
Proof-of-stake can also be described in two processes: selection and attestation.

To become a validator, participants need to set a certain amount of the cryptocurrency aside, and depending on the blockchain, validators are selected differently. One of the more popular selection methods is randomised block selection, which will be used by Ethereum. The mechanism randomly selects a group of validators based on the amount of cryptocurrency they have staked. The more wealth one stakes, the more likely they are selected.

After being selected, the attestation process begins.

Validators need to stake an amount of cryptocurrency that covers the transaction fee and their potential reward until the block is successfully appended. Validators individually attest to the block and broadcast their decision to the network. If a certain number of validators approve it, the block gets appended and a proportionate reward is given to the validators. If the block ends up being rejected by the group of validators, the block will not be appended.

Fraud is detected through a pre-coded set of rules that will be triggered by inconsistent, absent, and abnormal behaviours. Dishonest participants could lose their stakes and be banned from the network.



PoS reduces mining energy as it only requires staking. It also doesn't require validators to have advanced machines, which lowers barrier for entry and makes it less concentrated than PoW[3]. However, PoS faces several potential exploits from the nothing-at-stake problem[4] and long-range attacks that demand mitigations from other areas.

DELEGATED PROOF-OF-STAKE (DPOS)

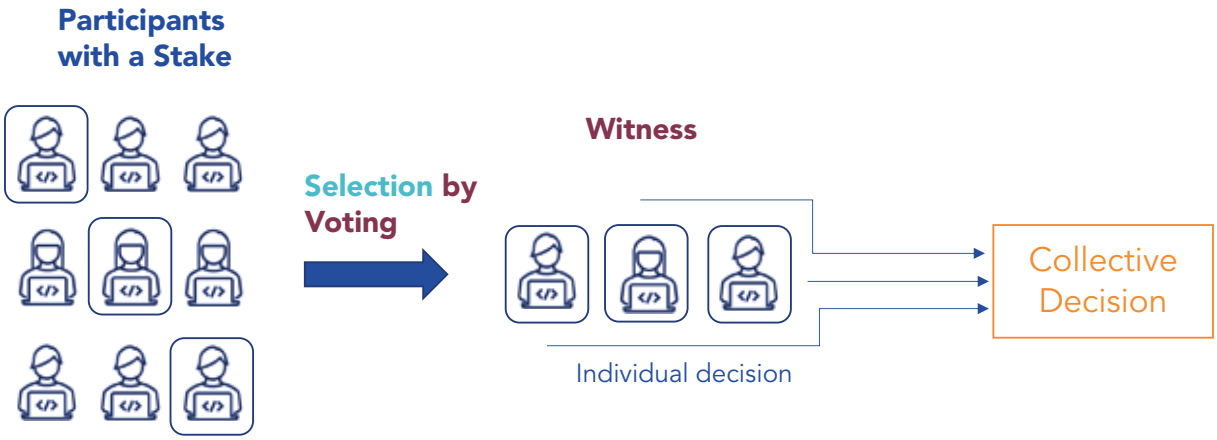
Delegated proof-of-stake is a variation of proof-of-stake. It changes the selection process in PoS from randomised algorithms to a more democratic approach.

Coin holders with a stake in a DPoS network constantly select block validators by voting. Voting power increases with one's wealth. All coin holders have the potential to be elected by convincing other participants to vote for them. Some of the considerations that play into the voting decision includes hardware robustness, dedicated teams, etc.

3 https://vitalik.ca/general/2020/11/06/pos2020.html.

4 https://medium.com/@abhisharm/understanding-proof-of-stake-through-its-flaws-pt-1-6728020994a1

Elected validators are called **delegates** or **witnesses**, and they are responsible for signing and verifying new blocks. To prevent manipulation, a group of witnesses (normally 21-100) are selected for a certain period.[5] During that period (called an epoch), witnesses take turns verifying and signing new blocks with their private keys. These signed blocks are then left unconfirmed until a majority of the witness group approves.



Approved blocks reward witnesses, and these rewards are usually shared with voters. Failed blocks leave no reward. Malicious actors would be quickly voted down once discovered.

DPoS introduces collective human judgement to replace a competition in pure computational power. It can process many more transactions even when compared to PoS. It also reduces the locking time for collateral being staked. By allowing participants to vote, it makes the network more democratic than PoW and PoS.

However, the voting process may also centralise the network as coin holders with a small stake would forfeit their votes given their insignificance.

OTHER CONSENSUS MECHANISMS

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.

These mechanisms are more commonly used in permissioned protocols, which require prior permissions to join. They are early solutions of the Byzantine General Problem[6], which is the same problem Bitcoin tries to solve.

5 https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-stake/delegated-proof-of-stake-dpos

6 Is a term that describes a situation where all participants in a system need to agree on a strategy in order to avoid catastrophic failure of the system, however, some participants are unreliable or malicious.

The advantages of these mechanisms include energy efficiency, transaction finality, which requires less validations from nodes to confirm a transaction, and increased ability to coordinate in a closed system. However, they have a lower tolerance for malicious nodes in the network and maybe hard to scale, so they are not an ideal candidate for public blockchains.

TECHNICAL COMPARISON OF MAJOR CONSENSUS MECHANISMS				
Property	**PoW**	**PoS**	**DPoS**	**pBFT**
Type	Probabilistic-finalist	Probabilistic-finalist	Probabilistic-finalist	Absolute-finalist
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.

When examining a consensus mechanism, it is important to consider its functionality based on three aspects: degree of decentralisation, security, and scalability. Most of the consensus mechanisms can only optimise on two of the three factors – security comes at a cost of scalability and the risk of centralisation, and scalable networks might be more susceptible to attacks.

Therefore, different consensus mechanisms must be analysed based on the needs of the particular network.

IMPORTANT INFORMATION

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.

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.

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.

This document may contain independent market commentary prepared by WisdomTree based on publicly available information. Although WisdomTree endeavours to ensure the accuracy of the content in this document, WisdomTree does not warrant or guarantee its accuracy or correctness. Any third party data providers used to source the information in this document make no warranties or representation of any kind relating to such data. 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.

This document may contain forward looking statements including statements regarding current expectations or beliefs with regards to the performance of certain assets classes and/or sectors. Forward looking statements are subject to certain risks, uncertainties and assumptions. There can be no assurance that such statements will be accurate and actual results could differ materially from those anticipated in such statements. WisdomTree strongly recommends that you do not place undue reliance on these forward-looking statements.

Any historical performance included in this document may be based on back testing. Back testing is the process of evaluating an investment strategy by applying it to historical data to simulate what the performance of such strategy would have been. However, back tested performance is purely hypothetical and is provided in this document solely for informational purposes. Back tested data does not represent actual performance and should not be interpreted as an indication of actual or future performance.