
title: Consensus mechanisms description: An explanation of consensus protocols in distributed systems and the role they play in Ethereum. lang: en

The term 'consensus mechanism' is often used colloquially to refer to 'proof-of-stake', 'proof-of-work' or 'proof-of-authority' protocols. However, these are just components in consensus mechanisms that protect against Sybil attacks. Consensus mechanisms are the complete stack of ideas, protocols and incentives that enable a distributed set of nodes to agree on the state of a blockchain.

Prerequisites {#prerequisites}

To better understand this page, we recommend you first read our [introduction to Ethereum](#).

What is consensus? {#what-is-consensus}

By consensus, we mean that a general agreement has been reached. Consider a group of people going to the cinema. If there is no disagreement on a proposed choice of film, then a consensus is achieved. If there is disagreement, the group must have the means to decide which film to see. In extreme cases, the group will eventually split.

In regard to the Ethereum blockchain, the process is formalized, and reaching consensus means that at least 66% of the nodes on the network agree on the global state of the network.

What is a consensus mechanism? {#what-is-a-consensus-mechanism}

The term consensus mechanism refers to the entire stack of protocols, incentives and ideas that allow a network of nodes to agree on the state of a blockchain.

Ethereum uses a proof-of-stake-based consensus mechanism that derives its crypto-economic security from a set of rewards and penalties applied to capital locked by stakers. This incentive structure encourages individual stakers to operate honest validators, punishes those who don't, and creates an extremely high cost to attack the network.

Then, there is a protocol that governs how honest validators are selected to propose or validate blocks, process transactions and vote for their view of the head of the chain. In the rare situations where multiple blocks are in the same position near the head of the chain, there is a fork-choice mechanism that selects blocks that make up the 'heaviest' chain, measured by the number of validators that voted for the blocks weighted by their staked ether balance.

Some concepts are important to consensus that are not explicitly defined in code, such as the additional security offered by potential out-of-band social coordination as a last line of defense against attacks on the network.

These components together form the consensus mechanism.

Types of consensus mechanisms {#types-of-consensus-mechanisms}

Proof-of-work based {#proof-of-work}

Like Bitcoin, Ethereum once used a **proof-of-work (PoW)** based consensus protocol.

Block creation {#pow-block-creation}

Miners compete to create new blocks filled with processed transactions. The winner shares the new block with the rest of the network and earns some freshly minted ETH. The race is won by the computer which is able to solve a math puzzle fastest. This produces the cryptographic link between the current block and the block that went before. Solving this puzzle is the work in "proof-of-work". The canonical chain is then determined by a fork-choice rule that selects the set of blocks that have had the most work done to mine them.

Security {#pow-security}

The network is kept secure by the fact that you'd need 51% of the network's computing power to defraud the chain. This would require such huge investments in equipment and energy; you're likely to spend more than you'd gain.

More on [proof-of-work](#)

Proof-of-stake based {#proof-of-stake}

Ethereum now uses a **proof-of-stake (PoS)** based consensus protocol.

Block creation {#pos-block-creation}

Validators create blocks. One validator is randomly selected in each slot to be the block proposer. Their consensus client requests a bundle of transactions as an 'execution payload' from their paired execution client. They wrap this in consensus data to form a block, which they send to other nodes on the Ethereum network. This block production is rewarded in ETH. In rare cases when multiple possible blocks exist for a single slot, or nodes hear about blocks at different times, the fork choice algorithm picks the block that forms the chain with the greatest weight of attestations (where weight is the number of validators attesting scaled by their ETH balance).

Security {#pos-security}

A proof-of-stake system is secure crypto-economically because an attacker attempting to take control of the chain must destroy a massive amount of ETH. A system of rewards incentivizes individual stakers to behave honestly, and penalties disincentivize stakers from acting maliciously.

More on [proof-of-stake](#)

A visual guide {#types-of-consensus-video}

Watch more on the different types of consensus mechanisms used on Ethereum:

Sybil resistance & chain selection {#sybil-chain}

Proof-of-work and proof-of-stake alone are not consensus protocols, but they are often referred to as such for simplicity. They are actually Sybil resistance mechanisms and block author selectors; they are a way to decide who is the author of the latest block. Another important component is the chain selection (aka fork choice) algorithm that enables nodes to pick one single correct block at the head of the chain in scenarios where multiple blocks exist in the same position.

Sybil resistance measures how a protocol fares against a [Sybil attack](#). Sybil attacks are when one user or group pretends to be many users. Resistance to this type of attack is essential for a decentralized blockchain and enables miners and validators to be rewarded equally based on resources put in. Proof-of-work and proof-of-stake protect against this by making users expend a lot of energy or put up a lot of collateral. These protections are an economic deterrent to Sybil attacks.

A **chain selection rule** is used to decide which chain is the "correct" chain. Bitcoin uses the "longest chain" rule, which means that whichever blockchain is the longest will be the one the rest of the nodes accept as valid and work with. For proof-of-work chains, the longest chain is determined by the chain's total cumulative proof-of-work difficulty. Ethereum used to use the longest chain rule too; however, now that Ethereum runs on proof-of-stake it adopted an updated fork-choice algorithm that measures the 'weight' of the chain. The weight is the accumulated sum of validator votes, weighted by validator staked-ether balances.

Ethereum uses a consensus mechanism known as [Casper](#) that combines [Casper FFG proof-of-stake](#) with the [GHOST fork-choice rule](#).

Further reading {#further-reading}

- [What Is a Blockchain Consensus Algorithm?](#)
- [What is Nakamoto Consensus? Complete Beginner's Guide](#)
- [How Does Casper work?](#)

- [On the Security and Performance of Proof of Work Blockchains](#)
- [Byzantine fault](#)

Know of a community resource that helped you? Edit this page and add it!

Related topics {#related-topics}

- [Proof-of-work](#)
- [Mining](#)
- [Proof-of-stake](#)