Proof-of-Work vs. Proof-of-Stake

By

Decentralized Dog

Published on:
September 10, 2020

Proof-of-work and proof-of-stake are two of the most popular crypto mining mechanisms — but what makes them different?

Table of Contents

- Proof-of-Work at a Glance
- Proof-of-Stake at a Glance

In simplest terms, proof-of-work and proof-of-stake are two different ways that you can **mine** a cryptocurrency.

In more precise terms, proof-of-work and proof-of-stake are both types of **consensus** mechanisms that are designed to solve the issue of trust between the participants of a **blockchain** network.

The debate over **proof-of-work** vs. **proof-of-stake** may seem technical at first glance, yet it reflects fundamental differences of approach to achieving the objectives of cryptocurrency networks.

The stand-off between the two **algorithms** engages key questions of network security, environmental sustainability, barriers to entry and achieving **decentralization**.

Common references to blockchain networks as "**trustless**" reflect this core principle: the goal of a blockchain system is to guarantee that **transactions** are enforced and recorded as intended, without the need for social trust between parties or for an **intermediary**.

For this to be possible, the network needs to be designed so that it is impossible — or at least, highly unviable — for participants to **double-spend** units of cryptocurrency or to roll back prior transactions.

Proof-of-Work at a Glance

Proof-of-work is a **pioneering** system which in fact **pre-existed** Bitcoin (**BTC**), but has since become inherently connected to the world-renowned cryptocurrency.

For this reason, the mechanism is sometimes referred to as the **Nakamoto** Consensus, incorporating the pseudonym of the coin's still-mysterious inventor.

In proof-of-work, majority decision (consensus) is represented by the "longest-chain-wins" rule. This means that participants in the blockchain network accept the longest chain of **blocks** as being the only valid one.

The rule prevents multiple chains, each reflecting different versions of history, from existing side-by-side. The longer the consensual version of the

blockchain becomes, the more computing power and resources would be needed to — in theory — roll it back.

For the longest chain rule to function securely, adding new blocks to the chain is designed to be difficult — i.e, to be both costly and time-consuming. Network participants compete to solve complex cryptographic puzzles and become the first on the network to successfully validate each new block. Metaphorically, this process is referred to as “mining.”

A proof-of-work problem requires multiple, repeated attempts — consuming significant computing power (“work”) — before it is successfully solved. It’s largely a question of *try again, fail again, fail better*, as Sam Beckett would say.

Satoshi Nakomoto explained in the Bitcoin white paper that “the longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of **CPU** power.”

From this principle, we can understand that proof-of-work systems require significant computing resources to maintain.

This has led advocates of inclusivity and decentralization to argue that as the Bitcoin network grows, mining has become the near-exclusive privilege of those with the means to remain competitive by investing in the most sophisticated and powerful hardware.

Compute-intensivity has another significant implication. Powering the hardware required to mine the Bitcoin network consumes levels of electricity

comparable to small nations — a price that some critics argue is too high in an era of rising concern about climate change.

Proof-of-Stake at a Glance

Just like proof-of-work, proof-of-stake is designed to achieve distributed consensus over the valid ordering of transactions — i.e., reaching agreement on a shared, single version of history.

In blockchains that use proof-of-stake, nodes in the network engage in validating blocks, rather than allocating their computing resources to “mine” them.

Within these networks, security and consensus is achieved by participants committing a stake — their private or collective capital — to the enterprise in the form of the network’s native tokens.

A proof-of-stake systemfunctions as a cryptographic proof of ownership and proof of vested interest in the project’s ongoing success. To participate in maintaining the network, nodes “lock-up” native tokens using a smart contract, rendering them unspendable for the allocated time.

To extend the consensus history on the blockchain, a deterministic algorithm randomly selects which nodes become validators for each new block.

This randomized selection process, as well as stakeholders’ vested interest (stored value) in the network, is intended to disincentivize participants from attempting to sabotage history and choosing to undermine the system.

The cryptocurrency Ether (**ETH**) is a high-profile example of a project that is currently in the process of **migrating away** from proof-of-work toward proof-of-stake.

Its developers argue that, once successful, proof-of-stake will be more environmentally sustainable, as it dispenses with the dizzying amount of power needed to maintain Bitcoin.

They also claim that the system is more resistant to monopolies and centralization of power within the network, as participation is decoupled from the control over hardware and resources.