Web 3.0 Unveiled - Day 4

Mentored by FEC

How does Proof of Stake work?

On September 15th 2022, Ethereum famously had the **"The Merge"** event - where it transitioned from being a **Proof of Work network to a Proof of Stake network**. This was a collective effort of years of planning, and marked a major move for the Ethereum network.

Besides Ethereum, several other blockchains have been using Proof of Stake consensus algorithms even before it. Today, we will look at what Proof of Stake is and how it works.

What is Consensus?

Before we dig into the algorithm, we must be clear on what consensus even means. Not just the technical definition, but also just the English definition of the word. This section is repeated from the Proof of Work lesson, just in case you haven't read that one or just need a refresher.

The Merriam-Webster dictionary defines *Consensus* as follows:

> **a general agreement about something: an idea or opinion that is shared by all the people in a group**

When it comes to the technical definition in the context of blockchain technology, consensus means that all the nodes in a decentralized blockchain network agree upon the current state of the network - i.e. the transactions, account balances, and so on.

What is a Consensus Protocol?

When it comes to blockchains, it is important that **all nodes on a network can reach an agreement** on what the current state of the network is. Consensus protocols help us achieve that agreement. This section is also repeated from the Proof of Work lesson in case you need a refresher.

Although this topic isn't directly relevant to building dApps, having a deeper understanding of the technology you're building upon helps you make better decisions and ultimately makes you a better developer.

Consensus protocols are primarily economic systems that incentivize good behavior and disincentivize bad behavior by nodes on the network. Theoretically, it is possible to compromise the consensus of a blockchain by controlling a majority of the network. The goal of

a sound consensus protocol is to make that sort of attack economically unfeasible, at least for blockchains that people use and care about - like Bitcoin and Ethereum. Different protocols like Proof of Work and Proof of Stake take upon this problem differently.

Breaking down Proof of Stake

Proof of Stake underlies the consensus mechanism used by the Ethereum network and many other blockchains today. The core idea is as follows:

- Validators stake capital in the form of `$ETH` tokens into a smart contract on Ethereum mainnet
- The staked ETH acts as collateral and can be destroyed if the validator behaves maliciously by lying about the current state of the blockchain or not responding to requests made by other validators
- The validator is then responsible for checking that new blocks being formed are valid, and sometimes creating those blocks themselves

With the stake in place, lying as a validator can cause you to lose your staked capital. Therefore, validators are financially incentivized to not lie about their actions.

Proof of Stake vs. Proof of Work

The Proof of Stake system has a variety of advantages over Proof of Work:

- **Lowered energy usage**: moving Ethereum from PoW to PoS reduced the world's energy usage by 0.2%. On the scale of the entire world, that's a LOT of energy that was saved.
- **Lower barrier to entry**: In Proof of Work, miners have to have expensive, specialized hardware to be mining. Additionally, they need to cover electricity costs and have human resources available to manage the hardware and make sure everything keeps running smoothly. Also, they need to keep upgrading this hardware over time as improvements happen in computational power. In Proof of Stake, while there is a minimum 32 ETH staking requirement if you want to run a solo validator, the hardware requirements are significantly dropped and much more affordable, making 32 ETH look like a steal in comparison to what you'd be spending if you wanted to have a decent mining setup going.
- **Reduced centralization risk**: Due to the cost and specialized knowledge of setting up mining farms in PoW, there was a centralization risk associated with Ethereum. With Proof of Stake, validators just need to stake some capital up front with much more reasonable hardware requirements, which has led to significantly more nodes helping secure the network than in Proof of Work. As of writing, there are over 600,000 active validators on Ethereum, with over 90,000 waiting in the queue to become validators.

- **Reduced ETH issuance**: Due to lower energy requirements and cost, less ETH is required to incentivize validators leading to an overall reduction in the amount of ETH that is issued over time which helps reduce overall inflation of the ETH token.
- **Increased penalties**: Economic penalties for majority attacks are exponentially more expensive with the requirement of needing to stake capital up front compared to the cost of hardware on Proof of Work.

Block Production

Under Proof of Stake, it is validators who are responsible for creating new blocks. Different blockchains might refer to them differently (for example, Tezos calls them Bakers) - but we will use the term validators as is used in the Ethereum world.

There is no concept of a miner in the Proof of Stake world - and no need to solve any hard mathematical puzzles.

To become a validator, a user must simply deposit 32 ETH into the deposit contract on Ethereum mainnet, and run the required node software - an execution client, a consensus client, and a validator client.

The execution client is pretty much the same software that you would have run in Proof of Work Ethereum land - for example something like `go-ethereum` (Geth). This is responsible for executing transactions within the EVM and figuring out state changes. The consensus client is responsible for achieving consensus with other nodes in the chain through the Beacon Chain, and the validator client is responsible for voting on blocks and producing new blocks when necessary.

The validators then receive new blocks from their peers on the Ethereum network. The validator re-executes the transactions in that block, and confirms that the block is valid. They then send an attestation (a positive vote) in favor of the block to the whole network. If enough votes are collected in favor of the block, the block is added to the chain. This process is repeated for future blocks.

Every 12 seconds, the time of a new block on Proof of Stake Ethereum, a validator is randomly selected to be a block proposer. If selected as the proposer, this validator is responsible for creating a new block and sending it out to other nodes, which can then vote in favor or against that block.

Network Security

Becoming a validator is a commitment towards helping secure the Ethereum network. The validator is expected to maintain sufficient hardware, internet connectivity, and uptime to participate in block proposal and validation. In return, they are paid rewards in ETH.

If a validator fails to meet their commitments, they miss out on ETH rewards. By failing to participate when called upon (asked to vote on a block, for example) they fail to get the ETH reward. If they behave dishonestly or maliciously, then their stake can also be slashed, leading to a financial loss and them being kicked out of being a validator.

Behaving maliciously could include doing things like proposing multiple blocks in a single 12 second time period, or submitting false attestations during block validations. The amount of ETH that gets slashed by doing such malicious activities depends on how many *other* validators also got slashed around the same time. This is because a single validator's internet connection going out shouldn't have the same penalty as a hundred validators coordinating to act maliciously together as an attack on the network.

The Downsides

Not all are rainbows and unicorns however. With its many advantages, Proof of Stake does have a few cons that continue to make consensus mechanisms an active field of research and innovation.

1. **Proof of Stake is simply much younger and less battle tested than Proof of Work**, which has stood the test of time for over a decade since Bitcoin was created. In fact, one could argue that Bitcoin and its protocol implementation is the world's biggest bug bounty.
2. **Proof of Stake protocols are much more complex to implement in code**, which also means there is a higher risk of introducing bugs and allowing issues to arise.

Due to this, many in the Ethereum community and outside are still actively researching and working on ways to keep improving consensus mechanisms even further.

Additional Resources

The following are optional, but recommended, additional readings to help you understand even more about Proof of Stake:

- https://vitalik.ca/general/2017/12/31/pos_faq.html
- https://bitcoinmagazine.com/culture/what-proof-of-stake-is-and-why-it-matters-1377531463