CrushCrypto

What is Proof of Stake?

Educational Series

September 20, 2018

History

- The proof-of-stake consensus mechanism was first suggested on the Bitcointalk forum in 2011, but was not formally introduced until Sunny King and Scott Nadal wrote a paper on it in August 2012.
- Instead of relying on the energy dependent computational work of miners to securely add blocks to the chain, they proposed the method of staking - where an algorithm would choose block validators based on the number of coins a person has.
- They proposed this method to try and tackle Bitcoin's increasing energy costs and mining difficulty that was going to continue indefinitely as long as it is profitable for miners to purchase more hash power.
- Sunny King later created Peercoin based off this paper, the first cryptocurrency to implement a proof-of-stake consensus mechanism.

Overview

- Just like proof of work, proof-of-stake is a mechanism designed for deciding who gets to validate the current block and achieving consensus between the network's nodes on what data is valid. However, proof of work and proof-of-stake use completely different methods to achieve the same end goal.
- Proof-of-stake algorithms achieve consensus by requiring users to put a certain amount of their coins "at stake" to have a chance of being selected to validate a block of transactions and receiving that block reward. Malicious actors risk losing their stake.
- The more coins at stake, the higher chance the user will get to validate the next block and reap the block reward (newly minted coins and transaction fees generated in the block). Proof-of-stake validators are called "forgers" instead of "miners".

How does it work?

- Putting coins at stake can be thought of as locking the coins in a virtual safe and using it as collateral to have the chance of validating a block. Holding coins in a wallet is not enough to be considered for validation, and once the coins are staked there is a waiting period to withdraw them.
- If there is a malicious forger that tries to include faulty transactions in a block, they will lose all the coins they have at stake. This mechanism is called slashing, and it ensures that validators are incentivized to act in an honest manner.
- A forger of a new block is chosen by two-part process. The first part considers how many coins the user is staking, while the second part varies between networks.

51% attack

- The main attack vector for the proof-of-work consensus mechanism is a 51% attack. As mining pools continue to grow and a small set of entities/mining pools control more and more of the miner supply, the easier a theoretical proof of work 51% attack becomes.
- In a proof-of-stake system, a 51% attack is also a possible attack vector. However, this type of 51% attack requires a malicious actor to obtain 51% of more of the supply of that coin – theoretically a much more difficult (and expensive) feat than pooling 51% of a network's mining power.

51% attack (continued)

- Even if an attacker has enough funds to buy 51% or more of a coin's market cap, the purchasable supply at any time is well under 51% due to limited exchange liquidity.
- Large amount of money and time needed to gather the resources to launch a 51% attack on a proof-of-stake system of a major coin. The accumulation for the attacker would cause the coin's value to increase substantially, causing the attack to become more expensive.
- Reduced incentive to launch a 51% attack on a proof-of-stake system, as the person suffering the most from it would be the attacker that is now the majority stakeholder in the network.

Benefits

- **Energy savings**: Proof-of-stake uses an extremely low amount of computing power to secure the network when compared to proof of work.
- **Reduced 51% attack probability**: In general, a proof-of-stake system is harder to launch a 51% attack on than a proof of work system with the same market cap.
- **Low barrier to entry**: Any coin holder above a certain amount can enter the validator pool simply by staking their coins. There is no requirement to purchase mining equipment, set up a machine, and ensure it stays running in good condition.
- **Built-in incentives**: An attacker in a proof-of-stake system must have coins at stake, and their attack would directly devalue the coins they own. Compare this to proof of work, where mining equipment can be used to attack a network and will still hold the same monetary value after the attack and can be used to mine other coins.

Weaknesses

- **Validators with large stakes**: If a small number of people own a significant portion of a coin's supply, they will have a higher chance of validating blocks and reaping the rewards, in turn increasing their stake even more. This could lead to supply centralization over time.
- **Voting for multiple forks**: Proof-of-stake by itself is not an efficient way to achieve consensus because people staking can vote for multiple forks of a blockchain effortlessly. In proof of work this is far less likely, as validating blocks on multiple chains has a real-world cost associated with energy. As a result, many proof-of-stake systems have a mixture of PoS and PoW to ensure there is a final decision on the valid chain.
- **Other security concerns**: There are still some major security concerns with proof-of-stake, such as the nothing at stake problem and long-range attacks.

CrushCrypto