Proof of Capacity (PoC)

Return to Consensus Mechanism

The definition is provided by Hayes[1)]:

Proof of Capacity (PoC) is a consensus mechanism algorithm used in blockchains that allow for mining devices in the network to use their available hard drive space to decide mining rights and validate transactions. This is in contrast to using the mining device's computational power (as in the Proof of Work (PoW) algorithm) or the miner's stake in the cryptocurrencies (as in the Proof of Stake (PoS) algorithm).

- **Note:** PoC also includes variants such as **Proof of Space (PoSp)** and **Proof of Storage (PoSt)**.

PoC emerged as one of the many alternative solutions to the problem of high energy consumption in PoW systems and cryptocurrency hoarding in PoS systems.

PoC allows the mining devices, also known as nodes, on the blockchain network to use empty space on their hard drive to mine the available cryptocurrencies.

Instead of repeatedly altering the numbers in the block header and repeated hashing for the solution value as in a PoW system, PoC works by storing a list of possible solutions on the mining device's hard drive even before the mining activity commences.

The larger the hard drive, the more possible solution values one can store on the hard drive, the more chances a miner has to match the required hash value from his list, resulting in more chances to win the mining reward.

To draw an analogy, if lottery rewards are based on matching the most numbers on the winning ticket, then a player with a longer list of possible solutions will have better chances of winning. Additionally, the player is allowed to keep using the lottery ticket block numbers again and again repeatedly.

The proof-of-capacity protocol involves a two-step process that involves plotting and mining.

First, the hard drive is plotted: the list of all possible nonce values are created through repeated hashing of data, including a miner's account. Each such nonce contains 8192 hashes, which are numbered from 0 to 8191. All the hashes are paired into "scoops," which means adjacent hashes are combined to form a pair of two. For instance, hash 0 and 1 constitute scoop 0, hash 2 and 3 constitute hash 1, and so on.

The second step involves the actual mining exercise, during which a miner calculates a scoop number. For instance, if a miner begins the mining activity and generates a scoop number 38, the miner would then go to scoop number 38 of nonce 1 and use that scoop's data to calculate a deadline value.

The process is repeated for calculating the deadline for each nonce held upon on the miner's hard drive. Following the calculation of all the deadlines, the one with the minimum deadline is selected by the miner.

A deadline represents the duration of time in seconds that must elapse since the last block was forged before a miner is allowed to forge a new block. If no one else has forged a block within this time, the

miner can forge a block and claim the block reward.

For instance, if miner X comes up with a minimum deadline of 36 seconds and no other miners can forge the block within the next 36 seconds, X will secure the chance to forge the next block and get rewarded.

1)

Adam Hayes, Investopedia, Proof of Capacity (Cryptocurrency), 29 June 2021, Accessed: 18 July 2021, https://www.investopedia.com/terms/p/proof-capacity-cryptocurrency.asp