Blockchain Council™

Other Consensus Mechanisms in Blockchain

Blockchain Council™

Proof-of-Capacity

Proof-of-Capacity(PoC)

PoC is another consensus algorithm used in blockchains that allows mining devices in the network to decide mining rights and validate transactions with the help of their available hard drive space.

The larger the hard drive, the more solution values one can store on the hard drive, the better chances a miner has to meet the required hash value from his list, resulting in a higher possibility of acquiring and gaining the mining prize.

It has appeared as an alternatives to the problems of high energy consumption in PoW consensus and coin hoarding in PoS.

How PoC Works: Plotting and Mining

The Proof-of-Capacity system follows a two-step method that involves plotting and mining.

First, the hard drive is plotted: A list of all potential nonce values is constructed by hashing data, including a miner's account, over and over again. Each nonce is made up of 8192 hashes, numbered from 0 to 8191. All of the hashes are coupled into "scoops," which are groups of two neighboring hashes.

The second phase is the actual mining, which entails calculating a scoop number by a miner.

For example, if a miner starts mining and generates scoop number 38, the miner would then go to nonce 1's scoop number 38 and utilize the data from that scoop to calculate a deadline value.

This process is repeated again and again in order to calculate the deadline for each nonce held upon on the miner's hard drive. The miner chooses the one with the lowest deadline after calculating all of the deadlines.

Advantages and Disadvantages of PoC

Advantages:

- Any regular hard drive, including those with Android-based systems can be used by PoC.
- Secondly, Proof-of-Capacity is assumed to be up to 30 times more energy-efficient than ASIC-based bitcoin mining.
- The other benefit is that there is no need for dedicated hardware or frequent hard disc upgrades.
- Also, the mining data can be simply erased, and the drive can be repurposed for other data storage requirements.

Drawbacks:

- Not many developers have adopted the system.
- Malware can affect mining activities.
- PoC's widespread usage could spark an "arms race" to develop higher-capacity hard drives.

Projects Using PoC

There are various cryptocurrencies that incorporate PoC

BXTB

Burstcoin

BHD

Blockchain Council™

Proof-of-Activity (PoA)

Proof-of-Activity (PoA)

PoA is a consensus algorithm used in Blockchain technology that ensures that all transactions occurring on the network of Blockchain are genuine and authentic.

PoA consensus, which is a combination of proof-of-work and proof-of-stake, ensures that all miners arrive at a consensus.

In other words, PoA is an attempt to consolidate the best features of PoW and the PoS systems.

Conditions for a PoA consensus:

- The first condition is that the validators have to confirm their real identities.
- The second condition is that a candidate must be ready to invest and put his reputation at stake. A rigorous selection process decreases the danger of choosing shady validators and encourages long-term commitment to the Blockchain.
- The third condition is that a method for electing validators must be equal to all competitors.
- And the last condition is that the identity of validators must be verified to maintain the integrity of the Blockchain.

Block Generation in PoA

At first, each miner uses his or her hash power to create an empty block header.

When a miner's block header data hash is smaller than the current difficulty target, the miner has successfully created a block header. If the block header is successful, it is broadcast to the network.

The hash of the previous block is connected to the hash of the block header.

Following that, each combination is hashed, and follow-the-satoshi is run with each hash as input.

The block header from step two is then checked by active miners to see if it is valid.

Following validation, each miner determines whether they are a stakeholder in the block.

Successful miners sign the hash block header with a private key, exposing their satoshi and broadcasting their signature to the network. This method is repeated until each validator has signed the block.

Block Generation in PoA

The wrapped block is broadcast to the network by the last miner to sign it.

The block is considered a legitimate extension of the Blockchain once other nodes see validity in the above four steps.

Nodes try to extend the longest branch they are aware of by assessing PoW difficulty, similar to the Bitcoin Blockchain.

The fees earned by the final miner are split between them and the rest of the "winners."

Advantages and Disadvantages of PoA

Advantages:

- The major advantage of this consensus is that it has High-risk tolerance as long as 51 percent of the nodes are not acting maliciously.
- The other advantage is that the interval of time at which new blocks are created is predictable. But in the case of PoW and PoS, this time is not fixed and typically varies.
- The other crucial benefit of this consensus is that it offers high transaction rates.
- Last but not least, it is far more sustainable compared to POW, which requires computational power.

Disadvantages:

- The first drawback is massive energy consumption due to the mining feature.
- Second, it doesn't have any solution to put a stop to the double signing of the validators.
- Another drawback is that PoA is not decentralized but is just an effort to make centralized systems more efficient.
- Another concern related to POA is that here the validators are visible to anyone. Thus, knowing validators' identities could potentially cause third-party manipulation.

Decred: Example of PoA

Decred (DCR) is the popular digital currency that uses the PoA consensus.

Decred's mining process begins with nodes searching for a solution to a cryptographic puzzle of a defined difficulty level in order to generate a new block. So far, this procedure appears to be similar to a PoW method.

The solution is broadcast to the network once it has been discovered. The solution is then verified by the network. At this time, the system is classified as a Proof-of-Stake (PoS).

The more DCR a node mines, the more likely it is that it will be chosen to vote on the block. (Stakeholders gain tickets that offer them voting power in DCR's Blockchain in exchange for mining DCR.)

Five tickets are chosen at random from the ticket pool, and if at least three of the tickets vote "yes" to validate the block, it is put to the Blockchain network forever. Both miners and voters are rewarded with DCR.