Blockchain™
Council

Other Consensus Mechanisms in Blockchain

Proof-of-Capacity (PoC)

- PoC is a consensus algorithm that allows mining devices to decide on mining rights and validate transactions by using their available hard drive space as a metric.
- 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 placed itself 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.

- **Step 1: Plotting**
  - A list of all potential nonce values is constructed by hashing data, including a miner's account, over and over.
  - Each nonce comprises 8192 hashes, numbered from 0 to 8191.
  - All of the hashes are coupled into "**scoops**," which are groups of two neighboring hashes.

- **Step 2: Mining**
  - This entails calculating a scoop number by a miner.
  - For instance, if a miner starts mining and generates scoop number 38, the miner goes to nonce 1's scoop number 38 and utilizes that scoop's data to calculate a deadline value.
  - This process is repeated continually to calculate the deadline for each nonce.
  - After calculating all of the deadlines, the miner chooses the one with the lowest deadline.

Advantages and Disadvantages of PoC

Advantages:

- PoC can use any regular hard drive, including those with Android-based systems.
- Secondly, Proof-of-Capacity is assumed to be up to 30 times more energy-efficient than ASIC-based bitcoin mining.
- The entry requirements are very low as compared to other mining systems.
- 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.
- With Reduced entry requirements create an ecosystem where people can use large hard drives to mine the majority of network currency.

Projects Deploying PoC

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, is a hybrid entailing the best features of PoW and the PoS systems.

Conditions for a PoA consensus:

- POA requires the network to perform the work on the block twice, once while mining and once while validators are required to validate the block.
- POA requires the participants for validation to have a stake in the network, similar to Proof of Stake.

Block Generation in PoA

- At first, each miner uses their hash power to create an empty block header.
- If the block header is smaller than the difficulty target, the miner has created a block header; it is then broadcast to the network.
- Following that, each combination is hashed, and the follow-the-satoshi algorithm 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, miners, which are a stakeholder in the block, 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.

Advantages and Disadvantages of PoA

Advantages:

- This consensus has high-risk tolerance due to double security of both proof-of-work and proof-of-stake consensus.
- The other advantage in the case of POA is the time interval between blocks is not fixed and typically varies.
- POA follows users' participation using follow the satoshi and incentivized nodes to take part in consensus..
- POA allows connection between POW and POS working nodes promoting enhanced network topology.

Disadvantages:

- Due to the involvement of two different consensus algorithms, PoA has a massive energy Footprint.
- It is still susceptible to a double signing problem.

Decred: Example of PoA

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

- Decred's nodes search for solution of the cryptographic puzzle of a defined difficulty level.
- The solution is broadcast to the network once discovered to be verified.
- Nodes are chosen by the amount of token held by their wallet to vote on the block.
- Five tickets are chosen randomly from the ticket pool; at least three of the tickets vote yes to validate the block. Both miners and voters are rewarded with DCR.

Blockchain Council™

THANK YOU!

Any Questions?

Visit

community.blockchain-council.org

Mail Us

hello@blockchain-council.org