TCS332 Fundamental of Information Security and Blockchain

Consensus algorithms

Dr. Mohammad Wazid
Professor, Department of CSE, GEU Dehradun
India

Proof-of-Stake (PoS)

- It is a consensus algorithm that decides on who validates the next block, according to how many coins you hold, instead of miners cracking cryptographic puzzles using computing power to verify transactions as they do with traditional Proof-of-Work.
- The probability of validating a new block is determined by how large a stake a person has.
- The validator does not receive a block reward. Instead, they collect network fees as their reward.
- Peercoin was the first cryptocurrency to implement a full-scale PoS consensus model.

Proof of Weight (PoW)

- Proof of Weight is a blockchain-based consensus mechanism that gives users a weight based on how much cryptocurrency they are holding.
- It was launched in 2017 as a consensus algorithm on the Filecoin blockchain platform.
- It is a large upgrade of the Proof of Stake mechanism, which aims to remove the biased nature of PoS.
- The Proof of Weight is not a single consensus algorithm.
- Instead, it is an umbrella term for an entire array of consensus algorithms largely based on the Algorand.
- The Algorand consensus model was developed by researchers at MIT, where Algorand is a protocol that confirms transactions very quickly.

Proof of Weight (PoW)….

- The Proof-of-Weight considers some other factors than owning more tokens like in PoS, and these factors are known as "weighted factors," which play an integral role in reaching consensus without the risk of any fork.
- **Algorand and other users of the proof-of-weight consensus mechanism believe that if holders with the highest loss are invested in the safety of the network, the chances of these attacks occurring are lower.**
- Algorand is an excellent example of a proof-of-weight consensus mechanism.
- Algorand's native cryptocurrency is called ALGO.

Proof of capacity (PoC)

- Proof of capacity (PoC) is a consensus mechanism algorithm used in blockchains that allows for mining devices in the network to **use their available hard drive space to decide mining rights.**
- This is in contrast to using the mining device’s computational power (as in the proof of work algorithm) or the miner’s stake in the cryptocurrencies (as in the proof of stake algorithm).
- It uses spare space on a device's hard drive to store solutions to a cryptocurrency hashing problem.
- The main benefit of a PoC system is its efficiency compared to proof-of-work (PoW) and proof-of-stake (PoS) systems.
- **Blockchains that run on proof of capacity include Signum, Chia, and SpaceMint.**

References

- https://news.mit.edu/2021/unlocking-potential-blockchain-0616
- https://people.csail.mit.edu/nickolai/papers/gilad-algorand-eprint.pdf