Consensus Mechanisms

Blockchain @ uninsubria

Roberto Vicario

2024/2025

Contents

1 Proof of Work (PoW) 2
1.1 Incentives 2
1.2 Transaction Fees 2

2 Proof of Stake (PoS) 3
2.1 Slashing 3

1 Proof of Work (PoW)

Proof of Work (PoW) is a consensus mechanism used in blockchain systems to ensure that all participants agree on the state of the ledger. It requires participants (miners) to solve complex mathematical problems in order to add new blocks to the blockchain.

1.1 Incentives

With the purpose to create a secure and decentralized network, PoW mechanisms provide economic incentives for miners to participate honestly. The main incentives include:

- **Block Rewards:** Miners receive a reward for successfully mining a block, which is typically a fixed amount of cryptocurrency.
- **Transaction Fees:** Miners can also collect fees from transactions included in the blocks they mine.

Selfish Mining: A node can deviate from the protocol to increase its own rewards, potentially leading to a situation where it can earn more than its fair share of rewards.

There are two main cases to consider regarding selfish mining:

- **Case with $\alpha > 0.5$:** Node A can orphan honest blocks and earn approximately 100% of the rewards.
- **Case with $\alpha < 0.5$:** It is still possible to earn more than α of the total rewards through a strategy that: delays block announcements, selectively orphans blocks, and exploits tie-breaking in an adversarial manner.

In general, a selfish miner can obtain a share of rewards greater than their relative mining power α if α exceeds approximately *0.33*. This means that even with less than one-third of the total mining power, a selfish miner can outperform honest mining by strategically withholding and releasing blocks.

1.2 Transaction Fees

Transaction fees are an essential part of PoW mechanisms, as they provide an additional incentive for miners to include transactions in the blocks they mine. The fees are typically paid by users who want their transactions to be processed quickly.

Block Size Problem: The limited capacity of blocks leads to competition among transactions for inclusion, resulting in the need for transaction fees.

2 Proof of Stake (PoS)

Proof of Stake (PoS) is a consensus mechanism used in blockchain systems as an alternative to Proof of Work (PoW). It aims to achieve consensus without requiring extensive computational resources, making it more energy-efficient and environmentally friendly.

2.1 Slashing

Just like in PoW, validators in PoS systems are incentivized to act honestly through rewards and penalties. To discourage malicious behavior, PoS protocols often implement a mechanism called *Slashing*. This involves the partial or full loss of staked funds for validators who engage in misbehavior, such as:

- **Double Signing:** Attempting to validate multiple blocks at the same height.
- **Inactivity:** Failing to participate in the consensus process for an extended period.
- **Attestation Failure:** Not voting on blocks or not following the protocol rules.