Proof of Work (PoW) Mechanisms

Blockchain @ uninsubria

Roberto Vicario

2024/2025

Contents

1 Proof of Work (PoW) Mechanisms

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:

- **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.
  - Exploits tie-breaking in an adversarial manner.

Key finding:

$$\text{Reward share} > \alpha \text{ if } \alpha > 0.33 \tag{1}$$

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.

1.2.1 2.1 Problema del block size

- Capacità limitata: es. `1MB`, (≈1000) tx/block.
- Le transazioni competono per essere incluse: nasce il concetto di **transaction fee**.

1.2.2 2.2 Meccanismo di asta (First-Price Auction)

- Ogni transazione propone una fee.
- I miner selezionano le tx con la fee più alta.
- Problemi:
  - Strategia di bidding inefficiente.
  - Incentivi al selfish mining se `TxFees >> BlockReward`.

1.2.3 2.3 Meccanismo EIP-1559 (Ethereum)

- Introduce **base fee** deterministica `r`, calcolata dinamicamente:
  - Se \`text{block size} > c \Rightarrow r \uparrow`
  - Se \`text{block size} < c \Rightarrow r \downarrow`
- **Fee totale = base fee (bruciata) + tip (al miner).**
- Vantaggi:
  - Prevedibilità.
  - Mitigazione della collusione.
  - Riduzione dell'inflazione tramite burning.

???????????