Blockchain CheatSheet - Consensus

Table of Contents

§ Fundamentals

- Consensus
- Nodes
- Needs

§ Proof of Work (PoW)

- Overview
- Strengths
- Weaknesses
- Current PoW Systems

§ Economics

- Pools

§ Proof of Stake

- Overview
- Strengths
- Weaknesses
- Delegated Proof of Stake (DPoS)
- Current PoW Systems

§ The Byzantine Generals Problem

- Blockchain Application

§ Other Consensus Algorithm

---

§ Fundamentals

Consensus

Definition: Consensus in blockchain refers to the mechanism through which nodes (independent computers connected in a network) agree on the state of a distributed ledger. It ensures that all transactions are valid and irreversible, according to rules defined by the consensus algorithm.

Types

- Majority = 51%
- Super-Majority = +66%
- Unanimous = 100%
- Weighted = Proof of Stake Votes are weighted based on the stake (or the amount of cryptocurrency held) by each node.

Nodes

Definition: A node is a computer that runs software supporting a specific blockchain architecture, forming a part of the blockchain's distributed network.

Common nodes

Mining Node: Highly specialized and powerful computers that perform computations to propose new blocks. They receive mining rewards, covering the cost of their operations.

Full Node: Acts as a relay between the creation of blocks and their distribution. They maintain a complete copy of the blockchain's ledger and validate all transactions and blocks to ensure consistency and security.

Light Node: Acts as a relay between the creation of blocks and their distribution. They maintain a complete copy of the blockchain's ledger and validate all transactions and blocks to ensure consistency and security.

Needs

In a blockchain system, which is distributed and decentralized, a robust mechanism is essential since parties involved often cannot inherently trust each other. We need to ensure the integrity of the ledger so that the transaction history is reliable. This leads to the necessity of validating transactions without needing trust.

The consensus mechanism and its forms are designed to address these issues.

> **Consensus** is the process that allows trust in the outcome of a transaction or a block within a blockchain, without needing to trust the individual parties involved in the transaction or the entity that verifies it.

---

§ Proof of Work (PoW)

Overview

- **Purpose**: Ensure the immutability of the blockchain.
- **How it is done**: *Nonces* (Numbers Only Used Once) are added to the end of each block's hash to find a hash that meets a specific difficulty target, often requiring a certain number of leading zeros. This validates the block.
- **Why**: The system requires proof that computational work has been done. Finding a hash that meets the difficulty target is challenging and requires many attempts, demonstrating that significant computational work has been performed.
- **Security**: This process makes it difficult for anyone to alter the data without redoing all the computational work, thus enhancing the security of the blockchain.

Strengths

- **Predictable Block Times**: Maintains a consistent time interval between blocks.
- **Fully Decentralized**: Allows any participant to contribute to network security.
- **High Cost of Attack**: The expense of achieving a 51% attack makes it unfeasible.
- **Uncensorable and Public**: Transactions and blocks are broadcasted publicly and cannot easily be censored.

Weaknesses

- **High Energy Consumption**: PoW is resource-intensive, often criticized for its environmental impact.
- **Centralization of Mining Pools**: Can lead to potential centralization, as few pools might dominate the mining process.
- **Unfeasible for Standard Computers**: Mining has become impractical for ordinary computers due to the high computational requirements.
- **Variable Mining Profitability**: Mining profitability can fluctuate, sometimes making it less rewarding financially.

Current PoW Systems

> For the most accurate and up-to-date information, I recommend performing quick research with the help of AI assistants to stay current with the latest developments in PoW systems.

---

§ Economics

For most individuals, it is nearly impossible to successfully mine a block on their own due to the prohibitive costs of specialized mining hardware and electricity, especially when compared to the potential rewards.

Pools

The most feasible approach is to join a mining pool, which consolidates the processing power of multiple miners. These pools typically have access to cheaper energy sources and more efficient mining rigs. As a member, you would receive a portion of the rewards proportional to your contribution to the pool’s overall resources.

---

§ Proof of Stake (PoS)

Overview

Proof of Stake (PoS) is an alternative consensus mechanism to Proof of Work (PoW), offering a different approach to achieving consensus in a blockchain network.

Definition: In PoS, the "stake" refers to the amount of cryptocurrency an individual holds and commits as a means to gain the right to participate in the process of creating new blocks. The probability of being chosen to create a block is typically proportional to the amount of stake held.

Strengths

- **Energy Efficiency**: PoS is far less energy-intensive compared to PoW, reducing the environmental impact.
- **Interest-Based Security**: The more stake a validator has, the more they stand to lose from acting maliciously, aligning their interests with the well-being of the network.
- **Highest Cost of Attack**: The expense of achieving a 51% attack makes it the most unfeasible due to the interest that you achieve having more control.
- **Uncensorabile and Public**: Transactions and blocks are broadcasted publicly and cannot easily be censored.
- **Significantly more scalable**: Lower operational costs allow PoS to handle more transactions, enhancing scalability.

Weaknesses

- **Wealth Accumulation**: Higher stakes increase rewards, risking wealth centralization and power imbalances.
- **Security Concerns**: PoS may be perceived as less secure than PoW because stake-based security depends heavily on economic penalties, not computational efforts.
- **Sybil Attack Risk**: High entry barriers deter but do not eliminate Sybil attacks, where multiple fake identities influence the network.
- **Nothing at Stake Problem**: Validators may support multiple blockchain forks since doing so incurs no significant costs, potentially leading to double-spending issues.

Delegated Proof of Stake (DPoS)

DPoS aims to democratize the staking process by allowing stakeholders to delegate their staking power to "delegates," who validate transactions and create blocks on their behalf. This system can potentially address the centralization of rewards by spreading the opportunity to earn transaction fees and block rewards more broadly among participants.

Current PoW Systems

> For the most accurate and up-to-date information, I recommend performing quick research with the help of AI assistants to stay current with the latest developments in PoW systems.

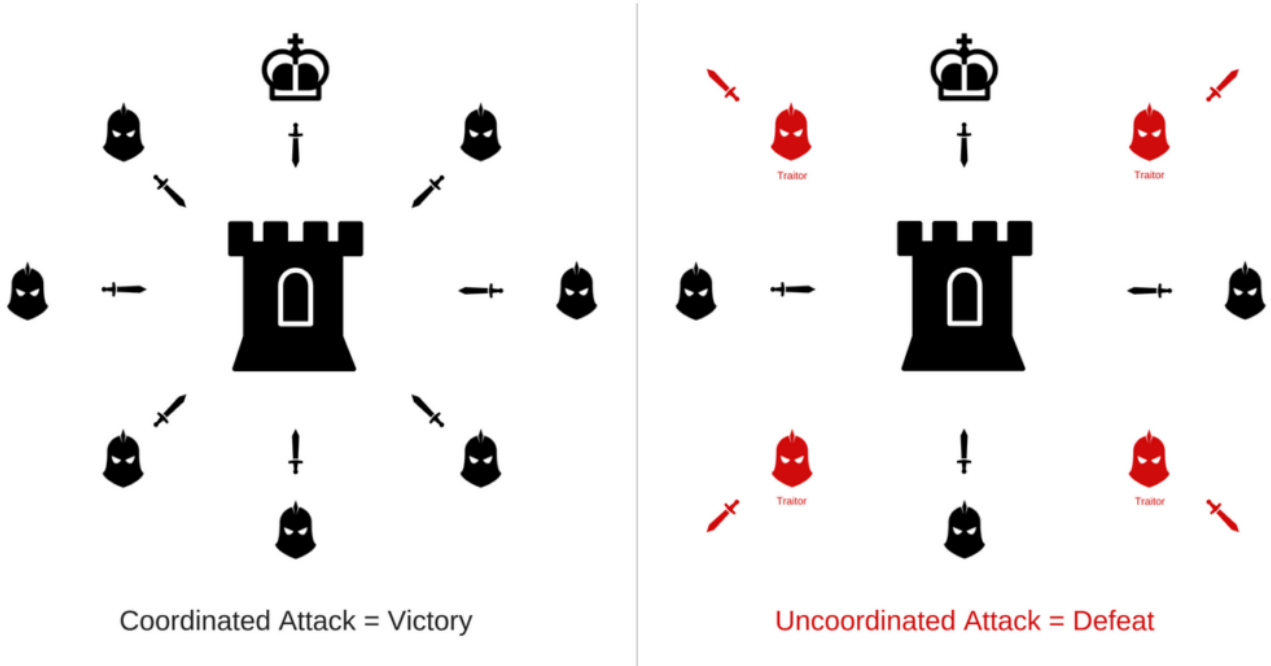
---

§ The Byzantine Generals Problem

The Byzantine Generals Problem illustrates a challenge in achieving consensus in distributed systems, especially under conditions where some participants (or "nodes") may act maliciously or fail to communicate reliably. The problem is named after an analogy involving Byzantine generals who must agree on a battle plan via messengers, knowing that some of the generals or messengers might be traitors.

Key Aspects:

- **Trust and Coordination**: Ensuring all loyal generals (or nodes in a blockchain) reach a common decision, despite the presence of traitors who may disrupt the consensus or send false information.
- **Consensus Reliability**: The need for a mechanism that guarantees agreement among the participants, ensuring that messages are not altered and that the agreed-upon strategy (or transaction) is executed consistently across the network.



Blockchain Application

- In blockchain technology, this problem is analogous to ensuring that all nodes in the network agree on the validity and order of transactions, despite potential attempts by some participants to cheat or disrupt the process. Solutions such as Proof of Work (PoW) and Proof of Stake (PoS) are designed to mitigate these risks by requiring participants to contribute work or stake, creating economic and computational barriers to dishonest behavior.

---

§ Other Consensus Algorithms

- **Practical Byzantine Fault Tolerance (pBFT)** : Democratic election of a leader who delegates the "shard" nodes for validation.
- **Federated Byzantine Fault Tolerance (fBFT)** : Federated elections of a leader who delegates the "shard" nodes for validation.
- **Delegated Byzantine Fault Tolerance**
- **Proof-of-Importance (PoI)** : How much you use your Stake.
- **Proof-of-Elapsed-Time (PoET)**
- **Proof-of-Capacity (PoC - aka P-o-Space)**
- **Proof-of-Authority (PoA)**
- **Raft** (more classical consensus, not blockchain specific)

Is not proven that a particular consensus algorithm is suitable for every case. May very well be the opposite case in many instances.

> Consensus algorithms needs to be fine tuned to the use case.

Suggested Follow-up

Blockchain CheatSheet - Cryptoapplications

Author: Kenneth Boldrini