Consensus Model: POW

Table of Content

1. Problem of Double-Spending and The Necessity of a Trustless System

Double-spending occurs when a digital currency holder maliciously or inadvertently spends the same digital tokens more than once. In a centralized system, this issue is typically prevented by a trusted intermediary or authority that ensures transactions are valid and prevents duplication.

In traditional digital currency or online payment systems, trust is placed in a central authority, like a bank or a payment processor, to verify and validate transactions. These authorities maintain ledgers, confirming the authenticity of transactions and preventing double-spending.

Vulnerabilities of Centralization:

Single Point of Failure:

Satoshi Nakamoto emphasized that centralized systems have a single point of failure. In the context of financial or digital systems, this means that if the central authority, such as a bank or payment processor, is compromised, the entire system could be at risk. This vulnerability is a fundamental issue in centralized models.

Third-Party Dependency:

Centralized systems necessitate trust in intermediaries or third-party entities. Users must trust these intermediaries to handle their transactions, validate their authenticity, and protect their assets.

Control and Manipulation:

Centralized systems are susceptible to manipulation or misuse of power by the controlling entity. This could involve censorship, restrictions on transactions, or unauthorized access to users' funds and data.

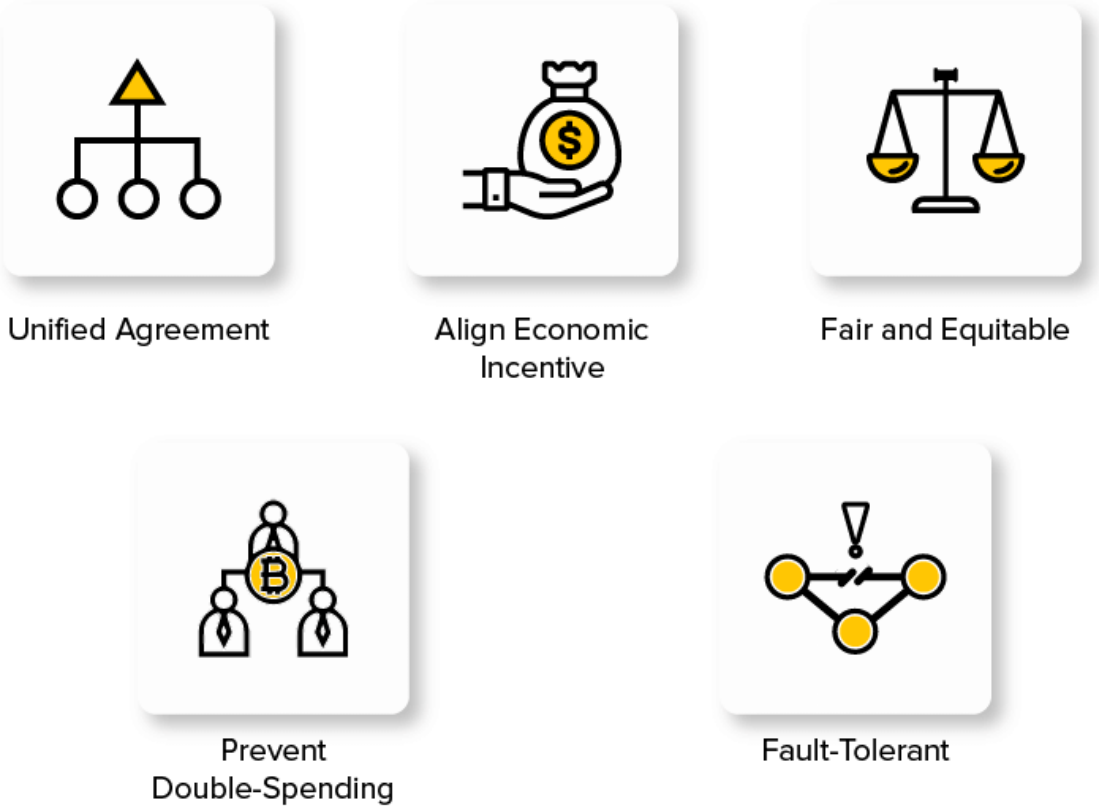
2. Proposed Solution: Consensus Mechanism

What is the Blockchain Consensus Algorithm?

The simplest answer to what is Blockchain consensus algorithm is that, it is a procedure via which all the peers of a Blockchain network reach a common acceptance or consensus about the real-time state of the distributed ledger.

A consensus mechanism enables the blockchain network to attain reliability and build a level of trust between different nodes, while ensuring security in the environment. This is the reason why it is one of the vital parts of every Blockchain app development guide and every dApp project in the distributed ledger environment.

Objectives of Blockchain Consensus Mechanism



- **Unified Agreement**
  One of the prime objectives of consensus mechanisms is attaining unified agreement. Unlike centralized systems where having a trust on authority is necessary, users can operate even without building trust in each other in a decentralized manner. The protocols embedded in the Distributed blockchain network ensures that the data involved in the process is true and accurate, and the status of the public ledger is up-to-date.

- **Align Economic Incentive**
  When it comes to building a trust-less system that regulates on its own, aligning the interests of participants in the network is a must.
  A consensus blockchain protocol, in this situation, offers rewards for good behaviour and punishes the bad actors. This way, it ensures regulating economic incentives too.

- **Fair & Equitable**

Consensus mechanisms enable anyone to participate in the network and use the same basics. This way, it justifies the open-source and decentralization property of the blockchain system.

- **Prevent Double Spending**
  Consensus mechanisms works on the basis of certain algorithms that ensures that only those transactions are included in the public transparent ledger which are verified and valid. This solves the traditional problem of double-spending, i.e., the problem of spending a digital currency twice.

- **Fault Tolerant**
  Another characteristic of the Consensus method is that it ensures that the blockchain is fault-tolerant, consistent, and reliable. That means, the governed system would work indefinite times even in the case of failures and threats.
  Currently, there are a plethora of Blockchain consensus algorithms in the ecosystem and many more are heading to enter the marketplace. This makes it imperative for every Blockchain development company and enthusiastic Entrepreneur to be familiar with the factors that defines a good consensus protocol, and the possible effect of going with a poor one.
  With the basics of Blockchain consensus methods being covered, let's dive deeper into the topic and look at the popular types of consensus mechanism.

Properties of a Good Blockchain Consensus Mechanism

- **Safety:** In a good consensus mechanism, all the nodes are capable of generating results that are valid according to the rules of protocol.

- **Inclusive:** A good consensus blockchain mechanism ensures that every particular node of the network participates in the process of voting.

- **Participatory:** A consensus mechanism where all the nodes actively participate and contribute to updating databases on Blockchain is called a good consensus model.

- **Egalitarian:** Another trait of a good mechanism is that it gives equal value and weightage to every vote received from the node.

Consequences of Choosing a Bad Consensus Protocol

- **Blockchain Forks**

  Choosing a poor blockchain consensus method increases the vulnerability of the chain. One such vulnerability that is faced by the blockchain enthusiasts and developers is Blockchain Forks.
  Blockchain forks, in a layman language, is a situation or circumstances under which a single chain diverges into two or more. A detailed explanation about Blockchain fork and its types is available in the video embedded below.
  When a Blockchain fork occurs, the application begins operating in an unpredictable manner, creating two or more diverged nodes ahead.

- **Poor Performance**

  When a bad consensus blockchain mechanism is considered, either the node gets malfunctioned or suffers from network partition. This delays the process of exchanging messages between nodes and increases the latency of the application, which ultimately lowers down the performance level.

- **Consensus Failure**

  Another effect of incorporating a bad consensus mechanism to your business model is consensus failure. In this situation, a fraction of nodes fails to participate in any process and thus, in the absence of their votes, the consensus fails to deliver accurate and desired outcomes.
  With the basics of Blockchain consensus methods now covered, let's dive deeper into the topic and look at the popular types of consensus mechanism.

3. Proof of Work in Detail

Proof of Work consensus is the mechanism of choice for the majority of cryptocurrencies currently in circulation. The algorithm is used to verify the transaction and create a new block in the blockchain. The idea for Proof of Work (PoW) was first published in 1993 by Cynthia Dwork and Moni Naor and was later applied by Satoshi Nakamoto in the Bitcoin paper in 2008. The term "proof of work" was first used by **Markus Jakobsson** and **Ari Juels** in a publication in 1999.
Cryptocurrencies like Litecoin, and Bitcoin are currently using PoW.

Bitcoin uses the Hashcash Proof of Work system as the mining basis. The **'hard mathematical problem'** can be written in an abstract way like below:

Given data A, find a number x such as that the hash of x appended to A results is a number less than B.

- The miners bundle up a group of transactions into a block and try to mine. To mine it, a hard mathematical problem has to be solved.
- This problem is called the proof of work problem which has to be solved to show that the miner has done some work in finding out the solution to the problem and hence the mined block must be valid.
- The answer to the problem needs to be a lower number than the hash of the block for it to be accepted, known as the '**target hash**'.

*A **target hash** is a number that the header of a hashed block must be equal to or less than for a new block, along with the reward, to be awarded to a miner. The lower a target is, the more difficult it is to generate a block.*

- A miner continues testing different unique values (known as a nonce(s)) until a suitable one is produced.
- The miner who manages to solve the problem gets the bitcoin reward and adds the block to the blockchain by broadcasting that the block has been mined.

Note: The target hash adjusts once every 2016 block or approximately once every 2 weeks. All the miners immediately stop working on the said block and start mining the next block.

Common cryptographic protocols used in PoW: The most widely used proof-of-work consensus is based on SHA-256 and was introduced as a part of Bitcoin. Others include Scrypt, SHA-3, scrypt-jane, scrypt-n, etc.

Purpose of PoW

The **purpose** of a consensus mechanism is to bring all the nodes in agreement, that is, trust one another, in an environment where the nodes don't trust each other.

- All the transactions in the new block are then validated and the new block is then added to the blockchain.
- The block will get added to the chain which has the longest block height (see blockchain forks to understand how multiple chains can exist at a point in time).
- Miners (special computers on the network) perform computation work in solving a complex mathematical problem to add the block to the network, hence named, Proof-of-Work.
- With time, the mathematical problem becomes more complex.

Features of PoW

There are mainly two features that have contributed to the wide popularity of this consensus protocol and they are:

- It is hard to find a solution to a mathematical problem.
- It is easy to verify the correctness of that solution.

Security features of PoW

- **Immutability:**
  Once a block of transactions is added to the blockchain, altering the data within that block becomes increasingly difficult due to the computational work required to create a new block that follows it. The subsequent blocks, linked by cryptographic hashes, create a chain that validates the previous blocks' integrity.

  Each block's creation involves solving a cryptographic puzzle (mining) that demands significant computational resources. This makes it extremely arduous and resource-intensive to alter previously confirmed blocks, ensuring the stability and immutability of the blockchain.

- **Resistance to Sybil Attacks:**
  A Sybil attack involves creating multiple identities to gain control over a network. The white paper discusses how PoW mitigates the risk of such attacks.

  To participate in the consensus process and add blocks to the chain, miners must invest computational power and resources (in the form of hardware and electricity). This investment acts as a deterrent against Sybil attacks because creating numerous identities (nodes) requires a proportional amount of computational power for each.

Miners are economically incentivized to follow the rules and behave honestly within the network. Their investments in mining hardware and energy costs are only valuable if they abide by the network's rules, further discouraging malicious behaviour.

- **Cost of Attacks:**
  Bitcoin's security model is designed around making attacks economically infeasible.

  51% Attack Mitigation: The white paper acknowledges the theoretical possibility of a 51% attack, where a malicious actor controls the majority of the network's hashing power. However, it emphasizes the impracticality and costliness of executing such an attack in a large, distributed network like Bitcoin's.

  Acquiring enough computational power to control the majority of the network would demand an exorbitant investment in hardware and electricity. Additionally, successfully attacking the network would compromise the trust in the system, rendering the attacker's investments worthless due to the potential collapse of the cryptocurrency's value.

Energy and Time consumption in Mining:
The process of verifying the transactions in the block to be added, organizing these transactions in chronological order in the block, and announcing the newly mined block to the entire network does not take much energy and time.

- The energy-consuming part is solving the ‘hard mathematical problem’ to link the new block to the last block in the valid blockchain.
- When a miner finally finds the right solution, the node broadcasts it to the whole network at the same time, receiving a cryptocurrency prize (the reward) provided by the PoW protocol.

Mining reward:
- Currently, mining a block in the bitcoin network gives the winning miner 6.25 bitcoins.
- The number of bitcoins won halves every four years. So, the next deduction in the amount of bitcoin is due at around 2024(with the current rate and growth).
- With more miners comes the inevitability of the time it takes to mine the new block getting shorter.
- This means that the new blocks are found faster. In order to consistently find 1 block every 10 minutes. (That is the amount of time that the bitcoin developers think is necessary for a steady and diminishing flow of new coins until the maximum number of 21 million is reached (expected some time with the current rate in around 2140)), the Bitcoin network regularly changes the difficulty level of mining a new block.

Challenges With PoW
The Proof-of-Work consensus mechanism has some issues which are as follows:

- **The 51% risk**: If a controlling entity owns 51% or more than 51% of nodes in the network, the entity can corrupt the blockchain by gaining the majority of the network.
- **Time-consuming**: Miners have to check over many nonce values to find the right solution to the puzzle that must be solved to mine the block, which is a time-consuming process.

- **Resource consumption**: Miners consume high amounts of computing power in order to find the solution to the hard mathematical puzzle. It leads to a waste of precious resources(money, energy, space, hardware). It is expected that 0.3% of the world's electricity will be spent to verify transactions by the end of 2028.
- **Not instantaneous transaction:** Transaction confirmation takes about 10–60 minutes. So, it is not an instantaneous transaction; because it takes some time to mine the transaction and add it to the blockchain thus committing the transaction.