8. Distributed Consensus Mechanism

(D.Geethanjali1, N.Umasankari2

1,2 Assistant Professor, Sathyabama Institute of Science and Technology, Chennai)

1. Introduction

2. History of consensus mechanism

3. Why consensus mechanism?

4. Types of consensus mechanism

5. How consensus algorithms work?

6. Applications of consensus mechanism

7. Pros & Cons of Consensus Mechanism

8. Future of consensus mechanism

**Introduction**

A consensus algorithm is a process that allows every peer in the Blockchain network to agree on the distributed ledger's current state. Consensus algorithms accomplish reliability in the Blockchain network and build confidence between unidentified peers in a distributed computing setting in this way. In essence, the consensus mechanism ensures that every new block added to the Blockchain is the sole version of the truth that has been accepted by every node. The Blockchain consensus protocol includes some specific goals like reaching an understanding, collaboration, cooperation, giving every node equal rights, and requiring each node to take part in the consensus process.

In blockchain systems, a consensus mechanism is a program that facilitates widespread consensus over the ledger's current state. It is typically applied in a network with plenty of users and operations. It is any method used to achieve agreement, trust, and security across a decentralized computer network. It is an essential part of securing information by encrypting it and using automated group verification.



**History of consensus mechanism**

The history of consensus mechanisms is a long and complex one that spans several decades. In the 1970s, researchers began exploring the problem of reaching consensus in distributed systems, which are composed of multiple nodes that communicate and coordinate with each other to achieve a common goal.

These shared databases became known as distributed ledgers because they recorded information and were networked for many users in different locations to access. One of the most significant issues that needed addressing was that of preventing data tampering and unauthorized access, whether it was malicious or not. A method to automate distributed database management was required to ensure data was not changed.

This need led to the creation of distributed autonomous consensus, where programs on a network agreed on a database's state using cryptographic techniques. Agreement was designed to be reached using encryption algorithms to create long strings of alphanumeric numbers—called a hash—which were then verified by programs running on the network. A hash only changes if the information input into the hashing algorithm is changed, so the programs were designed to compare hashes to ensure they matched.

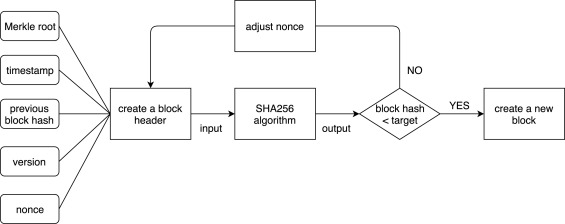
When each program running on the network created a matching alphanumeric string, the data was said to be agreed upon by consensus of the network. Thus, consensus mechanisms were made, with credit generally given to Satoshi Nakamoto, the anonymous Bitcoin creator. However, many people worked on consensus mechanisms for years before Nakamoto released the whitepaper that made Bitcoin famous.

**Why consensus mechanism?**

Every cryptocurrency blockchain operates using a consensus mechanism. It is a system that users of a blockchain network follow to agree on the legitimacy of transactions. This system ensures that all legitimate transactions are recorded on the blockchain and that each copy of the blockchain contains all valid transactions.

The computers that validate new transactions on most blockchains are called miners. In a proof-of-work protocol, these miners compete against each other to validate the next block of transactions. The winning miner earns a lucrative mining fee, paid for by those who send transactions on the network.

The consensus mechanism ensures all miners agree on the next block of transactions and distributes the information in each new block to all other miners. Anyone can download a copy of the blockchain to their device as a node. Every copy of the ledger matches exactly. The consensus mechanism ensures the continued agreement on which wallet owns which assets



**Types of consensus mechanism**

The basic goal of the consensus algorithm is to come to a consensus and assure the network's dependability, although it can be developed with a variety of functionalities. The various kinds of consensus algorithms are listed below:

>Proof-of-Stake

>Delegated Proof-of-Authority

>Proof-of-Work

>Proof-of-Authority

>Proof-of-Capacity

>Proof-of-Burn

>Proof-of-Importance

**1.Proof-of-Stake**

Proof of Stake is a cryptocurrency consensus mechanism used to validate transaction and to create new blocks in the blockchain. The Proof of Stake (PoS) is first introduced by Sunny King and Scott Nadal in 2012 in order to reduce the immense energy collection of Blockchain mining. They proposed an alternative way called "staking" where a random deterministic algorithm will choose nodes based on the number of coins staked by an individual node. To simplify, the stakers (nodes/users who stake coins) with more "staked" coins will get a higher chance of validating the blockchain and get transaction fees as reward.

“When blockchain participants verify that a transaction is legitimate and add it to the blockchain, we say that participants have achieved consensus,” says Marius Smith, head of business development at digital asset custodian Finoa.

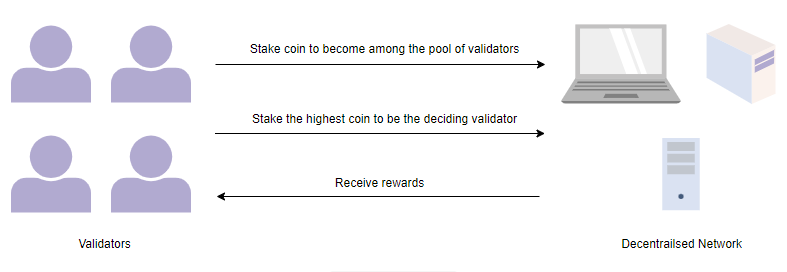


Fig: Proof-of-stake

**Working:**

In Proof of Stake the stakers are called as "Validators", who stake (or lock) a certain amount of cryptocurrency or tokens to validate new transactions and get some rewards but in the worst-case scenario if they carelessly validate the data or try to manipulate the transactions, they will end up losing some or all of their stake amount as a penalty. Hence, the validators are forced to be cautious and legitimate about the validating process.

A validator checks transactions, verifies activity, votes on outcome and maintain records

Staking is a scenario when the users lock up a certain amount of cryptocurrency in a collateral-staking method (minimum staking of Ethereum blockchain is 32 ether) into a withheld smart contract in the blockchain. The blockchain algorithm select validators slightly being bias to the number of tokens staked. The more token a user stakes, the more chance he gets to validate the block. When the block has been validated by the validator, the block will be added to the blockchain and the validator will get a newly minted crypto as his reward.

If the validator node commits some kind of bad data or proxy transactions then the user will be punished to redeem himself by "slashing" where their stake amount will be "burned", which means the stake will be transferred to an unusable wallet address where nobody can access it and will be remain useless forever. Blocks are validated by multiple validators and when a certain number of validators verify the integrity of the block then the block is finalized and added to the chain.

The Proof of Stake mechanism is aimed to drastically reduce the computational power required to validate information and transaction of block in a blockchain, which it achieved. It also managed to reduce the network congestion and removed the reward-based incentive system followed by traditional Proof of Work mechanisms effectively substituted staking for computational power where the blockchain system randomizes a starker’s validation ability which resulted in humongous drop in energy consumptions as the nodes do not have to be dependent on extravagant mining farms to gain hardware advantage. Ethereum's transition from Proof of Work to Proof of Stake mechanism resulted in reduction of Ethereum blockchain's energy consumption by 99.84%

The Proof of Stake consensus mechanism is immune to the 51% attack in which, an entity will have access to control 51% of the nodes in the system to manipulate transactions and validations, In PoS if a validator hypothetically gets the ability to control 51% of the staked crypto currency, then the honest validators in the network would vote to declare the block to be discarded and to burn the offenders’ stake amount. The other major security features of Proof of Stake mechanism are not publicly announced as preventive measure to bypass future potential threats.

**Currencies that use proof of stake:**

The PoS mechanism is currently becoming more predominant as a consensus mechanism and there are about 80+ cryptocurrencies that use Proof of Stake as their mode of validation through consensus mechanism.

Some noteworthy Proof of Stake coins are:

Ethereum (ETH)

Cardano (ADA)

Tron (TRX)

EOS (EOS)

Cosmos (ATOM)

Polkadot (DOT)

Solana (SOL)

Polygon (MATIC)

Cosmos (ATOM)

Avalanche (AVAX)

**Demerits of Proof Of stake:**

Accessibility Limitation: the biggest downside of PoS is the participation, in detail an individual must stake a certain minimum value of tokens in order to opt for the validator title which falls under capitalistic method where only the rich can stake the amount and receive incentives for validation. in short, the more crypto an individual can afford to buy the more he can stake and earn. Also the people with more stakes has the ability to influence the validation process even though they will get cross verified by honest validators the possibility is never zero and this also makes it hard for new validators to get a chance.

Another minor disadvantage is that the incentive reward for minting and forging is not as much as the reward obtained through mining a block.

**2.Delegated Proof Of Stake mechanism-**

Delegated Proof Of Stake (DPoS) is an enhanced form of Proof Of Stake as it is an advancement of the regular Proof Of Stake which makes it more efficient and more democratic than traditional Proof Of Stake. The DPoS algorithm is developed by Daniel Larimer in 2014. In the common Proof Of Stake algorithm the stakers or validators enrols themselves for a process called mintage by staking their tokens in which they add blocks to the blockchain and earn incentive for their honest work. DPoS algorithm works by a voting mechanism or an election system for choosing nodes which verify the blocks, such nodes are called as "witnesses" or "block producers"

In DPoS algorithm the nodes can vote directly or indirectly by transferring their voting power to another entity to vote on their behalf. The selected witnesses are responsible for creating blocks by verifying transactions. Whenever a block is created the witness will earn a reward which will be shared at proportions between the witness and the voters who opted the witness, If the witness fails to do so within the given timeframe, then the block will be discarded and no reward will be distributed among the witness and voters. The existing reward will be added to the reward of the next witness who verifies the block, such blocks are called "stolen"

Votes are not subjective to the witness's stake but respected to the voter’s stake. A user necessarily not needed to have a huge stake to enter the top tier member of this voting consensus but the votes from users with huge stake might play a significant role in taking a low stake witness to top tier.

The number of witnesses at the top tier is limited to a certain number of users like 30 - 101. These witnesses have the authority to prevent specific transactions from being added to the block but they lack the ability to alter the information of any transaction which makes their authority level resemble that of miners in Proof Of Work networks. This consensus mechanism forces the witnesses in top tier to maintain their reputation level high as they can be replaced anytime with witnesses with higher votes hence, making reputation a competition. Each witness must lock a certain amount of token as protection which will be revoked if they involve in fraudulent activities.

The voters will also vote a certain users called as "Delegates" who supervise the blockchain. They dont take part in transaction verification and they take part in determining the size of the block, amount of incentive a witness should be paid in return for validating. Once all these proposals are implemented the user<s vote on their own interest

Block validators are nodes that verify the integrity of blocks crafted by the witnesses, they primarily check if all the consensus rules are followed. Any user can run a block validator and verify the integrity of the block, these nodes get no incentive

**Advantages:**

They have good protection from double spending, the risk of using cryptocurrency twice or more.

It is more deocratic as the witnesses and delegates are voted and they don’t need high stake amounts also any node can verify the block using block validator.

Its not Power hungry like some of the consensus mechanisms which makes it more sustainable and more scalable

**Disadvantages:**

Ideal working of this mechanism will require highly knowledge delegators and needs witnesses to be truthful

with a limited number of witnesses and delegators this system will fall into centralization

This mechanism is biased on voter's stake this would mean with huge voting volumes vote of voter with less stake would mean nothing

Examples:

Zclassic ZCL

Eos EOS

Bitshares BTS

Steemdollars SBD

Steem STEEM

**3.Proof-of-Work (PoW)**

Nakamoto consensus, which utilizes proof-of-work, is the mechanism that once allowed the decentralized Ethereum network to come to consensus (i.e., all nodes agree) on things like account balances and the order of transactions. This prevented users from "double spending" their coins and ensured that the Ethereum chain was tremendously difficult to attack or manipulate. These security properties now come from proof-of-stake instead using the consensus mechanism known as Gasper.

Proof-of-work is the underlying algorithm that sets the difficulty and rules for the work miners do on proof-of-work blockchains. Mining is the "work" itself. It's the act of adding valid blocks to the chain. This is important because the chain's length helps the network follow the correct fork of the blockchain. The more "work" done, the longer the chain, and the higher the block number, the more certain the network can be of the current state of things.

**The work in proof-of-work**

The proof-of-work protocol, Ethash, required miners to go through an intense race of trial and error to find the nonce for a block. Only blocks with a valid nonce could be added to the chain.

When racing to create a block, a miner repeatedly put a dataset, that could only be obtained by downloading and running the full chain (as a miner does), through a mathematical function. The dataset was used to generate a mixHash below a target that is dictated by the block difficulty. The best way to do this is through trial and error.

The difficulty determined the target for the hash. The lower the target, the smaller the set of valid hashes. Once generated, this was incredibly easy for other miners and clients to verify. Even if one transaction were to change, the hash would be completely different, signalling fraud.

Hashing makes fraud easy to spot. But proof-of-work as a process was also a big deterrent to attacking the chain.

**Proof-of-work and security**

Miners were incentivized to do this work on the main Ethereum chain. There was little incentive for a subset of miners to start their own chain—it undermines the system. Blockchains rely on having a single state as a source of truth.

The objective of proof-of-work was to extend the chain. The longest chain was most believable as the valid one because it had the most computational work done to generate it. Within Ethereum's PoW system, it was nearly impossible to create new blocks that erase transactions, create fake ones, or maintain a second chain. That's because a malicious miner would have needed to always solve the block nonce faster than everyone else.

To consistently create malicious yet valid blocks, a malicious miner would have needed over 51% of the network mining power to beat everyone else. That amount of "work" requires a lot of expensive computing power and the energy spent might even have outweighed the gains made in an attack.

**Proof-of-Work Energy-Usage**

A major criticism of proof-of-work is the amount of energy output required to keep the network safe. To maintain security and decentralization, Ethereum on proof-of-work consumed large amounts of energy. Shortly before switching to proof-of-stake, Ethereum miners were collectively consuming about 70 TWh/yr. (about the same as the Czech Republic - according to dichotomist on 18-July-2022).

**Compared to Proof-Of-Stake**

At a high level, proof-of-stake has the same end goal as proof-of-work: to help the decentralized network reach consensus securely. But it has some differences in process and personnel:

Proof-of-stake switches out the importance of computational power for staked ETH.

Proof-of-stake replaces miners with validators. Validators stake their ETH to activate the ability to create new blocks.

Validators don't compete to create blocks, instead they are chosen at random by an algorithm.

Finality is clearer: at certain checkpoints, if 2/3 validators agree on the state of the block it is considered final. Validators must bet their entire stake on this, so if they try to collude down the line, they'll lose their entire stake.

**4.Proof Of Authority:**

A blockchain network can be divided into two based on the participation of nodes namely permissionless and permissioned. Permissionless networks are public and anyone can become a node while a permissioned network is a private network only selective users are chosen as nodes. This makes it highly suitable for private blockchain networks. PoA was coined by Gavin Wood in 2017.

**Working:**

In PoA blocks can only be created by nodes with authority, these nodes are called "Validators" and they insert the transaction into the blocks, this process is done with the help of a software and can be automated. PoA can be implemented in both public and private networks.

As only nodes with authority are given the ability to add blocks, validators don’t stake coins but their own reputation instead. Each of these validators must verify their real identity and must be daring enough to stake money, reputation and commit themselves for a long period of time.

In short PoA is not a decentralised mechanism but an idea to make centralised systems to be better.

**Advantages:**

There are more transactions per second that can be executed.

Less computational resources are needed.

**Disadvantages:**

It is more of a centralised mechanism and hence fails to satisfy one of the main goal of blockchain

Identity of the validators are publicly available to everyone on that network

**5.Proof Of Capacity**

It is one of the very recent mining methods that is adapted only by Burstcoin blockchain network. It enables mining through the use of space present in the physical hard disk of a node. This method comes with various benefit and it can be adapted for a lot of upcoming projects.

**Purpose:**

Proof of capacity is different from traditional PoW as PoW uses computational resources to solve complex mathematical hash functions (mostly SHA-256). These hashing functions are functions with a single solution and requires raw computational power to locate the exact solution for the hashing function. Nonce - Number Only Used Once, is the input taken by the hashing algorithm the miners will enter these nonce until they find the correct hash. This brute-force method is very demanding of power and time. With the growth of bitcoin's popularity, the bitcoin network is made to make the mining difficult higher in order to make block timings consistent, This resulted in need of more computational power and relatively demanded more resources. This made small miners have lower influence in major choices made. So this situation gave pressure for the rise of new consensus mechanism and this is where Proof-Of-Capacity came.

**Features:**

PoC is an enhancement for the well known PoW. Processing power and hard disk storage is allocated before the mining process hence making it faster than PoW, on comparison PoC only takes 4 minutes to create a block while PoW takes about 10 minutes. There is a higher chance of winning the mining conflict if there are more solutions or plots available on the computer.

**Working:**

Plotting: It might take weeks to plot files with respect to the hard disk size. Plotting is done with shabal hash, a crypto currency on burstcoin network. Shabal is a sluggish cryptocurrency hence making it suitable for Burstcoin, this is due to the fact that the precomputed hashes are stored while still being able to do smaller live verifications. Burst makes use of Shabal256, a 256-bit variant of Shabal. The Shabal hashes are precomputed and saved on a hard drive because they are difficult to calculate. The hard disk is plotted first. By hashing data, including a miner's account, repeatedly, a list of all potential nonce values is generated. Each nonce is composed of 8192 hashes ranging from 0 to 8191. All of the hashes are linked together to form "scoops," which are groupings of two nearby hashes.

**Mining:**

The second part is actual mining, which involves a miner determining a scoop number. For instance, if a miner begins mining and creates scoop number 40, the miner will then go to nonce 1's scoop number 40 and use the data from that scoop to compute a deadline value. The operation is repeated for each nonce saved on the miner's hard drive to compute the deadline. After calculating all of the deadlines, the miner selects the one with the shortest deadline. A deadline defines the length of time in seconds that has transpired since the last block was created before a miner is permitted to generate a new block. If no one else is mining, the miner can create a block and claim the block reward. If no one else has created a block and claimed the block reward during this time window, the miner may do so. For example, if miner A sets a minimum deadline of 40 seconds and no other miners are able to forge the block within that time, A is guaranteed the opportunity to forge the next block and be compensated.

**Applications:**

Burstcoin is a cryptocurrency that uses the Proof-of-Capacity algorithm. The Burstcoin team intends to investigate a wide range of use cases, including payment solutions, smart contracts, crowdsourcing, and random messages. Burstcoin is a good endeavour for putting PoC to the test since it presents a compelling idea to consumers, businesses, developers, and miners. Despite the fact that there aren't many cryptocurrencies that employ Proof-of-Capacity at the moment, a few initiatives are gaining popularity.

According to BXTB (which is a dual blockchain, dual token platform maintained by the BXTB business), Proof-of-Capacity has appeal in allowing users to mine the BXTB governance token.

**Advantages:**

Because any regular hard drive may be used, there is a competitive advantage over other miners who have invested in specialized equipment, such as ASIC mining for Bitcoin.

Hard disk mining saves 30 times more energy than ASIC mining.

Because everyone has a hard disk, capacity proof is more decentralized. We could even mine from the Android phone's hard drive.

Miners are not compelled to regularly improve their equipment. Older hard drives may store data equally as well as newer ones.

After mining is finished, the hard disk may be wiped and returned to its intended use.

**Disadvantages:**

A limited number of developers have embraced technology.

The data plotted on the hard disk is meaningless outside of coin mining. This implies that there is a lot of unutilized space.

Although Proof-of-Capacity mining has decreased entry barriers, users may opt for larger hard drives. Nothing precludes someone from purchasing significantly larger hard disks and using them to mine the majority of the money.

**6.Proof of Burn (PoB):**

Instead of investing in expensive hardware equipment, validators use PoB to perform the following procedure:

They destroy coins by sending them to an address where they cannot be recovered.

Validators acquire the right to mine on the system based on a random selection procedure by committing the coins to an unreachable address.

As a result, burning coins implies that validators have made a long-term commitment in exchange for a short-term loss.

Miners may burn the native money of the Blockchain application or the currency of an alternate chain, such as bitcoin, depending on how the PoB is implemented.

The more bitcoin validators burn, the more likely it is that they will be chosen to mine the next block.

While PoB is an interesting alternative to PoW, it still wastes resources inefficiently. It is also questioned whether mining power is merely distributed to those willing to burn more money.

**Why is Burn Proof Required?**

The PoW consensus process has some flaws, which prompted academics to develop a new consensus algorithm, PoB.

The first disadvantage is that PoW consumes a lot of electricity. Under a POW mechanism, miners are rewarded by upgrading the ledger. In return for payment, computational power is used to answer a math problem. The more money a miner spends to address the problem, the more likely it is that they will be permitted to mine blocks.

PoW necessitates large financial investments.

**How Does PoB Work?**

As the term implies, there is something that should be burnt. Because we are discussing virtual currency, it is evident that virtual currency gets burnt in PoB. The more money miners burn, the more power they have to build blocks.

We don't precisely mean burning when we say that. It signifies that you should not use the currency. This is possible if it is sent to a location where it cannot be spent. As a result, miners transmit these coins to locations where they cannot be utilised. It is delivered to a publicly verified address that cannot be accessed and so cannot be utilized.

When a coin is burned, its availability reduces, potentially increasing the coin's value.

The question now is why we need to burn the currency. The primary rationale behind this is that by destroying the money, the consumer demonstrates a strong commitment to the currency by forsaking a small profit in exchange for a larger benefit in the long run.

To prevent giving early adopters an unfair edge, the PoB has designed a technique that allows for the periodic burning of crypto currency in order to preserve mining capacity. When a new block is mined, the energy of burnt coins is somewhat reduced. It is a deflationary concept in which the number of currencies decreases with time, increasing deficiency and, hence, the value of currency holders. Coins that increase in quantity over time, on the other hand, lose value.

**Advantages of PoB over PoS:**

Market scarcity is not permanent in Pos blockchain. The scarcity is just temporary, lasting until the forger bets their coin, which is commonly done by locking them away. However, the coins return to circulation if the departing forger purchases them and sells them in the market. In the event of PoB, the coins are destroyed, making scarcity permanent.

**Benefits of PoB:**

In comparison to PoW, it took extremely little electricity.

When coins are burnt, it minimizes energy usage by discarding negligible resources.

It fosters long-term engagement in a project since a customer is demonstrating a strong commitment to the currency by forsaking a small profit in exchange for a larger benefit in the long run.

In comparison to all previous consensuses, the coin distribution is more equitable.

**PoB disadvantages:**

It is dangerous since one does not sure whether they will recover the wealth they have lost in the future.

Because coins are burned, we might conclude that resources are squandered.

It may be affected by the rich growing richer phenomenon. In which the affluent become wealthier by amassing more coins.

**7.Proof-of-Importance (PoI) :**

It is a blockchain consensus technique developed by NEM that is based on the Proof of Stake (PoS) algorithm.

The PoI assigns a score to each node in the network based on network theory.

In PoI, nodes must vest a quantity of coins before they are permitted to mine blocks in accordance to the score reflecting their contribution to the network.

However, unlike Proof of Stake (PoS), the score is determined by several additional factors such as total amount, activity clusters, reputation, and transactions conducted through any specific address.

**What is Proof of Importance (PoI)?**

Proof of Importance is the technique that determines which nodes in the network are eligible to add a block to the blockchain through a process known as 'harvesting' or ‘vesting' by NEM, which stands for New Economy Movement and is a blockchain.

Nodes can collect transaction fees within a block in exchange for harvesting it, which the validator receives as a reward. To be eligible for the calculation or 'harvest,' an account holder must have at least 10,000 vested XEM (XEM is the cryptocurrency that powers the NEM blockchain, which is rapidly gaining popularity recently), and accounts with a high score have a better chance of being chosen to harvest a block.

NEM determines an account's total network support or score by taking into consideration the three following crucial characteristics: -

**Vesting**: Also known as 'Harvesting,' this consensus method is the most important aspect. Before any node can begin harvesting or vesting, it must first contain at least 10,000 XEM coins. The consensus method calculates the node's Proof of Importance score by counting the quantity of coins in your account for a predetermined period of days (usually 30). As a result, the bigger the amount of XEM coins, the better the node's score.

Transaction partnership: Proof of significance rewards users who conduct transactions with other NEM accounts on the network, and both accounts are recognized as partners.

The network theory calculation examines transaction behaviour to assign a significance score to each node and prevent the user from forming any pseudo partnerships.

Number and size of transactions: Each transaction that exceeds a certain minimum size affects the Importance score and improves the likelihood of harvesting a block to receive rewards. Larger and more frequent transactions will boost the PoI score on the NEM network, which is dependent on the number of transactions a node does in a 30-day period.

**The difference between Proof of Importance (PoI) and Proof of Stake (PoS)**

Many blockchains employ Proof of Stake (POS) to distribute rewards, although this process favors currency hoarders since with PoS, the affluent node receives more coins than other nodes with fewer coins. In Proof-of-Stake, the score is one's entire vested amount, but Proof of Importance (PoI) considers additional criteria; as a consequence, the PoI process provides more fairness. For example, a proof of stake miner who owns 20% of all cryptocurrencies has the right to mine 20% of all blocks on the blockchain network, resulting in a scenario in which the 'rich grow wealthier'.

**Is the PoI Mechanism in Blockchain Susceptible to Sybil Attacks?**

The nickname "Sybil" is derived from a case study of an artist called Shirley Ardell Mason, alias Sybil Dorsett, who was diagnosed with Multiple Personality Disorder. A Sybil attack is an effort to gain control of a peer network by using several aliases. These phony identities look to outside observers to be distinct users. However, there is a single entity that owns several identities at the same time, giving that entity greater voting power with which to influence the blockchain network.

Sybil attacks are difficult to resist and cause havoc on the blockchain network, but the Proof of Importance mechanism's basic idea is to award a score based on the coins held by the node, which affects the node's impact in the network.

Now that there is a penalty to creating an identity, the malevolent entity will be unable to construct nodes with enough money to acquire control of the network since it is prohibitively expensive. As a result, the PoI technique provides some protection against Sybil's Attack.

**Advantages of Proof of Importance (PoI)**

**Energy Efficient**: Those that employ Proof of Work (PoW) in a blockchain network have an unfair edge over other nodes in terms of high computer power for mining blocks. These POW methods also affect the environment by consuming large quantities of electricity and burdening miners with hefty electricity bills, whereas the Proof of Importance (PoI) is extremely energy efficient.

**Avoids currency hoarding and promotes transactions**: The Proof of Stake (PoS) mechanism concentrates wealth around a few nodes since users may simply hoard as many coins as they like and reap the benefits of block generation. They earn more money if they maintain more coins in their accounts. As a result, everyone has an incentive to store coins rather than use them, reducing transactions and enriching the affluent. The significance score will be higher as nodes share XEM money and lower when nodes hoard the coins, hence the proof of significance (PoI) mechanism is ideal.

**Lower Incentive**: Because miners in the Proof of Importance mechanism are not required to mine blocks using high computation power and heavy power consumption as in the Proof of Work mechanism, the incentive given as rewards for adding blocks to the blockchain network does not need to be as high as in the Proof of Work mechanism. This significantly reduces the transaction costs charged by miners for validation.

**Discourages Forks**: In classic PoS systems, the marginal cost of producing a block is zero, and users may continue validating blocks without difficulty even if a fork occurs. However, with Proof of relevance, each node's relevance ranking is dynamic and depending on network activity. As a result, blockchain splits are discouraged since the new user must waste energy on both branched networks in order to preserve their score.

Despite the fact that all consensus algorithms seek to create consensus within a decentralized network, different methods differ in how they do so. Although ideal consensus may not exist, it is crucial to highlight that consensus mechanisms have evolved and altered over time to satisfy a system's ever-changing demands. As a result, it is critical to select the most appropriate method depending on network needs. Proof of Importance (PoI) is one such approach that seeks to provide fair consensus while still favouring the network's rich node. However, one notable characteristic of PoI is that it enables an individual to select how much money is necessary to begin collecting rewards.

**How Consensus Mechanisms Work: -**

Every cryptocurrency blockchain operates using a consensus mechanism. It is a system that users of a blockchain network follow to agree on the legitimacy of transactions. This system ensures that all legitimate transactions are recorded on the blockchain and that each copy of the blockchain contains all valid transactions.

**Note**

The consensus mechanism is extremely important to the blockchain network. It influences how transactions are verified, how much energy is used, network fees, transaction speed, and other details for the currency and network applications.

The computers that validate new transactions on most blockchains are called miners. In a proof-of-work protocol, these miners compete against each other to validate the next block of transactions. The winning miner earns a lucrative mining fee, paid for by those who send transactions on the network.

The consensus mechanism ensures all miners agree on the next block of transactions and distributes the information in each new block to all other miners. Anyone can download a copy of the blockchain to their device as a node. Every copy of the ledger matches exactly. The consensus mechanism ensures the continued agreement on which wallet owns which assets.1

**Examples of Consensus Mechanism**

For example, if you buy one bitcoin and transfer it to your cryptocurrency wallet, everyone else must agree that you own the bitcoin. If they did not, your currency would be worthless. The first consensus mechanism was bitcoin’s “proof-of-work” (PoW) method. It required approval by the network (in the form of a unique hash) for each new block added to the chain with each transaction. This validated new transactions and ensured agreement on past transactions.

**Applications of Consensus Algorithm: -**

We use Consensus Algorithms for decentralized systems but we can use them for centralized networks as well. There are multiple applications of this mechanism like:

Whether a transaction needs to be implemented or not in a decentralized network. In most blockchain this basic application of Consensus Algorithm is applied.

It is useful in giving nodes a leader status.

It is used to synchronize data across all the decentralized networks to ensure consistency.

Over the time there have been many applications of Consensus Algorithms like in the fields of - state machine replication, load balancing, UAV control, clock synchronization etc. But one of the most popular applications of this algorithm has been in the field of “Blockchain”.

In Blockchain also there are multiple applications, thus consensus algorithms are designed based on the needs and demands of it

**Benefits of Using Blockchain in Payment: -**

Blockchain technology has brought a massive impact on payment solutions. It offers immense benefits detailed as below-

Firstly, blockchain technology offers a highly secure platform for transaction processes. Using blockchain for payment processing results in new opportunities for both the consumer and the company.

The cryptographic hash function ensures that no one can hack into the system and alter its data. In this way, blockchain safeguards the network from both outside and inside attacks.

**Pros Explained**

Forms agreement foundational to the crypto-market: -Consensus mechanisms synchronize data between all participating users and enable trust in a blockchain.

Creates a secure environment: -Cryptocurrencies and distributed applications rely on consensus mechanisms for security.

Anyone can participate: - With the most popular consensus mechanisms, barriers to participating as a miner or operating their own nodes are not very high.

**Cons Explained**

May be energy-intensive: - Proof-of-work is extremely energy-intensive and requires as much electricity as many countries.

Potential for attacks: -There is a small chance for a type of hack called a 51% attack, among other minor weaknesses.

**Future of Consensus Mechanisms: -**

While used by all cryptocurrencies, consensus mechanisms are just as important in distributed ledger networks used by enterprises. Platforms have been created for business and government use, allowing each entity to choose from modules created for their needs, backed by consensus mechanisms. Hyperledger Fabric, one of the more well-known distributed ledger platforms, provides different consensus mechanisms. For example, one entity might not need proof-of-work, considered byzantine fault tolerant, whereas another might not need that level of consensus.

Cryptocurrency's future may be unknown and volatile, but consensus mechanisms remain an essential part of emerging technology. They ensure data safety and integrity and keep those with nefarious intentions locked out of distributed ledgers.

As the blockchain payment platform follows a distributed natured network leaving no central governing authority. This ensures minimum control of central authorities over the systems. As a result, consumers can finally trust the system to offer the full security they deserve.