UNIT – 6 : CONSENSUS ALGORITHMS & BLOCKCHAIN USE CASE

Consensus Algorithms:

A consensus algorithm is a procedure through which all the peers of the Blockchain network reach a **common agreement** about the present state of the distributed ledger. In this way, consensus algorithms achieve reliability in the Blockchain network and establish trust between unknown peers in a distributed computing environment.

Essentially, the consensus protocol makes sure that every new block that is added to the Blockchain is the one and only version of the truth that is agreed upon by all the nodes in the Blockchain. The Blockchain consensus protocol consists of some specific objectives such as coming to an agreement, collaboration, cooperation, equal rights to every node, and mandatory participation of each node in the consensus process.

Thus, a consensus algorithm aims at finding a common agreement that is a win for the entire network.

Types of Consensus Algorithms:

Proof of Stake (PoS):

Proof of Stake (PoS) is a type of algorithm which aims to achieve distributed consensus in a Blockchain. This way to achieve consensus was first suggested by Quantum Mechanic and later Sunny King and his peer wrote a paper on it. This led to Proof-of-Stake (PoS) based Peercoin.

A **stake** is value/money we bet on a certain outcome. The process is called **staking**.

Why Proof-of-Stake:

Before proof of stake, the most popular way to achieve distributed consensus was through Proof-of-Work (implemented in Bitcoin). But Proof-of-Work is quite energy (electrical energy in mining a bitcoin) intensive. So, a proof-of-work based consensus mechanism increases an entity's chances of mining a new block if it has more computation resources. Apart from the upper two points, there are other weaknesses of a PoW based consensus mechanism which we will discuss later on. In such a scenario, a Proof-of-Stake based mechanism holds merit.

What is Proof-of-Stake:

As understandable from the name, nodes on a network stake an amount of cryptocurrency to become candidates to validate the new block and earn the fee from it. Then, an algorithm chooses from the pool of candidates the node which will validate the new block. This selection algorithm combines the quantity of stake (amount of cryptocurrency) with other factors (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

- **Coin-age based selection:** The algorithm tracks the time every validator candidate node stays a validator. The older the node becomes, the higher the chances of it becoming the new validator.
- **Random Block selection:** The validator is chosen with a combination of 'lowest hash value' and 'highest stake'. The node having the best weighted-combination of these becomes the new validator.

A typical PoS based mechanism workflow:

1. Nodes make transactions. The PoS algorithm puts all these transactions in a pool.
2. All the nodes contending to become validator for the next block raise a stake. This stake is combined with other factors like 'coin-age' or 'randomized block selection' to select the validator.
3. The validator verifies all the transactions and publishes the block. His stake still remains locked and the forging reward is also not granted yet. This is so that the nodes on the network can 'OK' the new block.
4. If the block is 'OK'-ed, the validator gets the stake back and the reward too. If the algorithm is using a coin-age based mechanism to select validators, the validator for the current block's has its coin-age reset to 0. This puts him in a low-priority for the next validator election.
5. If the block is not verified by other nodes on the network, the validator loses its stake and is marked as 'bad' by the algorithm. The process again starts from step 1 to forge the new block.

Features:

- **Fixed coins in existence:** There is only a finite number of coins that always circulate in the network. There is no existence of bringing new coins into existence (as in by mining in case of bitcoin and other PoW based systems). Note that the network starts with a finite number of coins or 'initially starts with PoW, then shifts to PoS' in some cases. This initiation with PoW is meant to bring coins/cryptocurrency in the network.

- **Transaction fee as reward to minters/forgers:** Every transaction is charged some amount of fee. This is accumulated and given to the entity who forges the new block. Note that if the forged block is found fraudulent, the transaction fee is not rewarded. Moreover, the stake of the validator is also lost(which is also known as **slashing**).
- **Impracticality of the 51% attack:** To conduct a 51% attack, the attacker will have to own 51% of the total cryptocurrency in the network which is quite expensive. This deems doing the attack too tedious, expensive and not so profitable. There will occur problems when amassing such a share of total cryptocurrency as there might not be so much currency to buy, also that buying more and more coins/value will become more expensive. Also validating wrong transactions will cause the validator to lose its stake, thereby being reward-negative.

Advantages of PoS:

- **Energy-efficient:** As all the nodes are not competing against each other to attach a new block to the blockchain, energy is saved. Also, no problem has to be solved (as in case of Proof-of-Work system) thus saving the energy.
- **Decentralization:** In blockchains like Bitcoin (Proof of Work system to achieve distributed consensus), an extra incentive of exponential rewards are in place to join a mining pool leading to a more centralized nature of blockchain. In the case of a Proof-of-Stake based system (like Peercoin), rewards are proportional(linear) to the amount of stake. So, it provides absolutely no extra edge to join a mining pool; thus promoting decentralization.
- **Security:** A person attempting to attack a network will have to own 51% of the stakes(pretty expensive). This leads to a secure network.

Weakness of a PoS mechanism:

- **Large stake validators:** If a group of validator candidates combine and own a significant share of total cryptocurrency, they will have more chances of becoming validators. Increased chances lead to increased selections, which lead to more and more forging reward earning, which lead to owning a huge currency share. This can cause the network to become centralized over time.
- **New technology:** PoS is still relatively new. Research is ongoing to find flaws, fix them and making it viable for a live network with actual currency transactions.
- **The 'Nothing at Stake' problem:** This problem describes the little to no disadvantage to the nodes in case they support multiple blockchains in the event of a blockchain split(blockchain forking). In the worst-case scenario, every fork will lead to multiple blockchains and validators will work and the nodes in the network will never achieve consensus.

Blockchains using Proof-of-Stake:

- Ethereum (Casper update)
- Peercoin
- Nxt

Proof of Work (PoW):

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. Ethereum was using PoW mechanism, but now shifted to Proof of Stake (PoS).

Principle: A solution that is difficult to find but is easy to verify.

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.

How Does PoW Work?

The PoW consensus algorithm involves verifying a transaction through the mining process. This section focuses on discussing the mining process and resource consumption during the mining process.

Mining:

The Proof of Work consensus algorithm involves solving a computationally challenging puzzle in order to create new blocks in the Bitcoin blockchain. The process is known as 'mining', and the nodes in the network that engages in mining are known as 'miners'.

- The incentive for mining transactions lies in economic payoffs, where competing miners are rewarded with 6.25 bitcoins and a small transaction fee.
- This reward will get reduced by half its current value with time.

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 amount 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.

Delegated Proof of Stake (DPoS):

Delegated Proof of Stake (DPoS) is a consensus algorithm which is an advancement of the fundamental concepts of Proof of Stake. Delegated Proof of Stake (DPoS) consensus algorithm was developed by Daniel Larimer, founder of BitShares, Steemit and EOS in 2014.

In Proof of Stake consensus system, each person who stakes a token can participate to the **"mintage"** process which means that they get a chance to select layer two nodes which further validates block and be rewarded for adding blocks to blockchain. DPos system is maintained by an election system for choosing nodes which verify blocks. These nodes are called **"witnesses"** or **"block producers"**.

Here is how DPoS consensus works:

Voting:

In DPoS consensus users can either directly vote or give their voting power to another entity to vote on their behalf. Selected witness are responsible for creating blocks by verifying transactions. If they verify and sign all transactions in a block, they receive a reward, which is usually shared with those who have voted for witness. If a witness fails to verify all transactions in the given time, block is missed, all transactions are left unverified and no reward is distributed to that witness. The reward is added up to reward of the next witness which verifies that block. Such transactions are collected by the next witness, and such a block is called **stolen**.

Votes are proProof Elapsed Timeportionate to size of each voter's stake. A user need not have a large stake to enter the top tier of witnesses. Rather, votes from users with large stakes can result in users with relatively small stakes being elevated to the top tier of witnesses.

Witnesses:

Number of witnesses in the top tier is capped at a certain number which is usually in the range of 21-101. These witnesses are responsible for validating transactions and creating blocks, and are in return awarded associated fees. Witnesses can prevent specific transactions from being included in block but they cannot change information of any transaction which makes them similar to miners in Proof of Work blockchains. Voting is a continuous process and each witness in the top tier is always at risk of being replaced by a user who gets more votes and is therefore considered more trusted. As number of applicants for witness grows, competition grows and reputation becomes critical for each witness to remain competitive.

A witness is kept in check by threat to its loss of income, locking of stake and reputation score. Witnesses have to lock certain part of their stake which is seized if they act maliciously or try to attack blockchain.

A round in a DPoS blockchain with N block producers/witnesses follows a round robin order as follows:

- N block producers get elected from the pool of witnesses candidates.
- The kth block producer signs the kth block, until k=N.
- A block is finalized when it is voted on by (2/3+1) of block producers. In case of two chains, the longest chain rule is followed. Block added cannot be reversed.

Delegates:

Users in DPoS systems also vote for a group of delegates who oversee blockchain governance. They do not play a part in transaction control. Delegates can propose changing size of a block, or the amount a witness should be paid in return for validating a block. Once delegates propose such changes, blockchain's users vote on whether to adopt them.

Block validators:

Block validators in DPoS refer to full nodes who verify that blocks created by witnesses follow the consensus rules. Any user is able run a block validator and verify network. There is no incentive to be a block validator.

Advantages:

1. DPoS blockchains have good protection from double-spending.
2. DPoS is more democratic and financially inclusive due to lesser staking amount required by a user/node.
3. DPoS provides more decentralization as more people take part in the consensus due to low entry threshold.
4. DPoS doesn't require lots of power to run network, which makes it more sustainable.
5. Transactions in DPoS is not dependent on computing power required to run network, hence it is more scalable.
6. DPoS separates election of block producers from block production itself which opens door for more creative models to solve both problems in isolation.
7. DPoS method provides foundation for implementing interesting governance models in blockchain applications. In a sense, it forms a kind of democracy.

Disadvantages:

1. Effective operation and decision making of network requires delegators to be well informed and appoint honest witnesses.
2. Limited number of witnesses can lead to centralization of network.
3. DPoS blockchain is susceptible to problems of weighted voting. Users with smaller stake can refuse from taking part in votings after considering that their vote is insignificant.

Here is example of some DPoS blockchains:

Blockchain	**Number of Witnesses**
EOS	21
BitShares	101
Steemit	21
Lisk	101
Ark	51

Proof of Elapsed Time (PoET):

Proof of Elapsed Time (PoET) is a network consensus algorithm that prevents high resource utilization and energy consumption. It implements a fair lottery system to keep the process more efficient.

After numerous other consensus mechanisms have been experimented with and introduced, the Proof of Elapsed Time (PoET) concept is one such mechanism which was invented in early 2016 by Intel Corporation as part of the Hyperledger Sawtooth blockchain platform and it is one of the fairest blockchain consensus algorithms that enables permissioned blockchain networks to determine who creates the next block.

This mechanism is based on Byzantine Fault Tolerance and aims to reduce the energy consumption associated with proof of work's mining process.

- This algorithm assigns an amount of time to each node in the network randomly.
- The node must sleep or do another task for that random wait time.
- The node that gets the shortest waiting time wakes up and adds its block to the network.
- The newly updated information floods among the network participants.

3 Factors Need to Be in Favor for PoEt to Work:

1. Ensure that the node gets the random waiting time instead.
2. Check if the nodes are not choosing the shortest wait time on purpose.
3. Verify if a node has completed the given waiting time or not.

How Does PoET Work?

The PoET mechanism replaces the need for mining intensive rights required in Proof of Work with a randomized timer system. The PoET consensus mechanism distributes the chances of winning across the largest possible number of network participants and every node is likely to be selected by a fair lottery system.

- Every node in the blockchain network will generate a random wait time and then sleeps for that specified duration.
- Now the first one to wake up, that is, the first node in the network to have its timer expire after completing its specified waiting time wins the block round and it now becomes the block leader which produces the new block and signs the new block with its private key address before adding it to the blockchain network.

- After this necessary information is broadcasted to the whole peer network and the same process then repeats for the discovery of the next block.

In this consensus mechanism the problem is "how to determine the leader of a round of consensus" and whoever solves the computationally intensive cryptographic puzzle of each block round is selected as the leader for the round. For the node to participate in consensus, it downloads the trusted code which requires code attestation by Intel Software Guard Extension (SGX). SGX functions as a Trusted Execution Environment (TEE), which allows selecting, trusted code to run independently of the application that it runs in.

The PoET consensus mechanism is divided into 2 phases:

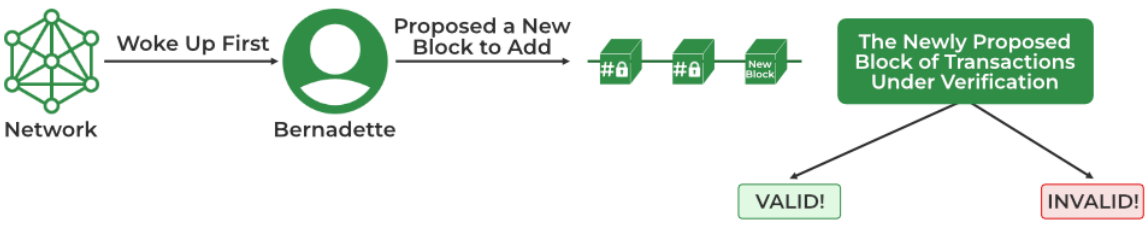
1. Selection Process: This process involves the following activities:

- Every node in the network will share its certificate by Intel Software Guard Extension (SGX) which ensures the validity of the node to generate a new block in the network. After this, the node is eligible to get a timer object.
- The numbers are assigned to each node as a timer object by Intel's RAND i.e. random number generator. RAND generates difficult-to-detect random numbers.
- The time object given to each participating node activates.

2. Generation Process: This process involves the following activities:

- After the timer object expires, and the node wakes up then the node is eligible to forge a new block to the network.
- The active node generates the hash of its block of transactions and submits it for acceptance.
- The update gets flooded to the network.

Therefore, this ends the iteration of mining a new block in a permissioned blockchain network using the PoET consensus algorithm.



Benefits of PoET:

- **Less power consumption:** PoET doesn't require much electricity consumption, and the nodes can "go to sleep" and switch to other tasks for the specified time thereby making the network time and energy efficient.
- **Less resource intensive:** PoET also provides a great solution to the "Random Leader Selection Problem" without being resource-intensive or requiring complex mechanisms. It is easily scalable as it allows the network to reach consensus more quickly thus allowing faster processing of transactions.
- **High transaction rate:** PoET can go up to a million transactions per second.
- **Equal opportunity:** PoET allows for the same opportunity for the network participants with time object and activation.
- **Permissioned:** Since it is a permissioned blockchain network, the process of selecting validators ensures network security against cyberattacks.

Limitations of PoET:

- **Specialized hardware required:** Even though it's cheap there is a requirement for specialized hardware for incorporating the Proof of Elapsed Time consensus algorithm as a result, it cannot be used by most people.
- **Compatibility issues:** PoET highly depends on tools by Intel technology which might raise compatibility issues with the other tools.

Deposite-Based Consensus:

Proof of Deposit (POD):

Proof-of-Deposit (PoD) is a consensus mechanism that falls under the category of Deposit-Based Consensus. A proof of deposit shows that you have the funds you plan to use for a large purchase, such as down payment for a house, and that those funds are from a legitimate source.

Key Takeaways:

- A proof of deposit proves you have the funds you plan to use to cover a large expense, like make mortgage payments, fund a down payment, or pay closing costs.
- Personal savings, property sales, inheritances, and gifts are among common sources of funding that may require proof of deposit.
- You use a proof of funds to show you have enough cash to make a purchase, and you use a proof of deposit to verify where you got the money from.

How a Proof of Deposit Works?

Lenders may ask you to provide proof of deposit in several cases. For example, you may have to provide several months' worth of bank statements, pay stubs, or W-2s to show regular deposits from your employer.

Here are some other sources of money you may have to prove:

- **Personal savings**: To use your savings for proof of deposit, you'll likely need several months of bank statements. These statements should show the money being added to your account. Lenders prefer to see money that is "seasoned," meaning it has been in your account for a longer period of time, so is less likely to be a loan. You may have to write a letter explaining the source of the funds.
- **Property sale**: If you've sold a property and plan to use the funds for a large purchase like a house, you'll need to show your bank account that contains them. Documents that prove you owned the property may also be required.
- **Equity release**: If you use the same lender to buy a second home using equity from your first one, you may not need proof of deposit. They might, however, ask you to show that you can pay the mortgage on both properties.
- **Inheritance**: To use the money, you received in a will, you'll likely need to provide documents that state how much you received as well as a bank statement that shows the money in your accounts.
- **Gifts**: If you're using gift money, you'll have to show a legal agreement that explains the money was a gift and the person who gifted it does not expect to be paid back and that they don't want a portion of the property.

Lenders may also accept funds from savings bonds, investments, 401(k)s, and IRAs as well as other sources to be used toward a deposit.

Advantages of Proof-of-Deposit (PoD):

- **Enhanced Security**: PoD enhances the security of the network by requiring participants to stake cryptocurrency as collateral. This financial commitment incentivizes honest behavior and discourages malicious actors.
- **Decentralization**: By allowing anyone to participate as a validator, PoD promotes decentralization and prevents control from being concentrated in the hands of a few entities.
- **Efficiency**: Compared to Proof of Work (PoW) consensus mechanisms, PoD is more energy-efficient since it does not require extensive computational power to validate transactions.

Disadvantages of Proof-of-Deposit (PoD):

- **Wealth Centralization**: Participants with larger deposits have a greater chance of being selected as validators, potentially leading to wealth centralization and oligopoly-like control over the network.
- **Sybil Attacks**: PoD mitigates Sybil attacks by requiring participants to stake cryptocurrency, but it is still vulnerable to attacks if a malicious actor accumulates enough funds to control a significant portion of the network.
- **Barriers to Entry**: The requirement to deposit cryptocurrency as collateral may pose barriers to entry for smaller participants who cannot afford to stake large amounts of cryptocurrency.

Examples of Proof-of-Deposit (PoD):

1. **Ethereum 2.0**: Ethereum is transitioning from Proof of Work (PoW) to Proof of Stake (PoS) consensus with its Ethereum 2.0 upgrade. Validators in Ethereum 2.0 are required to deposit a certain amount of Ether (ETH) as collateral to participate in the network.
2. **Tezos**: Tezos is a blockchain platform that utilizes a variation of Proof of Stake (PoS) called Liquid Proof of Stake (LPoS). Participants, known as bakers, must deposit a certain amount of Tezos (XTZ) as collateral to become validators and participate in block validation.

Proof-of-Burn (PoB):

Proof-of-Burn (PoB) is a consensus mechanism used in blockchain networks that involves participants burning, or permanently destroying, cryptocurrency tokens to demonstrate commitment to the network. PoB is a form of Deposit-Based Consensus, where participants stake their cryptocurrency by sacrificing it, rather than locking it in a deposit.

With PoB, instead of investing in expensive hardware equipment, the validators follow the following approach:

- They burn coins by sending them to an address from where they are irretrievable.
- By committing the coins to an unreachable address, validators earn a privilege to mine on the system based on a random selection process.
- Thus, burning coins means that validators have a long-term commitment in exchange for their short-term loss.

- Depending on how the PoB is implemented, miners may burn the native currency of the Blockchain application or the currency of an alternative chain, such as bitcoin.
- The more coins validators burn, the better are their chances of being selected to mine the next block.

While PoB is an interesting alternative to PoW, the protocol still wastes resources needlessly. It is also questioned that mining power simply goes to those who are willing to burn more money.

How PoB Works?

1. As the name itself suggests, there is something which should be burned. Here as we are talking in the context of virtual currency so it's obvious that in PoB virtual currency is burned. The more the currencies are burned by miners the more they have the power to create blocks.
2. By burning we don't exactly mean burning. It means not using that coin. This may be done if it is sent to somewhere where it can't be spent. So, miners send these coins to such addresses from where they can't be used. It is sent to a public verifiable address where it cannot be accessed and thus can not be used.
3. When the coin is burnt its availability decreases leading to a potential increase in the value of the coin.
4. Now the question is why do we need to burn the coin? The basic explanation for this is that by destroying the currency, the consumer is displaying a big commitment to the currency by foregoing a narrow profit in exchange for a long-term profit.
5. To avoid any undue advantages for early adopters, the PoB has devised a method that allows for the periodic burning of crypto coins in order to maintain mining capacity. Any time a fresh block is mined, the energy of burned coins decreases slightly.
6. It is a deflationary idea in which the quantity of currencies reduces over time, increasing deficiency and, as a result, the currency holders' value. Coins that grow their quantity over time, on the other hand, tend to lose value.

Advantages of PoB:

- It required very little power compared to PoW.
- It reduces energy consumption by wasting insignificant resources when coins are burned.

- It encourages long-term involvement in a project as a consumer is displaying a big commitment to the currency by foregoing a narrow profit in exchange for a long-term profit.
- The coin distribution is more fair compared to all other consensuses.

Disadvantages Of PoB:

- It is risky because one doesn't know that will they gain the wealth they have burnt in the future or not.
- As coins are burnt, so technically if we see then resources are wasted.
- It may suffer from rich getting richer phenomena. In which those who are wealthy are getting wealthier by having more coins.

Proof of Importance (PoI):

Ever since the inception of Blockchain and the Proof of Work (PoW) consensus mechanisms to authenticate a new node or any transaction happening over the blockchain, there have been many new consensus mechanisms that have been introduced and Proof of Importance (PoI) is one such mechanism based on Byzantine Fault Tolerance.

- Proof-of-Importance (PoI) is a blockchain consensus mechanism introduced by NEM and this concept is a further build-up on the Proof of Stake (PoS) algorithm.
- The PoI uses network theory to assign a score for each node's importance in the network.
- In PoI the nodes have to vest a number of coins before they are eligible to carry out the mining of blocks in proportion to the score indicating their contribution made by them to the network.
- But unlike Proof of Stake (PoS) the score not only depends on the total vested amount of a node but also on many other variables like total amount, activity clusters, reputation, and transactions made through any given address.

How does Proof of Importance (PoI) Work?

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

- In exchange for harvesting a block, nodes are able to collect the transaction fees within that block which the validator gets as a reward.
- In order to be even eligible for the calculation or 'harvest', the NEM protocol requires that an account holder have at least 10,000 vested XEM (XEM is the cryptocurrency that powers the NEM blockchain which is rapidly gaining popularity recently) in its account and the accounts having high score will have a higher chance of getting selected to harvest a block.

NEM identifies an account's overall support of the network or score by considering the following three important characteristics: –

1. **Vesting:** Also known as 'Harvesting' is the most integral part of this consensus mechanism. First, any node should have at least 10,000 XEM coins before they can start harvesting or vesting. The consensus mechanism counts the number of coins present in your account for a set number of days (mostly 30 days) for calculating the Proof of Importance score of the node. Therefore, the higher the number of XEM coins higher will be the node's score.
2. **Transaction partnership:** Proof of importance rewards the users who make transactions with other NEM accounts on the network and will acknowledge both accounts as partners. The network theory calculation looks at transaction behavior to assign each node an importance score and stop the user from having any pseudo partnership.
3. **Number and size of transactions:** Each transaction above a minimum size has an impact on the Importance score and increases the chances of harvesting a block to collect rewards. Larger and more frequent transactions will improve the PoI score on the NEM network and the score is based on the transaction node makes in the period of 30 days.

Is the PoI Mechanism Prone to Sybil Attacks in Blockchain?

The term "Sybil" comes from the case study of an artist named Shirley Ardell Mason, aka Sybil Dorsett, who was diagnosed with Multiple Personality Disorder. A Sybil attack is an attempt to control a peer network by creating multiple fake identities. To outside observers, these fake identities appear to be unique users. But there is a single entity that controls many identities at once, as a result of which that entity has additional voting power using which it can influence the blockchain network.

- Sybil Attacks are hard to prevent and create havoc on the blockchain network, but the Proof of Importance mechanism's base principle is assigning a score based on the coins held by the node which will affect the influence of the node in the network.

- Now as there exists a cost to create an identity the malicious entity won't be able to create nodes with sufficient coins to gain control over the network as it is very expensive. So PoI mechanism provides some extent of safety against Sybil's Attack.

Benefits of Proof of Importance (PoI):

1. **Energy Efficient:** In a blockchain network those who use Proof of Work (PoW) have an unfair advantage over other nodes in terms of high computing power for mining blocks. These POW systems also harm the environment by consuming very high amounts of electricity and burdening miners with expensive power bills, whereas the Proof of Importance (PoI) is very energy efficient.
2. **Avoid coin hoarding and encourages transaction:** The Proof of Stake (PoS) system concentrates wealth among a few nodes since users can simply hoard as many coins as possible and reap the rewards from block creation. The more coins they keep in their accounts, the more they earn. So, everyone has the incentive to save coins instead of spending them thereby discouraging transactions and the rich getting richer. The importance score will be higher when nodes spread XEM coins and lower in case they hoard the coins, thereby proof of Importance (PoI) mechanism is very suitable.
3. **Lower Incentive:** As the miners in the Proof of Importance mechanism are not required to mine blocks like in Proof of Work by using high computation power and heavy power consumption, the incentive given as rewards for adding blocks to the blockchain network also need not be higher as in Proof of Work mechanism. This helps greatly in reducing the transaction fees that are applied for validation by the miners.
4. **Discourages Forks:** In traditional PoS mechanisms the marginal cost of creating a block is zero and users can continue effortlessly validating blocks in the event of a fork. But, in Proof of Importance, each node's importance score is based on network activity and dynamic. So, this discourages the blockchain forks as the new user needs to expend resources on both forked networks to remain active to maintain their score.

Federated Consensus or Federated Byzantine Consensus:

Federated Consensus, also known as **Federated Byzantine Agreement (FBA)**, is a consensus mechanism used in permissioned blockchain networks, where a group of pre-selected nodes or validators are responsible for validating transactions and creating new blocks.

In a Federated Consensus system, the participating nodes are typically organizations or entities that have been granted permission to join the network and participate in the consensus process. These nodes are often referred to as "validators" or "endorsers."

Here's how Federated Consensus works:

1. **Validator Selection**: A group of nodes or organizations is selected to act as validators or endorsers for the network. This selection process can be based on various criteria, such as reputation, stake, or voting.
2. **Transaction Endorsement**: When a new transaction is submitted to the network, a subset of validators (often called a "quorum") is chosen to endorse or validate the transaction. This endorsement process can involve executing smart contracts, verifying signatures, or performing other checks.
3. **Consensus Process**: Once a quorum of validators has endorsed the transaction, a consensus protocol is used to reach agreement among all validators on the order and validity of the transactions. Common consensus protocols used in Federated Consensus include Practical Byzantine Fault Tolerance (PBFT), Raft, and Paxos.
4. **Block Creation**: After consensus is reached, one of the validators is responsible for creating a new block containing the validated transactions and adding it to the blockchain.
5. **Block Propagation**: The new block is then propagated to all nodes in the network, and the process repeats for the next set of transactions.

Advantages of Federated Consensus:

1. **High Performance**: Since the number of validators is limited and known in advance, the consensus process can be optimized for higher transaction throughput and lower latency compared to fully decentralized systems.
2. **Efficiency**: Federated Consensus can be more energy-efficient than Proof-of-Work, as it does not require extensive computational power for mining.
3. **Permissioned Network**: The permissioned nature of the network allows for better control over access and governance, making it suitable for enterprise and consortium applications.

Drawbacks of Federated Consensus:

1. **Centralization Risk**: If the validators or endorsers are controlled by a small number of entities, there is a risk of centralization and potential censorship or manipulation of the network.
2. **Trust Assumptions**: Participants must trust the validators or endorsers to behave honestly and follow the protocol, as they have a significant influence over the network.
3. **Limited Decentralization**: While more decentralized than a fully centralized system, Federated Consensus is still less decentralized than fully permissionless blockchain networks.

Federated Consensus is often used in enterprise blockchain platforms, such as Hyperledger Fabric, Quorum, and Corda, as well as in consortium blockchain networks involving multiple organizations or entities.

Practical Byzantine Fault Tolerance (pBFT):

Practical Byzantine Fault Tolerance (pBFT) is a consensus algorithm used in distributed systems, including some blockchain networks, to achieve consensus among nodes in the presence of faulty or malicious nodes. It was introduced by **Barbara Liskov** and **Miguel Castro** in the 90s.

The Byzantine Fault Tolerance problem refers to the challenge of reaching agreement in a distributed system where some nodes may behave in a Byzantine (arbitrary or malicious) manner, such as sending conflicting information to different nodes or failing to respond.

PBFT addresses this problem by providing a practical solution that can tolerate up to one-third of the nodes being faulty or malicious, while still allowing the system to reach consensus on the state of the network.

Byzantine General Problem:

The Byzantine Fault Tolerance can be controlled if the correctly working nodes reach the agreement of network values. There should be a network value that is given to every node of the network. That means if we assume, there is a faulty node and the network value may not reach the agreement. But we can overcome this problem with the help of the Byzantine General problem. Also, if there is a majority of certain values given by every node, then we assign that certain value to the entire nodes of the network. Leslie Lamport proves that if we have a 3m+1 number of processors working perfectly, then m is the number of processes that are faulty.

Types of Byzantine Failure:

Types of Byzantine failures can be divided into the following two categories:

1. **Fail-stop failure:** Node permanently stops working and does not return any result.
2. **Arbitrary node failure:** Node does not stop permanently and shows one of the following behaviors:

    a. It does not return a result.

    b. It returns an incorrect result.

    c. It deliberately returns a misleading result.

    d. It returns different results to different parts of the system.

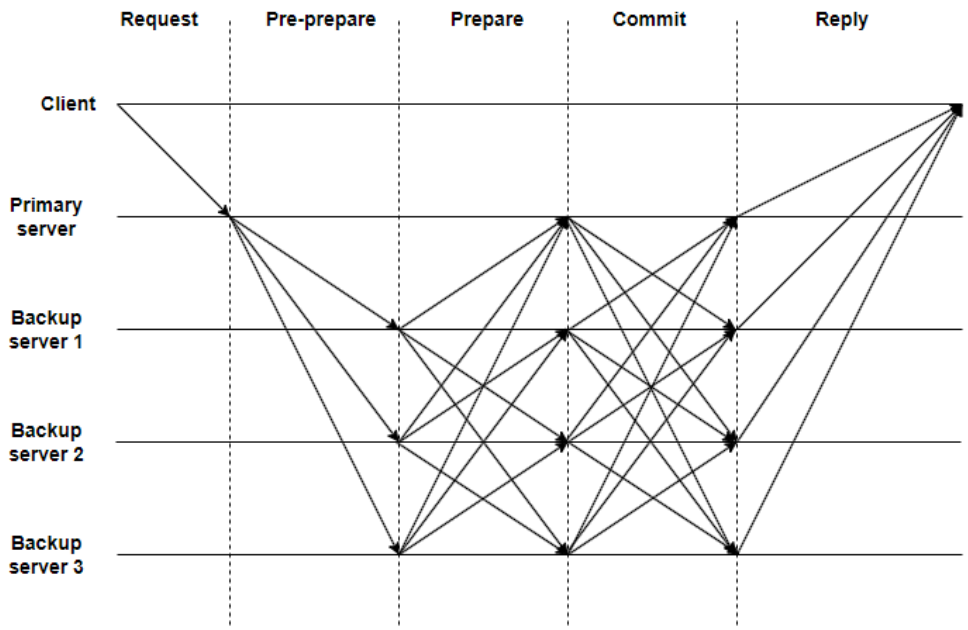
How does pBFT work?

The pBFT algorithm provides practical state machine replication in which all nodes are sequentially ordered, with one node as the primary node and others as secondary nodes (backup/replica nodes). A pBFT can function on the condition that the total number of malicious nodes must be less than one-third of the total nodes nn in the system.

The pBFT consensus happens in the following five steps:

1. The client makes a request and sends it to the primary node.
2. The primary node broadcasts the request to all the secondary(backup) nodes. It is called the pre-prepare phase.
3. Then every node (primary and secondary) sends a prepare message to all other nodes.
4. Once every node receives $(n/3)+1$ prepare messages, it sends a commit message to all other nodes and commits the changes made by the client's request.
5. Once every node receives $(n/3)+1$ commit messages from other nodes, it sends a reply to the client.

The primary(leader) node is changed during every view (pBFT consensus rounds) and can be substituted by a **view change protocol** if a predefined quantity of time has passed without the leading node broadcasting a request to the backups(secondary). If needed, a majority of the honest nodes can vote on the legitimacy of the current leading node and replace it with the next leading node in line.



Working of a practical Byzantine fault tolerant consensus algorithm

Advantages of pBFT:

The following are a few advantages of using pBFT over other consensus algorithms:

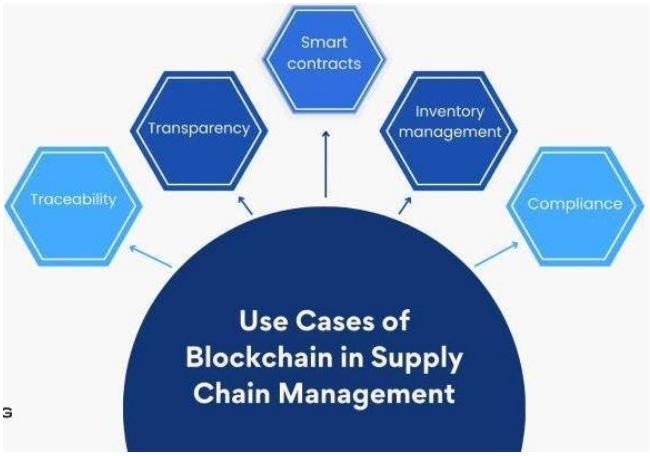
1. **Energy efficient:** pBFT does not need to compute complex mathematical problems to reach a consensus. Therefore, it is much faster and energy efficient than algorithms such as proof of work.
2. **Faster transaction finality:** Consensus algorithms such as proof of work require confirmations from other nodes before adding it to their journal (which takes 10–60 minutes). However, pBFT does not require any confirmations, it is much more efficient than other consensus algorithms.
3. **Low reward variance:** In pBFT, every node is participating in processing the client's request. Hence, every node can be incentivized, resulting in low reward variance and a more fair reward system.

Limitations of pBFT:

1. **Sybil attacks:** A distributed network using pBFT is susceptible to Sybil attacks if one entity controls many nodes in the network. As the number of nodes increases, it becomes difficult to carry out a Sybil attack.
2. **Scalability:** As the number of nodes in the network increases, communication overhead (messages sent to other nodes) increases. It is shown by the equation - $O(n^k)$, where n is the messages and k is the number of nodes.

Blockchain Use Case - Supply Chain Management:

Supply chain management involves the coordination of materials, information, and finances as they move from supplier to manufacturer to wholesaler to retailer to consumer. This process traditionally involves multiple parties, each with their own records, making it complex and often inefficient. Blockchain technology offers a solution by providing a decentralized, transparent, and secure method of recording transactions.



The prominent use cases of blockchain for supply chain management include:

1. Traceability: Traceability is one of blockchain's most compelling use cases in supply chain management. Blockchain empowers businesses to create an immutable ledger of every product's journey, from its origin to its final destination. With blockchain's transparent and tamper-proof record-keeping, companies can trace the movement of goods with unparalleled accuracy.

The high level of traceability enhances accountability and serves as a critical tool for product recalls and quality assurance. The consumers also gain deeper insight into the origins of the products they purchase, fostering trust and strong relationships with the companies.

2. Transparency: Transparency is a significant use case of blockchain for supply chain management. Traditional supply chains often suffer from a lack of visibility and trust among participants. Blockchain technology addresses this challenge by providing a decentralized and immutable ledger that all stakeholders can access and verify.

Every transaction recorded on the blockchain is transparent and cannot be altered, ensuring a single source of truth for all involved parties. This transparency enables real-time tracking of goods, from raw materials to the end product, allowing businesses to identify bottlenecks, inefficiencies, and potential areas for improvement.

3. Smart Contracts: Smart contracts represent a transformative use case of blockchain technology in supply chain management. Smart contracts are self-executing agreements with predefined rules and conditions encoded on the blockchain. These contracts automate and streamline various supply chain processes, such as procurement, payments, and compliance.

By leveraging blockchain's decentralized and transparent nature, smart contracts eliminate the need for intermediaries, reduce administrative costs, and minimize the risk of errors or disputes.

For instance, when a shipment reaches a specific location, the smart contract can automatically trigger the payment to the supplier. This automation improves efficiency and enhances accountability among supply chain participants, ensuring fulfillment of contractual obligations.

4. Inventory Management: Inventory management represents a crucial use case for blockchain technology in supply chain management. Traditional inventory management systems often suffer from inefficiencies, inaccuracies, and a lack of real-time visibility. Blockchain addresses these challenges by providing a secure and transparent ledger that tracks the movement and status of inventory items across the supply chain.

Through IoT devices and sensors, real-time data can be recorded on the blockchain, allowing stakeholders to accurately monitor inventory levels, locations, and conditions. This transparency reduces the risk of overstocking or stockouts and helps to optimize supply chain operations.

5. Compliance: With its immutable and transparent nature, blockchain provides a reliable and auditable record of all transactions and activities throughout the supply chain. This data enables businesses to demonstrate compliance with various regulations, standards, and certifications.

By securely storing and sharing data on the blockchain, supply chain participants can easily verify the authenticity and integrity of documents, such as certificates of origin, quality inspections, and regulatory compliance records.

Blockchain also facilitates the automation of compliance processes through smart contracts, ensuring that all parties adhere to predefined rules and regulations. By leveraging blockchain for compliance, businesses can mitigate risks, improve regulatory reporting, and enhance trust among stakeholders in the supply chain ecosystem.