DISTRIBUTED CONSENSUS MECHANISM

Abstract

The distributed consensus algorithm which is a collection of guidelines or protocols known as consensus algorithms enable dispersed nodes to decide on a value or course of action based on messages from other nodes as well as their own local data. The following characteristics are the goals of consensus algorithms: fault-tolerance, validity, agreement, and termination. This paper provides the outline and study about the different consensus algorithms in blockchain. The proposed paper describes about the working mechanisms of different consensus algorithms such as proof of work, proof of stake and etc., Also explains the requirement of consensus algorithms, advantages and disadvantages of each consensus algorithm.

Keywords: Consensus, protocols, algorithms, fault-tolerance, blockchain.

Authors

D. Geethanjali
Assistant Professor
Department of CSE
Sathyabama Institute of Science and Technoloy
Chennai, Tamilnadu, India.
anjali.geetha81@gmail.com

N. Umasankari
Assistant Professor
Department of CSE
Sathyabama Institute of Science and Technoloy
Chennai, Tamilnadu, India.
san_june18@yahoo.com

P. Umamaheswari
Assistant Professor
Department of CSE
SASTRA Deemed University
SR, Kumbakonam, Tamilnadu, India.
pum@it.sastra.edu

Siddikeshwer Reddy
Student
Department of CSE
Sathyabama Institute of Science and Technoloy
Chennai, Tamilnadu, India.

I. INTRODUCTION TO CONSENSUS MECHANISM

Through the use of a consensus mechanism, any peer in the Blockchain network can concur on the present state of the distributed ledger. In a distributed computing environment, consensus methods create credibility in the Blockchain network and promote it among anonymous peers. In other words, the consensus mechanism ensures that each new block that is added to the Blockchain is the only one that every node has acknowledged as the single source of the unchanging truth. Some of the specific goals of the Blockchain consensus protocol include achieving comprehension, collaboration, and cooperation as well as giving each node equal rights and requiring each node to take part in the consensus process.

Figure 1: Consensus Mechanism

A consensus mechanism in blockchain systems is a program that enables broad agreement on the state of the ledger at the moment. Usually, it is used in a network with a large number of users and operations. It refers to any technique used to establish security, trust, and agreement within a decentralized computer network. By implementing automatic group verification and encryption, it is a crucial component of information security.

II. HISTORY OF CONSENSUS MECHANISM

The techniques of consensus have a lengthy and complex history that dates back several decades. In the 1970s, Researchers started looking into the issue of reaching consensus in distributed systems, which are made up of numerous nodes that interact and work together to accomplish a shared goal.

Due to the fact that they stored data and were networked so that numerous people in various locations could access it, these shared databases came to be known as distributed ledgers. Preventing data manipulation and illegal access, whether intentional or not, was among the most pressing problems that needed to be solved. To prevent data from being modified, a mechanism for automating distributed database maintenance was needed.

This requirement inspired the development of distributed autonomous consensus, in which programs on a network used cryptographic methods to agree on the state of a database. A hash, or lengthy string of alphanumeric numbers, was intended to be produced by

encryption methods in order to reach agreement. Programs running on the network would then verify the hash. The programs were made to compare hashes to make sure they matched because a hash can only change if the data entered into the hashing process is altered.

The data was referred to as being agreed upon by the network by consensus when each application executing on the network produced a matched alphanumeric string. Thus, consensus procedures were developed, with Satoshi Nakamoto, the mysterious person who created Bitcoin, receiving the majority of the credit. Before Nakamoto published the whitepaper that made Bitcoin famous, many individuals had spent years developing consensus techniques.

III. WHY CONSENSUS MECHANISM?

Every blockchain for a cryptocurrency uses a consensus process to function. Users of a blockchain network adhere to this approach to determine the validity of transactions. This technique makes sure that each copy of the blockchain contains all valid transactions and that all lawful transactions are recorded on the blockchain.

On the majority of blockchains, new transactions are validated by computers known as miners. These miners compete with one another in a proof-of-work system to validate the subsequent block of transactions. The network's transaction senders fund the mining fee that the successful miner receives as payment.

The consensus technique ensures that all miners concur on the next block of transactions by sending each new block of transactions to all other miners. A copy of the blockchain is available for download by anyone with a node-capable device. Every duplicate of the ledger is an exact match. There is always agreement thanks to the consensus mechanism over which assets go in which wallet.

The Consensus mechanism rule achieves the following

- Consistency or reliability and agreement between nodes.
- Aligning participants’ incentives.
- Prevent the double spending
- It can be able to handle the node failure.

IV. PROPERTIES OF A GOOD BLOCKCHAIN CONSENSUS MECHANISM

1. **Safety:** A solid consensus method allows all nodes to produce results that are valid in accordance with the protocol's requirements.

2. **Inclusive:** A good consensus blockchain system makes sure that each specific network node takes part in the voting process.

3. **Active participation:** Good consensus architecture involves all nodes contributing actively to the updating of databases on the blockchain.

4. **Egalitarian:** Giving equal worth and weight to each vote received from the node is another quality of a successful mechanism.

5. **Accessibility:** Regardless of their computing capacity or financial resources, all network participants should be able to access the consensus process.

When the user must consider the above factors before going to introduce or develop the consensus model. Otherwise poor consensus model may occur in the user development process.

V. TYPES OF CONSENSUS MECHANISM

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

1. Proof of Work (PoW)
2. Proof of Stake(PoS)
   - Delegated Proof of Stake (DPoS)
   - Leased Proof of Stake (LPoS)
3. Proof of Capacity (PoC)
4. Proof of Burn (PoB)
5. Proof of Identity (PoI)
6. Proof of Importance (PoI)
7. Proof of Activity (PoA)
8. Proof of Elapsed Time (PoET)
   - Practical Byzantine Fault Tolerance (PBFT)
   - Delegated Byzantine Fault Tolerance (DBFT)

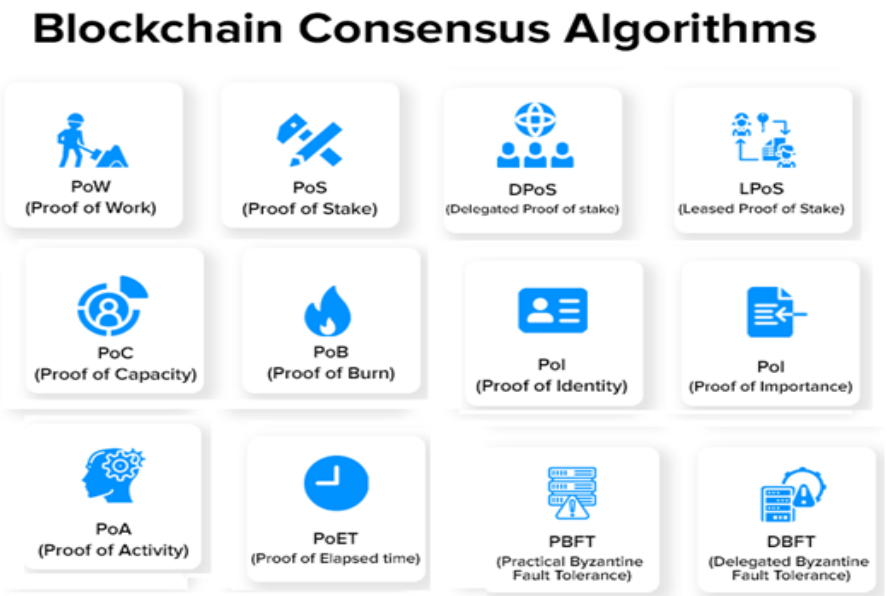

Figure 2: Types of Blockchain Consensus Algorithms

1. **Proof of Work:** The process of creating fresh blocks of transactions to a cryptocurrency's blockchain is known as proof of work (PoW). Proof of Work, the first consensus mechanism utilized in the blockchain industry, was created by Satoshi Nakamoto. It is also referred to as mining, with miners denoting the participating nodes.

The underlying algorithm used by proof-of-work blockchains determines the rules and level of difficulty for mining operations. The "work" itself is mining. It involves adding legitimate blocks to the chain. This is significant because it enables the network to follow the right blockchain fork because to the length of the chain. The network can be more confident in the condition of the world as long as there is more "work" being done, a longer chain, and a higher block number.

- **How Proof-of-Work (PoW) works?**

  - Using powerful computing capacity, the miners in this mechanism must solve challenging mathematical riddles.
  - The miners employ a variety of mining techniques, including GPU, CPU, ASIC, and FPGA mining. And as a prize, the one who solves the puzzle first receives a block.
  - The procedure is not straightforward, though. A riddle can only be solved by trial and error.
  - In addition, the difficulty of the problem rises in proportion to the rate of block mining. In order to keep up with the difficulty level, it is necessary to produce a new block within a set amount of time.
  - To find the nonce for a block, miners had to compete in a difficult game of trial and error using the proof-of-work protocol Ethash. To the chain could only be added blocks with a working nonce. The following figure 3 shows the working process of a Proof of Work consensus algorithm.

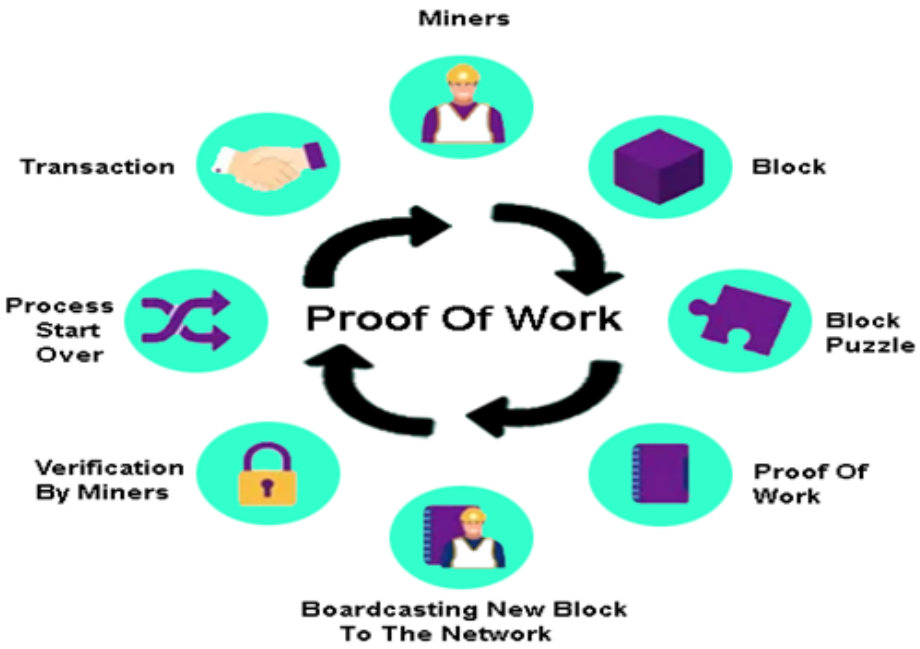

Figure 3: Working process of Proof-of-Work (PoW)

The following cryptocurrencies employ the Proof of Work mechanism. Those are Bitcoin, Litecoin, ZCash, Primecoin, Monero, and Vertcoin.

Advantages and Disadvantages of Proof of Work (PoW)

Sl.No	Advantages of PoW	Disadvantages PoW
1	High level of security.	Due to high fees and slow transaction speeds, useless.
2	It provides a decentralised way to verify transactions.	High energy usage.
3	Allows miners to earn crypto rewards.	Costly equipment is frequently required in mining.

2. **Proof-of-Stake:** A consensus process for cryptocurrencies called Proof of Stake is used to verify transactions and add new blocks to the network. In order to lessen the enormous energy consumption of blockchain mining, Sunny King and Scott Nadal originally created the Proof of Stake (PoS) in 2012.

They put out an alternate method termed "staking," in which nodes are selected using a random deterministic mechanism depending on the quantity of coins that each node has staked. To put it simply, the stakers (nodes/users who stake coins) who have more coins "staked" will have a higher likelihood of validating the blockchain and earning transaction fees as compensation.

The nodes of a network must stake a specific amount of cryptocurrency to be eligible to validate new blocks and collect a fee. The node that will validate the new block is then chosen from a pool of candidates via an algorithm. This technique combines the stake amount (the total amount of bitcoin) with other factors (such coin-age-based selection and randomization procedure) to guarantee that the selection is fair for everyone on the network.

- **Coin-age-based selection:** The method monitors the duration of each validator candidate node's validity. With time, a validator is more likely to be replaced by a node.

- **Random Block selection:** Using the criterion of "lowest hash value" and "highest stake," the validator is chosen in a random block selection. The node with the best weighted combination of these is the new validator.

- **How Proof of Stake (PoS) Works?**
  The figure 4 shows the working process of a Proof of Stake (PoS) consensus mechanism.

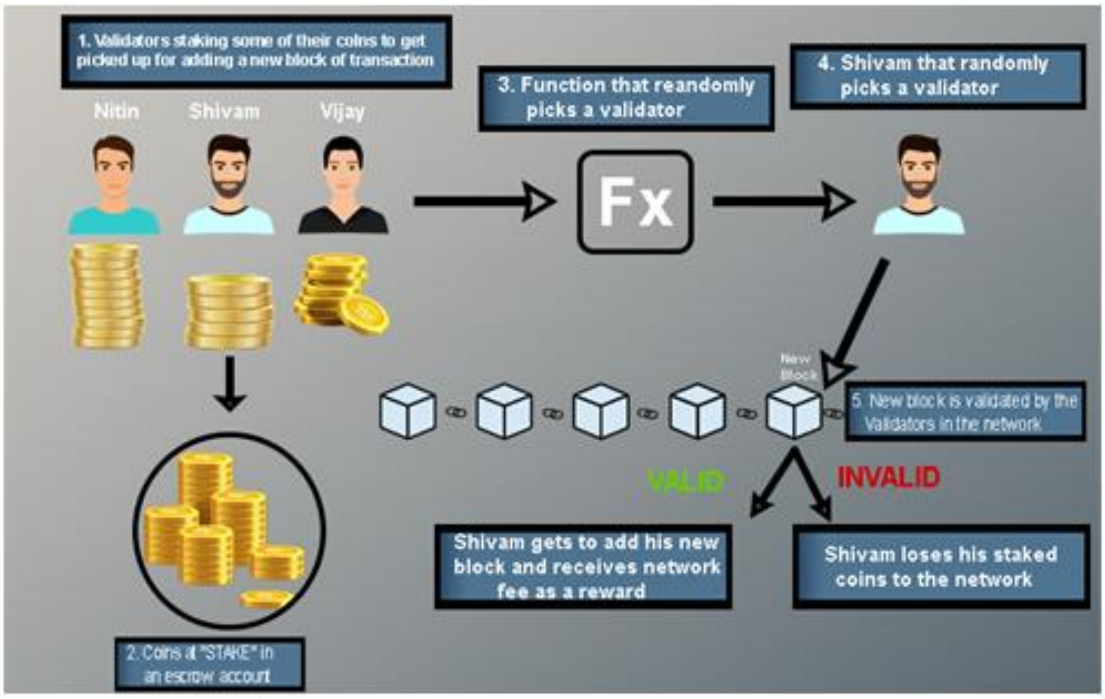

Figure 4: Working Process of Proof-of-stake (PoS)

- Nodes execute transactions. The PoS algorithm is used to aggregate all of these transactions together.
- ii. Each node seeking to be the validator of the upcoming block increases a stake. This stake is combined with other criteria like "coin-age" or "randomised block selection" to determine the validator.
- iii. The validator validates every transaction and publishes the block. He hasn't received the forging award, and his stake is still locked. In order for the network's nodes to "OK" the new block, this is required.
- If the block is approved, the validator receives both the stake and the reward. If the algorithm selects validators based on coin age, the coinage of the validator for the current block is reset to 0. As a result, he is now of low priority for the future validator election.
- If the block is not verified by further network nodes, the validator loses their stake and is classified as "bad" by the algorithm. Step 1 of the process to forge the new block is where it all starts.

- **Currencies that Use Proof of Stake:** There are already more than 80 cryptocurrencies that employ the Proof of Stake mechanism as their way of validation through the consensus mechanism, and PoS is currently becoming increasingly prevalent as a 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)
  - Avalanche (AVAX)

- **Advantages and Disadvantages of Proof of Work (PoS)**

Sl.No	Advantages of PoW	Disadvantages PoW
1	**Energy:** Energy Efficiency and quicker processing.	**Complexity:** To protect against fictitious dangers like long-range attacks and the nothing at stake problem, further constraints are needed.
2	**Hardware requirements:** Less hardware is needed, and a larger number of people can take part in the consensus process.	**Accessibility Limitation:** A block validator that controls a higher percentage of staked coins exclusively receives transaction fees and all newly minted coins as payment for his validating labor.
3	**Security:** Fraudulent validators must pay a higher price or risk losing more money than they make. It is hence safer.	Lack of decentralization and centralization of power.
4	**Manipulations:** Fewer manipulations and flexibility.	**Initial distribution:** Without coins, no one can become a validator and earn coins to stake.

The Proof of Stake has the Following Two Types of Consensus Mechanism. They are

- Delegated Proof of Stake
- Leased Proof of Stake

- **Delegated Proof of Stake mechanism:** It is a one type of Proof of Stake consensus algorithm. The cornerstone for this particular consensus process is the voting delegation. Other users are given the users' votes by the users. The rewards will be given to the users who delegated to that particular vote by whichever user mines the block next.

  The DPoS algorithm is developed by Daniel Larimer in 2014. By staking their tokens in the common Proof of Stake algorithm, stakers or validators sign up for a process called mintage in which they add blocks to the blockchain and receive compensation for their truthful work. With Delegated Proof of Stake (DPoS), participants stake their cryptocurrency and cast their votes for a predetermined number of delegates, with the amount of investment determining the voting weight. As an illustration, if user A pays 10 coins for a delegate and user B invests 5 coins, user A's vote will be given greater weight than B's.

  Additionally, the delegates are compensated with transaction fees or a fixed number of coins. DPoS is one of the quickest blockchain consensus algorithms and is favored as a digital democracy due to its stake-weighted voting mechanism.

- **How Delegated Proofof Stake Works?**

  DPoS algorithm works based on a mechanism of voting or an election system.

  - The delegates who validate the blocks are chosen by the network's users. Only a certain number of these delegates are allowed, and they can vary as other delegates can be elected in their place. These nodes are represented as "witnesses" or "block producers."
  - DPoS enables network users to pool tokens into a staking pool and vote for a certain delegate of their choosing. Instead of sending their tokens to a single wallet, network users can stake utilising a staking mechanism or service provider.
  - Delegates are essential because they ensure the accuracy of the transactions. They receive transaction fees for successfully validating the block, which they can subsequently give to the supporters that supported them. The more a person is able to stake, the more they can receive as an allocation.
  - The amount of the overall stake that a user represents affects the payment they receive from their delegate. For instance, if a user only contributes 10% to the total stake pool, they could still be eligible for up to 10% of the prize.

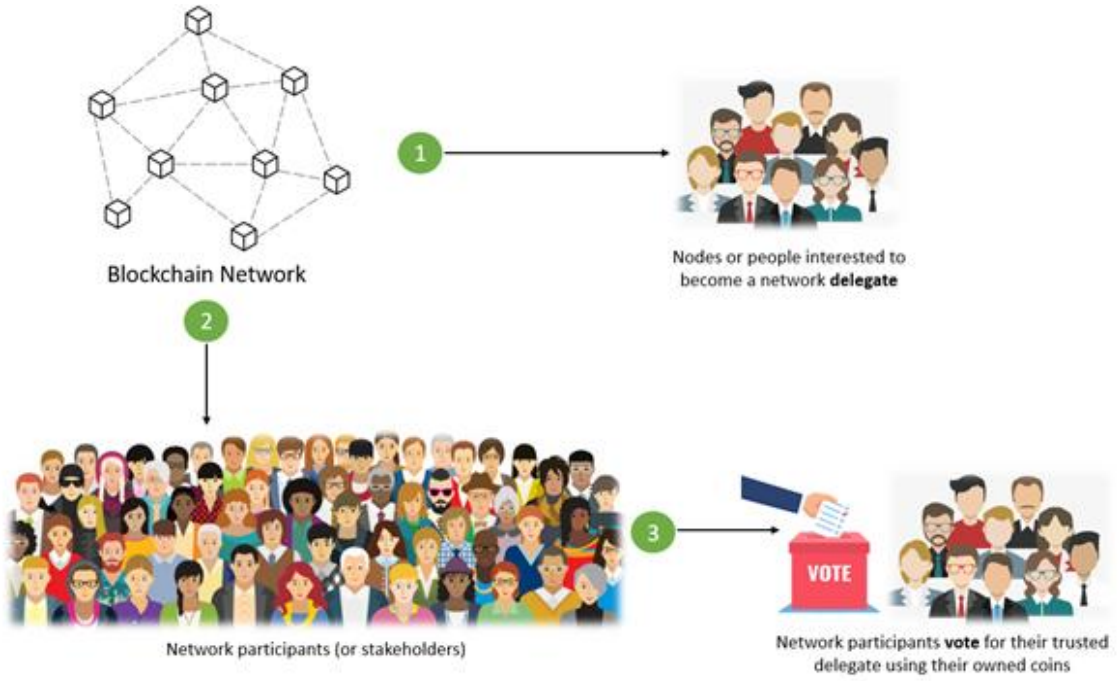

Figure 5: Voting Process of DPoS

- **Voting:**
  - In DPoS consensus, users have the option of casting their votes themselves or delegating that responsibility to another party.
  - The chosen witness is in charge of building blocks by authenticating transactions.
  - They receive a reward for validating and signing every transaction in a block, which is often distributed among those who voted for witness.

- If a witness does not complete the required number of transactions in the allotted time, the block is missed, all transactions are left unconfirmed, and the witness receives no reward.

➢ In addition to their own prize, the following witness who verifies that block is given a reward. The block is considered to as stolen after the subsequent witness gathers these transactions.

The weight of each voter's vote on the result is proportionate. A user does not required to have a significant stake to join the top tier of witnesses. Instead, as a result of votes from users with large stakes, individuals with less stake may be elevated to the top tier of witnesses.

- **Points to keep in mind before Voting:**

➢ Network participants vote using their coins or tokens.
➢ Each network participant (or stakeholder) receives the same number of votes as the amount of coins they own.
➢ The stakeholder may also give coins to another stakeholder for that person to cast a vote on their behalf.

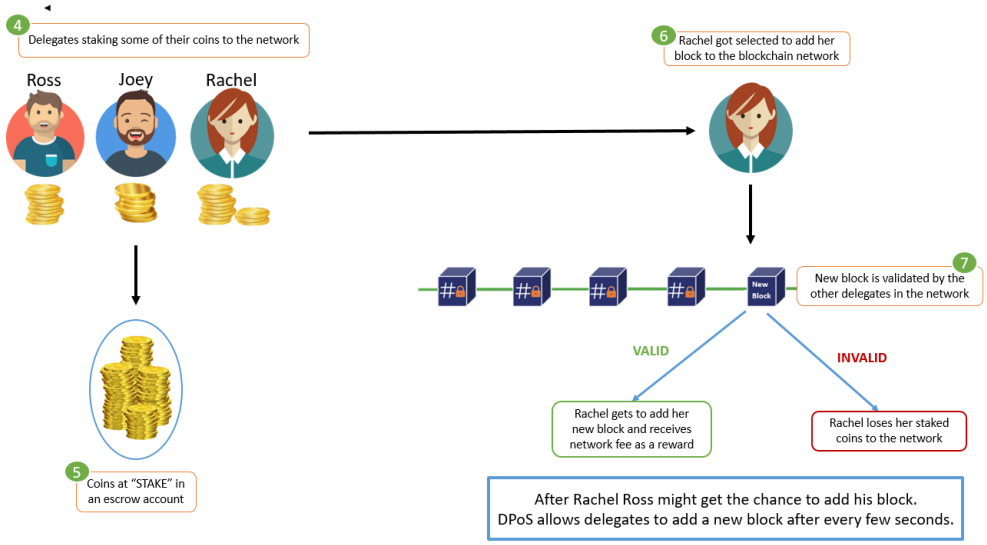

Figure 6: Process of Selection A Single Delegate Among Selected Delegates

- **Witnesses:** Threats of financial loss, stake lockup, and reputational harm are used to restrain witnesses. A portion of the stake that witnesses must lock will be forfeited if they commit fraud or try to attack the blockchain.

➢ The number of witnesses in the first tier is restricted, and is typically between 21 and 101.
➢ These witnesses are responsible with authenticating transactions and creating blocks, and they are paid appropriately.
➢ In Proof of Work blockchains, witnesses are similar to miners in that they can prevent some transactions from being included in a block but cannot modify any transaction's specifics.

- Each witness in the top tier runs the risk of being replaced by a user who receives more votes and is subsequently perceived as more trustworthy.
- As the number of witnesses increases, so does the competition, and each witness's ability to compete depends increasingly on their reputation.

A round robin method is followed in a round of DPoS blockchain with N block producers/witnesses:

- N block producers are selected from a pool of candidates who can serve as witnesses.
- Until k=N, the kth block creator signs each succeeding block.
- A block is deemed complete when it receives (2/3+1) of the vote from block producers. When there are two chains, the longest chain rule is applied. Block addition is irreversible.

- **Delegates:** Users in DPoS systems can also select the delegates in charge of overseeing blockchain governance. They are powerless to affect transaction control. Delegates may recommend changing a block's dimensions or the payment a witness ought to get for validating a block. When delegates propose these changes, the users of the blockchain decide whether to accept them or not.

- **Role of Selected Delegates (or Witness):**

  - The chosen delegates (or witnesses) confirm the adding block's transactions.
  - Each delegate has the ability to contribute their own block of transactions to the network.
  - Delegates are rewarded for successfully verifying additional blocks or for adding a new, legitimate block.

- **Block Validators:** The term "block validator" in DPoS refers to full nodes that verify that blocks created by witnesses follow the consensus rules. A block validator can be used by anyone to examine the network. A validator of blocks has little motivation to do their job.

  Some of the real-life use cases of this blockchain consensus mechanism are
  - Steem, EOS
  - BitShares
  - Zclassic ZCL
  - Bitshares BTS
  - Steemdollars SBD

- **Advantages and Disadvantages of Proof of Work (DPoS)**

Sl.No	Advantages of DPoS	Disadvantages DPoS
1	They are well protected against the risk of using cryptocurrencies more than once, or twice that means	If there are only a few witnesses and delegators, the mechanism won't function as it should since it needs highly knowledgeable

	double spending.	delegators and witnesses who will tell the truth.
2	It is more democratic because witnesses and delegates are elected and don't require large stake amounts. Additionally, any node can use a block validator to validate a block.	Due to the mechanism's bias against voters' stakes, votes cast by voters with low stakes in large numbers would be meaningless.

❖ **Leased Proof of Stake (LPoS):** On the Waves platform, an enhanced PoS consensus procedure called LPoS is used. In this consensus algorithm blockchain, users can lease their balance to full nodes as opposed to the traditional Proof-of-Stake method, where each node must hold a particular amount of money in order to add the next blockchain. And the person who leases the greater amount to the entire node has a higher chance of producing the next block. The remainder of the transaction fee that the entire node has received is then paid to the leaser. This PoS variation is a dependable and practical option for the development of open-source coins.

- **How does Leased Proof of Stake (LPoS) work?**
  In leased proof-of-stake (LPoS), users rent cryptocurrency to a particular node that aspires to be the blockchain's "block producer." A node has a better probability of getting chosen to add new blocks and receive rewards when the stakes are higher. The lease can be ended at any time by the user.

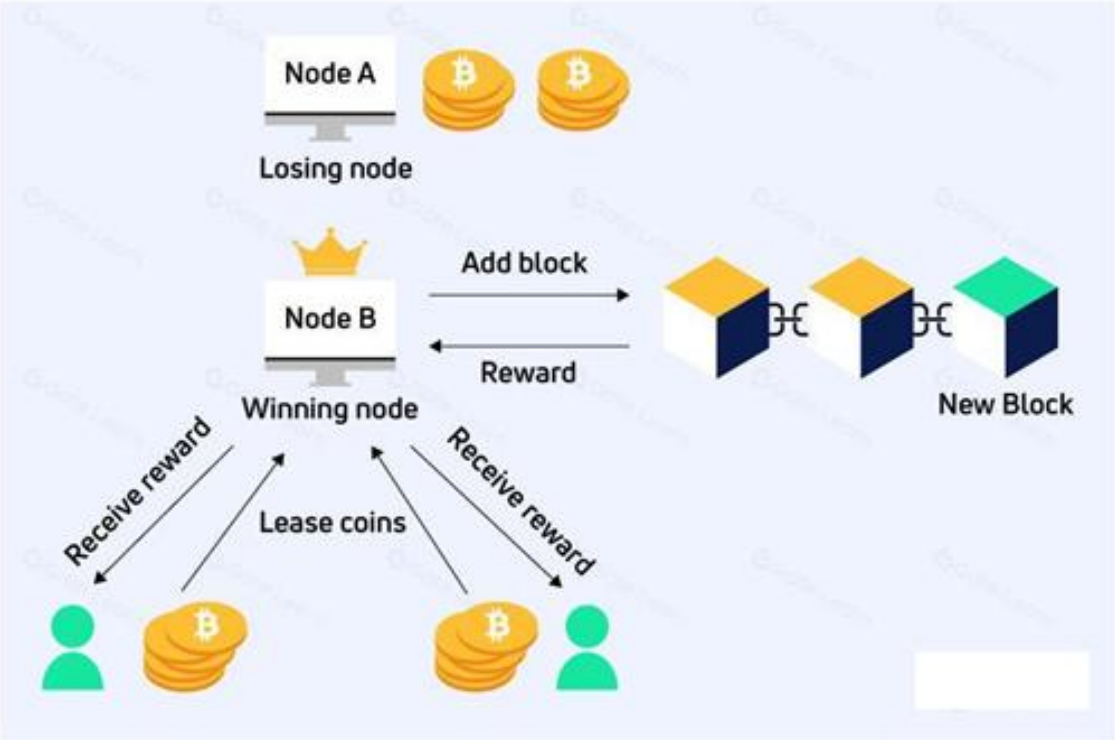

Figure 7: Working Process of LPoS

- The coin owner must create a lease transaction and include the recipient node address and the number of coins to be leased in order to begin leasing. Leasing can always be stopped by entering a cancel lease transaction.
- The coin holder/lessor retains complete control over the leased cash. Although the leaser can link the coins to the nodes they want to lease from, the coins never leave their wallet. The coins do not actually go to the node; instead, they simply remain unusable and cannot be exchanged or transferred until the leaser ends the agreement.
- LPoS allows leasers to take part in the consensus mechanism since the more money a node has leased from it, the more likely it is to be chosen to create the next block. For instance, in the Fig. below, node B is the recipient of the monies from two lessees. The node's stake weight is raised by using the tokens that are leased to it, which improves its chances of being chosen to validate transactions and add the next block to the Blockchain.
- The node compiles a block of pending transactions after winning. The transaction fees are subsequently given to the winning node as compensation.
- The node operators distribute a portion of their node rewards to their leasers after receiving them. The leaser will receive more compensation the more is rented.

- **How to Execute LPoS Transactions?**
  To construct a lease transaction, the token owner must specify the token amount they desire to lease as well as the destination address (node address).
  There are two distinct transaction types used by the LPoS:

  - The leasing procedure is initiated by the execution of a lease transaction.
  - The leasing process is terminated by executing a lease cancellation transaction.

- **Benefits of Leasing to Token Holders**

  - With LPoS, token owners can rent out their tokens to nodes in exchange for a share of the dividend payment.
  - Because Waves nodes are more likely to be selected to produce the following block when a higher quantity is leased to them, lessees will be able to participate in the process of creating new blocks by using LPoS. The lessor will be paid if that node is selected.
  - When a user first starts renting tokens, the tokens are locked and retained at the same address under the full ownership of their owner (they are not moved to the node, they simply stay unavailable for use until the lessor cancels the lease).

- **Benefits of Leasing to the Node Owner:** The node owner or lessor receives the mining incentive when nodes use the leased tokens to build blocks.

  The leased tokens can be used by nodes to create blocks and the node owner or lessor receives the mining reward.

  - The likelihood that a node will add blocks to the blockchain improves as more coins are leased to it, increasing its mining power.

- The node owner may choose the percentage of incentives that the lessor receives according on his criteria.
- Based on the amount leased, the probability that a node will be picked to build the next block rises.

Examples of Blockchains that Utilize LPoS

- Waves
- Nix

- **Features of Leased Proof of Stake**

  - **Balance Leasing**: Users can profit passively from using LPoS by leasing money from their wallets or any other form of cold storage to miners.
  - **Fixed Tokens:** In LPoS, tokens are not created by mining and are instead fixed to the network. Tokens can instead be rented and fixed. Leased tokens are locked in the leaseholders' accounts and cannot be traded or transferred unless the owner cancels the lease.
  - **Decentralized:** Most blockchains incentivize users for signing up for mining pools, which creates a centralized structure. With LPoS, however, rewards are distributed equally based on the amount staked, eliminating the need for a mining pool. Leasing also follows a peer-to-peer protocol to avoid interference from outside parties.
  - **Rewards in place of transaction fees:** Transaction fees are rewarded to miners rather than block rewards on LPoS, in contrast to other blockchains.

- **Benefits of Leased Proof of Stake (LPoS)**

  - On a normal proof-of-stake network, every node has the capacity to create a new block and add it to the blockchain. In a Leased Proof-of-Stake setting, users have the choice of running a full node or leasing their stake to a full node while still receiving rewards. This method allows anyone to participate in the Waves network maintenance.
  - In a Proof of Stake network, validators are selected based on their stake. This raises concerns about the system's fairness when some nodes are consistently selected. In LPoS, users can, however, potentially improve their selection odds by accepting a lease from another user.
  - LPoS enables minor token holders to earn money by renting out their limited tokens to full node owners. So, a portion of the money earned by the entire network goes to minority token owners.
  - Leased tokens are automatically locked and cannot be exchanged or transferred. Although the locked money are not usable, the lessor does have the ability to end the lease and release the leased funds for usage.
  - A lease can be started using a mobile phone. A work that previously required many nodes with significant computer power can now be completed by a small group of nodes with the help of phone users, saving energy.
  - LPoS-based systems are rapid and efficient because only a few nodes are involved in verifying a transaction at once.

- **Disadvantages of Leased Proof of Stake (LPoS):** On the LPoS, where users lease to a single full node, heinous acts can be planned. This node has an advantage over other nodes because it will always be in front of the validators' pool and favored to validate blocks of transactions.

3. **Proof of Capacity (PoC):** Proof-of-capacity (PoC), also known as proof-of-space (PoSpace), is a method for proving one's legitimate interest in a service (such as sending an email) by allocating a significant amount of memory or disc space to solve a challenge posed by the service provider. The concept was created in 2015 by Dziembowski et al. and independently by Ateniese et al. Proofs of capacity are very similar to proofs of labour, however instead of using calculation, proofs of capacity employ storage.

- **How Proof of Capacity (PoC) Works?**
  The two-step proof-of-capacity methodology consists of mining and plotting.

- **Plotting Process:**

  - Full nodes or miners must set aside some storage space before mining even begins to store the list of potential solutions. This action is referred to as "plotting."
  - The hashing algorithm is used to each nonce kept in the blockchain header during the plotting stage. The results of this hashing are kept in a brand-new file known as a plot file.
  - A list of hashes that match the header values may be found in the plot file. Miners can begin mining by validating blocks and adding them to the chain after the plotting procedure is finished.

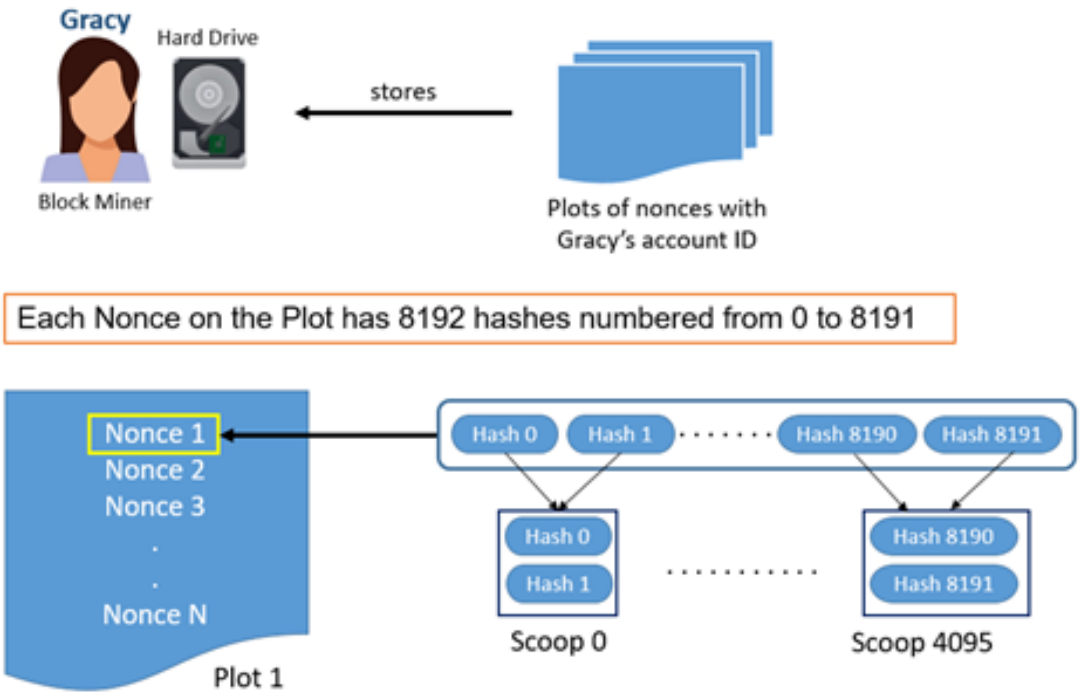

Figure 8: Working Process of PoC

- **Plotting the Hard Drive**

  - Creating a list of every possible nonce value using cryptographic hashing techniques like SHA-256.
  - The list of probable nonces is a plot, where each plot has a unique account ID.
  - Account ID enables the separation of miner plot files even when the nonce numbers are the same.
  - Data is hashed by Burstcoin (which uses PoC) using the Shabal 256 hash function. The result is a 256-bit (32 byte) hash.
  - Each nonce on the list has 8192 hashes, with values ranging from 0 to 8191.
  - The adjoining hashes of a nonce are paired into 4096 scoops. As an illustration, hash 0 and 1 yield scoop 0, but hash 2 and 3 yield 1 and more.
  - 64 bytes of data with two hash values make up each scoop. The PoC's sample produced plot value is depicted in the figure.

- **Mining the Block**

  - Here, the miner calculates the scoop number mathematically. The scoop number can then be used to create scoop data.
  - The value of a deadline is determined using the scoop data.
  - Deadlines are calculated iteratively until every nonce on the hard disc has been utilised. As a result, the miner selects the minimum deadline.
  - Therefore, a miner must set a minimal deadline so that they can add their block after it.
  - However, if another miner sets a shorter deadline and pushes back the current deadline, he will still have the opportunity to add his block. As a result, he gets the block reward.
  - Examples for PoC
    - Permacoin,
    - SpaceMint,
    - Burstcoin
    - Chia
    - Storj
    - Safe

- **Pros of Proof of Capacity**

  - **Compatible:** Any standard hard drive, even those used by Android-based systems, is compatible with the PoC.
  - **Cheap:** Storage costs are very cheap.
  - **ASIC Resistant:** It is allegedly up to 30 times more energy efficient than bitcoin cryptocurrency ASIC-based mining.
  - **Hardware Requirements:** There is no requirement for specialized hardware or ongoing hard disk upgrades.
  - **Data Storage:** Mining data may be quickly deleted, allowing the disk to be used for other types of data storage.

- **Cons of Proof of Capacity**

  - Few developers have started using the system.
  - **Susceptible to Grinding Attacks:** Malware has the potential to interfere with mining operations.
  - The widespread use of PoC might ignite a "arms race" to create hard drives with greater storage capacities.
  - **Increased Space Requirements:** • A greater need for space Even though it is inexpensive, if the algorithm doesn't distribute the load appropriately and equally, additional storage may be needed.

4. **Proof of Burn (PoB):** This algorithm offers a less energy-intensive alternative to PoW and PoS. The idea behind it is to let miners "burn" tokens of digital money. The right to write blocks is then handed to them in accordance with the amount of money burned. In the proof of burn consensus mechanism, users of the network must "burn" (or destroy) a specified number of coins in order to participate. The more coins a user burns, the more likely it is that they will be chosen as a validator. Validators are rewarded with newly created currencies and transaction fees. PoB seeks to emulate the idea of proof of work (PoW), the original consensus method of Bitcoin, without the burdensome hardware and excessive energy consumption.

   - **Why Proof of Burn Required?**
     Because of several drawbacks in the PoW consensus algorithm, researchers created the PoB consensus algorithm.

     - The primary drawback of PoW is how much power it uses. By updating the ledger, miners are rewarded via a POW process.
     - A mathematical problem is solved using processing resources in return for cash.
     - PoW requires very big cash commitments, and the more money a miner puts into solving the problem, the more likely it is that they will be given permission to mine blocks.
     - PoW demands very significant capital commitments.

   - **Proof of Burn (PoB):** The validators use PoB and adopt the following strategy rather than shelling out cash for expensive hardware equipment:

     - By delivering the money to a place from which it cannot be retrieved, they destroy it.
     - Burning money therefore implies a long-term commitment on the part of validators in exchange for a temporary loss.
     - Validators gain the right to mine on the network based on a random selection process by committing the coins to an unreachable address.
     - Miners may burn either the native money of the Blockchain application or the currency of an alternative chain, such as bitcoin, depending on how the PoB is implemented.
     - Validators' chances of getting chosen to mine the upcoming block increase with the amount of money they burn.

- **How Proof of Burn (PoB) Works?**

  - As implied by the word, anything must be burned. It is clear that PoB burns virtual currency because we are talking about it in this context. As more of the cash is burned by miners, their ability to build blocks grows.
  - When we say that, we don't necessarily intend to burn. Alternatively, avoid using that currency. This is possible if it is delivered to a location where it cannot be used. Miners send these currencies to these addresses to prevent their use. It is sent to a location that is open to the public, yet it cannot be accessed and is therefore useless.
  - When a coin is burned, its supply is reduced, potentially increasing the coin's value.
  - The question "Why do we need to burn the coin?" must now be considered by us. The primary argument for this is that the client is showing a strong commitment to the money by destroying it by forgoing a short-term advantage in favour of a long-term profit.
  - To prevent unfair advantages for early adopters, the PoB has created a system that allows the periodic burning of cryptocurrency tokens to maintain mining capacity. Coin energy burns somewhat less when a new block is mined.
  - According to this deflationary theory, as the number of currencies gradually declines, the deficit rises and, as a result, so does the value of the currency holders. Coins, on the other hand, tend to lose value over time as their supply grows.

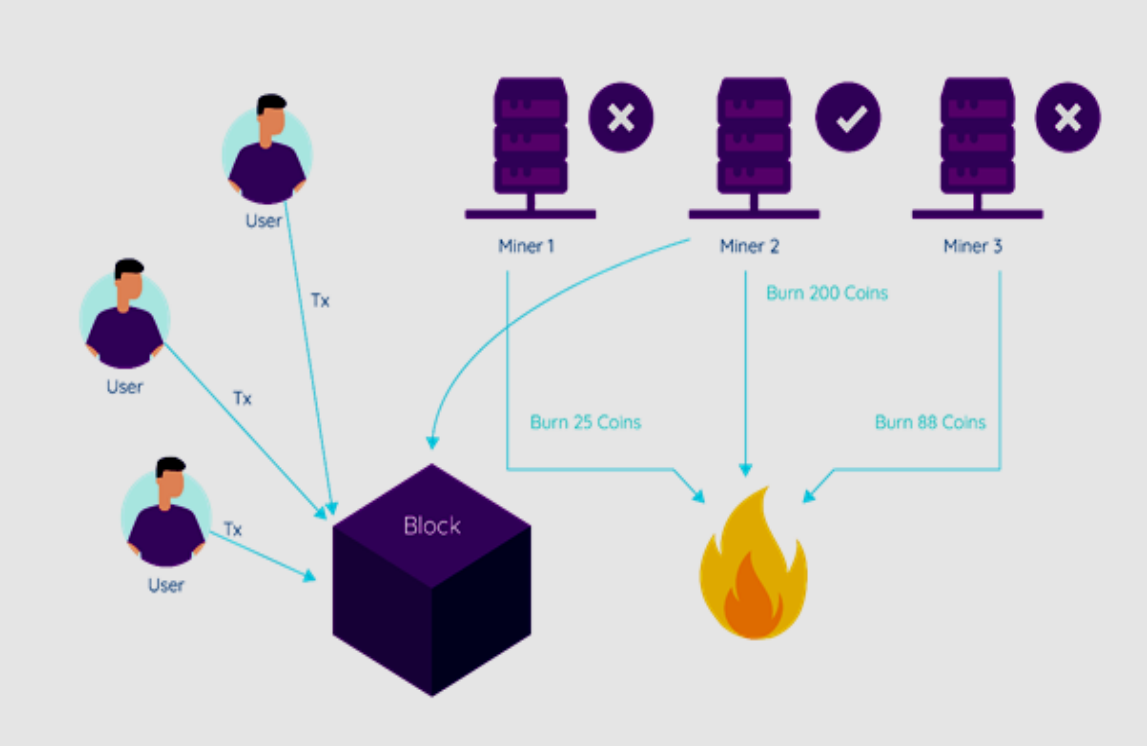

Figure 9: Working Process of Proof of Burn

- **Advantages of PoB**

➢ More long-lasting. decreased use of electricity.
➢ No demand for mining equipment. Coin burns are fictitious mining equipment.
➢ Burning coins results in less money in circulation (market scarcity).
➢ Promotes the miners' continued dedication.
➢ Coin mining and distribution are typically less centralized

.

- **Disadvantages of PoB**

  ➢ Some claim that PoB is not really environmentally benign because PoW mining, which uses a lot of energy, creates the Bitcoins that are burned.
  ➢ Not shown to be effective on bigger scales. To confirm its effectiveness and security, additional testing is required.
  ➢ The verification of the miners' work frequently takes longer than expected. It is slower than in blockchains with proof of work.
  ➢ The burning of coins is not always transparent or simple for the typical user to verify.

  Example cryptocurrencies used a PoB such as Slimcoin (SLM), Counterparty (XCP), and Factom (FCT).

  - **Proof of burn has some advantages over proof of stake and proof of work.**
  - First, it reduces the risk of centralization and collusion, as the validators have to prove their commitment to the network by burning their own coins.
  - Second, it eliminates the problem of "nothing at stake", which occurs when validators have no incentive to act honestly and can stake on multiple competing chains.
  - Third, it creates a deflationary effect on the coin supply, as the burned coins are permanently removed from circulation.

5. **Proof of Identity (PoI):** PoI (Proof of Identity) is a notion that is similar to authorized identity. It is a piece of cryptographic indication that a user's private key is associated with a certain transaction. A block of data can be created and managed by each identifiable user and made available to other network users. The produced data's validity and integrity are guaranteed by the blockchain consensus model. This mechanism mostly used in the permissioned blockchain networks; here the user nodes are already registered nodes. Gavin Wood, a co-founder of Ethereum and Parity Technologies, made the term official in 2017.

   - **How PoI working?**

     It is works like Proof of Authority (PoA) consensus mechanism.
     ➢ In PoA, nodes who have proven their authority to do so are given permission to spawn new blocks. The nodes that run the software that enables them to add transactions to blocks are referred to as "Validators" since they do so. Validators do not need to constantly monitor their computers because the procedure is

automated, but they do need to keep them secure. PoA is suitable for distributed-trust private and public networks, such the POA Network.

- Why Block validators stake their reputations rather than actual money since the PoA consensus mechanism takes use of the value of identities. PoA is safeguarded through trust in the selected identities.

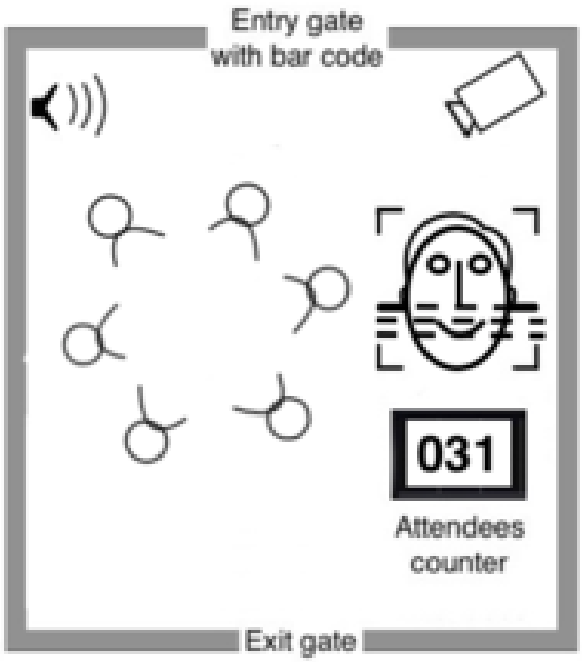

Figure 10: Working of Proof of Authority Consensus Mechanism

- **Conditions for PoA consensus:**
  Although PoA consensus may vary depending on implementation, they are often used in the following circumstances:

  - Candidates must be willing to put their reputation and financial investment at stake, and validators must attest to their actual identities.
  - A thorough selection procedure reduces the possibility of selecting suspect validators and promotes commitment to the blockchain over the long run.
  - The validators' identities must be verified in order to protect the blockchain's integrity, and the selection process must be equitable to all candidates. There must to be a process in place to select reliable validators.

- **Advantages of PoA Consensus :**

  - High risk tolerance provided that 51 percent of the nodes are not operating maliciously.
  - Predictable time interval at which new blocks are generated. This period varies for consensuses in PoW and PoS.
  - More transactions per second can be processed
  - Less processing power is required.

- Far more environmentally friendly than computationally intensive methods like Proof of Work.

- **Limitations of PoA Consensus :**

  - PoA is just an attempt to make centralized systems more effective; it is not decentralized.
  - PoA validators are open to everyone's view. Knowing the identities of validators may enable third-party tampering.

- **Application of PoA Consensus :**

  - The PoA consensus algorithm can be applied in a variety of circumstances and is an excellent choice for logistical applications like supply chains.
  - Thanks to the Proof of Authority method, businesses may maintain their anonymity while taking use of blockchain technology's benefits.
  - Microsoft Azure is just another instance of how PoA is employed. The Azure platform provides possibilities for private networks with a mechanism that does not require local currency like ether 'gas' on Ethereum because mining is not necessary. The utilisation of pre-selected Azure nodes.

6. Proof of Importance

- **What is Proof of Importance (PoI)?**
  Since the invention of blockchain technology and the Proof of Work (PoW) consensus procedures to authenticate a new node or any transaction taking place over the blockchain, Proof of Importance (PoI), a new consensus mechanism based on Byzantine Fault Tolerance, has been introduced. NEM (New Economy Movement) established the Proof-of-Importance (PoI) blockchain consensus method, which is a development of the Proof of Stake (PoS) algorithm.

  - Prior to being allowed to mine blocks in PoI, nodes must vest a certain number of coins that correspond to the score reflecting the contribution they provided to the network.
  - In contrast to Proof of Stake (PoS), the score is determined by a variety of variables, such as the overall sum, activity clusters, reputation, and transactions carried out through a certain address.

- **How does Proof of Importance (PoI) Work?**
  'Harvesting' or'vesting' is the process of figuring out which nodes in the network are qualified to add a block to the blockchain, and it uses the Proof of Importance mechanism.

  Nodes can obtain the transaction fees contained in a block, which the validator receives as payment for validating it, in exchange for harvesting that block.

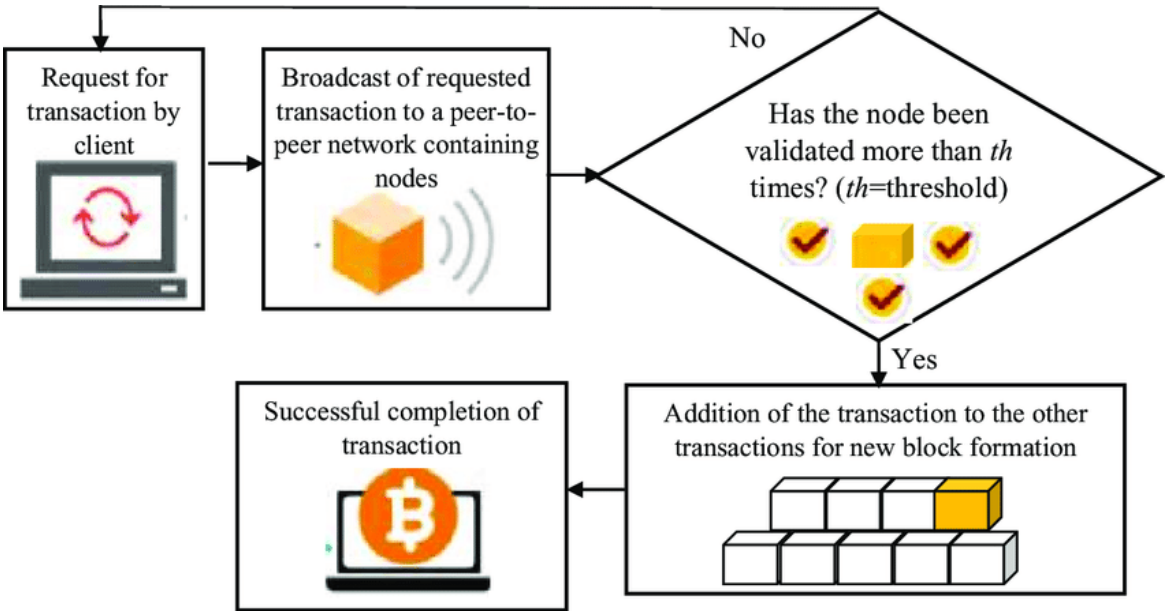

Figure 11: Working process of Proof of Importance (PoI)

For the purpose of determining an account's overall network support or score, NEM assesses the three critical aspects listed below:

- **Vesting:** The most crucial element of this consensus mechanism is vesting, also known as harvesting. Before any node can begin harvesting or vesting, they must first have at least 10,000 XEM coins. For the purpose of determining the node's Proof of Importance score, the consensus mechanism counts the quantity of coins that have been in your account for a predetermined period of time (often 30 days). As a result, the node will score higher the more XEM coins it has.
- **Transaction partnership:** Proof of relevance recognises two NEM accounts as partners and compensates users who perform network transactions using distinct NEM accounts. The network theory computation analyses transaction behaviour to give each node a score for relevance and prevent the user from building any false relationships.
- **Transaction volume and size:** Each transaction that exceeds a predetermined threshold has an impact on the Importance score and increases the likelihood that a block can be harvested to obtain rewards. The PoI score on the NEM network, which is based on the transactions a node conducts over the course of 30 days, will rise with larger and more frequent transactions.

- **Benefits of Proof of Importance (PoI)**

  - Energy Efficient
  - Discourage coin hoarding and promote transaction
  - Lower Incentive
  - Discourages Forks

7. **Proof of Activity (PoA):** Proof of Activity is a blend of proof of work (PoW) and proof of Stake (PoS) mechanism.

- **How does the Proof of Activity (PoA) Algorithm work?**
  - Process of Mining the Block (by Miners): Similar to PoW, miners attempt to submit their nearly empty block (with header information and miner's reward address) by obtaining the right nonce and block hash by solving a challenging mathematical challenge.
  - Process of Signing the Block (by Validators)

- The Proof of Stake (PoS) technique is used in this stage to leverage network validators. Validators and miners are independent entities in this case, though.
- The block that the miners have submitted is validated by a group of network users known as validators (or signers). These network validators are chosen according to the network currency they hold. A validator has the greatest probability of having their signed block selected the more bitcoin they have.
- Blocks are classified as signed or unsigned by validators after they have examined the header data and the reward address provided by the miners.

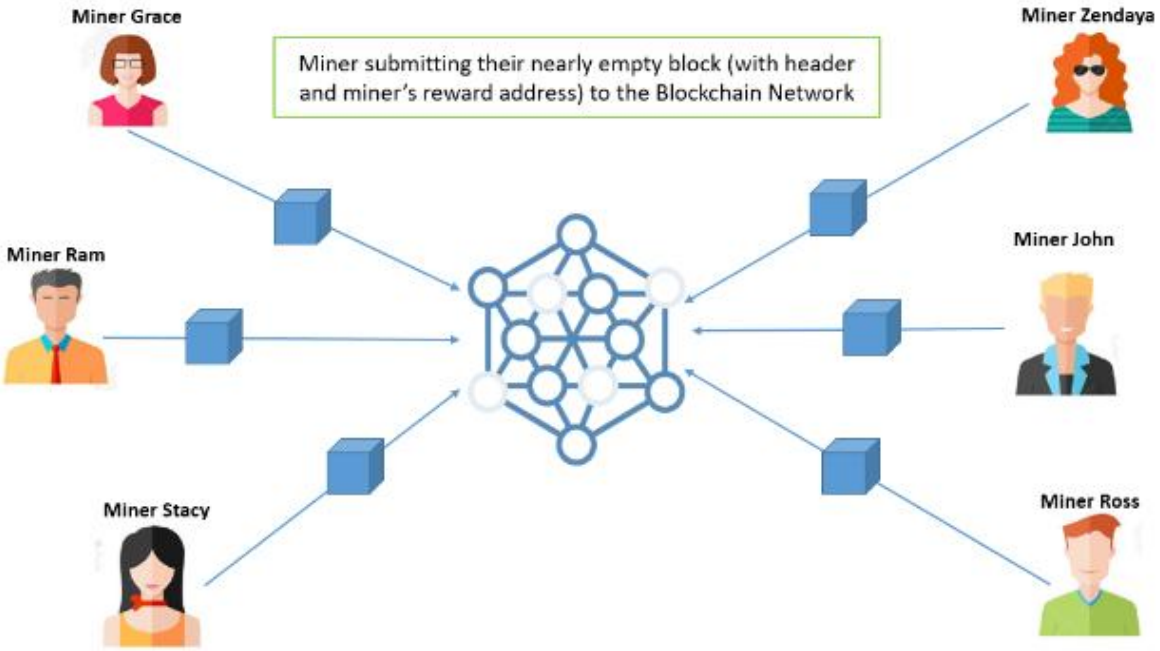

Figure 12: Process of Proof of Activity

- **Adding Transactions**
  - Once the required amount of validators have signed a block. It designates a legitimate and entire block. The block is then supplemented by fresh transactions from the transaction pool. The block is then included in the blockchain network.
  - The miner of the winning block and the validators share the mining reward in appreciation of their network-wide service.

- The most well-known cryptocurrency that makes use of proof of activity is Decred (D-Cred).

- **Advantages of Proof of Activity**

  - PoW and PoS's digital signing and hashing systems are combined to form PoA.
  - It significantly lowers the likelihood of a 51% attack on the network.
  - maintains the network's protection challenge level.
  - Due to the fact that the system will never completely shut down, PoA has excellent fault tolerance.
  - Give network validators and miners the chance to earn money.

- **Proof of Activity (PoA) Restrictions**

  These are the drawbacks of the mechanism for proving activity:
  - Excessive energy use when mining bricks.
  - The mining process is time-consuming since it requires extensive calculation.
  - Costly gear is needed for calculation.
  - Internal disagreements and a bad reputation result from the fact that neither miners nor validators have anything to gain.
  - Because of a lack of interest, there can be fewer validators.

8. **Proof of Elapsed Time (PoET):** The network consensus mechanism known as Proof of Elapsed Time (PoET) guards against excessive resource use and power consumption. To maintain the process' efficiency, a fair lottery technique is used. It is introduced in the year 2016 by Intel Corporation.

   - **How PoET works?**

     This technique, which is based on Byzantine Fault Tolerance, tries to cut down on the energy needed for the mining phase of proof of work.

     - Each node in the network receives a random length of time according to this procedure.
     - For that arbitrary waiting period, the node must rest or perform some other work.
     - The node with the shortest waiting time gets up and joins the network with its block.
     - The network's users are inundated with the most recent information.

   - **For PoEt to Succeed, these 3 Conditions Must be Met.**
     - Ensure that the random waiting time is delivered to the node in its place.
     - Make sure the nodes aren't choosing the shortest wait time on purpose.
     - Verify whether a node has completed the required waiting period.

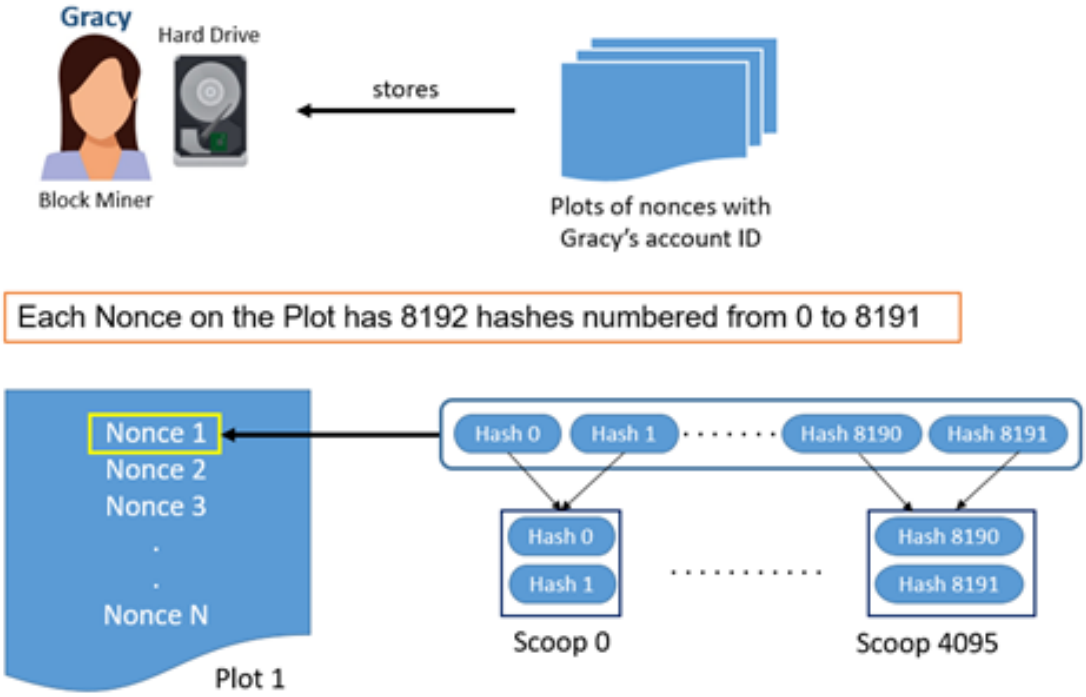

Figure 13: Process of PoET Consensus Mechanism

With the PoET method, a randomized timed scheme takes the place of the Proof of Work's requirement for mining-intensive rights. Every node is likely to be chosen by a fair lottery system according to the PoET consensus mechanism, which distributes the odds of winning across the greatest number of network users feasible.

Phases 1 and 2 of the PoET consensus method are as follows:

❖ **Selection Process:** The following tasks are included in this process:

- Every node in the network will exchange its certificate using Intel Software Guard Extension (SGX), verifying that it is legitimate for adding a new block to the network. After that, the node is eligible to receive a timer object.
- The numbers are assigned to each node as a timer object by the Intel RAND, or random number generator. RAND generates inconsistent numbers that are hard to pinpoint.
- Each participating node's time object becomes active.

❖ **Generation Process:** The following actions are part of this process:

- When the timer object expires and the node wakes up, it is then permitted to create a new block for the network.
- A hash of the transactions in the active node's block is produced and sent for approval.
- The network is inundated with the update.

Thus, utilizing the PoET consensus method, mining a new block in a permissioned blockchain network comes to a stop at this point.

Figure 14: End Point of the PoET Consensus Algorithm

- **Benefits of PoET**

  - **Less energy use:** PoET uses a small amount of electricity, and because nodes can "go to sleep" and move to other duties for the designated period of time, the network is both time and energy efficient.
  - **Requires fewer resources:** PoET provides a great solution to the "Random Leader Selection Problem" without requiring a lot of resources or intricate procedures. Because it lets the network to reach consensus more quickly, allowing for quicker transaction processing, it is easily scalable.
  - **High Transaction rate:** PoET has a high transaction rate that can reach one million per second.
  - **Equal opportunity:** PoET gives network participants with time object and activation the similar opportunity.
  - **Permissioned:** The choice of validators ensures network security against cyberattacks in a permissioned blockchain network.

- **Limitations of PoET:**

  - **Specialized hardware required**: Despite being inexpensive, the Proof of Elapsed Time consensus process requires specialized hardware, making it inaccessible to most users.
  - **Compatibility problems:** PoET heavily relies on Intel technology, which could cause problems with other tools.

❖ **Byzantine Fault Tolerance:** Byzantine Error the Byzantine Generals Problem, also known as the Byzantine Fault, is a situation where the system's actors must agree on a workable plan to prevent the system from failing catastrophically, but some of them are unsure. As the name suggests, tolerance is used to address this issue.

The most widely used BFT consensus model versions in the blockchain community are PBFT and DBFT.

- **Practical Byzantine Fault Tolerance**

- PBFT is a straightforward blockchain algorithm that resolves the problems with the Byzantine General by enabling users to verify the messages that have been relayed to them by conducting a computation to assess the decision regarding the message's authenticity.
- The party then communicates its choice to more nodes, who eventually decide on it. In this manner, the final choice is based on the information gathered from the other nodes.
- Some applications of this blockchain consensus process include Stellar, Ripple, and Hyperledger Fabric.

- **How pBFT works?**

pBFT seeks to provide byzantine state machine replication that can run even in the presence of malicious nodes.A

- The nodes of a distributed system with pBFT support are sequentially ordered, with one node acting as the primary (also known as the leader node) and the others as secondary (also known as backup nodes).
- It should be remembered that any system node that qualifies can change its status from secondary to primary at any time (often in the event of a primary node failure).
- The goal is for all reliable nodes to collaborate in using the majority rule to determine the present state of the system.
- A beneficial Byzantine fault that allows tolerant systems to function as long as the proportion of malicious nodes is kept under or at one-third of the total number of nodes in the system. As the number of nodes increases, the system gets more secure.

In order to provide a useful Byzantine state machine replication, pBFT divides consensus rounds into 4 phases (see the graphic below for a reference):

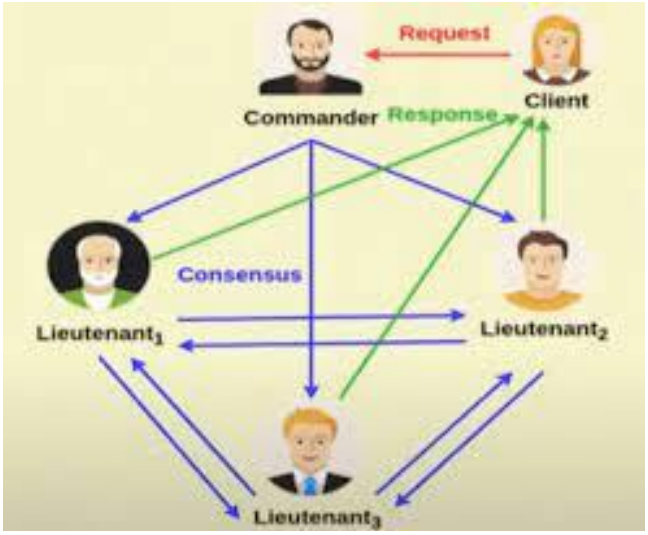

Figure 15: Working Process of PBFT

- The client makes a request to the principal (leading) node.
- The principal (leader) node broadcasts the request to all secondary (backup) nodes.
- The nodes (main and secondary) respond to the client after completing the requested service.
- When the client receives'm+1' responses with the same result from various network nodes, where m is the maximum number of erroneous nodes allowed, the request is considered to have been successfully made.

Every view (pBFT consensus round) requires switching the primary (leader) node; however, if a preset length of time has passed without the leading node broadcasting a request to the backups (secondary), a view change protocol can be used in its place. If necessary, a majority of the honest nodes voting on the legitimacy of the current leading node may choose the subsequent leading node in line.

- **Limitations of pBFT:**

  - **Communication Overhead:** The pBFT consensus model only performs well when the number of nodes in the distributed network is modest due to the significant communication overhead that increases exponentially with each additional node in the network.
  - **Sybil attacks:** The pBFT mechanisms are at risk from sybil assaults, in which one individual (party) controls multiple identities. As the network's nodes increase in size, Sybil attacks become more difficult to carry out. However, additional processes are used in addition to the pBFT mechanism since pBFT techniques also have scaling issues.
  - **Scaling:** pBFT does not scale well due to its communication overhead (with all the other nodes at every step). The time it takes to respond to a request grows as O(nk), where n is the number of messages and k is the number of nodes, in proportion to the number of nodes in the network.

❖ **Delegated Byzantine Fault Tolerance** The Delegated Byzantine Fault Tolerance technique, introduced by NEO, is comparable to the DPoS consensus paradigm. Holders of NEO tokens have the chance to elect the delegates in this case as well. By digitising assets and providing smart contracts on the blockchain, this sort of Blockchain consensus protocol, also known as "Ethereum of China," can be a valuable tool in creating a "smart economy."

- **How does the dBFT mechanism works?**

  Delegated Proof-of-Stake is comparable to the dBFT consensus algorithm. Holders of NEO tokens have the option to choose delegates through a voting mechanism. No matter how much money they have in their possession, this is.

  - As long as they match the conditions, anyone can serve as a delegate. This entails a dependable internet connection, the appropriate tools, a verified identity, and 1,000 GAS, the incentive users receive for their network activity. A speaker from among the delegates is selected at random.

- Out of the transactions awaiting verification, the speaker creates a new block. The chosen delegates will then receive the proposal from the speaker. They have a duty to keep an eye on every transaction and record it on the network.
- The suggestion is open for discussion and comparison by the delegates in order to assess the speaker's sincerity and the veracity of the information. The block is submitted to the blockchain if more than two-thirds of the delegates approve and confirm it.

In the NEO network, voting takes place in real time.

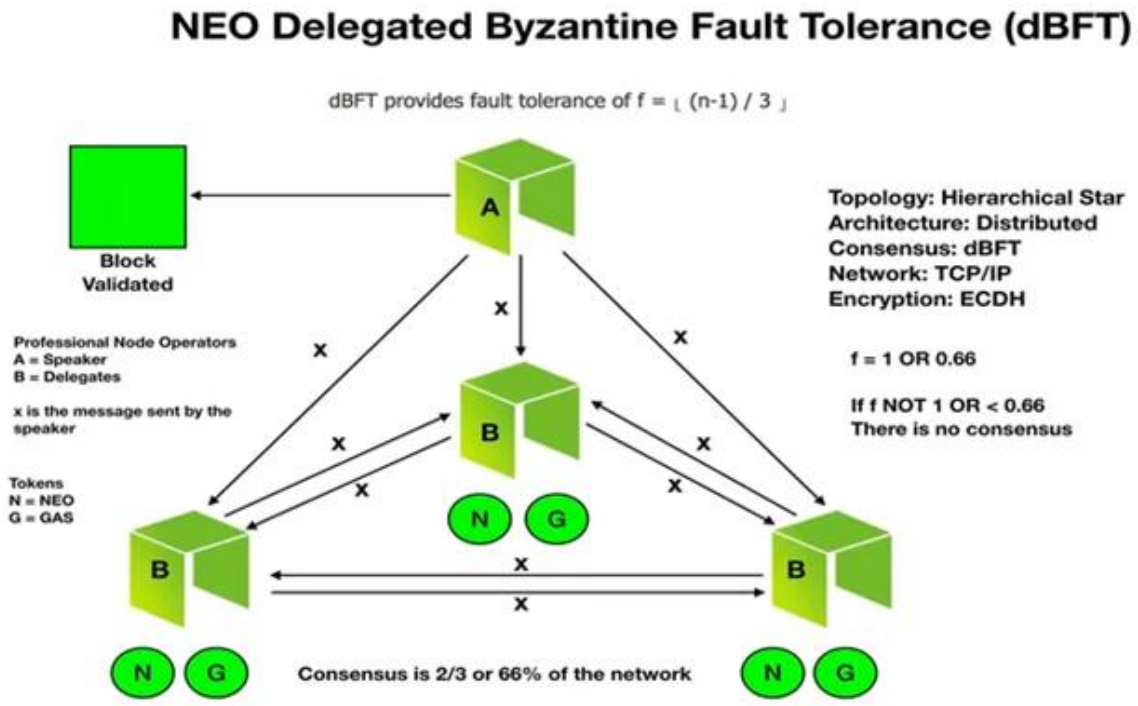

Figure 16: Working of dBFT Consensus

- **dBFT pros:**
  - A new block on the chain needs to be generated every 15 to 20 seconds.
  - The throughput of transactions is very nearly 1,000 TPS. In order for the network to enable significant commercial applications, NEO intends to attain 100,000 TPS.
  - No energy expenditure is required (in contrast to the Proof-of-Work consensus technique).
  - Complete closure of transactions following confirmation.
  - The NEO blockchain does not have any forks.

- **dBFT Cons:**
  - There is no anonymity on the blockchain since delegate operations must be conducted using real identities in order to be elected.
  - A certain degree of centralization—exactly what blockchains like Bitcoin and Ethereum are aiming for—is a need of the mechanism for regulated blockchains.

VI. FUTURE OF CONSENSUS MECHANISMS

Consensus methods are essential in distributed ledger networks used by businesses and are employed by all cryptocurrencies. Platforms for corporate and government usage have been developed, enabling each organisation to select modules tailored to their requirements and supported by consensus procedures. One of the more well-known distributed ledger technologies, Hyperledger Fabric, offers a variety of consensus algorithms. One entity might not require proof-of-work, which is regarded as being byzantine fault tolerant, while another might not.

Although the future of cryptocurrency is uncertain and unstable, consensus methods are still a crucial component of new technologies. They protect the security and integrity of data and prevent individuals with malicious intentions from accessing distributed ledgers.

Due to the distributed structure of the blockchain payment technology, there is no single centralised authority. As a result, there is minimal control of the systems by central authorities. Customers may now confidently expect the system to provide them with the complete security they require.

REFERENCES

[1] Qihao Bao, Bixin Li, Tianyuan Hu, Xueyong Sun, "A survey of blockchain consensus safety and security: State-of-the-art, challenges, and future work", Journal of Systems and Software , Volume 196, February 2023, 111555.

[2] Nasim Nezhadsistani [a], Seyed Mojtaba Hosseini Bamakan [b], Naghmeh Sadat Moayedian , Chapter 9 - Blockchain consensus algorithms: Past, present, and future trends, Distributed Computing to Blockchain, Architecture, Technology, and Applications, 2023, Pages 145-171.

[3] X. Deng, K. Li, Z. Wang, J. Li and Z. Luo, "A Survey of Blockchain Consensus Algorithms," *2022 International Conference on Blockchain Technology and Information Security (ICBCTIS)*, Huaihua City, China, 2022, pp. 188-192, doi: 10.1109/ICBCTIS55569.2022.00050.

[4] Jannah Yusoff, Zarina Mohamad, Mohd Anuar, "A Review: Consensus Algorithms on Blockchain" written by *Jannah Yusoff, Zarina Mohamad, Mohd Anuar*, published by *Journal of Computer and Communications*, *Vol.10 No.9, 2022.*

[5] Huanliang Xiong, Muxi Chen, Canghai Wu, Yingding Zhao and Wenlong Yi, Research on Progress of Blockchain Consensus Algorithm: A Review on Recent Progress of Blockchain Consensus Algorithms", *Future Internet* 2022, *14*(2), 47; https://doi.org/10.3390/fi14020047

[6] Sivleen Kaur, Sheetal Chaturvedi, Aabha Sharma, and Jayaprakash Ka, **"** A Research Survey on Applications of Consensus Protocols in Blockchain" , Security and communication network, Volume 2021 | Article ID 6693731 | https://doi.org/10.1155/2021/6693731

[7] Rameez Yousuf;Zubair Jeelani;Dawood Ashraf Khan;Owais Bhat;Tawseef Ahmed Teli; (2021). *Consensus Algorithms in Blockchain-Based Cryptocurrencies. 2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT), (), –* . doi:10.1109/icaect49130.2021.9392489

[8] R. Yousuf, Z. Jeelani, D. A. Khan, O. Bhat and T. A. Teli, "Consensus Algorithms in Blockchain-Based Cryptocurrencies," *2021 International Conference on Advances in Electrical, Computing, Communication and Sustainable Technologies (ICAECT)*, Bhilai, India, 2021, pp. 1-6, doi: 10.1109/ICAECT49130.2021.9392489.

[9] Chaudhry, Natalia; Yousaf, Muhammad Murtaza (2018). *[IEEE 2018 12th International Conference on Open Source Systems and Technologies (ICOSST) - Lahore, Pakistan (2018.12.19-2018.12.21)] 2018 12th International Conference on Open Source Systems and Technologies (ICOSST) - Consensus Algorithms in Blockchain: Comparative Analysis, Challenges and Opportunities. , (), 54–63.* doi:10.1109/ICOSST.2018.8632190

[10] Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei and C. Qijun, "A review on consensus algorithm of blockchain," *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, Banff, AB, Canada, 2017, pp. 2567-2572, doi: 10.1109/SMC.2017.8123011.

