Comparative analysis of Consensus Algorithms in Blockchain Technologies

Ridha P.
3rd Year, Dept. of Computer Science & Engineering
RNS Institute of Technology
Bengaluru, India

Varnika Bagaria
3rd Year, Dept. of Computer Science & Engineering
RNS Institute of Technology
Bengaluru, India

Sampada K.S.
Dept. of Computer Science & Engineering
RNS Institute of Technology
Bengaluru, India

ABSTRACT
The blockchain is a decentralized framework that gives immutability, protection, security, and transparency. There is no central authority present to approve and check the transaction, yet every transaction in the Blockchain is viewed as totally secured and verified. This is conceivable simply because of the presence of the consensus convention which is a centerpiece of any Blockchain network. The consensus mechanism numerically permits millions of nodes spread throughout the planet to concur on the production of blocks. Thusly, consensus algorithms accomplish unwavering quality in the Blockchain arrangement and build up trust between obscure peers in a distributed processing environment.

Keywords
Blockchain, consensus, PoW, PoS, DPoS, PBFT

1. INTRODUCTION
Blockchains or distributed ledgers are frameworks that offer reliable support to a group of nodes or parties that don't completely confide in one another. Blockchains also contain many elements from cryptocurrencies, although a blockchain framework can be imagined without currency or value tokens[1]. The belief over the data is decreased radically, inflicting an increment in secrecy and safety concerns every day. The blockchain is a standout amongst other arising advancements for guaranteeing secrecy and protection by utilizing cryptological algorithms.

Blockchain technology is the compelling use of existing innovations like decentralization, hashing algorithm, HashCash,public ledger, public-key encoding, and consensus. Decentralization can be taken into consideration as the greatest significant viewpoint of the blockchain era. Essentially, decentralization is a stage where different peers can take an interest to create a block having a similar position or authority and coordinate among themselves.

Each companion associated will have a similar position to make adjustmentswithin the open record if appropriate. Each peer makes their separate network. Due to this any kind of failure of the network at any point doesn't influence the operation a lot[2]. A public ledger is evidence or testament of each fruitful transaction that is accessible and shareable to all its peers(Fig. 1).

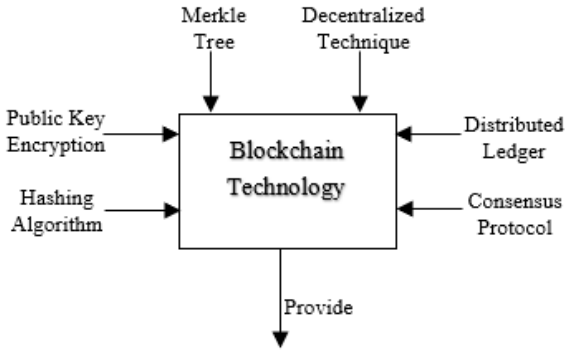

Fig 1: A component of blockchain and overview

The motivation behind this paper is to give an outline of consensus protocols being utilized with regards to consented blockchains, to survey the hidden standards, and to look at the flexibility and dependability of certain protocols.

The paper starts by bringing up the foundation and sorts of agreement conventions and proceeds onward to exploring some most significant agreement calculations and do a near investigation. The most typically utilized consensus algorithmsin blockchain technology are PoW,PoS, DPoS, and PBFT, along with anassortment of algorithms.

2. BACKGROUND AND TYPES OF CONSENSUS PROTOCOL
The most vital aspect of the whole blockchain system is the consensus algorithmbecause of its proficiencythat governs the blockchain's routineat once. The concept of HashCash was changed into recommended one with the aid of Adam Back in 1997. HashCash maybe a mining algorithm used as a PoW consensus procedure. One in all its makes use of is to confine mail and preservethestructure from denial of attacks. The HashCash is executed in the best manner by the brute force method[3]. The consensus is taken under consideration as the support of the entire blockchain. A lot many efficient consensus algorithms are recommended to urge the structure to be protected from any malevolent activity in blockchain technology: Proof of stake (PoS), Practical Byzantine Fault Tolerance (PBFT), Delegated proof of stake (DPoS), Proof of Work (PoW), and so on.

Consensus guarantees the achievement of rational decisions so each peer ought to approveif a transaction has to be committed or not. Blockchain makes use of the method of the nonce, Merkle tree, hash function, and others to supply data centralization, privacy and security, automation, transparency, smart contract, immutable ledger non-repudiation, and

tamper-proof replicated ledger, a replacement way of storing, and irreversibility of records.

3. CONSENSUS ALGORITHMS

3.1 Proof of Work

The PoW agreement system is to tackle the trust between nodes dependent on decentralization. The issue is that the blockchain can arrive at harmony among the numerous nodes.[4] The blockchain record has some straightforwardness, all agreement nodes are needed to affirm every single exchange before they arrive at an agreement. The question of reliability has established the framework for the safekeeping of the Bitcoin framework. When blockchain utilizes PoW for blockage, coordinating with Block Hash which comprises of N driving zeros which rely upon the trouble worth of the organization. To get a sensible Block Hash requires a plenty of preliminary estimations, the computation period relies upon:

- Machine's hash swiftness
- Size of network
- Number of blocks in the network

At the point when a node gives a fair Block Hash esteem, it shows that a great deal of preliminary estimations has occurred by the node. Notwithstanding, the absolute worth of the number of computations cannot be gotten by determining just a decenthash is a likelihood occasion. For instance, if a node has a registering force of n% of the whole organization, at that point the node has a likelihood of its hundredth to discover the Block Hash.

There are inspirations in the framework to urge clients to profit by keeping up the blockchain framework. The clients taking part in the agreement interaction gather the recently produced exchange record development block and endeavors to change the worth of nonce within the block till the hash worth of the block is lower than the hash value of the particular strain. The block is confirmed and endorsed by different clients. On the effective expansion of the principal chain, the client can get the relating reward.

To arrive at an agreement, the framework levels the node development block to take care of a difficult issue and puts its difficulty value to 'D'. 'D' characterizes the quantity of driving zeros is required for the present block hash value. The higher the quantity of driving zeroes, the higher is the difficulty. Since changing any piece in nonce will alter the hash H(B) of the whole block, it is highly unlikely to anticipate which type of nonce can satisfy the prerequisites. Subsequently, to arrive at the block necessities, the node utilizes its figuring assets to attempt countless potential qualities to such an extent that $H(B) < D$.

The way toward implanting the agreement calculation into the computerized currency structure is as demonstrated in Figure2:

1. Group the transactions needed for the block to be confirmed.
2. Each blockgathers the transaction records and makes anoriginal tree.
3. The server generates a mathematical puzzle.
4. The miners use registering assets to discover if the present difficulty value is satisfied by any of the nonces and contend to address the puzzle.
5. The miner that tracks down an attainable nonce arrangement communicates the block to the whole organization.
6. Others willcheck the block.
7. If the transaction made in the current block is substantial, and the difficultyvalue is satisfied by the hash, then this block is the best block amid every one of the forks.At that point,different legit nodes are allowed to build the subsequent blocks after this block.
8. Otherwise, the block is dropped and steps are rehashed from 1.[5]

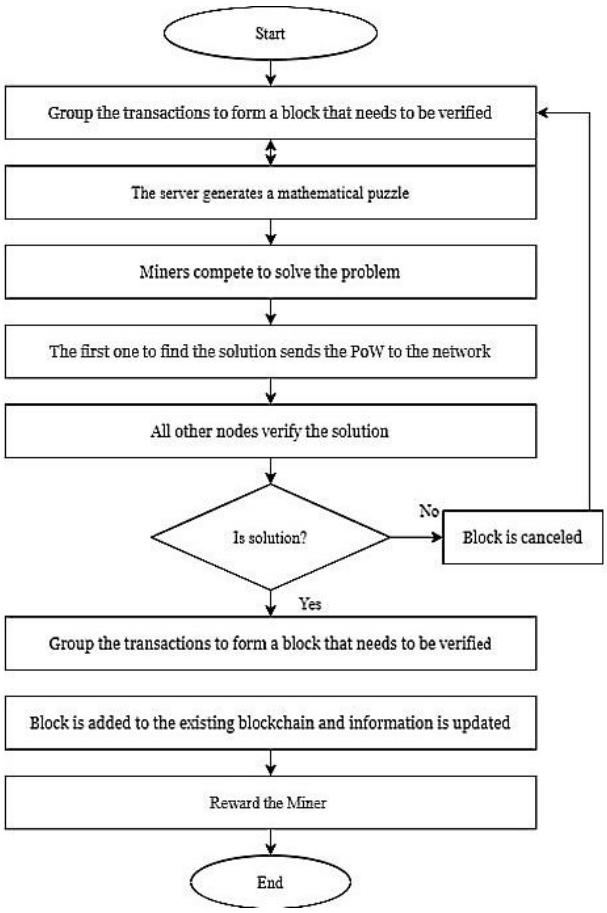

Fig 2: Flowchart of PoW

3.1.1 Advantages

1. *No human belief:*The decision of block makers is addressed by the node-tackling hash work. The nodes can arrive at an agreement without trading extra data. In the entire cycle, no human contribution is required.
2. *Very high reliability*: Harm to the framework requires an enormous venture, reliability is very high.
3. *Very high grade of decentralization:*The calculation is basic and simple to execute, the nodes can arrive openly, and hence the level of decentralization is at the peak.

3.1.2 Disadvantages

1. *Highaffirmation time*: To guarantee the level of decentralization, the affirmation time of the block is hard to abbreviate.
2. *Wastage of assets*: The trouble of mining, combined with the overhaul of equipment, bringing about two-fold misuse of equipment + assets.
3. *Poor expansion*: No irrevocability, the requirement for designated spot system to compensate for the absolution, yet the chance of arriving at an agreement with the increment in the number of affirmations has likewise expanded dramatically.

4. *The 51% risk:*In the event that a controlling substance claims 51% or over 51% of nodes in the organization, the element can ruin the blockchain by acquiring most of the organization.

3.1.3 Blockchains using Proof Of Work

- Litecoin
- Ethereum
- Monero coin
- Dogecoin

3.2 Proof of Stake

Proof of stake is associated with making the consensus mechanism completely virtual. In PoS, there are validators instead of miners or excavators. Like a stake within the ecosystem, these validators bolt up their crypto.[6] Taking after that, the block is included near the chain when the validator binds the block which he approves. The point when the block gets added, a block as aprize in relation to their stake is granted to the validator. PoS become first proposed via way of means of Quantum Technician and afterward Sunny King and his partner composed a paper subsequently. This prompted Proof-of-Stake (PoS) primarily based on Peercoin.

The consensus interplay of the blockchain is frequently visible as a pacesetter election mechanism that randomly selects the chief via a hard and fast mechanism, and consequently, the individual releases a replacement block, averting a single group or user to control the ledger for a significant time frame due to the unique information shape of the blockchain, A stake is the value/cashthat iswagered on a sure outcome. The technique is called staking. As comprehensible from the name, the charge is gathered when the nodes on a network stake a certain amount of cryptocurrency to approve the new block. At that point, an algorithm browses the pool of applicants, the node that could approve the new block. This choice set of rules combines the amount of stake with different variables to shape the decision reasonable for everybody in the network.

- Coin-age-based determination:The time for which each validator applicant node remains a validator is tracked and calculated. The more established the node turns into, the upper the probabilities of it turning into the new validator.
- Random Block selection: Based on the ‘lowest hash value’ and ‘highest stake’, the validator is selected. The best weighted-mixture node among the selected nodes turns into the new validator. [7]

During the time spent consensus, the node should present an exchange or transaction record to demonstrate the responsibility for blockchain resources. Simultaneously, the more blockchain resources that are claimed, the more extended the waiting time, the better the mining will be. The equity proof algorithm trusts that clients can make an exchange to themselves to demonstrate a specific figure of blockchain resources. The issue of mining the miners in the blockchainis influenced by these resources. Thus, the hashing issue we've to disentangle becomes:

$$Proofhash < coins \cdot age \cdot target \quad (2)$$

PoS calls for an exceptional deal of computing or processing strength to run special cryptographic calculations so as to unencumber the computational challenges. The computing strength interprets right into an excessive quantity of power and strength wished for the proof of work.

This implies that the person basically losestheir stake at whatever point they are doing an assault on a PoS framework, while in PoW the person doesnot lose their mining gear or their coins in the event that attack the framework; instead, they just make it difficult to execute.

In any case, one issue which might emerge is that the “nothing-at-stake” problem, wherein block generators don't have anything to lose with the aid of using identifying in desire of various blockchain histories, thereby stopping a consensus from being accomplished.

In PoS a person shall stake his or her resources on each side of the chain(“nothing-at-stake” problem)at the same time while in PoW he or she cannot mine on eachside.

*The impracticality of the 51% attack:*To lead a 51% assault, the attacker should possess 51% of the whole cryptographic money inside the network which is somewhat costly. There'll occur issues when hoarding such a portion of complete cryptographic money as there will not be a currency to purchase, likewise acquainting an ever-increasing number of coins/values will get costlier. It is considered a tedious way of doing the attack, costly, and not all that beneficial. The validator will lose its stake in case of approving an incorrect transaction, consequently being reward-negative[9].

A typical PoS based mechanism workflow is as shown in Figure 3:

1. Transactions are made by Nodes: A pool of transactions is collected based on the PoS algorithm.
2. To become a validator for the next block every node which is battling raises a stake. Upon joining with different component elements like 'coin-age determination' or 'randomized block determination' the stake picks the validator.
3. The validator checks and verifies each transaction and circulates the block. His stake actually is bolted and accordingly, the forging prize is likewise now no longer conceded at this point. This is in order that the nodes on the network can now ‘OK’ the new block.
4. The validator will get the stake back and thusly the prize as well, if and only if the block is ‘OK’-ed. In the event, if the set of rules is utilizing a coin-age-primarily based totally mechanism to choose validators, the coin-age is reset to 0 for that particular validator. This places him in a low need for the ensuing validator selection.
5. If the block isn't checked by different nodeson the network, the validator loses its stake and is set apart as 'bad' by the algorithm. The technique again begins from step 1 to forge the new block.

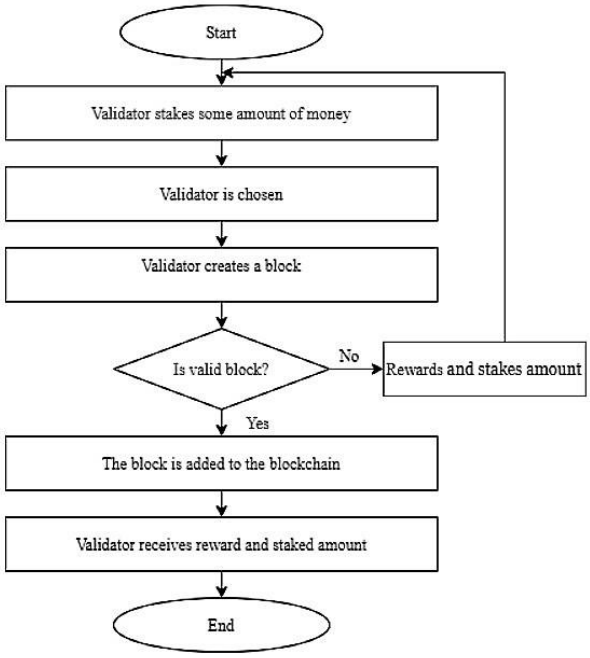

Fig 3: Flowchart of PoS

3.2.1 Advantages

1. *The confirmation time of the block is faster*: The block confirmation productivity is improved with the usage of the PoS consensus algorithm,as node mining just requires value evidence, which significantly lessens the ideal opportunity for consensus affirmation.
2. *Save resources*: Wastage of power and energy resources is reduced by mining, and accordingly, the cash is in a premium-bearing mode.

3.2.2 Disadvantages

1. *Security is poor:* Consists of perplexing execution rules and hence there are many moderate advances and lots of human factors included in order to get through safetyloops.
2. *Checkpoint*: There is no finality like how it is in the PoW consensus mechanism and to frame up for the certainty a designated checkpoint mechanism is essential.
3. *Matthew effect:* The whole measure of value under the PoS consensus system is duplicated by the measure of coins held at the time of protecting the currency. It's certain to frame a victor-bring-home-all-the-glory circumstance.
4. *Nothing-at-Stake attack*: Since mining doesn't cost, along these lines the fork assault achievement degree is amazingly inflated, it's smooth to split attack. Also, the person can effectively dispatch a fork assault even without a 51% premium.

3.2.3Blockchains using Proof-of-Stake

- Blackcoin
- Peercoin
- Nxt

3.3 Delegated Proof of Stake

Daniel Larimer proposed the Delegated Proof of Stake (DPoS) consensus estimation. Steem, Ark, Bitshares, and Lisk are a bit of the cryptocurrency projects that use the DPoS consensus algorithm.

DPoS (Designated Evidence of Stake) is the quickest, best, generally decentralized, and most adaptable consensus mechanism among all consensus algorithms.[10] The algorithm flow is shown in Figure 4. DPoS utilizes the privilege of stakeholders to endorse votes to take care of consensus issues in a popularity-based and reasonable way. All network boundaries, from cost assessment to block spacing and transaction size, can be changed by chosen delegates. The guideline is to allow every holder to cast a vote, bringing about a specific number of Representatives or Agents, which are confirmed and represented by these super-nodes for the benefit of the holder; the privileges of these super-nodes are equivalent. DPoS resembles the top board of directors voting. The coin holders cast a specific number of super-nodes. The chosen node produces blocks reciprocally, as indicated by the setup plan. In the event that a super-node neglects to practice its power appropriately, it will be taken out, and the network will choose another super-node to replace it.

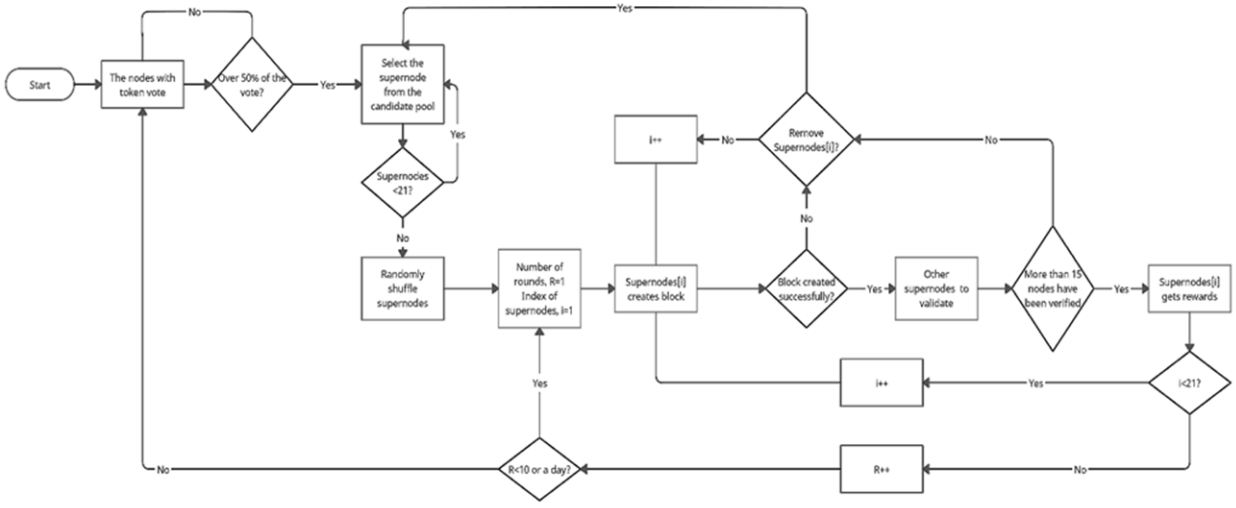

Fig 4: Algorithm of DPoS

DPoS's consensus process is divided into two processes namely - The witness's block and the witness's election decision measure. The transaction made is being witnessed or observed by the witness and the witness just checks the timestamp and the signature of the transaction and does not participate in the transaction. Every account in the network has the ability to decide in favor of its own witness. Hence,it could also be said that the number of votes the person can

have is directly proportional to the number of blockchain resources.

1. *Selection of the Witness*: The perpetual node with the option to make a choice recognizes the vote and picks the top N witnesses. The N votes will make up to 50% of the total. At regular customary intervals, the list of witnesses is rotated.
2. *Witnesses out of the block*:For every block being produced the witness are paid and based on the number of votes they received the salary levels are determined. The witness may not be paid if the witness doesn't have an original block, and maybe voted to drop the witness.[11]

The deterministic decision of block producers permits transactions to be affirmed in an average of one second. By shielding all members from pointless logical checks, DPoS incredibly diminishes the quantity of nodes participating in verification and accounting compared with the PoW and PoS algorithms. DPoS algorithm extraordinarily improves productivity and can arrive at the consensus verification at the second level. It doesn't have complete decentralization, yet has feeble centralization.

However, the plan of the DPoS algorithm doesn't ensure that there should be adequate genuine block makers. Due to an individual or an element may control numerous nodes, the entire framework might be significantly hoarded by one element. Simultaneously, the administrative power and economic interests of super-nodes are excessively centralized. If they conspire, they will shape a giant restraining infrastructure, which is at odds with the blockchain idea. Also, there are numerous challenges for the framework to manage the nodes. Community elections can't adequately forestall the development of some damaging nodes in time, which causes security risks to the network. Simultaneously, on account of few network nodes,the super-nodes elected are not delegated.

3.3.1Advantages

1. *Simple and proficient:*Altogether decrease the amount of partaking verification and bookkeeping nodes to get a second-level agreement confirmation.
2. *Assets are saved*: Only the primary node is required to authenticate the network.
3. High scalability: The strong furthest reaches in the primary network. Second-level identification, speedy block-out.
4. The whole agreement segment is based upon tokens, and numerous profitable applications needn't bother with tokens.

3.3.2 Disadvantages

1. *Centralization:*It reduces the number of verification nodes in the network, not the universal verification node, going astray from the fundamental connection among everybodywithin the blockchain world, which makes it unnecessary centralization
2. *The main network fails due to bribery:*The principal network vote can't be done notwithstanding the superseding node corruption to force the EOS administration befuddling and this is the remarkable EOS bribery issue.

3.3.3Blockchains using Delegated Proof Of Stake

- Bitshares
- Ark
- Lisk

3.4 Practical Byzantine Fault Tolerance Algorithm

Practical Byzantine Fault Tolerance is another consensus algorithm that was proposed by Miguel Castro and Barbara Liskov. Thiswas considered keeping in mind the asynchronous systems, to improve its efficiency. It has been mainly augmented for its low overhead period. Its main objective was to resolvethe existing problems relatedtoexisting Byzantine Fault Tolerance results.

PBFT is a state machine replica replication algorithm. In this, the state machinehas been displayed by the service, and therefore this performs replication at multiple nodes of the circulated system.[12]

A replica of every state machine saves the service condition and furthermore executes the service operation. A set comprising of everyduplicate is given by R, and every duplicate is ranged from 0 to |R|-1 and is an integer.

The entire algorithm operates reliably with the ensuing process as demonstrated in Figure 5.

1. There isa total of 3f + 1 nodes during the entire distributed framework, which can endure the Byzantine error nodes.
2. The customer then enquiresabout the calling facility from the first node.
3. The request to its secondary node will be multi-casted by the master node
4. The answer will be sent to the customer after the demand has been executed by the node
5. The customer will now receive f + 1 answers with an identical response andin additionto this,the customer now acquires the data he requested[13].

The PBFT agreement rounds are broken into five stages as demonstrated in Figure 6[14]:

1. *Request:* Customer sends a request to the primary.
2. *Pre-prepare:* Recognize a solitary succession number for the request
3. *Prepare:* The replicas agree on this succession number
4. *Commit:* Establish all-outorder across all the views
5. *Reply:* The replicas will directly send a response to the customer

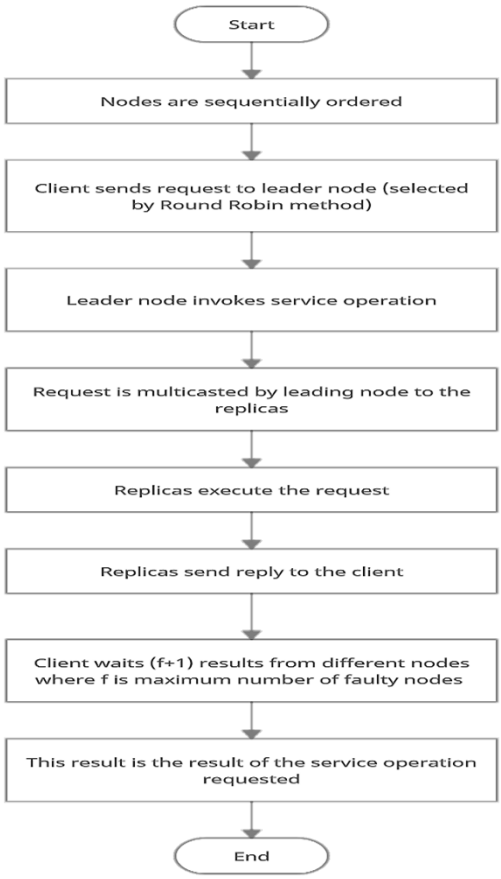

Fig 5: Flowchart of PBFT

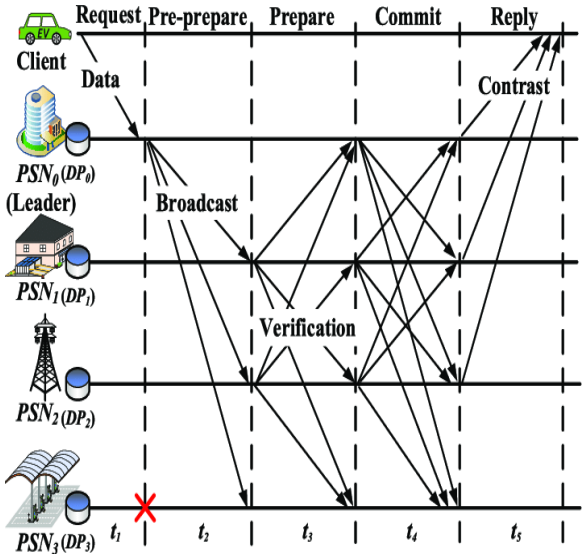

Fig 6: Phases of PBFT.

3.4.1Advantages

1. *Energy effectiveness*: PBFT can do distributed agreement without carrying out complex numerical calculations.
2. *Transaction finality:*The transactions don't require different confirmations' components in Bitcoin, in contrast to PoW.
3. *Low reward variance:*Every node inside the network partakes in responding to the request by the customer and consequently every node is regularly boosted resulting in low variance in rewarding the nodes that assistance in choosing.

3.4.2Disadvantages

1. *Low room of application:*It is applicable for onlyagreement chain and private chain
2. This framework has meager adaptability.
3. *The node of the system is fixed*: The node can be applied to only coalition chain or private.
4. *Low fault tolerance*: This algorithm wants the complete number of nodes that is n>=3f+1. The measure of the bombed nodes of the framework will not surpass one-third of the nodes of the entire framework, and therefore its adaptation to non-critical failure rate is comparatively low.
5. *Sybil attacks*: The PBFT systems are defenseless to Sybil assaults, where one substance controls numerous personalities. When the number of nodes in the network increase, Sybil assaults become increasingly hard to carry out.

3.4.3Blockchains using Practical Byzantine Fault Tolerance

- Zilliqa
- Hyperledger Fabric
- Tendermint

4. COMPARATIVE ANALYSIS

A brief comparison between the algorithms is as shown in Table 1:[15]

Table 1: Comparison

Consensus Protocols	Advantages	Disadvantages
PoW	Safe and stable High degree of decentralization, open node system	Weak scalability Low performanceHardware equipment waste
PoS	Less Energy High degree of decentralization, open node system	Complex implementation process Security breach
DPoS	Less Energy High performanceFinality	Weak degree of decentralization, closed node system
PBFT	HigherperformanceFinality High Security	Weak degree of decentralization, closed Low fault tolerance

5. CONCLUSION

This paper has summed up the absolute most noticeable blockchain agreement conventions. . By depicting its various prerequisites and circumstances, the internal execution, benefits, as well as hindrances of the four agreement calculations of PoW, PoS, DPoS, and BPFT are clarified. The overview of consensus protocols and their properties contributes to the present effort, by establishing a standard ground for formal protocol reviews and more technical comparisons. While PoW and PoS are the most mainstream choices, there are many mechanisms and instruments coming up occasionally. There is no consensus algorithm that is "perfect", and the probability is that that there never will be, however, it will be intriguing to notice each of these newer cryptocurrencies beginning with their protocols.

Currently,the PoW-PoS hybrid agreement instrument and Conflux Tree-Graph Consensus system are the focal points of study. It is likewise another course to utilize keenagreements to construct betterclear agreement rules. The new assault strategy can cause us to understand the deficiencies of the current agreement algorithm. Furthermore, for agreement calculations on the license chain, pluggable switchable is a trend. For various throughput necessities, business situations, and safety, diverse fundamental consensus components can be utilizedto serve high-level routines readily.

6. ACKNOWLEDGMENT

Our thanks to Prof. Sampada K. S., Assistant Professor, CSE Department, RNSIT for mentoring us to present this paper successfully

7. REFERENCES

[1] Christian Cachin Marko Vukoli´ "Blockchain Consensus Protocols in the Wild"

[2] Sigrid Seibold, George Samman "Consensus Immutable agreement for the Internet of Value"

[3] S. A. Xie, H. N. Dai, Z. B. Zheng, X. Chen and H. Wang "An overview of blockchain technology: Architecture consensus and future trends", Proc. IEEE Int. Congr. Big Data, pp. 557-564, Jun. 2017

[4] Parikshit Hooda"Proof of Work (PoW) Consensus"

[5] Karan Singh, Ashok Kumar Yadav"Comparative Analysis of Consensus Algorithms of Blockchain Technology"

[6] L. Ren "Proof of Stake Velocity: Building the Social Currency of the Digital Age", Apr. 2014, [online]

[7] Parikshit Hooda"Proof of Stake (PoS) in Blockchain"

[8] Vitalik Buterin "A Proof of Stake Design Philosophy"

[9] L. Ren "Proof of Stake Velocity: Building the Social Currency of the Digital Age", Apr. 2014, [online]

[10] Baocheng Wang 1,*, Zetao Li 1 and Haibin Li 2 "Hybrid Consensus Algorithm Based on ModifiedProof-of-Probability and DPoS"

[11] Baocheng Wang 1,*, Zetao Li 1 and Haibin Li 2 "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism "

[12] B. Liskov and M. Castro, "Practical Byzantine fault tolerance", Proc. Symp. Operating Syst. Design Implement., pp. 173-186, 1999.

[13] Ashok Kumar Yadav, Karan Singh "Comprehensive Study on Incorporation of Blockchain Technology With IoT Enterprises"

[14] Kashish Khullar "Implementing PBFT in Blockchain".

[15] HUPAYX "Consensus Algorithm= POW, PoS and DPoS".