ISSN 2278-3091
Volume 9, No.5, September - October 2020
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse323952020.pdf
https://doi.org/10.30534/ijatcse/2020/323952020

A Survey on Consensus Algorithms used in Blockchain Platforms

Devi Mukundan[1] , Dr.R.Sasikumar[2], Badi Alekhya [3] .Arun.S[4]
Assistant Professor[1] ,Professor[2] ,Research Scholar[3],IT Engineer[4]
R.M.D Engineering College[1,2,3], Royal Cyber Pvt.Ltd[4]
Kavaraipettai[1,2,3], Guindy [4] ,Tamil Nadu, India.
devimukundan92@gmail.com[1],
rsn.cse@rmd.ac.in[2],alekhyareddy1@gmail.com[3],arun.s@royalcyber.com[4]

ABSTRACT

Blockchain Technology is one of the widely appreciated technologies in recent years. It adopts decentralization where no central authority controls the network. Blockchain is a form of distributed ledger where each node in the network contains records of transactions called blocks. The block is linked to another block using a cryptographic hash. Though Bitcoin was the first implementation of the blockchain technology it can be used for a wide range of applications including finance, healthcare, banking etc. Today various platforms adopt blockchain technology. The consensus algorithm plays a main role in the blockchain architecture. The consensus algorithm decides how new blocks can be added to the blockchain. There are different consensus algorithms. Every blockchain platform adopts the consensus algorithm which they find to be more efficient according to their needs. In this paper, we discuss the various consensus algorithms that are used by the blockchain platforms, how they work and we also analyze their advantages and drawbacks. We also discuss how consensus is reached in some of the popular blockchain platforms. This paper can be used for further development and research in this area.

Key words- Blockchain, Consensus Algorithms, istributed ledger, Blockchain platforms

1. INTRODUCTION

THE role and impact of technology in our lives is evergrowing. people are open to accepting technologies that benefit them in their personal and working life. Blockchain is one such technology that can be applied for a wide range of applications including finance, healthcare, banking, supply chain management, real estate etc

In the earlier years, there have been various implementations similar to blockchain. In 1991, Stuart Haber and W.Scott Stornetta introduced their work on a cryptographically secured chain of blocks [1] that could be used to avoid the tampering of documents by introducing timestamps. This technique was not well utilized until it was improved in an important way, incorporated other techniques and introduced as a core component of the cryptocurrency Bitcoin [2] by Satoshi Nakamoto in 2008.

Bitcoin eliminates the need for a trusted third party as required in the conventional money transactions. Bitcoin uses a distributed ledger technology where all the transactions made by the nodes are available to all the nodes in the network. The records of transactions are called as the block. The blocks were linked to one another using a cryptographic hash, hence the name “Blockchain”.

Bitcoin has made the blockchain technology widely accepted. It finds application in various fields. Today, many companies are adopting Blockchain technology and developing blockchain-based applications that can improve the transparency and efficiency in business operations. IBM, Walmart are some of the giants that have incorporated blockchains in their applications. Blockchain platforms can be used for the development of blockchain-based applications. Numerous blockchain platforms have emerged in recent years and used in various business applications. Blockchain platforms can be public or private. Ethereum is one of the popular public blockchain platforms that use smart contracts to build decentralized applications. Blockchain can be applied to businesses that require high reliability and transparency to attract customers. Since blockchain uses distributed ledger it avoids a single point of failure.

Though blockchain technology has many advantages it also faces technical challenges. Scalability is one of the major concern that has to be dealt with [3] in blockchain based platforms. Different issues may arise due to transaction delays, increased transaction fees, blockchain congestion problem that needs to be addressed [4].

The rest of the paper is organized as follows. Section 2 Blockchain Architecture Section 3 Consensus Algorithms Section 4 Various Consensus Algorithms Section 5 Consensus of popular Blockchain Platforms Section 6 Conclusion.

2. BLOCKCHAIN ARCHITECTURE

A Blockchain is a chain of blocks where each block in the chain contains a number of transactions [5]. The blockchain

is a type of distributed ledger technology where all the Blocks similar to a ledger are distributed to all the participants of the blockchain network. Every time a new transaction occurs on the blockchain a record of that transaction is updated in every participant's ledger. The transactions that are added in the block are immutable. Figure.1 shows the transaction flow in blockchain.

Each block is identified by a hash on the header of the block. SHA256 cryptographic hash algorithm is used to generate the hash. Each block also contains the previous block hash in the block header, this connects this block to the previous block in the blockchain.

A block consists of two main parts the block header and the transactions. Transactions are the information that is saved in the blocks. The block header consists of some of the important fields such as block version, the Merkle tree roothash, timestamp, nBits, Nonce and parent block hash.

i) Block version: It contains version number to track the upgrades. [6]

ii) Merkle tree root hash: It is a hash that is obtained by the consolidation of all the transactions in the block. A Slight modification in any transaction in the block will change its Merkle tree root hash[7].

iii) Timestamp: current time as seconds in the universal time since January 1,1970[6].

iv)nBits: target threshold of a valid block hash[6].

v) Nonce: This is a 4-byte field, starts with 0 and keeps increasing for each hash calculation. The miner adjusts the nonce that it becomes a valid number that can be used for hashing the value of block[8].

vi) Parent block hash: a 256-bit hash value that points to the previous block[6].

There are three types of Blockchain. Public blockchain, Private Blockchain and consortium blockchain. In the public blockchain there is no restriction on the participants and validator of the network. Everyone can join or leave the network as they wish. Bitcoin and Ethereum are public blockchains. Private blockchain requires the participants to be invited before they can join the network. A Private blockchain can be used within an organization or enterprises where only employees of the organization or enterprise are part of the blockchain network. Multichain uses private blockchain. In the case of consortium blockchain instead of a single organization, multiple organization are in charge of the network. Only the group of network nodes that have been pre-approved are allowed tobe part of the consensus process. Hyperledger, Corda and Quorum are consortium blockchains. The public blockchain is also known as the permission less blockchain. The private blockchain and consortium blockchain are permissioned blockchains. Permissioned blockchains are faster, offers low-energy consumption and easier to implement when compared to permission less blockchain.

3. CONSENSUS ALGORITHMS

In Blockchains, there is no central authority that controls or ensures that all the ledgers in the distributed nodes are all the same. Trust needs to be accomplished among the nodes. Consensus algorithm , ensures that ledgers in the different nodes are consistent. The consensus algorithm is being used in distributed system from a very long time [9] . Consensus algorithms are one of the important concepts in

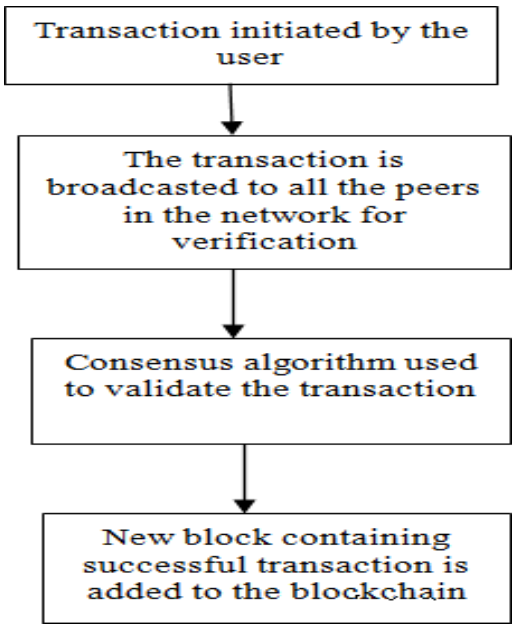

Figure 1: Transaction flow in Blockchain

blockchain that ensures that only the same truth is agreed by all the nodes. There are several popular consensus methods by which all the nodes in the network can reach agreement over a new block. The consensus algorithm needs to provide consistency, availability and partition fault tolerance[10].

Besides, the consensus protocol must also overcome the byzantine general's problem where there will be malicious nodes in the network that may deliberately work against the consensus process [11].

4. VARIOUS CONSENSUS ALGORITHMS

4.1 Proof of Work

The proof of work is the initial consensus algorithm introduced in the blockchain network. It was first implemented in bit coin [2] by Satoshi Nakamoto for managing the transactions in the bitcoin network. In proof of work, the miners who are the special nodes in the network validate the block before addingtheblocktotheblockchain.Theminersoftheblockcompeteagainsteachothertosolve a cryptographic puzzle. The puzzle involves hash function .The only way for the miner to find the hash is through brute-force inputs. The minerguessesuntiltheygettherighthash.Theminerwhosolvesthepuzzlewillbegiven the right to add the block in the blockchainandalsogetrewarded.Ittakesabout10minutestoaddablockinablockchain by this method.POW is called mining in bit coin. Figure.2 shows the flow of POW.

The proof of work offers defense against the DDOS attacks. Efficient attack requires a lot of time to do the

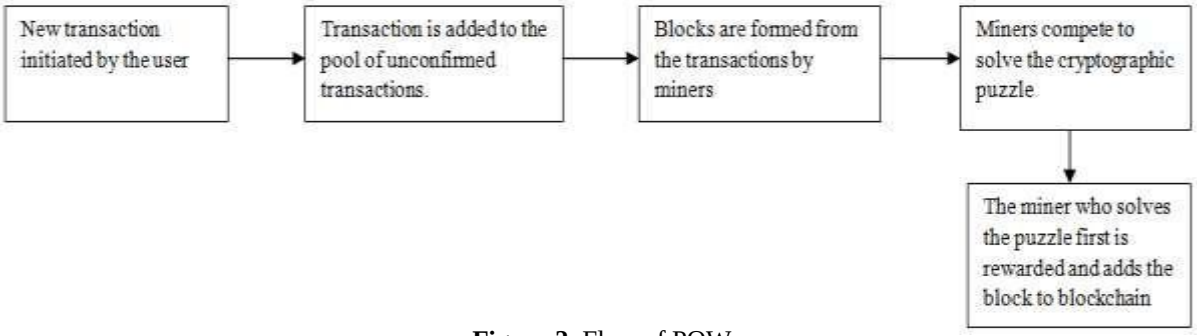

Figure 2: Flow of POW

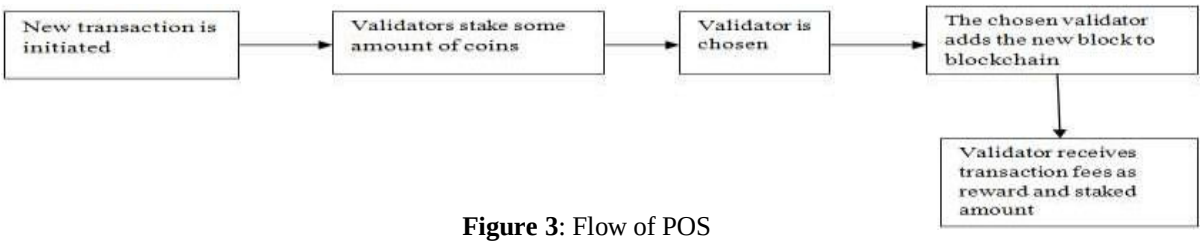

Figure 3: Flow of POS

calculations and it also requires lot of computational power. Therefore, the attack is possible but it is useless since the costs involved are too high. The main drawback of proof of work involves huge expenditures since mining requires highly specialized computer hardware to solve the puzzle. It requires high computational power and uselessness of computations since the calculations performed cannot be applied anywhere else. This algorithm may lead to a 51% attack where a user or a group of users control the majority of mining power.

Ethereum is one of the popular blockchain platforms that uses POW to attain a consensus. Ethereum is an open source blockchain platform. It enables developers to built decentralized applications called DApps. This can be accomplished using smart contracts, a set of rules that are executed only when certain conditions are satisfied[12].

Bitcoin , Litecoin , monero coin , dogecoin are some of the platforms that use Proof of work consensus method.

4.2 Proof Of Stake

The proof of stake algorithm is an alternative to proof of work which requires fewer CPU computations. In proof of stake the validators of the block stake a certain amount of coins into the network [13].The size of the stake determines the chances of a validator to be chosen to forge or add the next block. The chosen node upon validating the transactions will add the validated block into the blockchain and will receive transaction fees as rewards. The idea of putting coins to be 'staked' prevents attackers from making fraudulent validations because upon false validations of transactions, the amount staked will be forfeited. Hence, this encourages the validators to validate legitimately. Figure.3 shows the flow of POS.

It is saving energy since no puzzle has to be solved as in the case of proof of work system. In order for this process To not always favorthe richest node, methods such as *Randomized Block selection* and *Coin Age Selection* can be used. In the randomized block selection, least hash value and highest stake are considered for the selectionof the validators. In coin age selection the older node has the highest chance of becoming the new validator. A group of nodes can combine and own a significant share of total cryptocurrency which will help them in becoming the validators. This may lead the network to become centralized in the future. The 'nothing at stake' problem describes little to no loss for the nodes by voting or multiple blockchain histories which results in the prevention of consensus.

Ethereum is planning to move from POW to POS in the near future. Peercoin , NXT use POS consensus algorithm.

4.2.1Delegated Proof Of Stake

In Delegated Proof of stake (DPOS) the stakeholders of the network vote for the delegates who are responsible for validating the blocks. In DPOS voting for the delegates or witness is accessible to all stakeholders in the network and the voting power is directly proportional to the number of coins held by a certain node. The delegates can be added or removed at any time. The threat of loss of income and reputation forces the delegates to act honestly and secure the network. The delegates in return distribute the block rewards they received after validating the block among their voters in a proportional manner. If a delegate cannot create a new block within a specific time may be due to network issue or any other issue the stake holder will vote for a new delegate the will assign the task to it[14].

Compared to POW and POS, DPOS is high-efficiency

consensus protocol. The DPOS can process 10 transactions per second and as no miners are required for DPOS it is energy efficient. The drawback of DPOS is that the nodes that hold a large amount of stakes will have significantly more voting power and thus more influence in deciding delegates. A DPOS based blockchain will only work efficiently if the stakeholders participate in the voting process. Low participation rates will cause centralization of power and the network will not work as intended.

Bitshares is the first known implementation of DPOS[15], EOS, Ark are some of the blockchain platforms that use DPOS to achieve consensus. The new version of EOS blockchain platform has changed from following DPOS to Byzantine Fault Tolerance-DPOS [16].

4.2.2 Leased Proof Of Stake

The leased proof of stake is similar to Proof of stake with some changes. The leased proof of stake allows nodes with low balances to participate in the block validation by adding a leasing option. Leasing allows the stakeholders with high balances to lease their funds to the nodes with low balance for a specific amount of time. During the lease contract, the lease amount will be in possession of the wealthy stakeholders. However, this way increases the chances of validating a block for nodes with low balances. When the nodes validate the block, they will share their reward with the wealthy stakeholders from whom they got the lease proportionally. This algorithm solves the centrality problem that is seen in POS. The waves platform uses Leased Proof of Stake consensus algorithm [17].

4.3 Byzantine Fault Tolerance

It is derived from the Byzantine Generals problem that requires the involved members in a network to agree on a single strategy to avoid failure. However, it assumes that some of the members in the network might be unreliable or corrupted. We can imagine Byzantine general's problem as a group of generals trying to invade a city. The success of this invasion lies upon all of the generals acting in the same fashion. In order to attain success, all the generals should either attack together or retreat together. The Problem arises when the generals are corrupted or lie. These prevent the loyal generals to reach consensus and conquer the city. Byzantine fault tolerance can be considered as a system that can withstand the class of failures belonging to the byzantine general's problem.

4.3.1 Practical Byzantine Fault Tolerance

The PBFT algorithm optimizes the byzantinefaults[18]. All the nodes participate in the voting process to add the next block and consensus is reached when the majority of the nodes agree on the state of the system. For a PBFT algorithm to function the number of malicious nodes must not equal or exceed one-third of all nodes in the system in a given vulnerability window. Unlike Proof of work, PBFT can achieve consensus without requiring high energy computations. The PBFT algorithm performs well when there are small numbers of nodes but becomes inefficient in larger networks [19]. The PBFT models are also susceptible to Sybil attacks where a single node compromises a large number of nodes in the network. Hyperledger Fabric is using a permissioned version of PBFT for their platform. Ziliqa uses an optimized version of classified PBFT.

4.3.2 Delegated Byzantine Fault Tolerance

NEO is a blockchain platform that has come up with a better way to solve the faults of Byzantines generals. Delegated Byzantine Fault Tolerance involves the users of the blockchain to vote for *delegates* whom they think are trustworthy. The delegates take part in the validation of the new block. When a new block is put in the blockchain a speaker is randomly chosen from among the group of delegates. The speaker creates a new block and sends the proposal to the voted delegates and then if 66% of delegates approve this block it will be added to the blockchain otherwise the block will not be added and the speaker will also go back to just being a delegate. A new speaker will again be randomly chosen from among the delegates until they reach a consensus. This protects the whole network from traitorous or betraying delegates. The DBFT algorithm determines the delegators who are the validators according to real-time blockchain voting, bringing block time and transaction confirmation time savings[20].

4.4 Proof Of Elapsed Time(POET)

POET is a consensus algorithm which comes from INTEL. It is used by private or permissioned blockchain networks. In POET the nodes are assigned a waiting period by the network in order to mine or validate the block, the winning miner is the one who waiting period or timer expires first. POET relies on special instruction set called Intel Software Guard Extensions (SGX)for the verification of timer execution. Nodes interested in joining the network must download the trusted POET code run SGX in a Trusted Execution Environment (TEE). The POET algorithm consumes lower energy when compared to the POW. It may hold high potential due to the wider ability for more people to act as validators. Hyperledger Sawtooth supports POET consensus algorithm implementation [21].

4.5 Proof Of Activity(POA)

The POA combines the features of proof of work and proof of stake blockchain consensus models. In POA the mining process starts similar to Proof of Work algorithm. The miners have to solve a critical puzzle. But the difference here is that the miners mine only the template of the block. This template consists of the header information and the reward address for the miners. After the miners mine the block template the system converts to the proof of stake. Based on the header information a new group of validators are randomly selected from the blockchain network and they validate the new block. The more coins the validator owns, the more chance he has to be selected as a validator. Suppose the selected validator is unable tovalidate the block due to some network issues then the

process moves to the next winning block with a new set of randomly chosen validators from the blockchain network, and this process continues until the validator validates the block and add the particular block into the blockchain. Moreover, the network pays both the miners and the validators the transaction fees that are split among them.

It provides good security, low overhead and less storage space. This method makes it difficult for the attacker to own the majority of the blockchain network because it requires to owna large part of the total currencies created so far which is costly [22]. Though proof of activity has its own share of advantages it does contain some drawbacks. The first one being the massive amount of energy consumption due to mining. second, it does not prevent the double signing of validators.

Two popular blockchain platforms Decred and Espers adopt proof of activity to reach consensus.

4.6 Proof Of Importance(POI)

The POI is similar to the proof of stake in ways that you need to lock up a certain amount of cryptocurrency to validate or verify the transactions but the proof of importance differs from the proof of stake by assigning an importance score to the validator of the blockchain. The importance score can be considered as a reputation score or trust. The importance score given to a validator is not solely dependent on how much coins he hase at stake, but on how many transactions he has done in the past. This way solves the problem faced by the proof of stake method where the wealthy stakeholders get wealthier. The node with the higher importance score will have a higher chance of being chosen to validate or harvest the block. Harvesting is the term used for mining blocks or validating the block. As a reward, the validator collects network fees based on his importance in the network. POI yields high throughput and exhibits low latency.NEM is the blockchain based cryptocurrency that uses POI for achieving consensus[23].

4.7 Proof Of Capacity

Proof of Capacity(POC) is similar to POW but the difference here is that it depends on the hard disk capacity instead of relying on the computer power of the miners as in the case of POW. Before mining, the system generates large data sets called “plots”. Plots are supposed to store on a hard drive. The more plots one has the chances of getting a block to mine increases. Proof of capacity is also called as *proof of storage* or *proof of space*. This method does not require expensive mining rigs as in the case of POW. The hard disk of your home PC is sufficient to start mining in this consensus algorithm. It is partially motivated by the fact that users always have some free disk space available and in that case using POC is essentially free[24].

Some of the drawbacks that are faced by this method are that it created a massive amount of redundant disk spaces. Since this algorithm favors the miners with large disk space it might pose a threat to the decentralized concept. Burstcoin and spacemint are cryptocurrencies that rely on Proof of capacity algorithm.

4.8 Proof Of Burn

The proof of burn consensus algorithm requires the miners to burn their cryptocurrencies to get chance to mine or validate a block. The process of burning the coins means to spend their coins by sending it to public, verifiable, unspendable and invalid address [25]. The more coins you burn, the more are the chances of you getting selected to validate the block. Essentially, this burning activity keeps the network active and the validators are rewarded for their activities. The proof of burn method does not require high energy consumption as in the case of POW. The coin burning feature reduces the number of coins on the blockchain which leads to an increase in the value of the coins gradually. This method favors long-term investors by giving more stable currency and long-term commitment. This method prevents centralization and promotes a better distributed network. This system is criticized as the process of burning the coins involves wastage of a lot of resources. Slim coin makes use of the proof of burn consensus method to achieve consensus.

5. CONSENSUS OF POPULAR BLOCKCHAIN PLATFORMS

5.1 Hyperledger Fabric

The Hyperledger Fabric is a blockchain framework that is used by private enterprises for developing blockchain based applications. Hyperledger was initiated in December 2015, by the Linux Foundation. It can be used for a broad range of industry use-cases[26]. Table 1 shows the comparison of different blockchain platforms.

Transaction flow in hyper ledger fabric consists of three steps. Endorsement, ordering and validation. Endorsement allows for transaction execution by running the smart contracts which are called as chaincode in fabric. Ordering is achieved through consensus protocol after which the transaction validation takes place. Hyperledger Fabric follows a modular approach wherein different consensus protocols can be used as per the requirement. Hyperledger fabric currently uses the RAFT to achieve consensus. RAFT is a crash-fault tolerant consensus algorithm. The crash-fault tolerance prevents the system from failure even if some of the nodes in the network crash or fail. RAFT follows a “leader and follower” model where the nodes collectively select the leader and the other nodes become the followers [27]. The leader is selected by majority voting. The leader will propose a new transaction. If majority of the followers accept the particular transaction then the transaction is committed. If the leader becomes unavailable the followers will again initiate a new leader election and the new leader will be elected from one among them.

RAFT can tolerate N/2 -1 number of crash faults whereas it cannot tolerate Byzantine fault that is it cannot tolerate nodes behaving maliciously.

	Ethereum [12]	**Hyperledger fabric [26]**	**Corda [29]**	**Ripple[30]**	**Quorum[31]**	**Stellar[32]**
Type	Permission less	Permissioned	Permissioned	Permissioned	Permissioned	Permissioned
Governance	Ethereum Developers	Linux Foundation	R3	Ripple Labs	Ethereum Developers and JP Morgan Chase	Stellar Development Foundation
Currency	Ether	No native currency	No native currency	XRP	Ether	Lumens(XLM)
Consensus	POW	RAFT,Plugabble consensus	Notary nodes	Probabilistic voting	RAFT , Istanbul BFT	Federated Byzantine Agreement
Application Type	Build and deploy DApps	Enterprise focused	Financial services	Financial services	Enterprise focused	Financial services

Table 1: Comparison of Blockchain Platforms

5.2 Corda

Corda is an open-source blockchain platform. It is a permissioned blockchain platform that is designed for business. It focuses on finance domain. Corda was developed by R3, an enterprise blockchain software firm which is a consortium of more than 200 companies. Corda ensures privacy in business using smartcontracts.

The peers in Corda reach consensus in two ways transaction validity and transaction uniqueness [28]. In transaction validity, the peers ensure that the transaction and all its dependencies are signed by all the involved peers and it also ensures that all the constraints in the contract code are met. The transaction uniqueness mitigates the "double spend" problem that might arise. The transaction uniqueness is achieved by "notary services". The transaction can be committed only after the notary service signs the transaction [29]. The notaries maintain a map keyed with input state references. Only when an input state that is not already present in the map is proposed the notary will sign the transaction and commit the transaction otherwise the transaction will not get committed. The notaries in Corda can be implemented by adopting a consensus algorithm of its choice depending on the privacy, scalability and algorithmic agility. A notary can run an algorithm such as RAFT or BFT or any other consensus algorithm as it chooses.

5.3 Ripple

Ripple is a peer to peer payment network that uses blockchain technology. It enables banks, payment providers, Corporate to send money globally. It is an open-source platform that allows for fast and cheap transactions.

The ripple network consists of nodes called servers that take part in the consensus process [30]. Each server consists of Unique Node List(UNL). The UNL consists of the set of nodes that the server trusts. The server vote for the transactions which it thinks is valid by consulting the UNL. The ripple protocol consists of several rounds. The transaction that receives the majority of votes is passed onto the next round. The final round of consensus requires Minimum of 80% agreement from the servers UNL. All the transactions that make this 80% threshold are added to the ledger and the ledger becomes the last-closedledger.

5.4 Quorum

Quorum was developed by JP Morgan as a blockchain based platform based on Ethereum protocol. It is a permissioned blockchain network which solves the privacy and performance challenges faced by the permission less blockchain networks. It is an enterprise-focused blockchain. It is open source. It is a soft fork of the Ethereumblockchain.

Quorum uses RAFT and Istanbul BFT(IBFT) consensus algorithms. It uses RAFT for crash fault tolerance and IBFT for Byzantine fault tolerance. The RAFT algorithm uses leader, follower method as explained in Hyperledger Fabric. The IBFT is a Practical Byzantine Fault Tolerance inspired consensus algorithm. It can tolerate F faulty nodes with 3f+1 nodes in the network. It consists of 3-phases PRE-PREPARE, PREPARE and COMMIT [33]. It consists of several rounds of voting. In the initial round, the validators choose a proposer from among themselves. It is the duty of the proposer to propose a new block and broadcast it to all the validators in the network

with a PRE-PREPARE message. The validators of the network validate the incoming proposal with the pre-prepare message. After the validation of the proposal, the validators broadcast the PREPARE message. When every validator receives 2F+1 PREPARE messages from other validators in the network the validator enter the PREPARED state and then broadcastCOMMIT message. The validators again wait till they receive 2F+1 COMMIT messages from other validators and then add the block to the blockchain.

5.5 Stellar

The stellar network is a blockchain based network that allows for fast, cross-border transactions between any pair of currencies.

The Stellar consensus protocol is a Federated Byzantine Agreement (FBA) system that allows decentralized, leaderless computing nodes in the network to reach consensus. In FBA there is no central authority that chooses the validators of the network. The validator can choose the other validator whom he trusts and their list of validators who trust each other is called a “quorum slice”. The quorum slices is a subset of the quorum. A quorum in stellar is defined as the set of nodes that are needed to reach consensus in a distributednetwork.

The stellar consensus algorithm works in two steps[34].

1. Nomination protocol
2. Ballot protocol

In the nomination protocol, the nodes vote for a single value from among the new values called candidate values that are proposed for agreement. The goal of the nomination is to find unanimously selected values for that slot. After the nomination protocol the ballot protocol starts that involves the federated voting to either commit or abort the values selected in the nomination protocol. The aborted ballots are discarded and the stuck ballots are moved to a ballot with higher votes. Therefore the stuck ballots rely on the higher ballots decisions. In FBA the nodes wait for a greater part of the other nodes that it trusts to agree on the transaction as committed. The trusted nodes also agree on a transaction only if its trusted node accepts the transaction making this network impossible to attack.

Stellar Consensus Protocol (SCP) guarantees decentralized control, low latency, flexible trust and asymptotic security. SCP optimizes safety over liveness in case of misbehaving nodes. It halts the progress of the network until a consensus is reached. It does not guarantee safety if the user selects an inefficient or unauthorized quorum slice.

6. CONCLUSION

Reaching consensus among the nodes is an important part of the blockchain architecture. In this paper, we have discussed the different ways in which consensus is reached in blockchain platforms. We then presented the consensus method followed by some of the popular blockchain platforms. Comparison of the popular blockchain platforms was also presented. Consensus algorithms can be used to decide the blockchain platform to use. This paper will help researchers to gain knowledge about how the consensus algorithms work and also help them for selecting suitable algorithms for further exploration in the blockchain environment.

REFERENCES

[1] S. Haber and W. S. Stornetta, "**How To Time-Stamp a Digital Document**," J. Cryptal., vol. 3, no. 2, pp. 99-111,1991.https://doi.org/10.1007/BF00196791

[2] S. Nakamoto, "**Bitcoin: A Peer-to-Peer Electronic Cash System**," 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[3] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H.Wang,

"**Blockchain challenges and opportunities: A survey**," Int. J. Web Grid Services, vol. 14, no. 4, pp. 352_375, 2018. https://doi.org/10.1504/IJWGS.2018.10016848

[4] Ahmed Afif Monrat, Olov Scelen and Karl Anderson, "**A Survey of Blockchain from the perspectives of applications, challenges and opportunities**",IEEE Access,vol7,pp.117134-117151, 2019. https://doi.org/10.1109/ACCESS.2019.2936094

[5] D. Lee Kuo Chuen, Ed., **Handbook of Digital Currency**, 1st ed Elsevier,2015.[Online].Available: http://EconPapers.repec.org/RePEc: eee:monogr:9780128021170

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang," **An overview of blockchain technology: Architecture, Consensus and Future Trends**", Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017, pp. 557-564,2017. https://doi.org/10.1109/BigDataCongress.2017.85

[7] R.C Merkle," **A digital signature based on a conventional encryption function**," in Proceedings of the Conference on the Theory and Application of CryptographicTechniques.

[8] E. F. Jesus , V. R. L. Chicarino, C. V. N. Albuquerque, and A. A Rocha, "**A Survey of How to Use Blockchain to Secure Internet of Things and the Stalker Attack**," in Security and Communication Networks,vol.27, April 2018. https://doi.org/10.1155/2018/9675050

[9] D. Mingxia, M. Xiaofeng, Z. Zhe, W. Xiangwei,and

C. Qijun, "**A review on consensus algorithm of blockchain**," 2017 IEEE Int. Conf. Syst. Man, Cybern. SMC 2017, vol. 2017-Janua, pp. 2567-2572 2017.

[10] S.Gilbert, N.Lynch, Brewer's **conjecture and the feasibility of consistent, available, partition-tolerant web series**, ACM SIGACT New 33(2) (2002) 51-59. https://doi.org/10.1145/564585.564601

[11] L.Lamport, R.Shostak, M.Pease, **The byzantine generals problem,** ACM Trans. Program . Lang . Syst (TOPLAS) 4(3) 1982. 382-401.

https://doi.org/10.1145/357172.357176

[12]Ethereum. **Ethereum Project**[Online] Available: https://www.ethereum.org/

[13] E. Garcia Ribera, "**Design and implementation of a proof-of-stake consensus algorithm for blockchain**,"
B.S. thesis, Universität Polite'cnica de Catalunya, 2018.

[14] M. Snider, K. Samani, and T. Jain, "**Delegated Proof of Stake : Features & Tradeoffs,**" Multicoin Cap., pp. 1–19, 2018.

[15] "**BitShares 2.0 - Industrial-grade decentralized (DPoS)eco-system on blockchain**." [Online]. Available: https://bitshares.org/.

[16]**EOS.IOTechnicalWhitepaperv2**,https://github.com/EOSIO/Documentation/blob./master/technicalwhitepaper.md,2018.

[17]"**Leased Proof of Stake",** https://docs.waves.tech/en/blockchain/leasing. Accessed:2020-09-17.
https://doi.org/10.7566/JPSJNC.17.09

[18] C. Miguel and L. Barbara, "**Practical byzantine fault tolerance**," in Proceedings of the Third Symposium on Operating Systems Design and Implementation, vol. 99, New Orleans, USA, 1999, pp.173-186.

[19] Yuhao Wang; Shaobin Cai ; Changlong Lin ; Zuxi Chen ; Tian Wang ; Zhenguo Gao ; Changli Zhou," **Study of Blockchains's Consensus Mechanism Based on Credit**", IEEE Access ,Vol.7,p.p10224 - 10231,2019. https://doi.org/10.1109/ACCESS.2019.2891065

[20] **Neo Whitepaper**, https://docs.neo.org/docs/en-us/basic/whitepaper.html.Accessed:2020-09-17

[21]**Hyperledger_Sawtooth_Whitepaper**,https://www.hyperledger.org/wpcontent/uploads/2018/01/Hyperledger_Sawtooth_WhitePaper.pdf. Accessed:2020-09-17.

[22] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "**Proof of Activity: Extending Bitcoin's Proof of Work via Proof of Stake**," ACM SIGMETRICS Perform. Eval. Rev., vol. 42, no. 3, pp. 34–37, 2014.

[23] NEM, "**Technical Reference**," 2018. [Online]. Available:https://nem.io/wpcontent/themes/nem/files/NEM_techRef.pdf. Accessed:2020-09-17.

[24] S. Dziembowski, S. Faust, V. Kolmogorov, and K. Pietrzak, "**Proofs of space**" in Advances in Cryptology-CRYPTO 2015. Heidelberg: Springer, 2015, pp. 585- 605.
https://doi.org/10.1007/978-3-662-48000-7_29

[25] A. Baliga, **''The blockchain landscape,''** Persistent Syst.,2016.

[26]**Hyperledge**r[Online].Available: http://hyperledger.org/. Accessed:2020-09-17

[27] D. Ongaro and J. Ousterhout, "**In Search of an Understandable Consensus Algorithm,**" in 2014 USENIX Annual Technical Conference, 2014.

[28] Richard Gendal Brown, James Carlyle, Ian Grigg, Mike Hearn, **Corda: An Introduction**, August,2016

[29]**CordaDocumentation**[online].Available:https://docs.cor da.net/docs/corda-os.html.Accessed:2020-09-17.

[30] F. Armknecht, G. O. Karame, A. Mandal, F. Youssef, and E. Zenner "**Ripple: overview and outlook**," in Trust and Trustworthy Computing. Cham, Switzerland: Springer, 2015, pp. 163-180.

[31]**GoQuorum**[Online].Available:https://docs.goquorum.consensys.net/en/latest/ Accessed:2020-09-17.

[32] **Stellar**[Online]Available:https://www.stellar.org/learn/intro-to-stellar Accessed:2020-09-17.

[33] **IstanbulBFT**https://github.com/ethereum/EIPs/issues/650 Online Accessed:2020-09-17

[34] David Mazieres, **The Stellar Consensus Protocol: A Federated Model for Internet-level Consensus** , February 25,2016.