*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

# Performance Analysis of Reputation based Proof of Credibility Consensus Mechanism for Blockchain based Applications

**Jalpa Khamar[1], Hiren Patel[2]**
[1]Research scholar
Kadi Sarva Vishwavidyalaya, Sarva Vidyalaya Kelvani Mandal, Gandhinagar, Gujarat, India
[1]khamarjalpa7@gmail.com
[2]Principal Vidush Somany Institute of Technology and Research
Kadi Sarva Vishwavidyalaya, Sarva Vidyalaya Kelvani Mandal, Gandhinagar, Gujarat, India
[2]hbpatel1976@gmail.com

**Abstract**— Blockchain is a decentralized transaction and data management technology first developed for the Bitcoin cryptocurrency. Blockchain technology is gaining popularity due to its core attributes which provides security, anonymity and data integrity without any involvement of third party. Consensus mechanism is a procedure by which all peers in the blockchain network agrees to a common agreement on the current state of the distributed ledger. It plays vital role in increasing efficiency of any blockchain environment. Though we have many consensus mechanisms working currently in different areas but they still lack in parameters like status of validators, latency, node failure etc. In Our proposed algorithm Proof of credibility, we have tried to incorporate all above factors in it. We have also implemented two or more factors of proposed algorithm and have evaluated and compared with existing consensus algorithm. In future research we aim to implement RPoC in any blockchain network and then we will evaluate it in terms of different evaluation parameters such as performance, security, scalability.

**Keywords**-Blockchain, consensus, Bitcoin,Decentralization.

## I. INTRODUCTION

All In recent decades, consensus mechanisms have been widely studied in a classical distributed system. After the success of Bitcoin [1], the first cryptocurrency appeared in early 2009, Blockchain technology has gained the attention of the academic and industrial sectors [2]. Currently, the rise of Blockchain applications encompasses a diverse range far beyond cryptocurrencies, including insurance [3], medicine [4-6], economics [7-9], Internet of things [10-12], supply chain, software engineering [13-15], etc. The centrepiece of everything in the Blockchain application is consensus protocol for reaching consensus information exchange, by replicating the state and broadcast transactions between participants. This made the consensus mechanisms received have rekindled attention in recent years [16]. We have many consensus mechanisms already implemented in Blockchain environment followed by some in proposal.

An Integrity, resilience and transparency properties of blockchain make it a good option for companies to revolutionize their business processes. With the growth and integration of modernity technologies such as business process management (BPM), service workflow, Internet of Things (IoT), Cloud Computing, Service Oriented Architecture (SoA) and Cyber Physical Systems (CPS) in Industry 4.0, Centralized BPM tools face their limits by responding to conflicting requirements and a commitment to scalability, security, openness, trust and cost [18, 19]. To survive in a competitive market, building a flexible businesses process in open environments is inevitable, as promoting collaboration, knowledge sharing and collective decision [20].

Now a days Research on blockchain and consensus theories and applications is growing rapidly. Previous work in this area attempts to solve the problem of fundamental chord mainly exercised in the Byzantine asynchronous consensus exposed in distributed systems [16, 22], which can explain how a system with n asynchronous processes that always ensure agreement on a single value despite some faulty nodes.

In most current research, the way Blockchain is defined is very informal which particularly give emphasis on context of use and use of certain marketing words in terms of properties offered by Blockchain or how security can be reached. These include, for example, a public ledger to record transactions held by many nodes without central authority via a distributed cryptographic protocol [16]; a decentralized database with the ability to operate in a decentralized environment without depending on trusted intermediaries [17]; a decentralized,

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

immutable, tamper-proof and replicated record that allows anyone to read the data and verify its accuracy; at type of distributed ledger (data structure) that contains information about transactions or events, which is replicated and shared among network participants [2]. Most of them include terms of immutability, verifiability, transparency, distributed database or ledger and no trusted intermediary.

Consensus building has been widely studied in distributed systems to be resilient to node failures, network partitioning, message delays, out-of-service or missing messages, and compromised messages. In the context of Blockchain, consensus mechanisms must deal with selfish, faulty or malicious nodes and ensure that all nodes in the network accept a consistent overall state. Every Blockchain Consensus tries to involve three key properties on the basis of which their applicability and efficacy can be determined [25].

i. Safety: The safety property ensures that nothing bad will ever happen. It corresponds to the properties of validity and agreement in the traditional consensus that appear in distributed systems. Validity is defined as if some valid process offered the same v value, then process that decides, decides v. The agreement ensures that there are no two correct processes that decide differently. Generally, a consensus mechanism is safe if at least one honest node produces valid output, then all other nodes produce or receive the same output. The results are valid and the same for all nodes, with respect to the consistency of the shared state [26].

ii. Liveness: Liveness ensures that something good will eventually happen. This is also known as an end in the traditional consensus in distributed systems that establishes that each process ultimately decides a value. A consensus mechanism ensures liveness if all the nodes participating in a consensus ultimately produce a value and all successful requests will be finally processed.

iii. Fault tolerance: A Consensus mechanism ensures fault tolerance if it is resilient to failures of certain nodes participating in consensus at any time. With an assumption about limited faulty nodes, we can achieve true consensus. The failure of nodes revealed in two groups. Frist one is Fail-stop or crash-failure which deals with nodes which stop the process either temporary and permanent. Second one is Byzantine failures which deals with malicious nodes which are particularly designed to overcome the properties of a consensus protocol. The second category was well identified in the Byzantine General's Problem [28].

The consensus mechanisms allow the secure updating of a distributed shared state and have been a subject of research over the past three decades [26]. It is difficult to reach consensus in a distributed system. Consensus algorithms must be resistant to failure nodes, network partitioning, message delays, messages reaching faulty and corrupted messages. Several algorithms are proposed in the search of the literature to solve this problem, each algorithm making all the assumptions required in terms of synchrony, message deliveries, failures, malicious nodes, performance and security of exchanged messages. For a blockchain network, reaching consensus ensures that all nodes in the network agree on global consistency blockchain state. In the blockchain, how to reach consensus among unreliable nodes is a transformation of the Byzantine generals (BG) Problem, which was raised in [28]. In the BG problem, a group of generals who command a part of Byzantine army surrounds the city. Some generals prefer to attack while other generals prefer to retreat. However, the attack fails if only part of the generals attacks the city. So, they must reach an agreement to attack or retreat. How to reach consensus in a distributed environment is a challenge. This is also a challenge for blockchain as a blockchain network is distributed. In the blockchain, there is no central node that ensures that the ledgers on the distributed nodes are identical. Some protocols are needed to ensure that the ledgers of the different nodes are coherent.

The objective of our proposal is to overcome the gaps discussed above in connection of Identifying and countering (group of) malicious nodes trying to control the entire network, considering both the status of validators i.e. offline/online, considering predefined computational time for adding the block into the network and incorporating the practical aspects of network (failure of node/link, delay/latency, asynchronous).

For addressing the prior mentioned issues, we have selected some of the consensus algorithms like PoW, DPOS, PoI, BPFT for performance testing in our proposed blockchain environment. Considering different performance criterions of those existing algorithms, this paper proposes Proof of Credibility (RPoC) as consensus algorithm which act in accordance to credibility model. Credibility model is a layered architecture which consist of stakeholders with different owners working as a certificate authority for validation of stakeholders. These are paper's key contribution:

a. An intricate analysis of different consensus algorithms is discussed.

b. Proof of Credibility consensus algorithm has been proposed by combining the advantages of existing algorithms and reducing the limitations of the same.

c. A comprehensive comparison of existing consensus algorithms with the proposed RPoC is presented.

The rest of this paper is laid out as follows. Section II includes the related study about consensus algorithms with the gaps in

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

existing consensus mechanisms. Section III discusses about Mining and Consensus. Section IV introduces Credibility model and RPoC consensus algorithm. Section V shows implementation testbed for different parameters of RPoC. Section VI concludes the paper with conclusion and future work followed by list of references.

## II. RELATED STUDY

This section gives brief introduction about different existing consensus algorithm.

YAC [29] is decentralized consensus algorithm which overcomes two major problems of classical byzantine fault tolerant consensus which are Inefficient message passing and Strong leader. Using voting on block proposals, YAC guarantees safety and liveness for transaction processing. Also, Empirical results showed that the algorithm can increase scalability in terms of peers by adjusting the value of vote step delay.

An RDV [30]-Register, Deposit and Vote overcomes with the two disadvantages of PoW significant latency for Block validation and High-power consumption. It has no mining process, which makes it more suitable for low level energy devices and IoT. It prevents Double spending, Blockchain fork, Block-withholding, provides immutability of transactions history (with the help of vote Box and voteRbox parameter), Provides increase in transactions confirmation throughput.

Another paper proposes PoM [31] a consensus mechanism that works on reducing energy waste and improving efficiency and security in a private blockchain environment. There is no computation of hash values which overcomes with problems like high energy waste and performance. It provides trusted, closed and controlled environment. Several verification simulations regarding this algorithm can be done as an future enhancement.

Also, POSTER [32] proposes a mechanism which Proof of Probability (PoP) method which works on disadvantages of PoW (High Computation power) and PoS (Monopoly of Few stakers). It overcomes two limitations of PoW and PoS. Actual time limit for block validation and bit adjusting algorithms for nonce can be further analysed on the basis of future experiments on it. Further performance evaluation of PoP can be done in comparison with the existing methods in different perspectives.

In paper [33] author has contributed in providing consensus which is an extension of PoW working on robustness parameter. Author claimed to be the first one who has worked on properties of PoW effectively and correctly.

The sleepy model of consensus [34] discusses about the consensus in which nodes are classified as honest nodes and sleepy nodes. More precisely, author has formulated a new formal model where we classify honest nodes as alert or sleepy.

Author has described the Sleepy consensus protocol that provides security as long as at any time, the number of alert nodes exceeds the number of corrupted nodes.

In paper [35] author has introduced a new Proof of Stake (PoS) protocol, Ouroboros Genesis, which allows parties to securely join the protocol execution using only information from the genesis block. This capacity of the new parties to "start from the genesis" was a characteristic property of the Bitcoin blockchain and was seen as a major advantage.

In MBFT[36] a mixed byzantine fault tolerance model ,it combines layer technology and fragmentation technology. Lamination is used to separate node functions. By assigning all checks demodulation function and process at different nodes, layering can effectively reduce the load of individual nodes and improve the effectiveness of consensus. Partitioning is used to assign transactions to different groups of nodes. When the number of transactions increases significantly, the system can dynamically increase the number of nodes and fragments, thus improving processing power and reduced delay. Also, in Traditional blockchain nodes must verify all transactions whereas in contrast, verification nodes in MBFT are only responsible for a certain number of transactions. The performance of the blockchain is positively correlated with the number of nodes, and the blockchain has great scalability.

In paper[37] author introduced RPoC proof of Contribution as a consensus mechanism which has modified PoW ,also based on PoS for increasing efficiency. Bitcoin mining turns out to be a profitable business, but it wastes a lot of energy on computation. The honesty of miners is represented as success times are used as" participation" to ad- just the difficulty in the RPoC mining process. The RPoC algorithm favours honest miners and penalizes malicious behaviour. Experiments have shown that as the network grows, the cost of adding new hashing power increases. Here minors are being motivated to remain honest and abstain from any wrongdoing. It is achieved by integrating a PoS component, called success time. The blacklist concept is also used to maintain a register of misbehaving nodes.

## III. MINING AND CONSENSUS

In the real world, consensus is basically an agreement among two or more communicating parties and it is required because of the fact that these parties do not have faith in one another. There are multiple ways to resolve the issue, one of

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

them being a Byzantine Generals Problem [28]. Here, multiple generals of the same army with a fixed number of soldiers assigned to them are situated far away from each other and supposed to communicate for coordinated attack on the enemy. If the coordination fails due to miscommunication and/or the traitor general propagates the wrong message, they would lose. Hence, a mechanism is required, where a general receives a message from other generals and takes a decision whether to attack or retreat. Here, in case of different messages received from other generals of the same army, the recipient general should be able to discard the message from the traitor and rely on the communication from the honest generals. In Blockchain, all the nodes, which are distributed in nature, act as these generals, who receive information / data / messages from other nodes who could be dishonest. And the nodes need to make a binary decision based on algorithms such as the mentioned above. Further, any transaction made by any of these nodes, needs to be validated by other participating nodes. There could be two outcomes of such validations viz. (i) transaction is validated and added into the network or (ii) the transaction is not validated and discarded. Hence, consensus plays a primitive role in a distributed environment where the parties do not know / trust each other by making decisions regarding identifying a legitimate or spurious transaction.

Depending on the visibility and positioning of the nodes in the Blockchain, it is bifurcated into two categories viz. (a) Permissioned Blockchain where the network is a closed one and only permitted nodes are allowed to participate and (b) Permissionless Blockchain where the network is open & transparent and anyone having valid credentials can participate. This section described both these types of Blockchain network with their examples / protocols.

*PERMISSIONLESS BLOCKCHAIN*

In a PoW system, nodes are rewarded for their performancean operation accepted by most nodes in the system[2]. The caveat here is that participants are not punished for performing a malicious operation. As a result, PoW systems cannot discourage participants from making selfish mining [38] or participate in a 51% attack. In to solve this problem, the new generations of blockchains (Ethereum, Tendermint, etc.) started using proof-of-stake as a consensus algorithm. In a PoS mechanism, though engagednodes are treasured but at the same time unlikely to PoW, that nodes are punished also on any suspicious activity. PoS was firstly implemented by Sunny King's Peercoin. For simple understanding for PoS, the more stakes in form of resources, capitals or money or anything ,the more chances to win [39].DPoS[40] is a further improvement of PoW and PoS , which is consensus techniques based on voting process. A certain number of representatives are elected by the holders of the currency to exercise their power on behalf. The elected representatives participate in consensus and generate block in turn. Although DPoS greatly improves throughput and reduces latency, there are also problems such as low enthusiasm of voting nodes and the inability to handle malicious nodes to be handle in time.

PoW (Proof of work) is a consensus strategy used in the Bitcoin network [2]. In a decentralized network, someone has to be selected to record the transactions. The easiest way is random selection. However, random selection is vulnerable to attacks. So if a node wants to publish a block of transactions, a lot of work has to be done to prove that the node is not likely to attack the network. Generally the work means computer 2) Proof of StakePoS (Proof of stake) is an energy-saving alternative to PoW. Miners in PoS have to prove the ownership of the amount of currency. It is believed that people with more currencies would be less likely to attack the network. The selection based on account balance is quite unfair because the single richest person is bound to be dominant in the network. As a result, many solutions are proposed with the combination of the stake size to decide which one to forge the next block. In particular, Blackcoin [26] uses randomization to predict the next generator. It uses a formula that looks for the lowest hash value in combination with the size of the stake. Peercoin [21] favors coin age based selection. In Peercoin, older and larger sets of coins have a greater probability of mining the next block. Compared to PoW, PoS saves more energy and is more effective. Unfortunately, as the mining cost is nearly zero, attacks might come as a consequence. Many blockchains adopt PoW at the beginning and transform to PoS gradually. For instance, ethereum is planing to move from Ethash (a kind of PoW) [27] to Casper (a kind of PoS) [28]. PBFT (Practical byzantine fault tolerance) is a replication algorithm to tolerate byzantine faults [29]. Hyperledger Fabric [18] utilizes the PBFT as its consensus algorithm since PBFT could handle up to 1/3 malicious byzantine replicas. A new block is determined in a round. In each round, a primary would be selected according to some rules. And it is responsible for ordering the transaction. The whole process could be divided into three phase: pre-prepared,prepared and commit. In each phase, a node would enter next phase if it has received votes from over 2/3 of all nodes. So PBFT requires that every node is known to the network. Like PBFT, Stellar Consensus Protocol (SCP) [30] is also a Byzantine agreement protocol. In PBFT, each node has to query other nodes while SCP gives participants the right to choose which set of other participants to believe. Based on PBFT, Antshares [31] has implemented their dBFT (delegated byzantine fault tolerance). In dBFT, some professional nodes are voted to record the transactions. DPOS (Delegated proof of stake). The major difference between PoS and DPOS is that PoS is direct democratic while DPOS is representative

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

democratic. Stakeholders elect their delegates to generate and validate blocks. With significantly fewer nodes to validate the block, the block could be confirmed quickly, leading to the quick confirmation of transactions. Meanwhile, the parameters of the network such as block size and block intervals could be tuned by delegates. Additionally, 560 users need not to worry about the dishonest delegates as they could be voted out easily. DPOS is the backbone of Bitshares [22]. Ripple [23] is a consensus algorithm that utilizes collectively-trusted subnetworks within the larger network. In the network, nodes are divided into two types: server for participating consensus process and client for only transferring funds. Each server has an Unique Node List (UNL). UNL is important to the server. When determining whether to put a transaction into the ledger, the server would query the nodes in UNL and if the received agreements have reached 80%, the transaction would be packed into the ledger. For a node, the ledger will remain correct as long as the percentage of faulty nodes in UNL is less than 20%. Tendermint [24] is a byzantine consensus algorithm. A new block is determined in a round. A proposer would be selected to broadcast an unconfirmed block in this round. It could be divided into three steps: 1) Prevote step. Validators choose whether to broadcast a prevote for the proposed block. 2) Precommit step. If the node has received more than 2/3 of prevotes on the proposed block, it broadcasts a precommit for that block. If the node has received over 2/3 of precommits, it enters the commit step. 3) Commit step. The node validates the block and broadcasts a commit for that block. if the node has received 2/3 of the commits, it accepts the block. Contrast to PBFT, nodes have to lock their coins to become validators. Once a validator is found to be dishonest, it would be punished

### *B. PERMISSIONED BLOCKCHAIN*

It exhibits two environments, synchronous and asynchronous. Synchronous means working under the same clock pulse with fixed delay. Raft[41]is a synchronous consensus algorithm for managing a replicated ledger ineach node. At any time, each node is in one of threeindicates: leader, follower or candidate. split raft algorithmtime in terms of finite duration. The terms are numbered withconsecutive integers. Each mandate begins with an election, inwhich one or more candidates attempt to become leaders.If a candidate wins the election, he becomes the leader. In asynchronous mechanisms, there is no clock pulse to operate, no delay to work upon it. also in the presence of Byzantine knots; this turned out to be optimal.The Practical Byzantine Fault Tolerance (PBFT) [42] is one of the most well-established BFT algorithms. In PBFT there are two kinds of nodes: A leader node, and some validating peers (nodes); and these peers will execute some rounds for appending a block to the chain. Specifically, it relies on three cycles of message exchange; pre- prepare, prepare and commit phase before reaching an agreement. This ensures that 3f + 1 nodes can reach consensus also in the presence of Byzantine knots; this turned out to be optimal.

## IV. OUR PROPOSED CREDIBILITY MODEL RPOC: REPUTATION BASED PROOF OF CREDIBILITY

Figure 1 describes our Credibility model which we have used for implementing RPoC consensus mechanism.

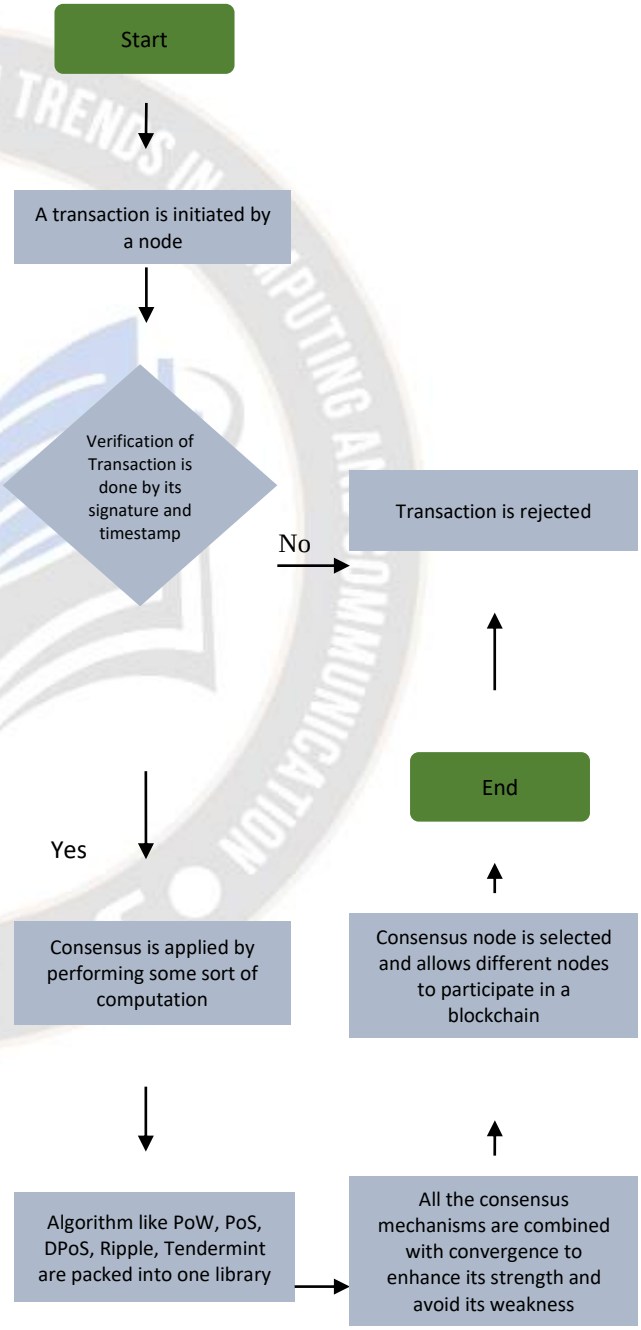


Figure-1

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

Proof of Credibility is a private blockchain which freezes the former history of all the transactions of a particular stakeholder/user. It validates user node by cryptographic signature and calculates credibility score, depending on which the stakeholders/users are added to the blockchain.

Our proposal aims to provide consensus mechanism considering following factors

- Credibility
- Node Status (Active/Inactive)
- Node Failure
- Link Failure
- Variation in Computational Speed among nodes
- Few miners/validators controlling entire network

We will look about all these factors in detail

Credibility

Every proposer and verifier/validator would have an *(credibility)* index associated with it. With every correct block proposed, the index of the respective proposer would increase by some scale factor. Also, all those verifiers/validators who verified/validated the correct block would get bonus points in their index.

On the contrary, those who propose invalid block or those who verified/validated invalid block, would get penalty on their index. There will be three thresholds on lower side, *Threshold 1*, *Threshold 2* and *Threshold 3*.

Upon reaching the index to *Threshold 1*, the node should be fined. Upon reaching the index to *Threshold 2*, the node should be suspended for some specific time period from the process of proposing/verifying. Upon reaching the index to *Threshold 3*, the node should be declared malicious and should be rejected from the network from further communication.

*A. Algorithm for Credibility*

for each node 'n' in list N do
if 'n' has proposed a block then
If the block proposed by 'n' accepted by the network then
increment credibilityIndexProposed[n]
else if block proposed by 'n' rejected due to invalid transactions then
decrement credibilityIndexProposed[n]
If credibilityIndexProposed[n] < Threshold3
Reject 'n' from all future transaction and process
else if credibilityIndexProposed[n] < Threshold2
Suspend 'n' for predefined duration
else if credibilityIndexProposed[n] < Threshold1
Impose penalty on 'n'
end if
end if
end if
If the block verified by 'n' accepted by the network then
increment credibilityIndexVarified[n]
else if the block has been rejected due to invalid transaction
decrement credibilityIndexProposed[n]
If credibilityIndexProposed[n] < Threshold3
Reject 'n' from all future transaction and process
else if credibilityIndexProposed[n] < Threshold2
Suspend 'n' for predefined duration
else if credibilityIndexProposed[n] < Threshold1
Impose penalty on 'n'
end if
end if
end for

Status of Node

It has been assumed in existing literatures that all the nodes are, by default, active or online. But, in reality, it may not be the case.

Hence, we wish to introduce a mechanism of pinging a node by its neighbors. Upon not receiving signal/message within certain time period, the neighbor would communicate the information about inactive/offline node to its group. And such inactive/offline nodes would be deducted from the total number of nodes from the network, at least, for the current round. Pinging process is repeated at regular interval.

*B. Algorithm for Status of Node:*

for each node 'n' in list N do
for each neighbor 'm' of 'n' in M do
'n' sends a signal to 'm' and waits for specific time t period for response
wait (t)
if 'n' receives acknowledgement from 'm'

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

then

'n' broadcast 'm' as active/online

else

'n' broadcast 'm' as inactive/offline

end if

end for

end for

for each node 'n' in list N do

for each neighbor 'm' of 'n' in M do

if status[m][n] is active then

increment active[m]

else

decrement active[m]

end if

end for

end for

for each node 'n' in list N do

if active[n] > (1/2 x size of(N)) then declare 'n' as active

else declare 'n' as inactive

end for

Node Failure

If a node is inactive/offline for a significant period of time, then the node is declared as fail node and further communication with the node is avoided.

When such nodes become active again, they need to register themselves to the network from the beginning process.

*C. Algorithm for Node Failure*

for each node 'n' in list N do

if a node ‘n’ is inactive for T time period then

declare ‘n’ as fail

end if

end for

Link Failure

During gossip/flooding messages among the group members, some nodes may not receive messages (directly) from their neighbor which are active/online.

In such cases, it may be presumed that the link may have failed. Upon sufficient checking, the link may be declared as failed and further communication may not be expected over that link. If the failure remains permanent, topology of network may be changed.

*D. Algorithm for Link Failure:*

row ← 0

for each node 'n' in list N do

for each neighbor 'm' of 'n' in M do

if 'n' does NOT receive a signal from 'm ‘then

FAIL1[row]=m

FAIL2[row]=n

increment row

end if

end for

end for

for each i in row do

for each j in row (where i is not equal to j) do

if (FAIL1[i] is equal to FAIL2[j]) AND

(FAIL1[j] is equal to FAIL2[i]) then

Declare the link between FAIL1[i] and FAIL1[j] as **FAILED**

end if

end for

end for

## V. Simulation Design and Results

An execution of the proposed consensus algorithm can be done using jdk1.8.0_162 and we have used NetBeans IDE 8.2. Database can be managed and handled using Xamp.

We have created complete distributed system which is needed to be authorized and authenticated for distributed data owners and users. Here, node initiates a transaction where client’s signature is created with timestamp. The cluster nodes receives and verifies signature and transaction. If the verification is successful, the transaction is forwarded to the master node in the cluster. The transaction must be verified by

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

the master node. It verifies that the cluster node's signature is correct and that transaction has not been registered in blockchain.

The consensus mechanism of Bitcoin is proof-of- work that nodes accept valid blocks by increasing them. To add new block to the chain, the node has A new consensus algorithm, namely Reputation based Proof of Credibility is proposed for blockchain. The RPoC is an efficient and scalable consensus algorithm that selects the consensus node dynamically and permits a large number of nodes to participate in the consensus process. We A new consensus algorithm, namely Reputation based Proof of Credibility is proposed for blockchain.The RPoC is an efficient and scalable consensus algorithm that selects the consensus node dynamically and permits a large number of nodes to participate in the consensus process. We have evaluated RPoC with respect to parameters like scalability in terms of nodes and clients, performance in terms of throughput and latency.

For evaluation of algorithm we can consider different parameters as:

a) Scalability: It is limited by the speed with which peer network participants can come to terms with the status of digital transaction bookings. This metric is the capacity estimation algorithm to be able to continue with their size or volume updated to a user request.

b) Latency: Network latency is the time between submission of a transaction to the network and the first confirmation of acceptance from the network. After the initial confirmation, the transaction becomes more final as more blocks are added outside the initial confirmation.

c) Throughput: It is expressed using TPS transactions per second), which can be measured by calculating how many dealing in terms of transactions are going on with context to time. It is used to measure how much blockchain processes builds a network.

Some Implementation Screenshots:

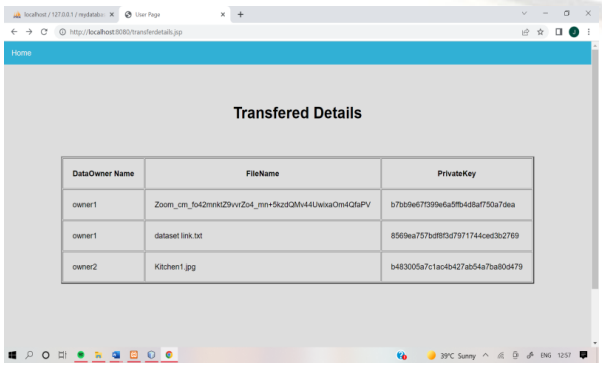


FIGURE-2

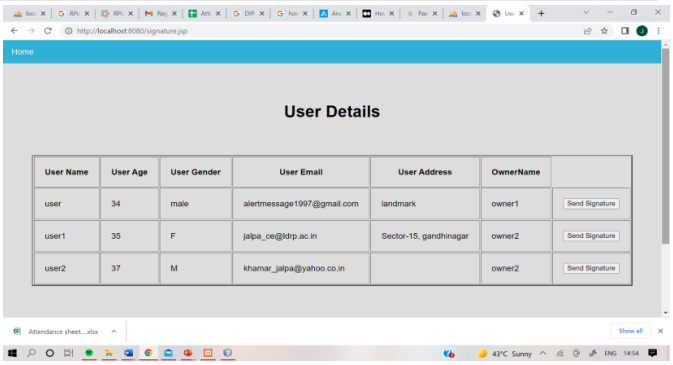


FIGURE-3

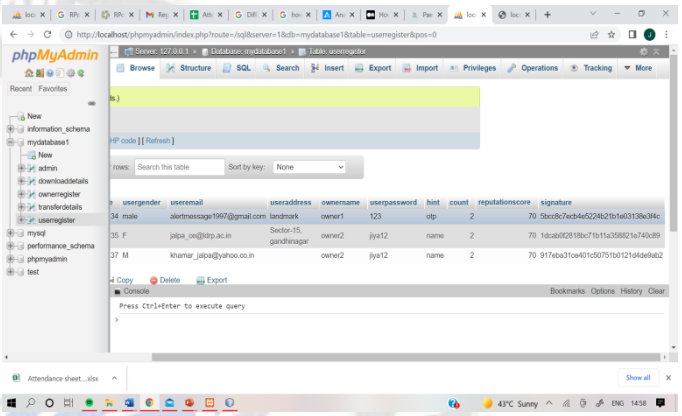


FIGURE-4

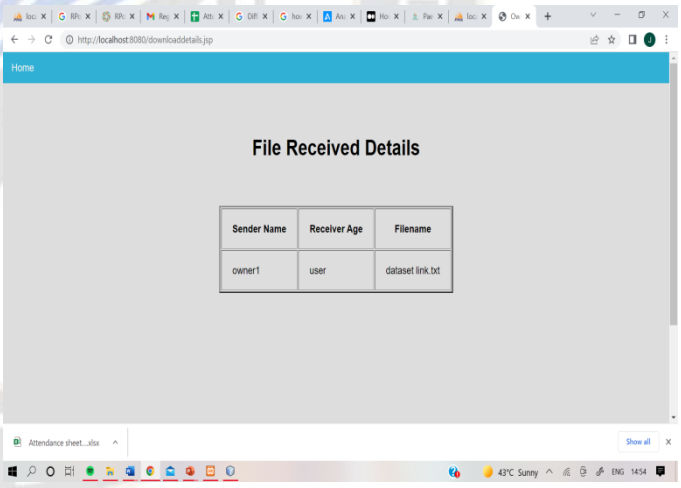


FIGURE-5

We got following results with context to throughput and latency in comparison to PoW.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

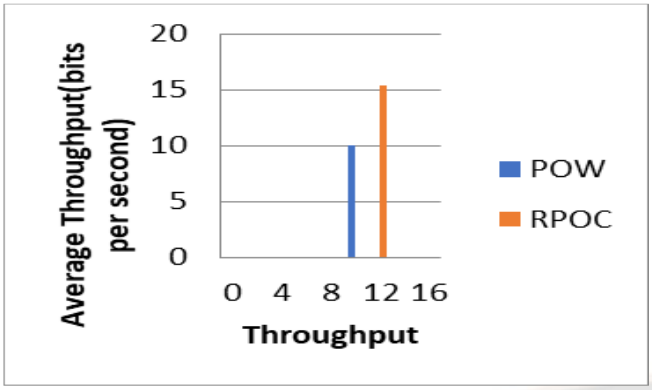


FIGURE-6


FIGURE-7

## VI. CONCLUSION AND FUTURE WORK

In today's Business market, Blockchain has become an indigenous platform to work upon supported by decentralized and immutable attribute in its environment. Consensus plays a vital role in functioning of blockchain by accelerating the addition of valid blocks in Blockchain. Though we have different consensus algorithms available for Blockchain, in this paper, we have proposed and implemented our consensus mechanism RPoC which considers reliability, credibility and efficiency as an important aspect in Blockchain environment. Also we have done performance analysis by showing comparison of our RPoC mechanism with existing PoW consensus mechanism. In future research, we will do feasibility study of our mechanism for the applicability in different platforms of Blockchain.

## REFERENCES

[1] N. Satoshi, Bitcoin: A peer-to-peer electronic cash system, Available: https://bitcoin.org/bitcoin.pdf, Accessed on 23rd of January, 2018.

[2] X. Li, P. Jiang, T. Chen, X. Luo, Q. Wen, A survey on the security of blockchain, Future Generation Computer Systems, pp. 1-13, 2017.

[3] Z. Hess, Y. Malahov, J. Pettersson, Eternity blockchain: The trustless, decentralized and purely functional oracle machine, White paper, 2017 Available: https://aeternity.com/aeternity-blockchain-whitepaper.pdf, Accessed on 23rd of January, 2018.

[4] A. Ekblad, A. Azaria, J.D. Halamka, A. Lippman, A case study for blockchain in healthcare: medrec prototype for electronic health records and medical research data, 2016, White paper, 2016, Available: https://www.media.mit.edu/publications/medrecwhitepaper/, Accessed on 23rd of January, 2018.

[5] A. Azaria, A. Ekblaw, T. Vieira, A. Lippman, Medrec: Using blockchain for medical data access and permission management, in: International Conference on Open and Big Data, OBD, pp. 25-30, 2016.

[6] X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control, J. Med. Syst., 2016, pp. 218, DOI: https://doi.org/10.1007/s10916-016-0574-6.

[7] S. Huckle, R. Bhattacharya, M. White, N. Beloff, Internet of things, blockchain and shared economy applications, Proc. Comput. Sci. 98, pp. 461-466, 2016.

[8] P. Bylica, Ł. Gleń, P. Janiuk, A. Skrzypczak, A. Zawłocki, A probabilistic nanopayment scheme for golem, Available: http://golemproject.net/doc/GolemNanopayments.pdf, 2015.

[9] P. Hurich, The virtual is real: An argument for characterizing bitcoins as private property, in: Banking & Finance Law Review, vol. 31, Carswell Publishing, 2016.

[10] Prof. Parvaneh Basaligheh. (2020). Mining Of Deep Web Interfaces Using Multi Stage Web Crawler. International Journal of New Practices in Management and Engineering, 9(04), 11 - 16. Retrieved from http://ijnpme.org/index.php/IJNPME/article/view/94

[11] A. Dorri, S.S. Kanhere, R. Jurdak, P. Gauravaram, Blockchain for iot security and privacy: The case study of a smart home, in: IEEE Percom Workshop on Security Privacy and Trust in the Internet of Thing, 2017.

[12] Y. Zhang, J. Wen, The IoT electric business model: Using blockchain technology for the internet of things, Peer-to- Peer Netw. Appl., pp. 1-12, 2016.

[13] J. Sun, J. Yan, K.Z. Zhang, Blockchain-based sharing services: What blockchain technology can contribute to smart cities, Financ. Innov., 2016, DOI: https://doi.org/10.1186/s40854-016-0040-y.

[14] X. Xu, C. Pautasso, L. Zhu, V. Gramoli, A. Ponomarev, A.B. Tran, S. Chen, The blockchain as a software connector, in: The 13th Working IEEE/IFIP Conference on Software Architecture, WICSA, 2016.

[15] E. Nordstr.m, Personal Clouds: Concedo (Master's thesis), Lulea University of Technology, 2015.

[16] J.S. Czepluch, N.Z. Lollike, S.O. Malone, The use of block chain technology in different application domains, in: The IT University of Copenhagen, 2015.

[17] M. Correia, G. S. Veronese, N. F. Neves, and P. Verissimo, Byzantine consensus in asynchronous message-passing systems: a survey, International Journal of Critical Computer-Based Systems, vol. 2, no. 2, pp. 141–161, 2011.

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

[18] S. Bano, A. Sonnino, M. Al-Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, G. Danezis, Consensus in the Age of Blockchains, Available: https://arxiv.org/pdf/1711.03936.pdf, Accessed on 23rd of January, 2018,

[19] Y. Li, Z. Luo, J. Yin, L. D. Xu, Y. Yin, Z. Wu, Enterprise pattern: integrating the business process into a unified enterprise model of modern service company, vol. 11, no. 1, 2015, DOI: https://doi.org/10.1080/17517575.2015.1053415.

[20] A. Meidan, J. A. Garcia-Garcia, M. J. Escalona, I. Ramos, A survey on business processes management suites, Computer Standards & Interfaces, vol. 51, pp. 71-86, 2017.

[21] H. Ariouat, C. Hanachi, E. Andonoff, F. Benaben, A conceptual framework for social business process management, Procedia Computer Science, vol. 112, pp. 703-712, 2017.

[22] F. Rahimi, C. Moller, L. Hvam, Business process management and IT management: the missing integration, International Journal of Information Management, vo. 36, no. 1, pp. 142-154, 2016.

[23] G. Bracha, S. Toueg, Asynchronous consensus and broadcast protocols, Journal of the ACM (JACM), vol.32 no.4, pp.824-840, Oct. 1985.

[24] M. Castro, B. Liskov, Practical Byzantine Fault Tolerance, in the Proceedings of the 3rd Symposium on Operating Systems Design and Implementation, New Orleans, USA, February 1999.

[25] 19 Industries The Blockchain Will Disrupt Online], Available: http://futurethinkers.org/industries-blockchaindisrupt/, Accessed on 5th of February, 2018.

[26] C. Hammerschmidt, Consensus in Blockchain Systems. In Short, Available:https://medium.com/@chrshmmmr/consensus-in-blockchain- systems-in-short-691fc7d1fefe, Accessed on 5th of February, 2018.

[27] A. Baliga, Understanding Blockchain Consensus Models, Whitepaper, 2017.

[28] Paul Garcia, Ian Martin, Laura López, Sigurðsson Ólafur, Matti Virtanen. Enhancing Student Engagement through Machine Learning: A Review. Kuwait Journal of Machine Learning, 2(1). Retrieved from http://kuwaitjournals.com/index.php/kjml/article/view/163

[29] M. Vukolc, The Quest for Scalable Blockchain Fabric: Proof-of-Work vs. BFT Replication, In Proc. IFIP WG 11.4 Workshop Open Res. Problems Netw. Secure. (iNetSec), pp. 112-125, 2015,

[30] L. Lamport, R. Shostak, M. Pease, The Byzantine Generals Problem, ACM Trans. Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, July 1982

[31] Fedor Muratov, Andrei Lebedev, Nikolai Iushkevich, Bulat Nasrulin,Makoto Takemiya Soramitsu, "YAC: BFT Consensus Algorithm for Blockchain", arXiv:1809.00554v1 cs. DC. 3 Sep 2018

[32] Siamak Solat "RDV: An Alternative to Proof-of- Work and a real Decentralized Consensus for Blockchain",ACM ISBN 978-1-4503-6050-0/18/11 http://doi.org/10.1145/3282278.3282283

[33] Tae Kim, Jungha Jin, Keecheon Kim ,"A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority)", 978-1-5386-5041-7/18/ ©2018 IEEE, http://doi.org/10.1145/3282278.3282283

[34] Sungmin Kim, Joongheon Kim "POSTER: Mining with proof of probability in blockchain", ACM ISBN 978-1-4503-5576-6/18/06, http://doi.org/10.1145/3196494.320192

[35] Phil Daian, Rafael Pass, Elaine Shi, "Snow white: Provably secure proofs of stake", Cryptology ePrint Archive Report 2016/919, 2016.

[36] Rafael Pass and Elaine Shi. 2017. The Sleepy Model of Consensus. In ASIACRYPT 2017, Part II (LNCS), Tsuyoshi Takagi and Thomas Peyrin (Eds.),Vol. 10625. Springer, Heidelberg, 380–409

[37] Badertscher, C., Gazi, P., Kiayias, A., Russell, A., & Zikas, V. (2018). Ouroboros Genesis: Composable Proof-of-Stake Blockchains with Dynamic Availability. ACM Conference on Computer and Communications Security

[38] M. Du, Q. Chen and X. Ma, "MBFT: A New Consensus Algorithm for Consortium Blockchain," in IEEE Access, vol. 8, pp. 87665-87675, 2020, doi: 10.1109/ACCESS.2020.2993759. 37. De Angelis, Stefano. (2018). Assessing Security and Performances of Consensus algorithms for Permissioned Blockchains.

[39] Sarfaraz, A., Chakrabortty, R.K. & Essam, D.L. Reputation based proof of cooperation: an efficient and scalable consensus algorithm for supply chain applications. J Ambient Intell Human Comput 14, 7795–7811 (2023). https://doi.org/10.1007/s12652-023-04592-y

[40] Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in International conference on financial cryptography anddata security. Springer, 2014, pp. 436–454.

[41] F. Yang, W. Zhou, Q. Wu, R. Long, N. N. Xiong and M. Zhou, "Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism," in IEEE Access, vol. 7, pp. 118541-118555, 2019, doi: 10.1109/ACCESS.2019.2935149.

[42] Larimer Daniel (2014)."Delegated proof-of-stake (dpos)." Bitshare whitepaper.

[43] RAFT M. Castro and B. Liskov, "Practical Byzantine fault tolerance," in Proc. Symposium on Operating Systems Design and Implementation, 1999, pp. 173-186

[44] Miguel Castro and Barbara Liskov." Practical Byzantine Fault Tolerance". http://pmg.csail.mit.edu/papers/osdi99.pdf, 1999

[45] J. Ray, "Proof of stake FAQ", https://github.com/ethereum/wiki/wiki/Proof-of-Stake-FAQ, 2018.

[46] Nguyen, Giang-Truong, and Kyungbaek Kim. "A Survey about Consensus Algorithms Used in Blockchain." Journal of Information processing systems 14.1 (2018).

[47] Bentov, I., et al. "Proof of activity: extending bitcoin's proof of work via proof of stake. ACM SIGMETRICS Perform." Eval. Rev 42.3 (2014): 34-37.

[48] Milutinovic, Mitar, et al. "Proof of luck: An efficient Blockchain consensus protocol." proceedings of the 1st

*International Journal on Recent and Innovation Trends in Computing and Communication*
*ISSN: 2321-8169 Volume: 11 Issue: 7s*
*DOI: https://doi.org/10.17762/ijritcc.v11i7s.7029*
***Article Received**: 05 April 2023 **Revised:** 22 May 2023 **Accepted:** 05 June 2023*

Workshop on System Software for Trusted Execution. ACM, 2016.

[49] Salimitari, Mehrdad, and Mainak Chatterjee. "An overview of blockchain and consensus protocols for IoT networks." arXiv preprint arXiv:1809.05613 (2018).

[50] Huang, Dongyan, Xiaoli Ma, and Shengli Zhang. "Performance analysis of the Raft consensus algorithm for private blockchains." IEEE Transactions on Systems, Man, and Cybernetics: Systems (2019).

[51] De Angelis, Stefano, et al. "Pbft vs proof-of-authority: applying the cap theorem to permissioned blockchain." (2018).

[52] Yuan, Yong, and Fei-Yue Wang. "Towards Blockchain-based intelligent transportation systems." 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC). IEEE, 2016.