Journal of Information & Optimization Sciences
ISSN 0252-2667 (Print), ISSN 2169-0103 (Online)
Vol. 45 (2024), No. 4, pp. 863–872
DOI : 10.47974/JIOS-1611

Blockchain consensus challenges and an efficient novel consensus mechanism

Avinash Kshirsagar *
Vinod Pachghare †
Department of Computer Engineering
College of Engineering Pune
Pune
Maharashtra
India

Abstract

The blockchain technology has gain great popularity in recent years. As its adoption for different domains is increasing the consensus mechanism, a core part of blockchain technology is also explored to make it more efficient for increasing applicability of blockchain for decentralised applications. Initially most of the application, in which financial domain is dominating, were developed using public blockchains but as different domains are explored the private and consortium blockchains are also used. After studying the challenges faced by the decentralised applications, we have proposed a voting based consensus for consortium blockchain which is efficient and gives high performance. The proposed consensus mechanism is analyzed to capture its performance in terms of throughput and latency.

Subject Classification: *68xx.*

Keywords: *Blockchain, Voting bases consensus mechanism, Performance, Distributed application.*

1. Introduction

Bitcoin, a cryptocurrency which does not require a central authority to regulate it and the very peers in the network can request, validate, execute and ledger transactions amongst the network, was proposed. An anonymous person or group called Satoshi Nakamoto published a whitepaper on it in 2008 [1]. Since the advent of bitcoin not only the cryptocurrencies or banking, finance and insurance domain are evolved

* *E-mail:* **kar18.comp@coeptech.ac.in (Corresponding Author)**
† *E-mail:* **vkp.comp@coeptech.ac.in**

but its underlying technology i.e. blockchain and its applicability in other domains are also drastically explored. The inbuilt features of blockchain that provide security, decentralization i.e. data integrity without presence or dependency on any third trusted party and obscurity creating interesting research areas and applications [2]

The blockchain technology behind Bitcoin consists of a peer-to-peer network in which nodes can communicate with each other. Nodes in the network can initiate a transaction and distribute it into the network, depending on the current pending transaction status, the transaction is processed or added to a queue called transaction pool. These transactions are processed by the miner nodes of the network. Miners are the nodes which take part in the mining process. Once the transaction is validated and upended to the distributed ledger it is then broadcasted in the peer-to-peer network. The process of validating the transactions and adding them to the blockchain is called a consensus mechanism [3].

The consensus mechanisms are broadly divided in two types, namely proof based and voting based consensus mechanism [4]. Each one uses a different mechanism to achieve consensus in the network. These consensus mechanisms have disadvantage which is limiting their use for different domains that is why there is need for new efficient consensus mechanisms [1, 5, 6, 7]. Figure 1 shows some of the challenges.

The blockchain based applications also called as decentralized applications are categorized in three types depending on how the nodes

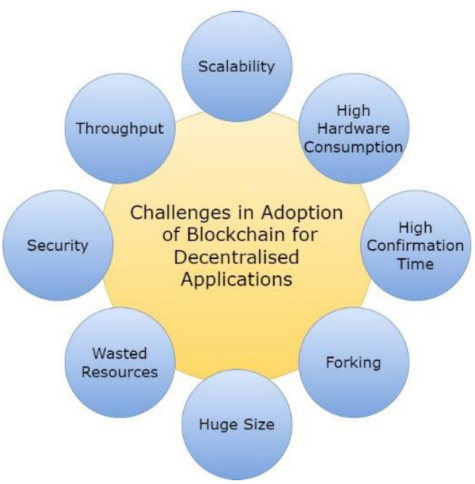

Figure 1

Challenges in Applicability Blockchain

in the network participate and reach consensus, namely Public, Private and Hybrid blockchain based applications [8]. Bitcoin, Ethereum, Litecoin, Monero, Bitcoin Cash, IOTA are a few examples of the public blockchain systems. The public blockchain system does not have a single authority to control the network. This makes it easy for any node to join, take part in the operations or to leave the network. all the data on the blockchain available to everyone in the network.

On the other extreme end, the private blockchain application is controlled by a particular participant of the network, including nodes joining the network or their rights to read or write data from ledger [9]. R3 Corda, Ethereum Enterprise, Multichain, Ripple are some examples of private blockchains. Private blockchain solutions are scalable, efficient and robust but they are permissioned, not as decentralized and have more security concerns [10].

Hybrid blockchain is also called federated blockchain. It is a middle way between the public and private blockchains [11]. Some of the redefined nodes in the network have the same rights over the network activities. Such type of blockchain is suitable for multiparty applications where every party will have equal say and they can reach consensus. These systems are secure and cost- efficient than that of public blockchain systems but are less decentralized so lack transparency [12]. Another type of semi-decentralised blockchain is consortium blockchain. It contains a group of organizations having their own private blockchain applications. A predefined group of nodes takes care of the consensus in the network. Energy web foundation, R3 are some examples of this type of blockchain system [13, 14]. There major benefits are validation is faster and secure, group control, cost and energy efficiency however the structure of the network induces threat, no unified framework and are less transparent.

The scenario of decentralised applications we are targeting while proposing this consensus is consortium blockchain. The proposed consensus is anticipated to solve throughput, consistency and efficiency related issues in the decentralised applications using this consensus mechanism.

The rest of the paper is sectioned to contain details of the consensus mechanisms in different blockchain technology with a focus on voting based consensus mechanisms. It is followed by the consensus mechanisms proposed by other researchers, then we describe the proposed consensus mechanism to improve performance of blockchain based applications with experimentation and result analysis, and finally the conclusions drawn.

2. Voting based Consensus Mechanisms

In a voting based consensus mechanism, the nodes of the network should be able to easily exchange messages between the other nodes of the network. The messages can be for deciding who will be mining the next blocks, validating transactions in the block, deciding new blocks being added to the blockchain or adding new blocks to the ledger or to maintain updated ledger etc.

The major issues faced by voting based consensus mechanism are related to leader failure leading to repetitive validation process, fault tolerance, Network latency - as the nodes in the network need to communicate with each other through messages to reach consensus, if network latency is high the process to get consensus in the network will require more time, or network attacks - as the multiple nodes are there in the network the risk of nodes getting attacked and in turn affecting the consensus happening in the network.

The voting based consensus mechanism should resist crashing of the nodes and subverting of crashed nodes. As in the case of crashed nodes, other nodes of the network keep waiting for receiving messages from the nodes which are crashed and not working in the network. In such a scenario there is not enough evidence to reach a decision, so for n crashed nodes in the network, at least n+1 nodes should be working to reach consensus. The subverted nodes case is defined by the Byzantine Generals problem where nodes of the network behave strangely which affects decision making of the network all together [14].

3. Proposed consensus mechanism

The voting based consensus mechanisms involve a high number of message flows between the network nodes, to reduce the number of these messages in the network, we have divided the network in smaller sub-networks, where a number of nodes come together to form a subnetwork which then communicates with other subnetworks through the leader selected by the nodes of the subnetwork.

3.1 *Network Structure*

There are three types of nodes in the network namely group leaders, leader candidate and group node or ordinary peers as shown in Figure 2. These peers are identified depending on their signatures while participating in different activities.

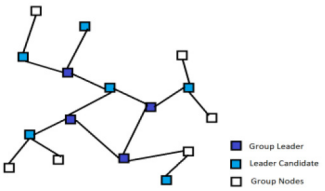

Figure 2

Network Structure

Group leader- representatives of the organizations participating in the blockchain network. They verify the transactions and add a block to the blockchain. Every group leader of the network has the same rights to validate transactions.

Leader candidate - nodes who participate in the election to be a group leader. Once elected they become group leader for the validity of the election otherwise, they need to wait for the next election and act as group node in the network.

Group nodes- ordinary peers on the network, who can join or leave network any time. They contribute to transactions in the network but cannot form a block

3.2 *Block formation and validation*

The total number of nodes of the network will always be less than or equal to the addition of number of group leaders, leader candidates and group nodes The group leader are appointed to generate a new block. Once, a block is generated it is broadcasted to other group leaders for validation, once a block receives confirmation of more than half of the group leaders the block is finalized and added to the blockchain. The last block generated in a tenure contains the information about the election results and from the elected leader blocks are validated in next tenure. The steps involved in the block formation process and the verification of the block to add it to blockchain ledger is given in Algorithm 1.

Algorithm 1: Consensus Mechanism

1: All nodes in the network generate transactions and add to Transaction Pool
2: Take transactions from Transaction Pool for validation
3: **If** Transaction is Valid, **then**

```
4:      Sign the transaction
5:      Send transaction to Group Leader
6:      Group leader generates the block and broadcast to other Group
        Leaders
7:      If block is verified by other Group Leaders, then
8:          Send signature to block sharing Group Leader
9:      If Majority of signatures received, then
10:             Check timestamp for voting cycle timeout
11:             If voting cycle is valid, then
12:             Finalize the block
13:                 Add to blockchain
14:             else
15:                 Neglect the block and form new block
16:             endif
17:         else
18:             Neglect the block and form new block
19:         endif
20:     else
21:         Reject the block and form new block
22:     endif
23: else
24:     Invalidate and reject the transaction
25: endif
26: Broadcast the block to the network
```

4. Comparative Analysis of Consensus Mechanisms

The key performance parameters considered here are the latency and throughput. Latency is the time required to validate a transaction after its been generated and throughput is the number of transactions validated per unit of time. The proposed consensus mechanism is designed considering reducing latency. Reducing latency leads to increasing throughput as the transactions are processed faster, faster they are added to the blockchain.

The comparison of the block generation time and confirmation time of proposed consensus mechanism with experimentation on a fixed number of transactions generation rate of 50 transactions per second with Proof of Work, Ethereum and Scrypt consensus mechanisms is given in Figure 3. Further experimentation is being done for varying workloads and varying number of network nodes.

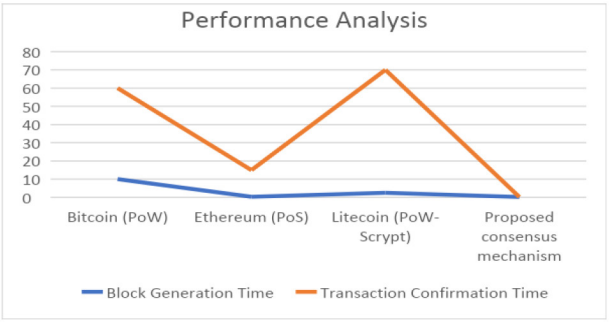

Figure 3

Performance Analysis of Consensus Mechanisms

The proposed consensus mechanism is designed considering reducing latency. Reducing latency leads to increasing throughput as the transactions are processed faster, faster they are added to the blockchain.

Hyperledger fabric platform is used to implement the proposed consensus mechanism. Environmental conditions and configurations are kept consistent during experimentation to evaluate and compare performance of proposed consensus mechanism with Raft and PoW-Ethash consensus mechanisms [8, 16, 17]. The transactions for transferring assets from one node to another node are considered for experimentation and count of transactions is varied between the 2 organizations having 5 peers each in the network. The CPU utilization is the percentage of CPU cores used while processing [18].

Performance of the proposed consensus mechanism is better in terms of throughput and latency as compared to the other consensus mechanisms. Figure 4 gives graphical representation of the throughput and latency of the consensus mechanism for varying number of assets. The proposed

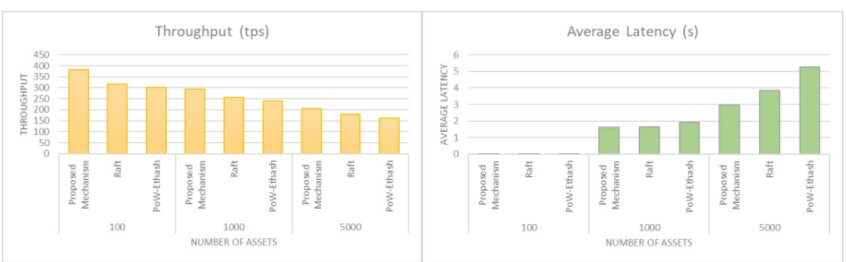

Figure 4

Throughput and Average Latency for Varied Transactions

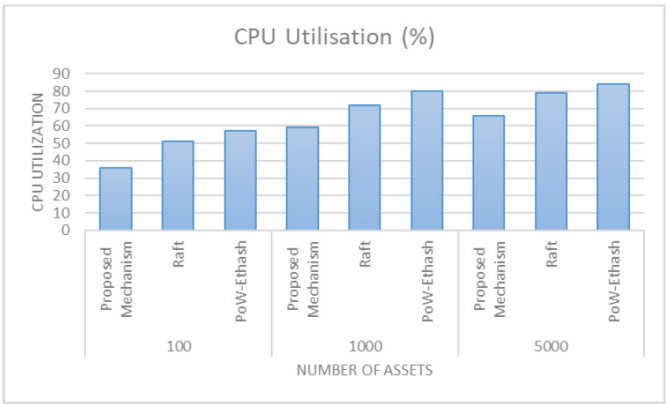

Figure 5

CPU Utilization for Varied Transactions

consensus mechanism's throughput is around 15% higher than that of Raft and 25% higher than that of Pow-Ethash. The CPU utilization indicates that the resources required by the proposed consensus mechanism is less i.e. it is it requires less computational resources. The Figure 5 gives the CPU utilization for the proposed consensus mechanism, raft and PoW-Ethash.

The proposed consensus mechanism is forking proof as there is no possibility of forming a fork to the existing blockchain except the network partitions contain equal number of group leaders. If the network is divided in two parts with different number of group leaders, the partition with a smaller number of group leaders cannot attain majority on validating a block as the number of group leaders is less than half.

5. Conclusion

A novel voting-based consensus mechanisms is proposed for consortium blockchain. The proposed consensus mechanism divides the network nodes in three categories to reduce the number of messages exchanged during the consensus mechanism. The experimentation of the proposed consensus mechanism is done for block generation time and confirmation time, The experimentation for varying number of network nodes and crashes in the network nodes is in progress. The proposed consensus mechanisms have lower block generation time and confirmation time, which increases latency of the network enabling processing of high number of transactions per unit time for the blockchain network.

References

[1] Singh, Arjun, et al. "Blockchain enabled security mechanism for preventing data forgery in IoT-based smart homes." *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 5, pp. 1437–1446 (2023), doi: 10.47974/JDMSC-1769.

[2] Singh, Arjun, Chauhan, Surbhi, Dargar, Shashi Kant, Tharewal, Sumegh, Gutte, Vitthal Sadashiv, Tiwari, Pradeep Kumar & Gupta, Sonam. Blockchain enabled security mechanism for preventing data forgery in IoT-based smart homes, *Journal of Discrete Mathematical Sciences and Cryptography*, 26:5, 1437–1446 ((2023)), DOI: 10.47974/JDMSC-1769.

[3] Ajitha, P., et al. "An IoT-based integrated health monitoring of bulk milk cooler." *Journal of Discrete Mathematical Sciences and Cryptography*, vol. 26, no. 3, (2023) pp. 851-860, doi: 10.47974/JDMSC-1764.

[4] Sharma, Raj Kumar, and Manisha Jailia. "Machine learning and IoT-based garbage detection system for smart cities." *Journal of Information and Optimization Sciences,* vol. 44, no. 3, (2023) pp. 393–406, doi: 10.47974/JIOS-1349.

[5] Hassan, S. I., et al. "A Systematic Review on Monitoring and Advanced Control Strategies in Smart Agriculture." IEEE Access, vol. 9, pp. 32517-32548 (2021), doi: 10.1109/ACCESS.2021.3057865.

[6] Zhao, J. W., et al. "Ground-Level Mapping and Navigating for Agriculture Based on IoT and Computer Vision." *IEEE Access,* vol. 8, pp. 221975-221985 (2020), doi: 10.1109/ACCESS.2020.3043662.

[7] Yang, X.-B., et al. "Hybrid deep learning predictor for smart agriculture sensing based on empirical mode decomposition and gated recurrent unit group model." Sensors, vol. 20, no. 5, pp. 1334 (2020), doi: 10.3390/s20051334.

[8] González-González, M. G., et al. "CitrusYield: A dashboard for mapping yield and fruit quality of citrus in precision agriculture." *Agronomy*, vol. 10, pp. 128 (2020).

[9] Muñoz, M., et al. "An IoT architecture for water resource management in agroindustrial environments: A case study in Almería (Spain)." Sensors, vol. 20, pp. 596 (2020).

[10] Poonia, Ramesh C., et al., eds. Smart Farming Technologies for Sustainable Agricultural Development. IGI Global (2018).

[11] Dadheech, Pankaj, et al. "A neural network-based approach for pest detection and control in modern agriculture using internet of things." Smart agricultural services using deep learning, big data, and IoT. IGI Global, 1-31 (2021).

[12] Ayaz, M., et al. "Internet-of-Things (IoT)-Based Smart Agriculture: Toward Making the Fields Talk." IEEE Access, vol. 7, pp. 129551-129583 (2019), doi: 10.1109/ACCESS.2019.2932609.

[13] Li, H., et al. "Application of Multi-Sensor Image Fusion of Internet of Things in Image Processing." IEEE Access, vol. 6, pp. 50776-50787 (2018), doi: 10.1109/ACCESS.2018.2868227.

[14] Vaibhav Nivrutti Patil and Vijay H. Kalmani, "Enhancing security and ensuring secure performance: A performance evaluation of consensus algorithms in a distributed healthcare blockchain system", *Journal of Statistics & Management Systems*, Vol. 26 (2023).

[15] L. Lamport, R. Shostak, and M. Pease, "The byzantine generals problem," ACM Transactions on Programming Languages and Systems (TOPLAS), vol. 4, no. 3, pp. 382–401 (1982).

[16] "Hyperledger Caliper", Hyperledger Foundation, available at https://github.com/hyperledger/caliper accessed on Nov (2022).

[17] "Hyperledger Besu for private networks", Hyperledger Foundation, available at https://besu.hyperledger.org/en/stable/private-networks/ accessed on Nov (2022).

[18] "Hyperledger Blockchain Performance Metrics", White paper, Hyperledger Foundation, available at hyperledger.org.

[19] A. Gervais, G. O. Karame, K. Wu¨st, et al. "On the security and performance of proof of work blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, March (2016).