SSURJET

Sir Syed University Research Journal of Engineering & Technology
2022, Vol. 12, No. 2,
https://doi.org/10.33317/ssurj.427

Investigating the Impact of Consensus Algorithm on Scalability in Blockchain Systems

Kashif Mehboob Khan[1], and Ansha Zahid[2]

[1]*Department of Software Engineering, NED University of Engineering and Technology, Karachi. Pakistan*

[2]*Department of Computer Science and Information Technology, NED University of Engineering and Technology, Karachi, Pakistan*

Correspondence Author: Kashif Mehboob Khan (kashifmehboob@neduet.edu.pk)

Received January 10, 2022; Revised March 07, 2022; Accepted May 09, 2022

Abstract

Blockchain technology has attracted significant attention primarily due to its potential with respect to achieving trustworthy decentralized architecture through features such as peer-to-peer networks, public ledger management, and an auditable data structure of its transactions. The applications of blockchain are not limited to cryptocurrency but have influenced wider domains through self-accountability, auditability, and transparency. However, blockchain technology has experienced serious challenges, which exposed its limitations to mitigate against undesired circumstances such as the demand for highly scalable solutions. Although there has been a comparative analysis of consensus algorithms and their impacts on scalability, but there have only been comparisons without any detailed empirical investigations and are just based upon the theoretical data shared in the white papers of various blockchain platforms. We have used an empirical analysis-based approach to evaluate the impact of two mostly used consensus algorithms when the system is loaded with the bulk of transactions. This has been achieved by incorporating Proof of Work (PoW) and round robin-based consensus algorithms using separate blockchain networks. The purpose was obvious to investigate and help future research propose more scalable solutions for blockchain systems along with their direct impact on a consensus mechanism. Our experimental investigations have shown that although round robin-based consensus has shown a higher rate of mining transactions into the main consensus blockchain, but at the same time PoW may become a preferred choice in public blockchain networks due to its incentives-based approach in most of the blockchain systems.

Index Terms: *Blockchain, Consensus Algorithm, Empirical Analysis, Multichain, Scalability.*

I. INTRODUCTION

Blockchain technology ensures a decentralized trust-less P2P network of nodes and transparency [1] and [2]. Blockchain network stores all the data in a public ledger which is distributed and shared across all the nodes in the network. This means that the changes are synchronized across all the nodes in real-time. A new transaction is confirmed to the blockchain immediately after the consensus occurs [3]. The state of the blockchain may be triggered with or without a smart contract. The consensus algorithm helps keep the chain intact by enforcing nodes to be agreed upon in the same state of blockchain [4].

The main reason why many applications are using blockchain today is mainly due to its immutability [5]. Blockchain provides a systematic architecture for storing and manipulating data in a way that makes it almost impossible to mutate. All the full running nodes keep a full copy of all the transactions which have ever happened within the network. These transactions are present in the blocks while the blocks are connected via hashes of the respective previous block of the blockchain. These hashes also become a part of the newly created block and are stored in the header of the following block. In this way, the information on the blockchain becomes very difficult to tamper with. Blockchain uses cryptographic functions and techniques to maintain the security and transparency of transactions in a blockchain [6]. Also, there are various consensus mechanisms and algorithms which are used to maintain the consensus and integrity among peers in the decentralized network of blockchain. The verification of a newly created transaction is done by peers for the blocks, which are proposed by miners [7]. The consensus algorithm is considered to be one of the most significant components of a blockchain. Consensus algorithms directly impact over the performance of blockchain whether in terms of security or the context of transaction throughput. There are different types of consensus algorithms, which are used in blockchain technology. These consensus algorithms vary in accordance with their working pattern to keep the blockchain in a consistent state. Proof of Work (PoW) requires a considerable amount of work and energy while proposing a block in a blockchain thereby creating equal opportunity for all the nodes in the network to earn a reward in a public network, while on the other hand, Proof of Stake (PoS) relies on the stake of the miner who is proposing a block in a blockchain [8]. There have been many investigations regarding the consensus mechanisms and algorithms on the basis of their performance, speed, and efficiency. With the advancement in blockchain technology, various types

of new consensus algorithms have been introduced satisfying different requirements of various application domains of blockchain systems [9]. A consensus algorithm can play a crucial role, in the scalability of blockchain applications and requires a thorough empirical investigation to determine scalable blockchain solutions [10]. To the best of our knowledge, there has not been any such detailed empirical analysis performed depending upon the proposed testbed architecture for experimentation in order to conclude their own scalability study of blockchain empirical analysis.

The rest of the paper is organized as follows. Section II highlights a summary of the prominent work in the area of consensus mechanism in blockchain performance for scalability by eminent researchers along with its critical review. Section III presents the proposed blockchain-based network architecture for conducting empirical study and its implementation on our own designed testbed for experimentation. Section III discusses the overall setup and implementation approaches which are needed to be taken care of before the actual execution of experimentation work. Section IV specifically deals with the insights of experimentation work while Section V discusses its outcome followed by Section VI, which elaborates on how our existing work may be extended for future research.

II. RELATED WORK

Table I lists major consensus algorithms which have been investigated and proposed for various blockchain networks. One of the initial primitive forms of consensus algorithms is known as the 'Paxos' algorithm, which is proposed by Leslie Lamport in 1989, whose simplified version was proposed in 2001. Paxos divides the nodes into several classes namely, acceptors, processors, and learners. The role of processors is to mark a tag for the acceptor in the message field. This includes the proposal number. This proposal number is the timely increment meaning that the highest proposal number is the representation of the latest update. The acceptor's role is to cross-check the value of the proposal with the current value of the update and accept or reject the update. This result is then forwarded to all the nodes. The proposer also cross-checks whether the majority of the nodes in the network have been accepted or rejected. If N/2 -1 nodes have accepted then the proposal number is updated to all nodes along with the recent update, else the proposal number is updated back to the recent update number [9]. Since the Paxos algorithm was too complex to implement in practical solutions, therefore the first profound success in the domain of consensus algorithms can be seen with the proposal of PoW. The idea for the PoW-based consensus algorithm in its early form was first originated in 1992 by Dwork and Naor [11]. The key idea was to counter email spamming by attaching a solution with the email. The solution is obtained by solving a computational resource utilizing problem. Nakamoto implemented this concept in his Bitcoin-based blockchain [12]. He categorized nodes of a blockchain network into mining and non-mining nodes. The block is proposed by a mining node after successfully solving the mathematical puzzle for PoW. The rest of the network approves or disapproves of the working of the miner by attempting to verify the PoW working. PoW is known to be a widely used consensus algorithm and has been adapted by many blockchain Platforms such as Ethereum and Bitcoin-based blockchain networks [13]. The second major development came in the form of 'Byzantine Fault Tolerance' in 1999 [14]. This algorithm eliminates one of the most common problems found in blockchains. This is due to the erroneous behavior of the nodes in the distributed ledger, which is known as the Byzantine Fault. Lamport was the one who initially highlighted this issue. This mechanism has the advantage of no stake and less energy usage but is less scalable and has issues of delayed processing and response [15]. A known private blockchain platform, 'Hyperledger' uses this type of algorithm. Although PoW is widely adapted, but the major issue in PoW is its overconsumption of energy. Sunny King shared the idea of PoS in 2012 [16]. The motivation behind the selection of any proposed block is the stake of any validator/miner and its random selection. Peercoin was the first cryptocurrency to adopt PoS. Each node is randomly selected for the generation of blocks which is dependent on the amount or asset of that blockchain network that is possessed by the node. Since the whole concept is based upon the holding of the assets, this arises a big issue of centralization. That is, the mining revolves around the pool of stakeholders only [17]. There are around more than 30 consensus algorithms that exist in the domain of distributed ledger technology. These algorithms are mostly the extension of either PoW or PoS [18]. Delegated PoS is the variant that was developed in 2014 [19]. It restricts or minimizes the number of representatives in a chain and allows sufficient time for proposing a block thereby compromising the decentralization of blockchain. Famous blockchain platforms like Cardano, EOS, and TRON used Delegated Proof of Stake (DPoS) while attempting to scale blockchain networks but lack the empirical investigation necessary to factor transaction throughput into the equation [20]. Proof of Burn (PoB) provides a way in which miners don't have to waste their time and energy but they have to burn some of their existing cryptocurrencies (tokens) in order to claim and get the rewards [21]. PoB has similarities with the PoW. Proof of Capacity, also known as the Proof of Space was introduced by Dziembowski, Faust, Kolmogorov, and Pietrzak in 2015 [22]. In Proof of Space, miners use their free spaces of disks to mine the coins. It is an extension of PoW. Proof of Importance is basically an extended version of the Proof of Stake (PoS) as discussed in detail by Bach et al, in their paper on comparative analysis of consensus algorithm [23]. Although a comparison has been presented by them, but the experimental evaluation and factors affecting the transaction throughput upon scaling the blockchain network were clearly missing. Proof of Weight is a type of consensus algorithm that combines different other algorithms based on the Algorand consensus mechanism [24] and [25]. In this mechanism, weight is attached to each user which is calculated by taking many other factors into consideration. Algorand and PoWeight have similarities with the Proof of Stake (PoS) mechanism. Round Robin consensus algorithm is the algorithm that is mostly used in permissioned chains [26].

In this algorithm, nodes are selected in a pseudo-random manner. The node can only be re-elected after the passage of a predefined time. To reach the consensus, the nodes have to take part in voting. A block is approved only when 66% of the nodes validate it.

Hamida et al discussed the challenges and opportunities for blockchain and also highlight the scalability of blockchain but there has been no thorough or partial empirical investigation of how a consensus algorithm may affect the performance of transaction throughput in a blockchain experimentally. Segregated Witness (also known as SegWit), initially came as a solution to address the scalability issue in the Bitcoin blockchain. One of the major problems of using 'SegWit' is compatibility [27]. The transactions following this scheme remain separated from the conventional transactions of blockchain has split up the bitcoin community into two groups; Bitcoin and Bitcoin Cash (BCH) which is a hard fork. BCH community does not use SegWit. The other problem associated with SegWit is its acceptance by the miners which is not more than one-third of the total network [28]. Although some other attempts to investigate scalable solutions using consensus algorithms such as have been made but either such attempts lack their own empirical investigation in the context of security or do not cover the conventional blockchain ecosystem in general [29] and [30]. We present detailed empirical investigations of consensus algorithms and their direct impacts on scalability using our own built architecture and testbed.

Table I: Summary of Four Kalman Filters used for Estimating Wheel-Rail Interaction Dynamics

Consensus Algorithm	Key Feature
Paxos Algorithm [9]	It divides nodes into several classes namely, acceptors, processors, and learners
Proof of Work [11]	It categorizes nodes of a blockchain network into mining and non-mining nodes. It was initially used for countering email spamming by attaching a solution to it
Byzantine Fault Tolerance [14]	It eliminates one of the most common problems in blockchain networks which occurs due to the erroneous behavior of the nodes in the distributed ledger. This is a Byzantine fault
Proof of Stake [16]	It is built upon the motivation that the selection of any proposed block will primarily be determined via the stake of any validator/miner
Delegated PoS [19]	It minimizes the number of representatives in a chain
Proof of Burn [21]	It lets miners save their time and energy
Proof of Space [22]	It is an extension of PoW and makes use of the disk space of the network for computational purposes
Proof of Importance [23]	It is also an extended version of Proof of Stake (PoS). In this algorithm, nodes are rated in accordance with their stake
Proof of Weight [24]	This algorithm attaches weight to each user which is calculated by taking many other factors into consideration
Round Robin Consensus Algorithm [26]	This is mostly used in permissioned blockchain networks. Nodes are selected in a pseudo-random manner
Segregated Witness [27]	It came as one of the solutions toward scalability but lacks compatibility [27]

III. PROPOSED TESTBED ARCHITECTURE

Figure I represent the architecture of our experimentation setup. It can be seen here that there is a client zone that is responsible for sending automated JSON-based RPC API commands for the multichain service cloud. This service has been called through java based remote clients. Since a blockchain may regulate only one consensus algorithm and it has to be configured while setting up the blockchain network, therefore we created two different blockchain setups for two different types of the consensus algorithm. This is not possible for any blockchain network to change the type of its consensus algorithm once it gets initialized and configured. Java-based remote clients are programmed to use the blockchain's node wallet addresses to utilize Remote Procedure Calls (RPC) commands which are being sent securely through private keys of the respective multichain's node wallet.

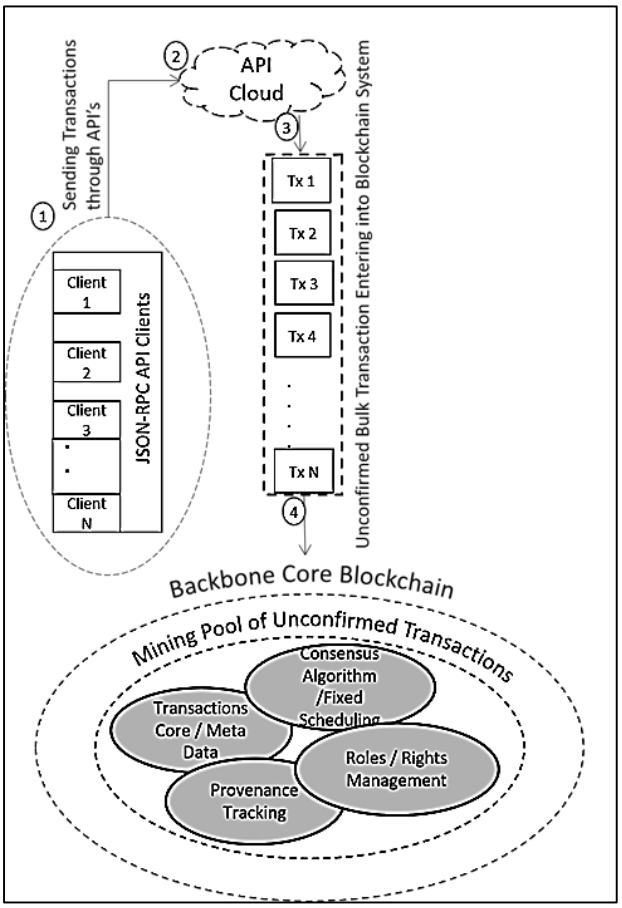

Figure I: Proposed Blockchain-Based Architecture

IV. EXPERIMENTATION

A. Testbed for Blockchain Experimentation

Figure II represents the proposed testbed that has been used in the experiment. We have created a blockchain network of five physical nodes containing one seed node (master node), two connected nodes, and two mining nodes (with varying numbers of independent parallel running mining processes). The network is accessed through JSON-based RPC, APIs by java remote clients. These clients have been programmed to connect to the blockchain network via connected nodes using their wallet addresses.

The same testbed (figure II) has been used for both the blockchain networks with different consensus algorithms (since a blockchain cannot change its major configuration parameters including the type of consensus algorithm after initialization) to observe the impact of the consensus algorithms (Round Robin and PoW) under same network resources and environmental settings [31].

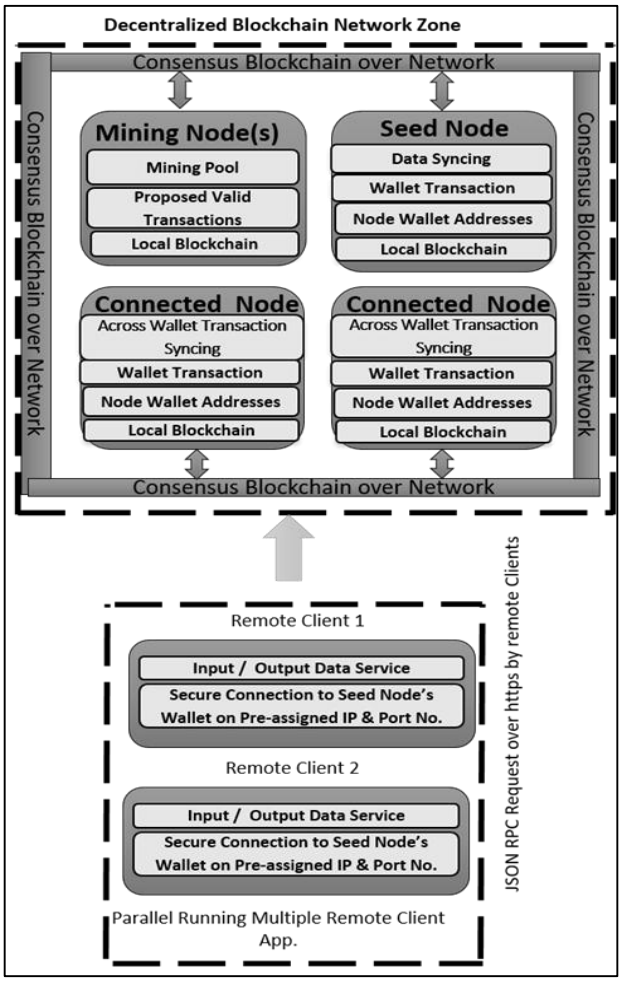

Figure II: Testbed for Experiment

B. System Specifications

The system specification is shown in table II. We performed scalability testing by sending a bulk transaction to each blockchain network. We observed the response in terms of transaction throughput against the same set of loads for incoming transaction flux to measure the impact of a specific consensus algorithm on scalability. In order to enable PoW-based consensus, we need to change the "skip-pow-check" parameter to true or false to enable and disable the PoW algorithm respectively [31]. Table III and table IV refer to our blockchain settings regarding this.

Table II: System Specifications

Platform	**Hardware Specifications**		
Windows	RAM	CPU Hash	Memory
	16 GB	595 h/s*	450 GB

**Hash rate may vary for different algorithms and different CPUs/ GPUs.*

Table III: PoW Based Blockchain Parameters

Parameters	**Values**
Mining Diversity	0.3
Max Block Size	8388608
Block Mining Rate	1 block / 15 s
No. of Miners	6
Skip-Pow-Check	True

Table IV: Round Robin Based Blockchain Parameters

Parameters	**Values**
Mining Diversity	0.4
Max Block Size	8388608
Block Mining Rate	1 block / 10 s
Skip-Pow-Check	False

Figure III: PoW Based Blockchain Specification

Figure IV: Round Robin Based Blockchain Specification

Figure III and figure IV show the console output for the two blockchain configurations.

V. RESULT AND ANALYSIS

A. Transaction Throughput and Execution Time for Single Client

Figure V shows the relations between the number of transactions and time elapsed for Round Robin consensus vs PoW consensus against a single client. It can be seen

evidently that after the passage of time and the system doing a larger number of transactions, the PoW consensus starts taking more time than Round Robin. The reason why initially the difference in the transaction throughput is lesser between round robin and PoW is due to a comparatively fewer number of transactions in the mining pool at the initial stage. As soon as the remote client starts to increase the rate of sending transactions to the network, the waiting time for transactions (in the case of PoW) starts to increase as miners start to engage in more and more back to back transactions causing to build a queue for unconfirmed transaction in the mining pool.

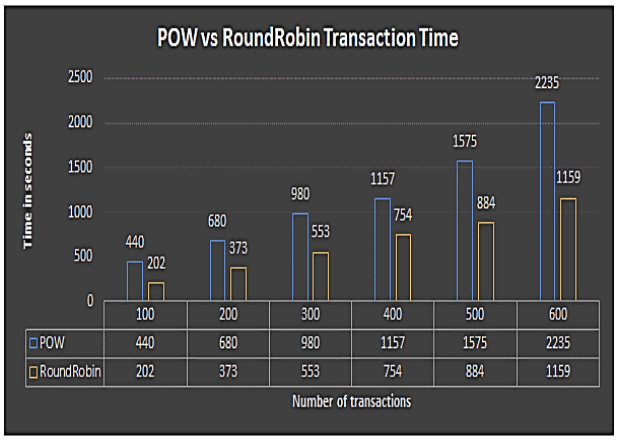

Figure V: POW vs Round Robin Single Client Transaction Time

Figure VI: POW vs Round Robin Single Client Throughput

Figure VI shows the rate of mining transactions and pushing them to the blockchain. Although, in general, round-robin provides a better mining rate, but it should also be put into consideration that round-robin may increase the transaction mining capability of the network in most of the cases, but it is not a preferred choice for permission-less public blockchain network as PoW based network is usually used for incentive-based blockchain model.

B. Transaction Throughput and Execution Time for Two Client

It is evident from figure VII, that PoW has already started to take more time as compared to the network when it is put under the same load using a round robin-based consensus algorithm. The trade-off is very clear, PoW is a preferred choice to avoid getting taking over the network by requiring a considerable amount of effort by a miner or group of miners and supports the cause of decentralization, especially in a larger public blockchain network. If the focus is directed toward increasing the rate of transaction mining, the round-robin is a better choice.

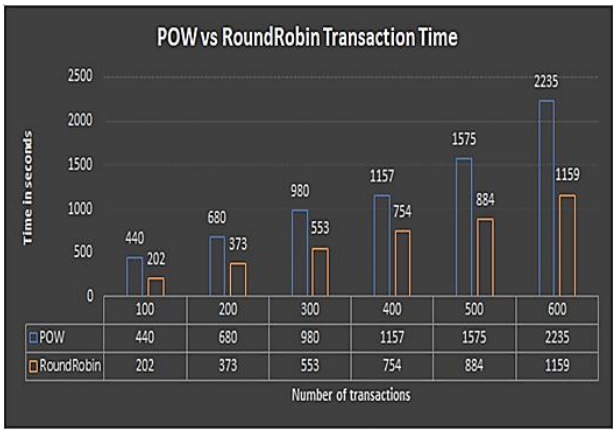

Figure VII: POW vs Round Robin Two Client Transaction Time

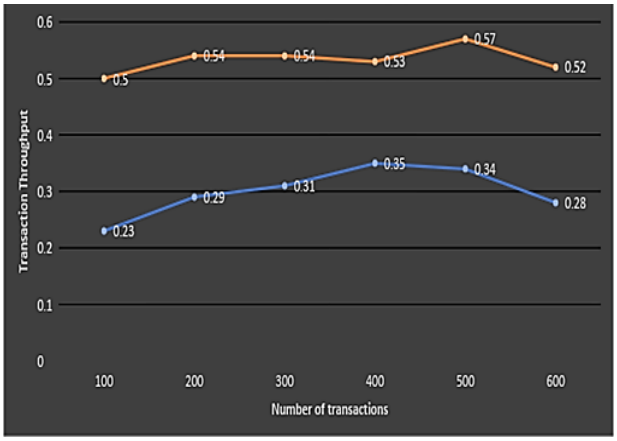

Figure VIII: POW vs Round Robin Two Client Throughput

Figure VIII illustrates the overall behavior of the system when two remote clients are sending bulk transactions to our blockchain network. There has been a significant difference in transaction mining speed against different consensus algorithms.

VI. FUTURE WORK

Our future work aims to determine the impact of consensus algorithms on security. We plan to achieve this by increasing the difficulty level of the mathematical puzzle, which a miner has to solve to claim for the proof of work. This will help determine future research regarding the trade-off and compromising level of security versus transaction throughput and how the consensus algorithm affects this trade-off.

Acknowledgment

The authors would like to thank the NED University of Engineering and Technology, Karachi. Pakistan, for all the support, provided to accomplish this research work.

Authors Contributions

Kashif Mehboob Khan's main contribution to this study was the concept development, correspondence, supervision, and methodology.

Ansha Zahid is an experienced faculty member of NED University. Her main contribution to this paper was the project administration, and paper writing.

Conflict of Interest

There is no conflict of interest between all the authors.

Data Availability Statement

The data has been obtained from the 'GitHub free repository and the links have been provided in the experimentation section where it has been evaluated.

Funding

This research received no external funding.

References

[1] Bitcoin.org. (n.d.). *Bitcoin is an innovative payment network and a new kind of money* : Get started with Bitcoin. Retrieved from: https://bitcoin.org/en/

[2] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain based secure e-voting system. *Future Generation Computer Systems*, *105*, 13-26.

[3] Mail, C. J. (1993, October). Pricing via Processing. In *Advances in Cryptology—CRYPTO'92: 12th Annual International Cryptology Conference, Santa Barbara, California, USA, August 16–20, 1992. Proceedings* (Vol. 740, p. 139). Springer.

[4] Poon, J., & Buterin, V. (2017). Plasma: Scalable autonomous smart contracts. *White paper*, 1-47.

[5] Antonopoulos, A. M. (2014). *Mastering Bitcoin: unlocking digital cryptocurrencies*. " O'Reilly Media, Inc.".

[6] Kogias, E. K., Jovanovic, P., Gailly, N., Khoffi, I., Gasser, L., & Ford, B. (2016). Enhancing bitcoin security and performance with strong consistency via collective signing. In *25th usenix security symposium (usenix security 16)* (pp. 279-296).

[7] Nguyen, G. T., & Kim, K. (2018). A survey about consensus algorithms used in blockchain. *Journal of Information processing systems*, *14*(1), 101-128.

[8] Wikipedia. (2020). *Proof of work*. Retrieved from: https://en.bitcoin.it/wiki/Proof_of_work

[9] Lamport, L. (2001). Paxos made simple. *ACM SIGACT News (Distributed Computing Column) 32, 4 (Whole Number 121, December 2001)*, 51-58.

[10] Eklund, P. W., & Beck, R. (2019, November). Factors that impact blockchain scalability. In *Proceedings of the 11th international conference on management of digital ecosystems* (pp. 126-133).

[11] Laurie, B., & Clayton, R. (2004, May). Proof-of-work proves not to work; version 0.2. In *Workshop on economics and information, security*.

[12] Buterin, V. (2013). Ethereum white paper. *GitHub repository*, *1*, 22-23.

[13] The History of Bitcoin Cash. (2022). *Bitcoin Cash.*. Retrieved from: https://www.bitcoincash.com/

[14] Castro, M., & Liskov, B. (1999, February). Practical byzantine fault tolerance. In *OsDI* (Vol. 99, No. 1999, pp. 173-186).

[15] Choi, B., Sohn, J. Y., Han, D. J., & Moon, J. (2019, July). Scalable network-coded PBFT consensus algorithm. In *2019 IEEE International Symposium on Information Theory (ISIT)* (pp. 857-861). IEEE.

[16] Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, *7*, 85727-85745.

[17] Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, *71*.

[18] Saini, V. (2018). Consensuspedia: An encyclopedia of 30+ consensus algorithms. vol. 30, pp. 1-40.

[19] Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access*, *7*, 118541-118555.

[20] Saad, S. M. S., & Radzi, R. Z. R. M. (2020). Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos). *International Journal of Innovative Computing*, *10*(2).

[21] Karantias, K., Kiayias, A., & Zindros, D. (2020, February). Proof-of-burn. *In International conference on financial cryptography and data security* (pp. 523-540). Springer, Cham.

[22] Li, W., Feng, C., Zhang, L., Xu, H., Cao, B., & Imran, M. A. (2020). A scalable multi-layer pbft consensus for blockchain. *IEEE Transactions on Parallel and Distributed Systems*, *32*(5), 1146-1160.

[23] Bach, L. M., Mihaljevic, B., & Zagar, M. (2018, May). Comparative analysis of blockchain consensus algorithms. In *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)* (pp. 1545-1550). IEEE.

[24] Andrey, A., & Petr, C. (2019, September). Review of existing consensus algorithms blockchain. In *2019 International Conference" Quality Management, Transport and Information Security, Information Technologies"(IT&QM&IS)* (pp. 124-127). IEEE.

[25] Bo, W. A. N. G., Yingqi, R. E. N., & Dongyan, H. U. A. N. G. (2020). H-Algorand: public blockchain consensus mechanism based on multi-block output. *Journal of Computer Applications*, *40*(7), 2150.

[26] Hamida, E. B., Brousmiche, K. L., Levard, H., & Thea, E. (2017, July). Blockchain for enterprise: overview, opportunities and challenges. In *The Thirteenth International Conference on Wireless and Mobile Communications (ICWMC 2017).*

[27] Singh, A., Parizi, R. M., Han, M., Dehghantanha, A., Karimipour, H., & Choo, K. K. R. (2020). Public blockchains scalability: An examination of sharding and segregated witness. In *Blockchain Cybersecurity, Trust and Privacy (pp. 203-232).* Springer, Cham.

[28] Bitclubnetwork.com . (n.d). Bit Club Network. Retrieved from : https://bitclubnetwork.com/.

[29] Biswas, S., Sharif, K., Li, F., Maharjan, S., Mohanty, S. P., & Wang, Y. (2019). PoBT: A lightweight consensus algorithm for scalable IoT business blockchain. *IEEE Internet of Things Journal*, *7*(3), 2343-2355.

[30] Eklund, P. W., & Beck, R. (2019, November). Factors that impact blockchain scalability. In *Proceedings of the 11th international conference on management of digital ecosystems* (pp. 126-133).

[31] Greenspan, G. (2015). Multichain private blockchain-white paper. *Retrieved from: : http://www. multichain. com/download/MultiChain-White-Paper. pdf*, 57-60.