Journal of Statistics & Management Systems
ISSN 0972-0510 (Print), ISSN 2169-0014 (Online)
Vol. 26 (2023), No. 6, pp. 1391–1406
DOI : 10.47974/JSMS-1079

Enhancing security and ensuring secure performance: A performance evaluation of consensus algorithms in a distributed healthcare blockchain system

Vaibhav Nivrutti Patil *
Vijay H. Kalmani †
Department of Computer Science of Engineering
Jain College of Engineering
Belagavi
Karnataka
India

Abstract

Blockchain is an emerging technology in today's real-time applications and database transaction systems—the primary motto is to determine transactional clarity to end-user without any fluctuation. According to the basic block policy, it is immutable or does not allow updating the existing transaction, which automatically maintains the security and transaction clarity. This paper proposes a system performance evaluation of various consensus algorithms in a distributed environment with a peer-to-peer network. The four different consensus algorithms have been evaluated in four peer nodes. Healthcare application has been successfully tested with the entire system. The first blockchain implementation has done in a Java environment with the custom hash generation, mining strategy, and smart contract for each level. Each algorithm provides different time complexity accordingly. The system evaluates the performance of four consensus algorithms sequentially and demonstrates the effectiveness and utilization of each algorithm according to the requirements.

Subject Classification: *Primary 93A30, Secondary 49K15.*

Keywords: *Blockchain, Hash generation, SHA-256, Mining, Smart contract, Consensus algorithms, Performance evaluation criteria.*

1. Introduction

Blockchain technology has slowly appeared in the imagination of people through the advancements in technology, and it has become a

*E-mail: vaibhavpatil521@gmail.com (Corresponding Author)
† E-mail: vijaykalmani@hotmail.com

subject of study by experts and scholars. It is steadily receiving attention from industry and academia. People have been aware of the specific impressive innovation that blockchain technologies bring about or have invested throughout research into financial aspects like finance, insurance, and quality control, further accelerating blockchain technology's maturity and landing by industry. The new blockchain technology is currently emerging in China; initially, the trend of market competition, as well as the independent intellectual property framework, was established. Meanwhile, microscopic properties and applied ecology in energy, medication, and libraries are forming. Its blockchain is a new parallel database and computing framework in which the chain data structure is used to validate the data structure and store data. The distributed node consensus algorithm is used to produce and update data. The cryptography approach is used to maintain data transfer and access protection, as well as intelligent contracts made up of automated scripting.

Decentralized Peer-to-Peer networks, hashed functioning, and smart contracts are the three pillars around which blockchain is built. The mechanism of agreement strongly influences the level of trust among the nodes of the whole blockchain system that getting a collection of processes to settle on a single value by tabulating their individual votes is referred to as "group consensus. We deploy (n) data modules network to the presented blockchain in the proposed system and define all functionalities that perform all consensus mechanisms. Each method produces operations on demand. The custom smart contract and extraction policy we have written will take some time and provide security appropriately. We will make the following modifications to the configuration. This paper studies the various consensus-appropriate performance algorithms using blockchain technology.

2. Review of Literature

The scalable Blockchain-less blockchain agreement algorithm ELASTICO [1] is suggested. The transaction throughput is directly proportional to the difficulty of the mining calculation. That is to say, with greater computer power, more transaction blocks can be handled. This method can deal with a quarter of the total computational power.

A novel computationally scalable byzantine-based consensus mechanism for blockchains, SCP [2], is suggested. By adjusting computational factors like the difficulty of the proof of work (PoW), an algorithm may be made scalable in terms of the amount of bandwidth it

consumes. We anticipate a rise in throughput in tandem with an increase in processing capability. Even miners with little hardware may participate in SCP elections and join the governing council. Furthermore, network decentralization occurs as a direct consequence of transactions being.

For a partly synchronous system, the byzantine consensus issue is explored in [3]. The transition from asynchronous to synchronous mode occurs gradually in a partly synchronous system. Designing a deterministic free leader method for a partly synchronous device is a challenging problem. However, in a leaderless algorithm, all of the nodes eventually come into touch with one another over a series of rounds. In this work, a leaderless procedure for reaching agreement in asynchronous systems was developed. The leaderless consensus procedure developed for synchronous systems is extended to handle partly synchronous systems.

In order to assess the robustness and efficiency of PoW consensus-based blockchains with respect to a variety of network- and consensus-related metrics, [4] implements a quantitative approach. PoW Consensus is supported by several existing blockchains. There is a lack of information in the literature on the safety assessment of PoW variants. The performance-security tradeoff of PoW blockchains requires further research. This article used a simulator to explore this connection by mimicking the blockchain's network and consensus procedure.

The system [5] examined extensive documentation to determine the average fork length, the amount of invalid blocks, the average time to mine a block, and the total number of blocks. The amount of time needed to mine additional blocks rises in tandem with the problem's magnitude. We also evaluate a variety of blockchain-based software. In many blockchain implementations, Proof-of-Work (PoW) is utilized as a consensus mechanism. The Bitcoin system initially appeared. In this process, each node casts its vote by using its computing capacity to solve a proof of work and create new blocks. Bitcoin uses a hash-based proof.

A consensus procedure without a signature, members, or randomization is shown in [7]. By using this approach, we may minimize the complexity of the Byzantine consensus issue from handling several values to only two. The constant-time calculation of a value is made possible by running many concurrent instances of the binary consensus algorithm. The suggested layout has been verified as optimum. According to [8] presents a concept of implicit consensus in which each node operates its own blockchain. The fundamental benefit of this is that capacity is not restricted in any way. The termination property of BFT is changed to a termination property of self-interest.

Implementing a consensus method for proof of stake (PoS) on the blockchain is the subject of this study [9]. Bitcoin's Proof-of-Work system is a hotly contested topic. The computational effort of miners in solving difficult mathematical problems is utilized to choose who will sign blocks. To combat this issue of wasted energy, Proof of Stake (PoS) has been created. The main concept is that nodes with more stakes may contribute to the network by adding blocks more often. Depending on the miner's stake, a new block signer is chosen at random. Block mining power requirements might be drastically reduced compared to PoW's brute-force computation. Both Ouroboros and Casper are widely used.

The proof-of-stake method, discussed in this study [10], reduces energy usage while maintaining the long-term security of a blockchain network. Created as a decentralized crypto currency, peers work together to verify transactions. The introduction of the energy-independent cryptocurrency PPcoin. The development of a proof of stake algorithm is discussed in relation to the concept of the coin period. The timeframe during which a coin's serial number is maintained is known as its "coinage." In contrast to Proof-of-Work, the inventor of a new block is picked in advance based on their wealth. The mining and creation of blocks provide no financial benefit. It saves money since miners aren't wasting time and energy trying to figure out the calculations.

A consensus method is proposed for use in crowdsourcing in [11]. Validators for a transaction are selected in accordance with each node's level of trust. The RAFT leader election method and Shamir's technique for secret sharing are used in its design. It solves the scalability problems that have plagued conventional BFT algorithms. There are four stages to the Consensus algorithm. In the first phase, the Raft Chief Electoral Algorithm is used to elect members to the consortium. In the next stage, voters will choose the transaction validators. The third phase involves a set of nodes (chosen in the second phase) validating the transactions. In the final stage, verified transactions are assembled and linked to the ledger. The impact of multi-transaction windows has also been extensively researched. According to the findings, PoT outperforms competing consensus methods in terms of precision, scalability, and overall performance.

The BFT consensus algorithm that takes into account several perspectives is the subject of [12]'s method. These two problems were present in the PoW and BFT algorithms, and they were fixed in this one. Overhead costs are paid for in PoW. With BFT, incorrect transactions cannot be avoided even if the number of hostile actors in a network were to exponentially increase. There are two groups involved in reaching a

consensus. A BFT algorithm is used in the first stage. The second step is to form clusters of related departments. Before that happens, a verifier is chosen for each section.

Attribute-based encryption is essential for the Internet of Things; say Naregal K. and Kalmani V. in [13]. The study reveals potential issues with implementing ABE for cloud-based IoT applications and suggests approaches to resolving them. The cloud is a multipurpose platform that may be used for a wide range of tasks like data storage, application development, and server management. Due to ABE's ability to grant or deny access to very tiny data sets, it has become a popular encryption method for use in cloud-based services.

The most efficient routing and clustering protocol in WSN, developed by Prakash K. Sonwalkar and Vijay Kalmani, uses a hop-by-hop energy-saving scheme [14]. In this research, we describe a modified load-balancing, energy-efficient sleep-active alert smart routing system for wireless sensor networks, expanding upon the current load-balancing, energy-efficient sleep-awake, aware smart sensor network routing protocol. Improved network coupling between nodes makes this protocol the best choice for clustering and routing in WSNs. Threats to WSNs may be reduced thanks to detection and key management approaches developed by Vijay H. Kalmani and others [15]. Security in WMNs is complicated by the fact that Mesh Clients are constantly moving around and opening themselves up to new threats. In this paper, a security technique is introduced to provide an effective key management system with key agreement, ensuring that the induced network is both linked and secure from any eavesdropping assaults. Based on simulation findings, it's clear that the technique described in this study provides a network secure against malicious eavesdropping attacks.

Himani Bhardwaj et. al. [16] impact of IoT on personalized advertisement on consumer buying behavior. The research is meant to uncover how Indian customers in the NCR feel about targeted marketing via connected devices like smartphones, smartwatches, and smart televisions. Considerations of relevance, usefulness, data collecting, and consumer education all play crucial roles in determining the success of targeted marketing and, eventually, product sales.

Gyana Ranjan Patra et. al. [17] An LSTM-GRU based hybrid framework for secured stock price prediction. The revised closing price of the S&P 500 index has been predicted using a hybrid LSTM-GRU network. The original six characteristics have been expanded to a total of 25 thanks to the addition of a number of technical indicators. The suggested model

is compared to standard LSTM, GRU, and MLP models using performance metrics such as Return ratio, R2, MSE, and the Happiness and Negative thinking ratios.

Rakesh Kumat Pattanaik et. al. [18] proposed a system multilayer recursive model for non-linear dynamic system identification. In this study, a recursive model called the Extreme Learning Machine (ELM) is used because of its quick training and convergence times. However, its flaw is that it only has 1 hidden neuron, which slows down evolution.

Lovleen Kumar Grover et. al. [19] proposed a system an efficient generalized randomized response model. To develop a reliable estimate of the sensitive population fraction, a generalized randomized response model was presented. We also find the variance of the suggested estimate. Our suggested generalized randomized response model has special examples in the pioneering randomized response theory by Warner and the well-known randomized response model of Mangat and Singh. Under relatively simple, achievable settings, we have shown that the suggested approach is more effective than the many current randomized response models.

Sinem Şahnagil et. al. [20] The structures include the creation of a digital transformation office, the establishment of a digital transformation council, the development of a digital transformation strategy, the implementation of digital transformation initiatives, the adoption of digital transformation technologies, and the establishment of a digital transformation governance framework. Additionally, the government has also taken steps to ensure that the digital transformation process is successful by providing resources and support to the public sector, encouraging collaboration between the public and private sectors, and creating a culture of innovation and experimentation.

Rita Roy et. al. [21] usability of the data and the transparency of the data will be improved by using blockchain technology. The data will be stored in a distributed ledger which will be immutable and secure. The data will be shared among the stakeholders in the food supply chain. This will help to reduce the cost of the food supply chain and will also reduce the time taken for the food products to reach the consumers. The blockchain technology will also help to reduce the food wastage and will improve the food safety.

3. Research Methodology

The consensus method that a cryptocurrency adheres to is directly responsible for the verification procedure, the network security, the validation time, and the processing expenses. Many cryptocurrencies add the highest impact on security and de-concentration. Consequently, more cryptocurrencies are using Proof of Work as a protocol for consensus. The other most popular consensus protocol is Proof of Stake because of its verification process. Specific consensus structures can be classified into five major classes based on their strategies and qualities: Work proof; Stake proof; a variant or mixture of PoW; Byzantine load balancing for various versions; and twist. Proof of Work, a formulated decentralized and stable protocol, requires considerable spatial energy to create a block. All cryptocurrencies which follow the PoW algorithm also face scalability problems. Figure 1 specifies proof of work, Figure no 2 specifies proof of stake and Figure no. 3 specifies the delegated proof of stake.

1. The algorithm used in digital currencies algorithm is called PoW, the process of proof of workload.

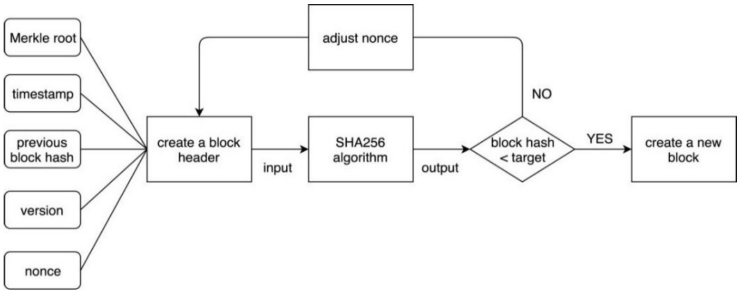

Figure 1

Proof of work

2. Specific function is the estimation of a specific hash value called mining. It is a Block Hash that satisfies demands.
3. The computation time will depend on the hash frequency of the computer to get the right Block Hash requires a lot of test calculations.
4. As long as the workload is complete but everyone listens to it, a new block is formed.
5. While PoW can assure the data consensus to a certain degree, it takes about ten minutes to generate a block. Still, too much computational and power energy to compete are wasted.

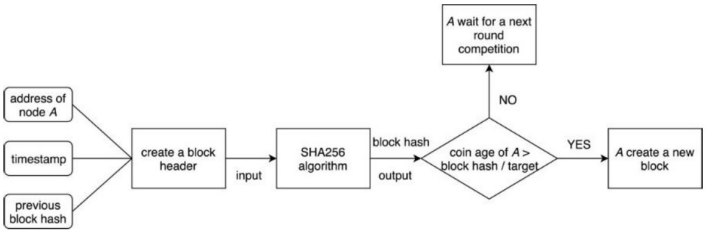

Figure 2

Proof of Stake

1. That form of the process is similar to a company's stock voting scheme, more shares, more control to make decisions.
2. Participants vote on new blocks using their in-band investment money, such as blockchain currency.
3. These methods often randomly choose a shareholder leader and upload a block to the blockchain.
4. The validator wants to mine the next block based on its network economic stake.
5. While PoS is energy efficient, stakeholders involved are more productive
6. If any participant attempts to cheat the system, the system loses its stake.

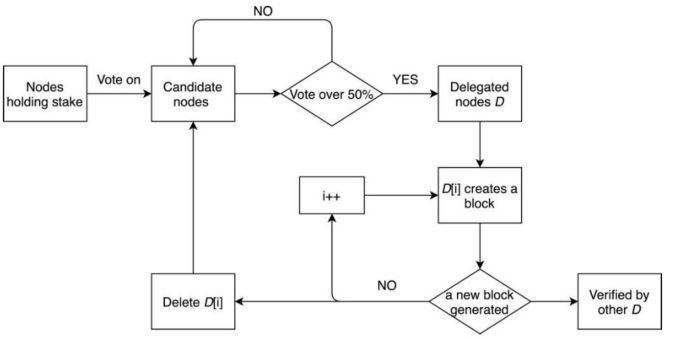

Figure 3

Delegated proof of Stake

1. Throughout the network, top N investigators who took part in the program and received the most votes have the right to be accounted for.

2. The number N of witnesses is formulated in such a way that at least 50% of stakeholders who cast ballots think the level of decentralization is just right.
3. The witnesses elected to build new blocks as allocated one by one and earn some incentives.
4. When a witness cannot establish his allocated block, the block's operation will be shifted to the next block, and the participants will vote to select a new witness.

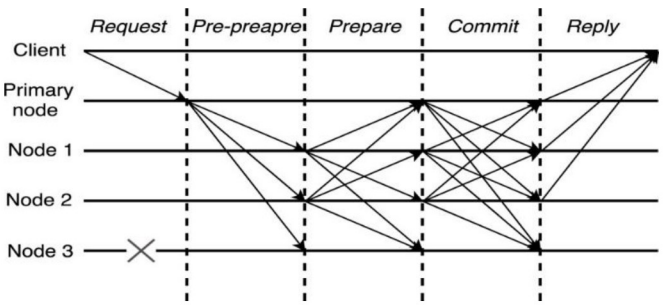

Figure 4

Practical Byzantine Fault Tolerance

1. First, it is an efficient Byzantine-tolerance technique that can be used in real-world distributed systems.
2. The five steps of a PBFT are "ask," "process," "prepare," "commit," and "answer." How PBFT works is explained in Figure 4. The client's message will be relayed to the other nodes in the network by the root node. If node 3 were to fail, it would take five iterations of a single message for such components to come to an agreement.
3. Third, these nodes will communicate with the client in order to reach an agreement. PBFT ensures that all nodes reach an agreement on a shared need and take decisive action when necessary. The goal of great consistency is achieved by PBFT, making it a final, irrevocable consensus algorithm. Figure 4 gives the representation of Practical Byzantine Fault Tolerance.

The proposed system is shown in Figure 5 below, which shows the execution phase, which included the creation of a bespoke blockchain. This study details the strategy for protecting sensitive information while using a blockchain and several consensus methods. The first stage of the

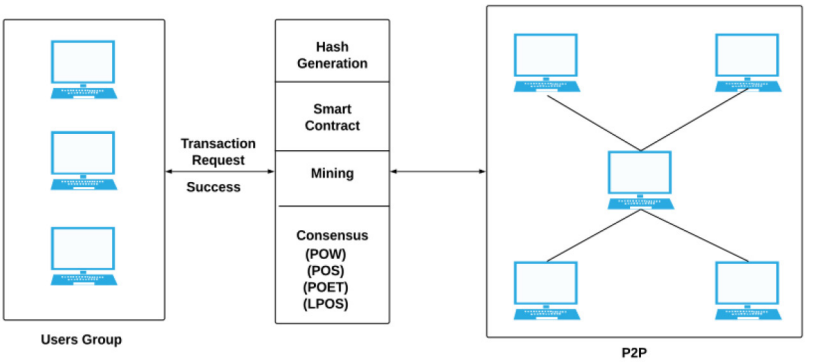

Figure 5

The basic blockchain architecture in cloud with various consensus algorithms

system is a Graphical User Interface through which the user may enter information. We transported an accessible Smart contract for the bespoke blockchain, and each uploading event is treated as a transaction for that block. A hash of the transaction data was generated using the Secure Hash Algorithm 256 (SHA-256). Combining the current hash with the prior hash is how mining policies ensure that a transaction is legitimate. The original transaction system treated this as a Genesis block, with the prior hash serving as the threshold value. The transaction system with many data nodes will become operational after the mining policy has been met. In order to ensure the integrity of all data nodes involved in a transaction, a P2P network uses a variety of consensus techniques. During deployment, we offer the Proof-of-Stake (PoS), Proof-of-Locality (LPoS), and Proof-of-Experience. Figure 5 gives the basic blockchain architecture in cloud with various consensus algorithms.

The simple majority technique was used by the corresponding consensus mechanisms to validate the reliability of the data. The blockchain technology compiles data from a variety of sources in such a way that the resulting material is inaccessible to tampering or modification. Blockchain is indeed a hyper ledger system that possesses various properties, like being distributed, being immutable, having each and almost every transaction recorded, and having the much more secure system possible. Blockchain was initially developed to track crypto currency transactions. Each and every block is combined together for each transaction in the manner of a logistics network, and the network's validity is ensured by the utilization

of transactional cryptography. Blocks were used for every transaction, which led to the system's status as the one with the highest level of security. This method utilizes a highly protected and centralized system, which prevents anyone from gaining unauthorized access to the system's data. It is a very safe ledger, which is also quite helpful when it comes to securing the data and avoiding the transmission of bogus news. Consider taking a look at the following figure 5, which presents an illustration of the framework of our suggested methodology for identifying fake news using blockchain technology.

According to our research problem, a block is a group of the following units: the hash of the parent block, the hash of the contents, the timestamp, the version, and the nonce. Before permanently saving transactions on the distributed ledger, consensus mechanism attempts to check and authenticate the legitimacy of the transactions. We make use of aspects of a consensus technique known as Proof of Work [19]. This algorithm is quite popular. In Proof-of-Work, a node's credibility is determined by its ability to complete a computationally intensive and mathematically challenging task.

4. Algorithm Design

Algorithm I: Initialization of generation of hash for transactional data

Input: input the textual data as Transactional_Data[]

Output: Gen_hash for input textual data

Steps

1. Choose the Transactional_Data[]
2. On Transactional_Data[], Apply the SHA-256 algo
3. Gen_hash= SHA-256(Transactional_Data[])
4. Final hash for input data as Gen_hash

Algorithm II: Peer to Peer verification protocol in m nodes

Input: Client input query as textual data Cur_Node[A_Ch], other silent nodes Nodes_Ch[VMNode_id] and [VMNode_Ch]

Output: In the event that the current cannot validate the chain, automated recovery of the blockchain will occur.

Steps

1. Data, either in the form of transactions or events, that is inputted into the blockchain.
2. Retreivalblockchain of current server for duration [d_duration]
   VMCur_ACh, VMCur_node[ACh]
3. for each

$$NodesCh\ [Nodeid,Ch]\sum_{i=1}^{m}(GetCh)$$

   End for
4. for each (j into VMNode_ACh)
   If (!equalsVMNodeACh[j] to (Current_ACh))
   Flag_Value = 1
   Else
   Continue transaction; to the other nodes, store the data
5. if (Flag_Value == 1)
   BnodeCnt = SimOfNodesBlockch()
6. Carry out the evaluation using the algorithm for majority voting.
   Recover the entirety of the chain based on the data from all servers.
7. End if; end for; end for

Algorithm III. Hash generation by Transaction Mining Technique

Input: SCnt[] Smart contract, CHT[]Current hash Transactions, PHash[] Previous hash

Output: Valid hash generation

Steps

1. Generation of hash_Val for the lth transaction
2. If (Generated_hash_Val is as per to Defined_SCnt [])
   Commit the generated current hash
   Flag_Value =1
   OtherwiseFlag_Value=0
   Continue with next cycle
3. Execute till flag_Value = 1
   Return valid_hash[]

5. Discussion and Conclusion

The consensus protocol is assurance that blockchain networks work stably. Using the consensus mechanism, nodes decide on a specified value or transaction. Through this research, we introduced some common protocols of blockchain consensus and, through review and evaluation, found their strengths, weaknesses, and possibilities for implementation. We hypothesized that the creation of a good consensus protocol would take into account not only strong error detection and also how best to use it in the correct proposed methodology. Figure 6 and 7 provides Time to Commit (4 Nodes), Figure 8 gives it for same nodes with one attack mode.

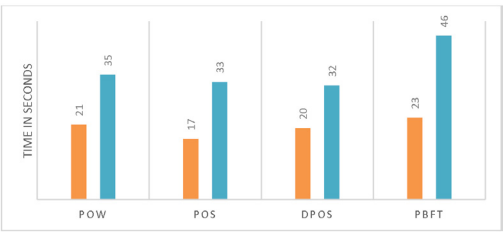

Figure 6

Time to Commit (4 Nodes)

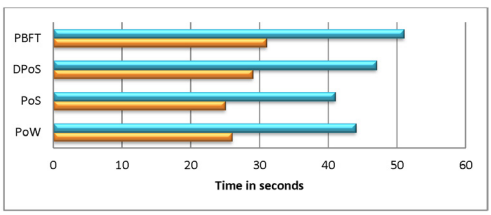

Figure 7

Time to Commit(4 Nodes)

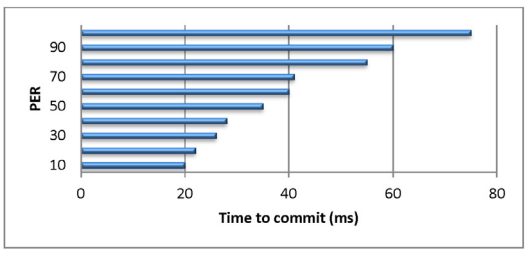

Figure 8

PER vs Time to Commit (4 nodes, network with one attack node)

6. Conclusion and Future Work

The most significant problems with the existing systems for sharing electronic medical records are identified, and effective alternatives to overcome these problems are suggested, all of which are shown using a working prototype. The work that is proposed focuses on building a reliable access-control system that is based upon a single smart contract in order to regulate user access for the purpose of guaranteeing that the transmission of EMRs is both safe and effective. For the purpose of achieving decentralized data storage and data exchange, the peer-to-peer DIFS storage system has been merged with blockchain technology. The results of the implementation reveal that the proposed methodology can, in contrast to existing methods, make it possible for users in the healthcare profession to share medical data across mobile cloud environments in a safe and expedient manner. Particularly, the access control can detect and efficiently prohibit illegal access to the e-health system. This is done with the goal of maintaining the level of patient confidentiality and information security that is sought. On the basis of the advantages of the model, that the blockchain-enabled approach that has been offered is a step towards the effective management of electronic medical data on mobile clouds, which is encouraging in a variety of healthcare uses.

References

[1] L. Luu, V. Narayanan, C. Zheng, K. Baweja, S. Gilbert, and P. Saxena, "A secure sharding protocol for open blockchains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 17–30 (2016).

[2] L. Luu, V. Narayanan, K. Baweja, C. Zheng, S. Gilbert, and P. Saxena, "Scp: A computationally-scalable byzantine consensus protocol for blockchains." IACR Cryptology ePrint Archive, vol. 2015, p. 1168 (2015).

[3] F. Borran and A. Schiper, "A leader-free byzantine consensus algorithm," in International Conference on Distributed Computing and Networking. Springer, pp. 67–78 (2010).

[4] Gervais, G. O. Karame, K. Wu¨st, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work block-

chains," in Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security. ACM, pp. 3–16 (2016).

[5] Porat, A. Pratap, P. Shah, and V. Adkar, "Blockchain consensus: An analysis of proof-of-work and its applications."

[6] Abraham, D. Malkhi et. al., "The blockchain consensus layer and bft," Bulletin of EATCS, vol. 3, no. 123 (2017).

[7] T. Crain, V. Gramoli, M. Larrea, and M. Raynal, "(leader/randomization/signature)-free byzantine consensus for consortium blockchains," (2017) arXiv preprint arXiv:1702.03068.

[8] Z. Ren, K. Cong, J. Pouwelse, and Z. Erkin, "Implicit con- sensus: Blockchain with unbounded throughput," arXiv preprint arXiv:1705.11046 (2017).

[9] E. Garcia Ribera, "Design and implementation of a proof-of-stake consensus algorithm for blockchain," B.S. thesis, UniversitatPolite`cnica de Catalunya (2018).

[10] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof- of-stake," self-published paper, August, vol. 19 (2012).

[11] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A proof-oftrust consensus protocol for enhancing accountability in crowdsourcing services," IEEE Transactions on Services Computing (2018).

[12] S. Jeon, I. Doh, and K. Chae, "Rmbc: Randomized mesh blockchain using dbft consensus algorithm," in Information Networking (ICOIN), 2018 International Conference on. IEEE, pp. 712–717 (2018).

[13] Naregal K, Kalmani V. Study of lightweight ABE for cloud based IoT. In 2020 Fourth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud)(I-SMAC), pp. 134-137. IEEE (2020 Oct 7).

[14] Sonwalkar PK, Kalmani V. Energy Efficient Hop-by-Hop Retransmission and Congestion Mitigation of an Optimum Routing and Clustering Protocol for WSNs. *International Journal of Advanced Computer Science and Applications*; 13(3) (2022).

[15] Kalmani VH, Alias SS, Jogadand RM, Rai HM. An Efficient Key Management Scheme with Key Agreement to Mitigate Malicious Attacks for Wireless Mesh Network. *International Journal of Computer Applications*. 56(6) (2012 Jan 1).

[16] Bhardwaj H, Jamal MS. Effect of using Internet of Things for personalized advertisements on consumer buying behaviour. *Journal of Statistics and Management Systems*; 25(5) : 1135-46 (2022 Jul 4).

[17] Patra GR, Mohanty MN. An LSTM-GRU based hybrid framework for secured stock price prediction. *Journal of Statistics and Management Systems*; 25(6) : 1491-9 (2022 Aug 18).

[18] Pattanaik RK, Pattanayak BK, Mohanty MN. Use of multilayer recursive model for non-linear dynamic system identification. *Journal of Statistics and Management Systems*. 25(6) : 1479-90 (2022 Aug 18).

[19] Grover LK, Kaur A. An efficient generalized randomized response model. *Journal of Statistics and Management Systems*; 25(6) : 1425-41 (2022 Aug 18).

[20] Sinem Şahnagil, H. Salahaddin Gezici, Mustafa Kocaoğlu. Evaluation of digital transformation process through the Presidential Government System: Digital transformation office. *Journal of Information and Optimization Sciences*. Volume 43, 2022 - Issue 7: 7th International Conference on Embracing Trasformation: Innovation and Creation Hybrid (May 26-28, 2022)

[21] Rita Roy, Kavitha Chekuri, G. Sandhya, Surya Kant Pal. Exploring the blockchain for sustainable food supply chain. *Journal of Information and Optimization Sciences*. Volume 43, 2022 - Issue 7: 7th International Conference on Embracing Trasformation: Innovation and Creation Hybrid (May 26-28,2022).

Received February, 2023