Received: January 5, 2024. Revised: February 2, 2024.

INASS

International Journal of
Intelligent Engineering & Systems

http://www.inass.org/

An Optimization of Blockchain Parameters for Improving Consensus and Security in eHealthChain

Sangapillai Banupriya[1]* **Palaniappan Sharmila[2]**

[1]*Department of Computer Science, Navarasam Arts and Science College for Women, Affiliated to Bharathiar University, Arachalur, Erode - 638101, Tamil Nadu, India*
[2]*School of Computing Science, KPR College of Arts Science and Research, Affiliated to Bharathiar University, Arasur, Coimbatore - 641048, Tamil Nadu, India*
*Corresponding author's Email: priyamca126phd@gmail.com

Abstract: In healthcare systems, blockchain technology plays a crucial role in transmitting COVID-19 data among multiple entities. Over time, various blockchain-based medical applications have emerged to handle medical information confidentially. One such system is the Scalable eHealthChain system (SeHealthChain), which utilizes a sharding scheme consisting of transaction chain and reputation chain structures to enhance throughput and security. However, the system employs a modified Raft-based Synchronous Consensus Scheme (RSCS) for generating the transaction blockchain, which can potentially introduce illegitimate transactions to the Hyperledger fabric network if a rogue node transfers them to the orderer. This poses a significant security risk in the worst-case scenarios. Additionally, as the hash rate fluctuates exponentially, the generation period of transaction blocks and computation difficulty increase. To address these issues, this article proposes an Optimized SeHealthChain (OSeHealthChain) system. It integrates a Tuna Swarm Optimization Algorithm (TSOA) with the modified RSCS to dynamically adjust the blockchain parameters in response to significant changes in the hash rate. The TSOA optimizes two variables, namely the Block Interval (BI) and Difficulty Adjustment Interval (DAI) of the Proof-of-Work (PoW) for the transaction blockchain, based on objective functions that consider the Standard Deviations (SD) of the mean BI and difficulty. By selecting appropriate variables, the system generates new transaction blocks with minimal nodes and overhead, effectively validating transactions and blocks to enhance the security level. Extensive simulations show that the OSeHealthChain achieves a throughput of 3918tps and a user-perceived latency of 63.8s for 1000 nodes, outperforming the SeHealthChain, eHealthChain, Permissionless Proof-of-Reputation-X (PL-PoRX), and hybrid Proof of Stake-Practical Byzantine Fault Tolerance (POS-PBFT) algorithms in blockchain systems. It also achieves throughputs of 7051tps, 6418tps, and 6290tps for simple, camouflage, and observe-act attacks, respectively, with 1000 nodes and a shard dimension of 200 during 20 epochs.

Keywords: Blockchain, SeHealthChain, Consensus, Transaction chain, Hyperledger fabric, PoW, Difficulty adjustment, Tuna swarm optimization.

1. Introduction

Blockchain is a decentralized, anonymous security architecture in which individuals inside a state's limits collaborate to validate the system as a whole. Users of a decentralized network, such as an Internet of Things network, need to be trained in the decisions of unknown third parties [1, 2]. Because transactions are recorded in a free ledger perceived by each user, fraudulent transactions can be easily identified. As a result, data privacy is ensured in a decentralized, interference-free fashion [3]. They play a crucial role in paving the way for numerous consequential applications, including industry 4.0, medicine, and smart homes [4-6]. Its main use case is the remote monitoring of medical data and photos [7]. Blockchain technology will be implemented in the pharmaceutical and healthcare industries to eliminate fraudulent transactions and improve traceability [8, 9]. The primary source of the problem can then be

addressed. If a treatment plan is created, patient privacy will be protected. Additionally, this data is unchangeable at this time. This distributed system is implemented using only dedicated machines.

Experts can use the time and resources preserved by these technologies to determine the efficacy of medications, drugs, and actions for a wide range of medical concerns [10]. Distributed ledgers are suitable for preserving and distributing clinical records in the medical sector [11] for the following reasons, according to the blockchain: (i) There are many participants in the medical sector (including patients, doctors, carers and pharmacists); (ii) there needs to be more faith between these participants than there currently is; (iii) without a broker, trustworthiness and profitability increase; (iv) it is vital to observe physiological bio-signals precisely and (v) bio-signatures can be stable over time for detailed inspection.

The proliferation of IoT devices and transaction records has given rise to a new type of Internet service provider: a data broker. Security regulations are buried in legalese, so customers are uncertain about how their private data is gathered, handled, and executed. Blockchain technology may be applied to securely store and share health information about patients generated by healthcare IoT devices. A blockchain-based Personal Health Information Management System (PHIMS) gives patients more authority over their data by facilitating direct interactions between them and healthcare providers, insurance companies, and other organizations [12-13]. However, to employ blockchain technologies for PHIMS applications, novel standards are needed to acquire data from the healthcare IoT system and distribute it to the blockchain for storage.

To solve this problem, Pawar et al. [14] developed eHealthChain, a PHIMS, which applies blockchain technology to manage patient health information. Though medical records can be stored on the blockchain, most solutions rely on off-chain storage techniques that are not decentralized or integrated with blockchain and so are not extensible. Moreover, there have been hardly any investigations of large records, like medical images. However, classical blockchain technology's lack of stability has hindered its widespread adoption in high-throughput, low-latency systems like COVID-19 medical image transfer. For this reason, the SeHealthChain system [15] was developed, which expands the eHealthChain with a novel sharding method based on reputation. A novel dual-chain design consisting of transaction and reputation chains was presented. The Byzantine Fault-Tolerant Consensus (BFTC) was utilized by the reputation chain, whereas a modified RSCS was used by the transaction chain to prevent attacks on the transaction blocks and the related reputation score. Also, the reputation-based sharding and leader decision technique was developed to enhance throughput and security levels.

1.1 Problem description

In modified RSCS for transaction chain structure, illegal transactions may be added to the ledger when a rouge node in the network transfers them to the orderer. It did not consider security measures at transaction block generation, resulting in degrading the system security in the worst case of SeHealthChain. It used a predetermined number of nodes for transaction verification and block generation. Also, the PoW was utilized to determine complex mathematical functions in blockchains. The computation burden was directed by the effort, occasionally modified to handle the hash rate at which novel transaction blocks were generated. If the hash rate increases, then the difficulty also increases. In addition, the transaction block generation period was not maintained when the hash rate increased or reduced exponentially. To combat these issues, the blockchain parameters must be optimized adaptively. Particularly, an optimization algorithm is essential to achieve maximum security level when the number of nodes is optimized for verification of both transactions and blocks a minimum overhead.

1.2 Main contributions

Therefore, in this manuscript, the TSOA is adopted as an additional mechanism to the modified RSCS to optimize the blockchain parameters. The main aim of this algorithm is to fine-tune the BI and DAI of the PoW for the transaction chain structure in SeHealthChain. It responds quickly to an abrupt change in hash rate, such as a huge decrease or increase. The TSOA can find appropriate intervals for difficulty adjustment, to decrease the SD of the mean BI for block generation. It achieves this by optimizing two variables: BI and DAI. Then, the best mixture of variables is elected, and a new transaction block is generated with reduced computation time. This ensures that each transaction chain in the network produces equal and consistent difficulty outcomes, while also achieving a high level of security against various attacks.

The following units are prepared as follows: Section 2 studies various consensus algorithms in blockchain systems. The TSOA for OSeHealthChain is discussed in Section 3 and its efficacy is shown in Section 4. Section 5 summarizes the findings and gives future enhancements.

2. Related works

This section provides a review of various consensus algorithms developed by academics for blockchain applications. One consensus method [16] utilized an enhanced genetic scheme to select the best primary node, improving consensus efficiency and transaction efficacy with backup nodes. However, it did not consider user-perceived latency in the objective function, resulting in high latency. Another blockchain hybrid consensus mechanism [17] integrated POS and PBFT algorithms to optimize delay, throughput, and scalability, but splitting the ledger degraded throughput.

A hybrid consensus method using adapted Proof-of-Probability (PoP) and Delegated POS [18] sent multiple target values across the network during transactions, but high user-perceived latency was observed due to a waiting period.

The PL-PoRX [19] aimed to enhance the PoRX method by replacing the trusted identity record with a novel admission procedure, but it was vulnerable to camouflage attacks. A Jointgraph BFTC mechanism [20] for consortium blockchains used a Dynamic Acyclic Graph (DAG) and observed member behaviors to improve consensus efficiency, but increasing the number of nodes affected throughput and mean interval to consensus.

A blockchain consensus optimization scheme for food traceability [21] used clustering and food credit to select upper consensus nodes, but it resulted in low throughput. Optimization of the PBFT consensus algorithm [22] was designed to improve efficiency, but the user-perceived latency remained high. A blockchain product traceability trusted data analysis and consensus method [23] aimed to enhance PBFT efficiency, especially when increasing the number of Byzantine nodes. The blockchain cross-chain consensus algorithm was improved using weighted PBFT [24], but throughput was inefficient and the security level was compromised. A new K-Nearest Neighbor (KNN)-based consensus mechanism [25] was designed to optimize the consensus mechanism with an SLA guarantee, but the throughput was not satisfactory.

Given the challenges of Hyperledger Fabric and consensus algorithms in the literature, there is a need for a new optimization solution to validate trades and blocks while achieving maximum security and minimizing latency in the blockchain. Therefore, the proposed optimization algorithm aims to minimize latency and maximize security compared to earlier algorithms.

Table 1. Lists of notations

Notations	Description
T	Threshold
D	Difficulty
T_{i+1}	New target
g_T	Genesis block
c_T	Present target
B	Block Interval (BI)
N	Number of blocks (tuna populations)
f_1	Standard variance of mean BI
f_2	Standard variance of difficulty
S_i^{ini}	i^{th} tuna
u_l, l_l	Upper and lower bounds of the search area, respectively
Dim	Population size
$rand$	Random vector
f	Fitness function
S_i^{t+1}	i^{th} tuna in $t+1$ iteration
S_{best}^t	Current best individual
S_{rand}^t	Reference point randomly elected in the tuna swarm
α_1	Weight to control the tuna whirling to the best individual
α_2	Weight to control the tuna whirling to the individual in front of it
a	Constant
t	Current iteration
t_{max}	Maximum iterations
b, γ	Random integers
z	Probability variable
ω	Sliding window parameter
Tx	Transactions

3. Proposed methodology

This section explains the OSeHealthChain system with an optimized consensus algorithm. It introduces TSOA to avoid oscillations in BI and difficulty, allowing quicker adjustment. The execution can respond quicker without waiting for consecutive difficulty adjustments. Also, the difficulty can be adjusted instantly based on important variations in block generation interval. Table 1 lists the notations used in this study.

3.1 Definition of block interval and difficulty adjustment

Blockchain uses PoW for resilience and security. Mining generates new transactions by solving a PoW algorithm (like modified RSCS) using a specific code. The user sets a threshold (T), i.e., target for the block hash to be effective. Difficulty (D) determines how rigid it is to discover a hash lower than the target.

A smaller T can increase D. The new target T_{i+1} is determined, as in Eq. (1):

$$T_{i+1} = T * \frac{\sum_{i=1}^{2016} X_i}{20160\, min} \quad (1)$$

Eq. (1) multiplies T by the original interval it took to generate 2016 blocks and splitting it by the anticipated interval, (i.e., 20160 min). Also, D is computed by Eq. (2).

$$D = \frac{g_T}{c_T} \quad (2)$$

In Eq. (2), g_T is the genesis block's target, and c_T is the present target. The BI (B) (i.e., an anticipated interval to generate a block in a transaction chain), is nearly 10 minutes. A retargeting method can ensure that B is as close as possible to the anticipated 10 minutes. T is adjusted periodically and adaptively to achieve the desired B of 10 minutes. If the BI becomes shorter due to a higher hash rate, T is reduced (maximizing D) during the adjustment, and vice versa. The adjustment is also constrained to prevent sudden changes to D.

On the other hand, when the hash rate suddenly changes, PoW does not respond efficiently. A few blockchain systems observed a drastic change in their hash rates when highly capable mining hardware from other networks was converted for use on their networks. Until the next retargeting event, if sufficient blocks are generated, mining blocks proceed at a glacial pace because it only retargets once every 2016 block.

By taking into account how long it takes to generate a block (the determined output), the difficulty adjustment scheme works as a feedback regulator, with the difficulty serving as the input. It includes some limitations:

1. The BI may fluctuate drastically when the difficulty adjustment over- or undershoots.

2. Transactions are vulnerable to coin-hopping attacks, where users decide only to generate a particular transaction if it is profitable, and alter the other if it is not.

To prevent such problems, a TSOA is adopted into the difficulty adjustment mechanism with a modified RSCS to fine-tune the different blockchain parameters: BI, retargeting period, and so on. It is promising to establish a robust adaptive retargeting method, which can satisfy the network objectives.

Table 2. Modifications between three blockchain network groups

Parameters	**Transaction 1**	**Transaction 2**	**Transaction 3**
BI	10 min	10 min	1 min
Block size	1 MB	1 MB	1 MB
DAI (block)	2016	60	Adaptable within limits
No. of past blocks	2016	60	Similar to difficulty adjustment

3.2 Learning blockchain behaviors using re-parameterization

For the initial analysis, a total of 1000 nodes with equal specifications are utilized to mimic and monitor the blockchain system (dual-chain structure) for various parameter configuration. The nodes are split into 3 independent blockchain system groups: Transaction 1, Transaction 2 and Transaction 3.

1. Transaction 1, a primary blockchain network group, is characterized by an actual transaction network.

2. For Transaction 2, typical values of 10 min and 1 MB are utilized for BI and block size, correspondingly. The difficulty is adjusted every 60 blocks based on Friedenbach's data [26].

3. For Transaction 3, the BI and block size are assigned to 1 min and 1 MB, correspondingly, when the DAI is allocated ranging between 1 and 20000.

These three blockchain networks are permitted to operate for a significant interval, therefore the BI and difficulty attained a steady state. The parameters utilized to deploy the blockchain network are presented in Table 2.

3.3 Parameter fine-tuning using tuna swarm optimization

This study introduces TSOA as a re-parameterization strategy for the PoW protocol to address inefficiencies caused by automatic difficulty adjustment. The TSOA establishes optimal parameters to minimize block generation time. The initial population in the TSOA is the overall actual interval necessary to generate earlier N blocks, ensuring uniformity across nodes. The parameters considered for optimization are BI (sec) and DAI (number of blocks).

The BI must be between 1 and 600 seconds. The DAI determines how many blocks are generated before the difficulty changes. In transaction blockchain, the difficulty changes every 2016 block.

In this study, the minimum DAI is set to retargeting after every 4032 blocks. A multi-objective TSOA is used to consider two objective functions.

- f_1: SD of mean BI.
- f_2: SD of difficulty.

The aim is to reduce the differences in the difficulty and mean BI, as well as to achieve quicker adjustment with the adoption of TSOA, and the objective functions are selected according to these criteria. The TSOA is explained below.

Tuna, a type of marine predatory fish, comes in different sizes. They are skilled hunters who consume various surface and midwater species [27]. Tuna use a unique swimming technique called the "fishtail form" where their inflexible body and long, thin tails allow them to swim swiftly. Tuna struggle to sustain with small fish's fast reaction, so they often engage in "group migratory" predation using their cunning to seek and catch prey. They employ two hunting strategies: spiral hunting and parabolic hunting.

***Initialization*:** TSOA randomly generates primary populations in the search region, as defined in Eq. (3) to optimize BI and DAI:

$$S_i^{ini} = rand \cdot (u_l - l_l) + l_l, i = 1, \dots, N \quad (3)$$

In Eq. (3), S_i^{ini} indicates i^{th} tuna, u_l and l_l are the upper and lower bounds of the hunt region, N denotes the quantity of tuna populations, Dim indicates the population size, and $rand$ defines homogeneously distributed random vector from 0 to N. All individuals S_i^{ini} in the tuna swarm signifies a candidate solution. All tunas have a set of Dim-dimensional integers.

All tunas in the search region determines their fitness function in every iteration.

$$f = [f_1, f_2] \quad (4)$$

The tradeoff between exploitation and exploration is attained by integrating genetic variables in all iterations to create a new population. Tuna locations are also updated based on two foraging strategies.

***1. Spiral hunting*:** Most tuna cannot determine which direction to swim in during hunting for food, but a small percentage of fish can lead the group. The rest of the tuna will follow these leaders when they start pursuing their prey, eventually forming a spiral pattern to capture their target. When using the spiral hunting approach, the tuna swarm can communicate to identify the best individuals to follow. However, even the most skilled individual may sometimes fail to direct the swarm effectively. In such cases, the tuna can choose to follow a random participant of the swarm. This strategy is known as spiral foraging.

$$S_t^{t+1} = \begin{cases} \alpha_1 \cdot \left(S_{rand}^t + \beta \cdot \left|S_{rand}^t - S_i^t\right|\right) + \alpha_2 \cdot S_i^t, \\ \alpha_1 \cdot \left(S_{rand}^t + \beta \cdot \left|S_{rand}^t - S_i^t\right|\right) + \alpha_2 \cdot S_{i-1}^t, \\ \quad i = 1 \\ \quad i = 2,3, \dots, N \quad if\ rand < \dfrac{t}{t_{max}} \\ \alpha_1 \cdot \left(S_{best}^t + \beta \cdot \left|S_{best}^t - S_i^t\right|\right) + \alpha_2 \cdot S_i^t, \\ \alpha_1 \cdot \left(S_{best}^t + \beta \cdot \left|S_{best}^t - S_i^t\right|\right) + \alpha_2 \cdot S_{i-1}^t, \\ \quad i = 1 \\ \quad i = 2,3, \dots, N \quad if\ rand \geq \dfrac{t}{t_{max}} \end{cases} \quad (5)$$

operators, S_{best}^t denotes the current best individual, S_{rand}^t is the reference point randomly elected in the tuna swarm, α_1 is the weight to control the tuna whirling to the best individual, α_2 is the weight to control the tuna whirling to the individual in front of it, β is the distance variable to control the distance between tuna and the best tuna, a is a constant to compute the range of tuna following, t indicates the present iteration, t_{max} denoes the maximum iterations and b indicates an arbitrary value ranging from 0 to 1.

$$\alpha_1 = a + (1 - a) \cdot \frac{t}{t_{max}} \quad (6)$$

$$\alpha_2 = (1 - a) - (1 - a) \cdot \frac{t}{t_{max}} \quad (7)$$

$$\beta = e^{bl} \cdot \cos(2\pi b) \quad (8)$$

$$l = e^{3\cos\left(\left((t_{max} + {}^1/_t) - 1\right)\pi\right)} \quad (9)$$

In Eqns. (5) – (9), S_i^{t+1} indicates i^{th} tuna in $t + 1$, which is created using the crossover and mutation

***2. Parabolic hunting*:** Tunas use both spiral and parabolic patterns to collaborate and feed. They form a parabolic shape based on the location of their prey and also search their surroundings for food. Such methods are utilized together with a 50% chance for all. It is represented by Eq. (10).

$$S_i^{t+1} \begin{cases} S_{best}^t + rand \cdot \left(S_{best}^t - S_i^t\right) + \\ \quad \gamma \cdot p^2 \cdot \left(S_{best}^t - S_i^t\right), \\ \gamma \cdot p^2 \cdot \left(S_{best}^t - S_i^t\right), \\ \quad if\ rand < 0.5 \\ \quad if\ rand \geq 0.5 \end{cases} \quad (10)$$

Where $p = \left(1 - \frac{t}{t_{max}}\right)^{\left(\frac{t}{t_{max}}\right)}$ (11)

In Eq. (10), γ indicates an arbitrary integer of 1 or -1. All tunas arbitrarily choose to use either the spiral or parabolic hunting strategy in every iteration. They can also create new individuals according to the crossover and mutation operators in the hunt space, based on a given probability z. These operators are performed between the best and worst tuna swarms to generate new offspring. This allows the TSOA to select different strategies and produce fresh individual locations. Each tuna is often adapted until the stopping condition is reached. Finally, the TSOA gives the best individual and its optimal BI and DAI. Algorithm 1 presents the optimized consensus mechanism using TSOA to find optimal intervals for block generation and difficulty adjustment.

Algorithm 1 OSeHealthChain System using TSOA

Input: Tuna population size N (i.e., number of blocks), maximum iteration t_{max}, BI, and DAI

Output: Optimal BI and DAI

1. Begin
2. Build a network according to the number of nodes, distribution of degree and region;
3. Repeat
4. Create transaction and reputation blocks;
5. $if\left(\begin{matrix} actual\ interval\ taken\ to\ mine\ the \\ latest\ N\ blocks\ are\ very\ high\ or\ very \\ low \end{matrix}\right)$

//Tuna swarm optimization

6. Generate the initial population of tunas S_i^{ini} $(i = 1, \dots, N)$ arbitrarily;
7. Allocate variables a and z;
8. $while(t < t_{max})$
9. Determine f of each tuna using Eq. (4);
10. Replace the position and value of the best tuna S_{best}^t;
11. $\boldsymbol{for}(all\ tunas)$
12. Modify α_1, α_2, p by Eqns. (6), (7), and (11);
13. $\boldsymbol{if}(rand < z)$
14. Modify S_i^{t+1} using Eq. (3);
15. $\boldsymbol{else\ if}(rand \geq z)$
16. $\boldsymbol{if}(rand < 0.5)$
17. Modify the location S_i^{t+1} using Eq. (5);
18. $\boldsymbol{else\ if}(rand \geq 0.5)$
19. Modify the location S_i^{t+1} using Eq. (10);
20. $\boldsymbol{end\ if}$
21. $\boldsymbol{end\ if}$
22. $\boldsymbol{end\ for}$
23. $\boldsymbol{end\ while}$
24. Discover S_{best} in a search space, and the best fitness value $(f(S_{best}))$;
25. $end\ if$
26. $if(current\ block\ height == difficulty\ adjustment\ interval)$
27. Fine-tune difficulty;
28. $end\ if$
29. Until current block height == 10000;
30. End

As described in Algorithm 1, the blockchain network is initially built based on nodes, degree distribution, and region. Each node is assigned transmission delay, upstream, and downstream bandwidths. Validation is performed on generated blocks to check for extreme mean actual intervals. TSOA is initiated if the interval is significantly different from the scheduled interval. TSOA uses a fitness function for optimization after mining 10000 blocks. This process continues until convergence and optimal solutions are achieved. Optimal results are applied to the network, and new blocks are generated. TSOA waits for difficulty fine-tuning before optimizing again to ensure system throughput and security.

4. Simulation results

This section discusses the simulation environment and provides outcomes of SeHealthChain's using TSOA with RSCS and BFTC mechanisms performance in comparison to other blockchain systems using different consensus algorithms: PL-PoRX [19], POS+PBFT [17], PoW (eHealthChain) [14] and BFTC+RSCS (SeHealthChain) [15]. Python program simulates 1000 nodes for all the existing and proposed SeHealthChain systems to compare the performance according to the throughput and user-perceived latency. Experiments are run on a system configured with a Windows 10 64-bit OS, 4GB of RAM, and a 1TB hard disc powered by an Intel ® Core TM i5-4210 processor running at 2.80GHz.

Table 3 lists the various settings used in the simulations for both existing and proposed blockchain systems. The TBlock's size is 4MB, and the sliding window parameter (ω) is set to 10. There isn't over one-third of the adverse nodes in the network. $S(j)$ is set to 0.1 if the solution is correct, 0 if it is unsure, -0.5 if the answer is incorrect and Tx should be approved but the evaluator erroneously elects to discard, and -1 if the solution is incorrect and Tx should be rejected but the evaluator incorrectly decides to admit. All evaluators are allowed to independently generate Txs and broadcast them to

Table 3. Simulation parameters for blockchain system in cloud-fog applications

Parameters	Global systems	Fog systems	Edge systems	IoT tools
Upstream bandwidth (Mbps)	162	80	33	12.7
Downstream bandwidth (Mbps)	85	37.8	20	8
Memory (GB)	16	8	4	1
CPU facilities (Million Instructions Per Second (MIPS))	14100-20500	8200-12600	4030-8050	500-1600
Transmission delay (ms)	148	50	7	1.3
Blockchain instructions (M)	22	12	6	-
Blockchain processing power (Watts)	20-80	12-40	1.4-20	-

one another. Additionally, the TSOA variables, a and z are assigned to 0.65 and 0.05, correspondingly.

4.1Throughput

It is the number of Txs per second that can be processed by the system. It is calculated as:

$$Throughput = \frac{Number\ of\ Txs}{Time} \quad (12)$$

Fig. 1 presents the mean throughput in terms of transactions per second (tps) of the proposed and existing consensus mechanisms in the blockchain networks. The mean throughput of the OSeHealthChain (TSOA-RSCS+BFTC) using 1000 nodes with a shard size of 200 is 3918tps, which is 55.85%, 36.47%, 26.18%, and 5.89% higher than the PL-PoRX, POS+PBFT, PoW, and BFTC+RSCS schemes in the blockchain system, respectively. Thus, it observed that the TSOA-RSCS+BFTC for the OSeHealthChain system has a better throughput by optimizing BI and DAI for generating blocks rapidl

4.2 User-perceived latency

It is an interval in which a client transmits Tx to the network until the period in which Tx is verified by an authentic node. It is computed by

$$Latency = Tx\ confirmation\ time - Tx\ broadcast\ time \quad (13)$$

Fig. 2 portrays the mean user-perceived latency of the proposed and existing consensus mechanisms in blockchain networks. The mean user-perceived latency of the proposed OSeHealthChain (TSOA-RSCS+BFTC) using 1000 nodes with a shard size of 200 is 63.8s, which is 19.24%, 16.05%, 13.67%, and 5.06% less than the PL-PoRX, POS+PBFT, PoW, and BFTC+RSCS schemes in the blockchain system, respectively. As a result, it is noticed that the TSOA-RSCS+BFTC for the OSeHealthChain system can reduce the transaction delay by adaptively adjusting the blockchain parameters to respond quickly if there is a huge variation in hashes. Also, it results from reducing the SD of mean BI and difficulty, in comparison with the other blockchain systems without an optimized consensus mechanism.

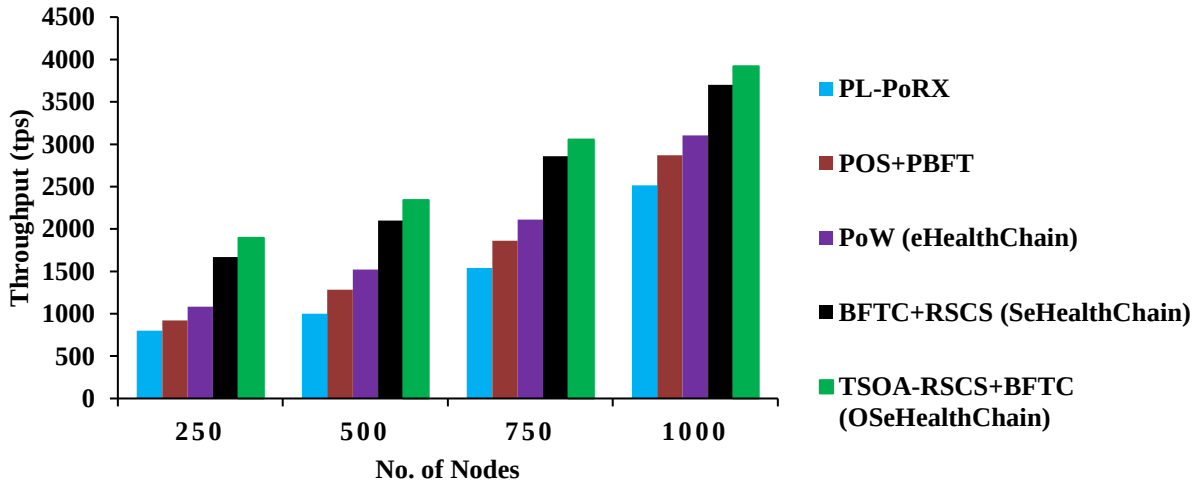

Figure. 1 Comparison of mean throughput vs. No. of nodes

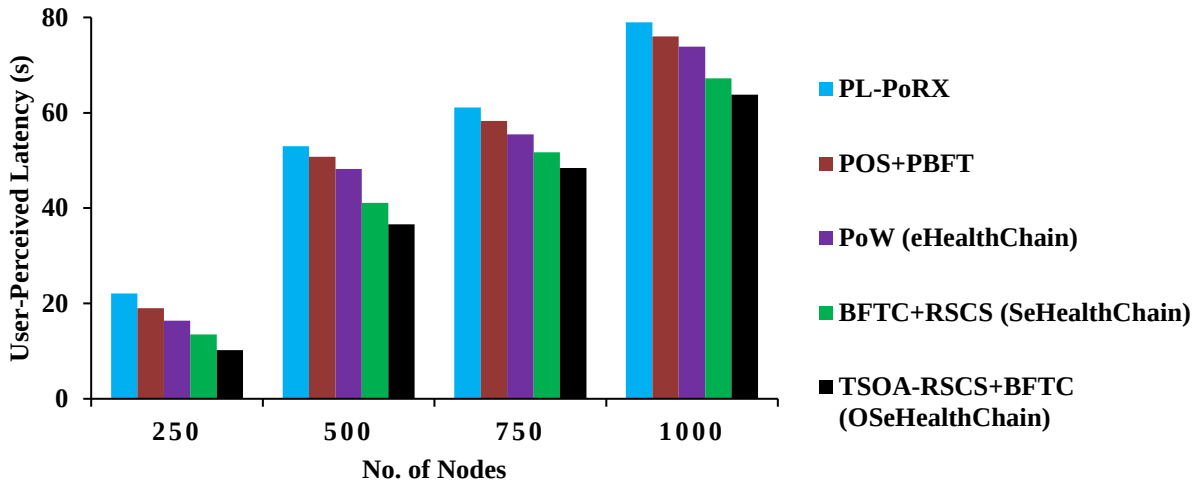

Figure. 2 Comparison of average user-perceived latency vs. No. of nodes

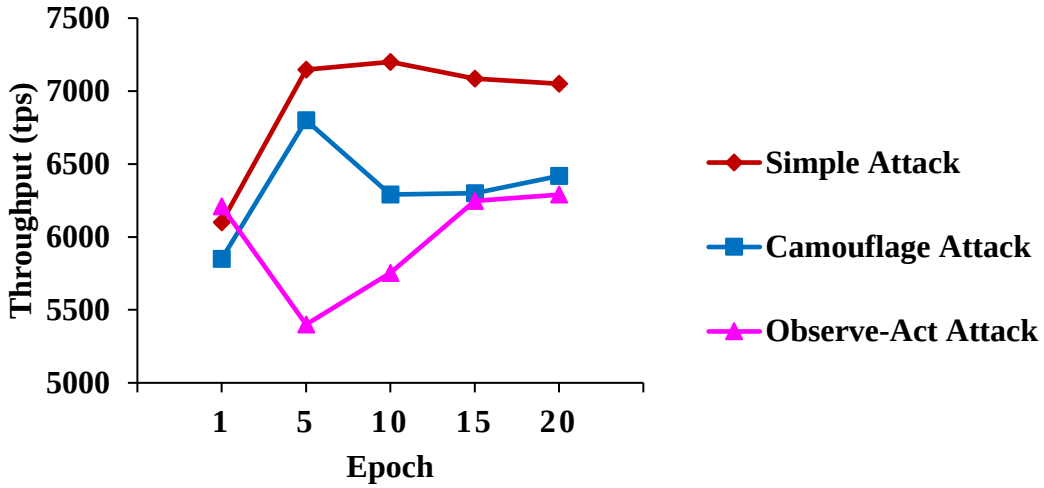

Figure. 3 Mean throughput for different attack models vs. No. of epochs

4.3 Security level

The security level of the proposed OSeHealthChain (using TSOA-RSCS+BFTC) is analyzed by modeling simple, camouflage, and observe-act attacks with 1000 nodes and a shard dimension of 200.

Fig. 3 illustrates the throughput of SeHealthChain under 3 kinds of attacks. It shows that the average throughput for the simple, camouflage, and observe-act attacks is 6916.4tps, 6331.8tps, and 5980.2tps, respectively. Thus, it is concluded that the proposed TSOA-RSCS+BFTC algorithm for the OSeHealthChain system can effectively provide maximum security and robustness against different attacks in the blockchain.

5. Conclusion

This manuscript designed the OSeHealthChain system by introducing TSOA with a difficulty adjustment strategy for modified RSCS for adaptively fine-tuning the blockchain parameters. This was conducted based on the mean BI and DAI of consensus taken for generating transaction blocks. Also, it optimized the SD of mean BI and difficulty for each block to generate a new block with minimum overhead. It ensured that the blockchain could rapidly respond to abrupt changes in hashes and attain a maximum security level against different attacks. The simulation results demonstrated that the OSeHealthChain system outperformed existing blockchain consensus algorithms in terms of throughput and security in medical applications. Specifically, the OSeHealthChain achieved a

throughput of 3918tps and a user-perceived latency of 63.8s for 1000 nodes, surpassing the performance of SeHealthChain, eHealthChain, PL-PoRX, and hybrid POS-PBFT algorithms. Additionally, the OSeHealthChain exhibited throughputs of 7051tps, 6418tps, and 6290tps for simple, camouflage, and observe-act attacks, respectively, with 1000 nodes and a shard dimension of 200 during 20 epochs.

Conflicts of Interest

The authors declare no conflict of interest.

Author Contributions

Conceptualization, methodology, software, validation, Banupriya; formal analysis, investigation, Sharmila; resources, data curation, writing—original draft preparation, Banupriya; writing—review and editing, Banupriya; visualization, supervision, Sharmila.

References

[1] O. Bischoff and S. Seuring, "Opportunities and Limitations of Public Blockchain-Based Supply Chain Traceability", *Modern Supply Chain Research and Applications*, Vol. 3, No. 3, pp. 226-243, 2021.

[2] N. O. Nawari and S. Ravindran, "Blockchain and the Built Environment: Potentials and Limitations", *Journal of Building Engineering*, Vol. 25, p. 100832, 2019.

[3] A. Erdem, S. Ö. Yildirim and P. Angin, "Blockchain for Ensuring Security, Privacy, and Trust in IoT Environments: The State of the Art", *Security, Privacy and Trust in the IoT Environment*, pp. 97-122, 2019.

[4] Y. Himeur, A. Sayed, A. Alsalemi, F. Bensaali, A. Amira, I. Varlamis and G. Dimitrakopoulos, "Blockchain-Based Recommender Systems: Applications, Challenges and Future Opportunities", *Computer Science Review*, Vol. 43, p. 100439, 2022.

[5] B. Bhushan, A. Khamparia, K. M. Sagayam, S. K. Sharma, M. A. Ahad and N. C. Debnath, "Blockchain for Smart Cities: A Review of Architectures, Integration Trends and Future Research Directions", *Sustainable Cities and Society*, Vol. 61, p. 102360, 2020.

[6] K. Yue, Y. Zhang, Y. Chen, Y. Li, L. Zhao, C. Rong and L. Chen, "A survey of Decentralizing Applications via Blockchain: The 5G and Beyond Perspective", *IEEE Communications Surveys & Tutorials*, Vol. 23, No. 4, pp. 2191-2217, 2021.

[7] V. Sharma, A. Gupta, N. U. Hasan, M. Shabaz and I. Ofori, "Blockchain in Secure Healthcare Systems: State of the Art, Limitations, and Future Directions", *Security and Communication Networks*, Vol. 2022, pp. 1-15, 2022.

[8] B. Zaabar, O. Cheikhrouhou, F. Jamil, M. Ammi and M. Abid, "HealthBlock: A Secure Blockchain-Based Healthcare Data Management System", *Computer Networks*, Vol. 200, p. 108500, 2021.

[9] M. Y. Jabarulla and H. N. Lee, "A Blockchain and Artificial Intelligence-Based, Patient-Centric Healthcare System for Combating the COVID-19 Pandemic: Opportunities and Applications", *Healthcare*, Vol. 9, No. 8, p. 1019, 2021.

[10] A. Haleem, M. Javaid, R. P. Singh, R. Suman and S. Rab, "Blockchain Technology Applications in Healthcare: An Overview", *International Journal of Intelligent Networks*, Vol. 2, pp. 130-139, 2021.

[11] P. Sharma, R. Jindal and M. D. Borah, "Healthify: A Blockchain-Based Distributed Application for Health Care", *Applications of Blockchain in Healthcare*, pp. 171-198, 2021.

[12] P. Pawar, T. O. Edoh, M. Singh and N. Parolia, "Hitching Medical IoT Devices to Blockchain for Personal Health Information Management", *Blockchain Technology for IoT Applications*, pp. 191-205, 2021.

[13] T. F. Lee, H. Z. Li and Y. P. Hsieh, "A Blockchain-Based Medical Data Preservation Scheme for Telecare Medical Information Systems", *International Journal of Information Security*, Vol. 20, pp. 589-601, 2021.

[14] S. Banupriya and P. Sharmila, "Reputation-Based Scalable Blockchain System Using Sharding Scheme for High Throughput Low Latency Application in e-Healthchain", *Journal of Data Acquisition and Processing*, Vol. 38, No. 2, pp. 254-270, 2023.

[15] P. Pawar, N. Parolia, S. Shinde, T. O. Edoh and M. Singh, "eHealthChain—A Blockchain-Based Personal Health Information Management System", *Annals of Telecommunications*, Vol. 77, pp. 33-45, 2022.

[16] C. Yang, T. Wang and K. Wang, "A Consensus Mechanism Based on an Improved Genetic Algorithm", *Open Access Library Journal*, Vol. 7, No. 9, pp. 1-6, 2020.

[17] Y. Wu, P. Song and F. Wang, "Hybrid Consensus Algorithm Optimization: A Mathematical Method Based On POS and PBFT

and Its Application in Blockchain", *Mathematical Problems in Engineering*, Vol. 2020, 2020.

[18] B. Wang, Z. Li and H. Li, "Hybrid Consensus Algorithm Based on Modified Proof-Of-Probability and DPoS", *Future Internet*, Vol. 12, No. 8, p. 122, 2020.

[19] J. Bou Abdo, R. El Sibai and J. Demerjian, "Permissionless Proof-Of-Reputation-X: A Hybrid Reputation-Based Consensus Algorithm for Permissionless Blockchains", *Transactions on Emerging Telecommunications Technologies*, Vol. 32, No. 1, p. e4148, 2021.

[20] F. Xiang, W. Huaimin, S. Peichang, O. Xue and Z. Xunhui, "Jointgraph: A DAG-Based Efficient Consensus Algorithm for Consortium Blockchains", *Software: Practice and Experience*, Vol. 51, No. 10, pp. 1987-1999, 2021.

[21] P. Liu, S. Ren, J. Wang, S. Yuan, Y. Nian and Y. Li, "A Blockchain Consensus Optimization-Based Algorithm for Food Traceability", *Mobile Information Systems*, Vol. 2022, pp. 1-7, 2022.

[22] Z. Zhou, X. Zhou, J. Han, P. Lu, Y. Yao and S. Hu, "Optimization Scheme of PBFT Consensus Algorithm Based on Changan Blockchain", *CEUR Workshop Proc.*, Vol. 3206, pp. 1-6, 2022.

[23] Y. Kang, Q. Li and Y. Liu, "Trusted Data Analysis and Consensus Mechanism of Product Traceability Based on Blockchain", *Computational Intelligence and Neuroscience*, Vol. 2022, pp. 1-10, 2022.

[24] L. Lei, L. Song and J. Wan, "Improved Method of Blockchain Cross-Chain Consensus Algorithm Based on Weighted PBFT", *Computational Intelligence and Neuroscience*, Vol. 2022, pp. 1-9, 2022.

[25] Q. Zheng, L. Wang, J. He and T. Li, "KNN-Based Consensus Algorithm for Better Service Level Agreement in Blockchain as a Service (BaaS) Systems", *Electronics*, Vol. 12, No. 6, pp. 1-21, 2023.

[26] M. Friedenbach, "Fast(er) Difficulty Adjustment for Secure Sidechains", (accessed on 20 March 2023). Available online: https://scalingbitcoin.org/transcript/milan2016/fast-difficulty-adjustment.

[27] L. Xie, T. Han, H. Zhou, Z. R. Zhang, B. Han and A. Tang, "Tuna Swarm Optimization: A Novel Swarm-Based Metaheuristic Algorithm for Global Optimization", *Computational Intelligence and Neuroscience*, Vol. 2021, pp. 1-22, 2021.