WJCMS

Wasit Journal of Computer and Mathematics Science

Journal Homepage: https://wjcm.uowasit.edu.iq/index.php/WJCM

e-ISSN: 2788-5879 p-ISSN: 2788-5879

SIMULATION AND EVALUATION OF DİSTRİBUTED CONSENSUS NETWORK FOR MULTİ-AGENT SYSTEMS FOR SYBİL ATTACKS

Jamel Baili[1,*] and Slaheddine JARBOUI[2]

[1]Department of Computer Engineering, College of Computer Science, King Khalid University, Abha 61413, Saudi Arabia
[2]College of Computer Science, King Khalid University. Saudi Arabia

*Corresponding Author: Jamel Baili

Received: September 2023; Accepted: November 2023; Available online: December 2023

ABSTRACT: Distributed average consensus represents the amount of computing of inputs held by multiple agents that communicate through peer-to-peer networks. Collaboration among operators is essential for any distributed standard consensus protocol as every specialist needs to contribute to different operators, typically the adjacent (neighbouring) operators. Internet-of-Things (IoT) implementation is challenging because of its heterogeneous, massively distributed nature. The challenges of this challenge can be addressed with blockchain-based platforms and technologies. Testing and evaluation platforms are required for Blockchain deployments in IoT. A realistic and configurable network environment is presented in this paper to evaluate consensus algorithms. Many blockchain evaluation platforms do not provide a configurable and realistic network environment or are tied to a specific consensus protocol. With our simulator, practitioners can evaluate how consensus algorithms affect network events in congested or contested scenarios to determine the best consensus algorithm. It is proposed to achieve this task by generalizing consensus methods. The Blockchain simulator employs Discrete event network simulations for increased fidelity and scalability. In addition to evaluating the time, state block rate (%), estimation error, average throughput, and simulation time, we evaluate the performance of the proposed techniques based on the number of peer nodes. A comparison of the average transaction delivery rate with a traditional protocol is shown. The proposed protocol has a higher throughput average than the traditional one.

Keywords: PoW, distributed mechanism, PoB, Sybil Attack, Internet-of-Things, distributed average consensus, PoS, agents, NS3.

1. INTRODUCTION

Due to the vast number of applications that blockchain technologies offer across many distributed systems and networks, the hype surrounding them is increasing [1–3]. It is being used in many different scenarios, including traceability, auditing, attestation-as-a-service, regulation, and cooperation, in addition to the fintech applications that made it famous. In distributed computing, sensor networks, autonomous vehicles, and the Internet of Things, researchers have studied cooperative control of multi-agent systems (MASs) for the past decade [4], [5]. Distributed and locally cooperative agents must be forced to agree on some topic in MASs. In consensus control, distributed and locally cooperative agents are controlled by combining graph theory and control systems. The MASs may experience consensus failure due to cyberattacks or network failures, as some agents may become non-cooperative or crash. Therefore, many researchers have studied resilient consensus, which persists in the face of faults or attacks on some agents in the network.

Much recent work has been devoted to MAS resilience to cyber-attacks and a wide range of network situations [6–8].

Resilient consensus prevents malicious agents from interfering with the consensus process by utilizing an appropriate consensus strategy and sufficient network redundancy [9]. According to the authors in [10], resilient consensus protocols can be designed for a time-varying network under certain conditions. Also, in [11], the author considered the resilient consensus problem when switching MASSes. Additionally, constructing corresponding control system attack models based on the impacts of different cyber-attack characteristics is an area of research interest [12], [13]. Data falsification (Byzantine) attacks are the most common attack strategy in MASs, where attackers send inconsistent data to their neighbours in an adversarial manner [14–16].

Every layer of a blockchain is related to a specific aspect. An overview of such a blockchain protocol stack can be seen in Figure 1. The Internet layer has at least three main layers at a coarse description level. Blocks and transactions are disseminated through peer-to-peer protocols that support the blockchain. Peer-to-peer overlays are built using peer-discovery mechanisms, while flooding mechanisms are often used to distribute information [17]. Bitcoin uses a random selection protocol for node discovery, while Ethereum uses a UDP-based protocol [18]. All nodes agree on the evolution of the blockchain using a consensus algorithm. Besides Proof-of-Work, notoriously adopted by Bitcoin, other consensus schemes exist, such as Proof-of-Stake, Proof-of-Authority, and Practical Byzantine Fault Tolerance [19]. Data and transactions are recorded on the consensus layer by the transaction ledger. Due to blockchain 2.0 technology, smart contracts can now be developed using Ethereum. Blockchain smart contracts are programs that represent agreements that are automatically executed and enforced by blockchain nodes. In this program, deterministic execution is triggered when a transaction is generated by an external account (e.g. a user) [1].

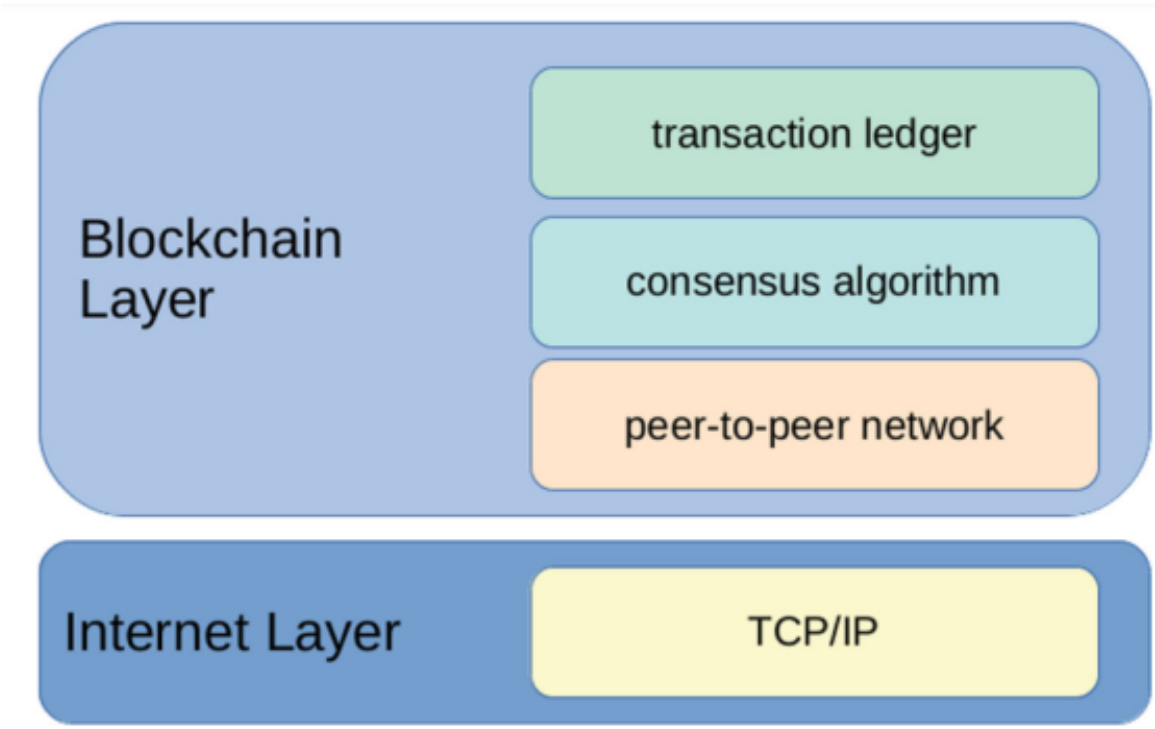

FIGURE 1. Blockchain protocol stack.

Distributed average consensus protocols play a major role in peer-to-peer networks. Distributed average consensus protocols allow agents to share their input values to measure intermediate inputs between agents. Global markets are highly volatile and require rapid and effective responses to the changing demands of high-quality products at low costs. In equipment, machining, assembly, material handling, inspection, and other applications, IoT-enabled Wireless Sensors (WSs) [20], [21] can generate Industrial Big Data (IBD), which can be used to control smart grids [22].

2. LITERATURE REVIEW

In addition to Polkadot [23], Cosmos [24], Blockstream's Liquid [25] and Interledger [26], several mechanisms have been created to facilitate cross-chain transfers. In contrast to our work, these constructions emphasize PoW or private blockchains (Byzantine), require federations, are not decentralized, and lack a formal security model. This study explores

ad-hoc features overlooked in previous threshold multi-signatures, such as [27]. Related primitives have been thought to be useful for enabling PoW sidechains (rather than PoS ones) [28], [29]; however, these works do not provide a formal definition of sidechain security or a complete construction of sidechains. Our definitions and model are also fully applicable to Proof-of-Work (PoW) settings. Open blockchains, or open membership (PoS) blockchains, feature a consensus protocol dedicated to PoS. As part of PoS, validators are responsible for proposing the ledger's next transaction(s). Blocks are used to broadcast these proposals on the network. Blockchains are composed of blocks that build on top of each other. Figure 2 shows the comparision between PoW vesus PoS.

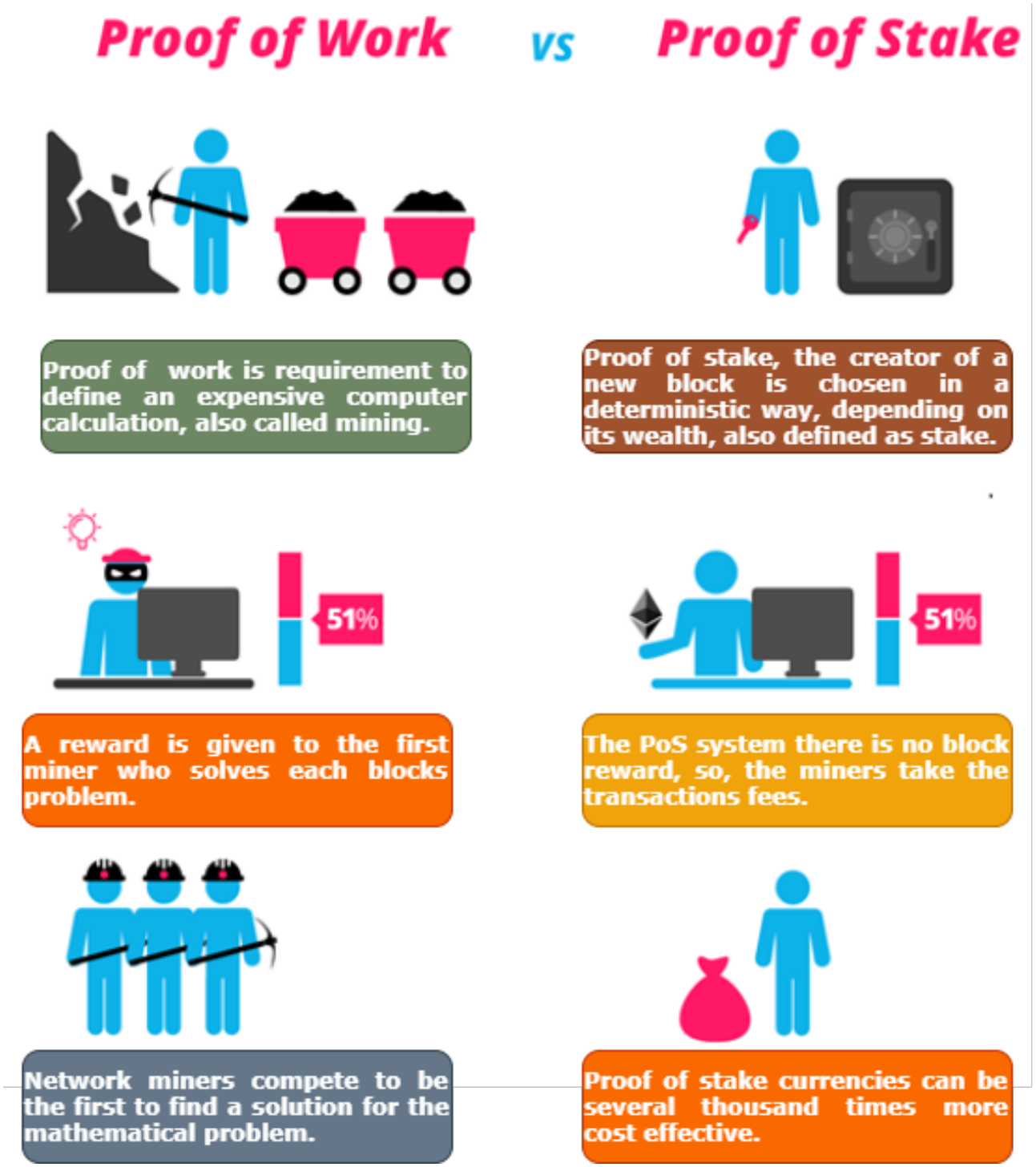

FIGURE 2. PoW vs. PoS.

2.1 PROOF OF WORK (POW)

Blockchain-based cryptocurrencies primarily use PoW as their consensus protocol. Cryptocurrencies like Bitcoin and Ethereum employ different kinds of PoW protocols. In the PoW protocol, each node competes to produce a hash that meets a set of criteria by finding a nonce value. Figure 3 illustrates PoW as a crucial consensus mechanism. The first cryptocurrency to use Bitcoin as a consensus mechanism was Bitcoin, which paved the way for other cryptocurrencies. Initially, Bitcoin [30] used the PoW protocol, followed by Ethereum after a few years [31]. A cryptographic puzzle (technically, a "zero-knowledge proof") must first be solved to determine the node entitled to add the following block to the chain to establish POW consensus. Nodes that add new blocks are known as miners, which is the mining process. When a new block is successfully mined, miners receive a reward in the native cryptocurrency (or part of it). The next block is being made by all nodes in a race. Only computer power is used to make decisions, not logic [32]. Upon finishing a block, a node sends its information to other nodes. Blocks are added to the (block)chain when they have been verified by the nodes that they are correct [33]. Practically, solving this puzzle has become more difficult with time. The process now requires special hardware (ASICs or application-specific integrated circuits), a pool of computing power, and a tremendous amount of electricity [34].

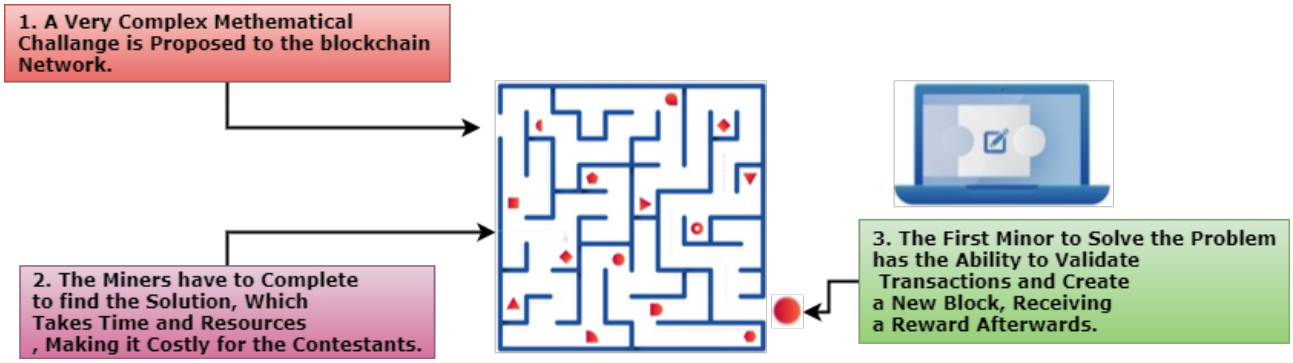

FIGURE 3. **Proof of Work.**

3. METHODOLOGY

Blockchain blocks are balanced in terms of increasing and decreasing blocks. Iteration follows the game theory approach. Network security is rewarded with incentives for miners. A Bitcoin is awarded to those who agree to the rules. The miner suffers when Bitcoin's value plummets because the network stops working. The Nakamoto Consensus has thus been successful in following the above-stated four points. Despite the lack of trust between blocks, it is reliable. Consensus relies on block selection. Competing miners win blocks. Lotteries are used to select the blocks. To read and write on the block, the winning block can be mined by the block's winner. The model is based on the principle of work. Chains are formed from blocks selected. The leader would choose which blocks to continue on the chain if it were BFT [35]; the addition is approved by 2/3 of the number of nodes.

Bitcoin does not use this voting process; mining is based on solving cryptographic puzzles. To reach the first node of the puzzle, you must start with 0.

We suppose that the readers know the Nakamoto consensus mechanism and directly consider the function, equation, and notations to introduce in Figure 4. Transactions are grouped into blocks in the Nakamoto consensus. Each block in the chain of PoW is linked with its predecessor. Blocks have heights equal to the heights of those before them plus one. Once the longest chain has been broadcast and mined, it is mined or received from other nodes through mining. If a trusted node accepts a chain with more than k blocks, it considers block B committed.

In this paper, we demonstrate that the Nakamoto consensus guarantees safety and liveliness in a highly reliable manner. The trusted nodes never commit distinct blocks at the same height.

According to recent research [36], [37], all trusted nodes finally commit every transaction. Two attributes of liveness make up the Nakamoto consensus: chain quality and chain growth.

Assumptions. Homogeneous Poisson point processes are assumed to model PoW mining. Suppose trusted and malicious nodes have mining rates combined and represented by α and β, respectively. This is assumed to be the upper bound of network delay between two trusted nodes. In a network with multiple hops, there is an upper limit to the network delay between two trusted nodes.

Theorem. Suppose $g = e^{-\alpha\triangle}$. The constant δ is assumed to be positive. As far as Nakamoto consensus with the k-confirmation commit rule is concerned, it ensures safety and liveness except in the case of $e^{-\Omega(\delta^2 g^2 k)}$ Probability.

$$g^2\alpha > (1+\delta)\beta \tag{1}$$

Considering network delay, the above condition represents the "trusted majority" condition. Using perfect coordination, malicious nodes can increase the chain's length at the rate β they desire (mining techniques). On the other hand, trusted nodes will experience a (bounded) decrease in their combined mining rate due to the (bounded) network latency. Trusted mining rate depreciation is the primary objective of the proof. Based on the results, liveness loss is at most, and safety loss is at most. g^2. In this paper, $0 < \delta < 1$ is assumed unless otherwise stated.

Poisson processes with rate λ follow a normal distribution with rate $\lambda(t_2 - t_1)$ for the number of events arriving over time intervals (t_1, t_2)

$Pr(T \leq t] = 1 - e^{\lambda t}$ Has a cumulative distribution function and separate exponential distributions for arrival times.

There will be frequent use of the tail bounds listed below. A well-known phenomenon is the Chernoff bound. The appendix contains proof for completeness. Almost identical to the Poisson tail bound is the Chernoff bound and proof. Poisson distributions are limiting cases of binomial distributions, so this is not surprising.

Procedure 1 (Chernoff): In this case, $X = \sum_{i=1}^{n} X_i$ Represent the sum of n independent Boolean random variables. This is μ what I expect from X. For $0 < \delta < 1, Pr(X \leq (1-\delta)\mu] < e^{-\frac{\delta^2\mu}{2}}$. For $0 < \delta < 1, Pr(X \leq (1+\delta)\mu] < e^{-\frac{\delta^2\mu}{2}}$.

Procedure 2 (Poisson tail): Assume that X represents a Poisson random variable with rate μ. For $0 < \delta < 1, Pr(X \leq (1-\delta)\mu] < e^{-\frac{\delta^2\mu}{2}}$. For $0 < \delta < 1, Pr(X \leq (1+\delta)\mu] < e^{-\frac{\delta^2\mu}{2}}$.

PoW requires expensive hardware to run. Mining pools tend to have a specific cost. These machines also consume a lot of power. A centralized system can result from it.

3.1 SECURITY OF BITCOIN

Given the simple rules discussed above, the next question arises: how can blockchain security be ensured? Anyone can join the Bitcoin network easily by creating a node. It is harder to trace the target and owner of the nodes due to their anonymity. A node doesn't determine anonymity but rather a chain of nodes connected, making it impossible to identify a particular node engaged in malicious behaviour.

Since you do not know who to hold responsible if anything goes wrong, many investors have hesitated to invest in Bitcoin technology. The owners aim to secure the system even if they decide to invest and not to add more chains as it grows. A validation rule ensures the chain is secure and malicious behaviour will not occur. Block selection rules ensure that only valid blocks receive enough computational resources. Monetary compensation will be required to add a node that can potentially cause damage to a network. The network's security is maintained because it is difficult for investors to invest. A "random serial dictatorship" approach is used in Bitcoin mining. Equitable resource distribution is a requirement of mechanical design. According to the owner's preferences, the resources are allocated. However, due to anonymity, most selections are based on randomness [38], [39].

One dictator directs the allocation of resources using the serial dictatorship approach; the dictator is not selected randomly but in a decent way. Prior commitments are used in the Bitcoin structure. The cost is high. Anyone may wish to join and can damage the internal workings of the network if they want. Therefore, Bitcoin can be an effective solution to the Byzantine problem. To manage bitcoins, it is necessary to have an understanding of their economic value. It is in the interests of the network to utilize resources equally, which justifies bitcoins.

3.2 SYBİL ATTACK IMPLEMENTATİON

In distributed systems theory, numerous failure modes have been analyzed, and mitigations have been proposed for most of them. It has also been documented that intruders targeted systems they were not members of from the outside and attacked computer systems, beginning in the 1960s [40]. This is despite telecommunication infrastructure abuse being documented as early as the 1960s [36]. The pre-blockchain era's research will most likely apply to permissioned/private systems when considering the previously outlined categories.

Normally, older results cannot be transferred to majority-based systems where potential leaders are unknown a priori (e.g., type II and IV systems) since those constitute a new phenomenon popularized by blockchains. Due to the lack of authority to differentiate between trustworthy and malicious entities, such systems fundamentally differ from prior deployments from an attack perspective. There is, therefore, no practical way to mitigate intrusion risks using common approaches such as identity management, user authentication, or encryption [37]. A scenario where malicious users may present arbitrarily large numbers of identities renders common strategies to improve fault tolerance useless. In large-scale peer-to-peer systems without trusted authorities, arbitrary entities presenting malice are commonly known as the Sybil

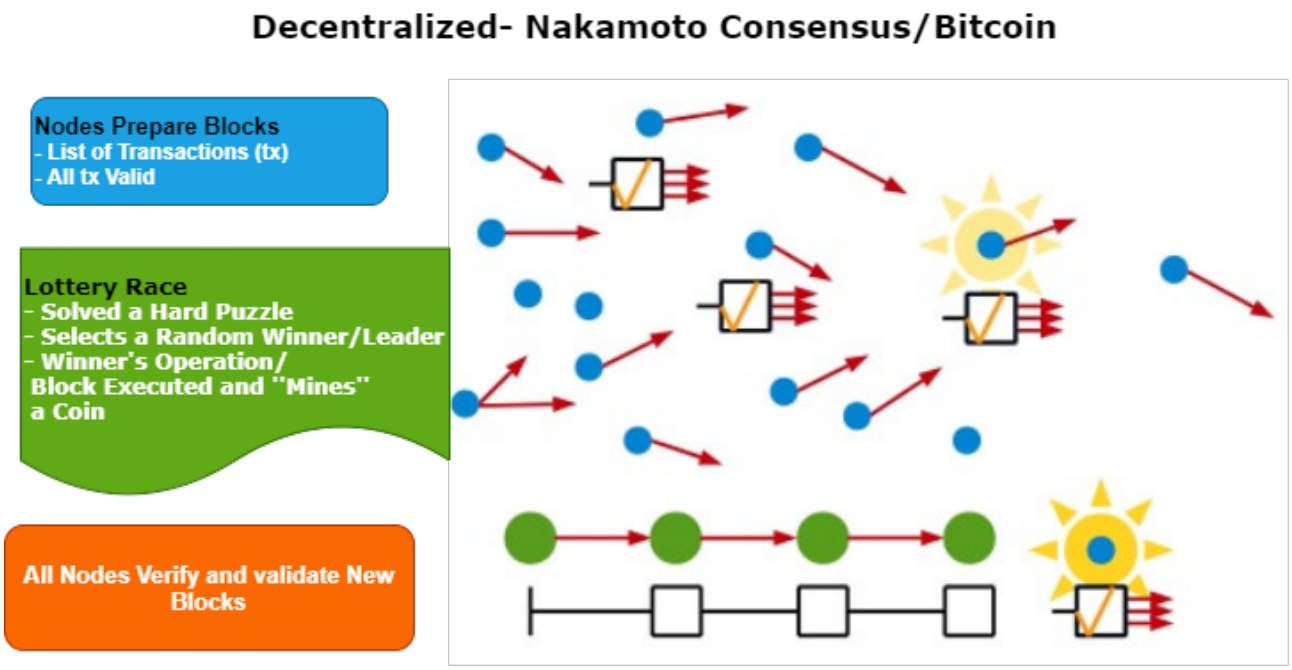

FIGURE 4. **Nakamoto Consensus.**

Attack [41]. In decentralised systems, conflicting information from multiple peers must be resolved to maintain a correct system state when faced with conflicting information from multiple peers. The main challenge when dealing with such scenarios is determining which information is correct. Sybil attacks were carried out by creating an overwhelming number of fake identities on the network, as illustrated in Figure 5.

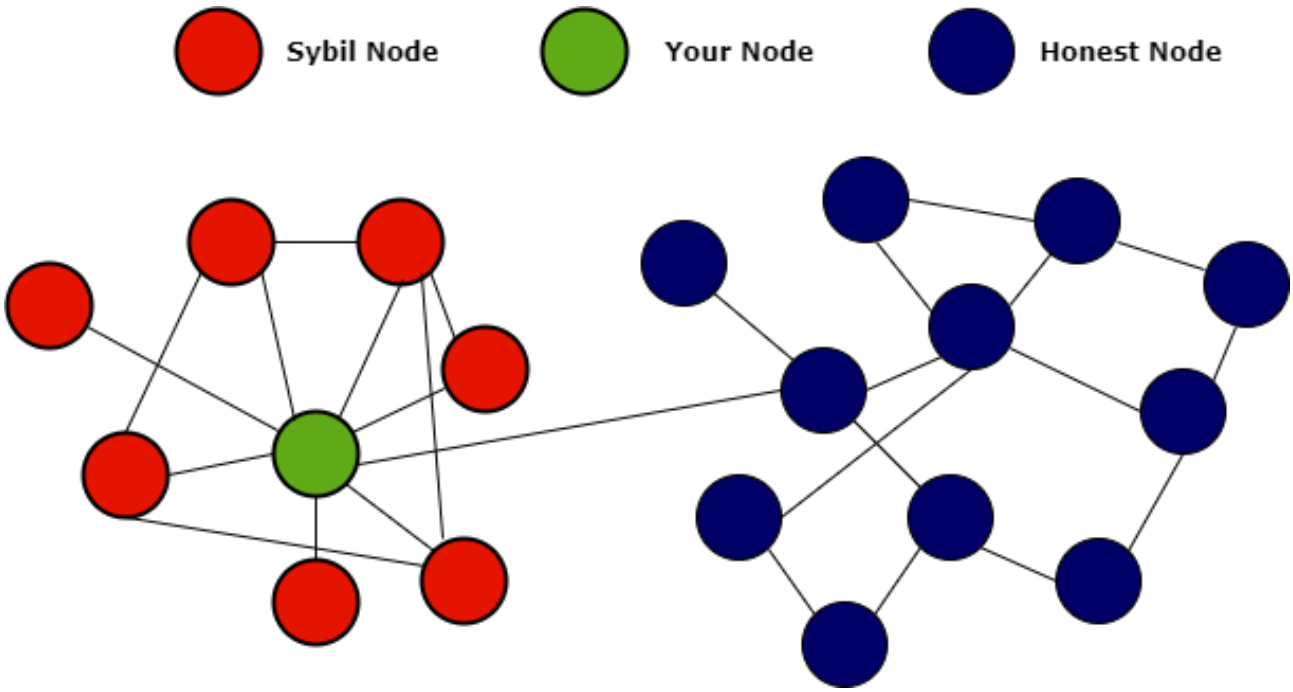

FIGURE 5. **Sybil attack**

Technology has made energy production less complex, thanks to advancements in science. Energy plays a significant role in technological discoveries. It is natural to ask how much power can be generated to advance technologies without

compromising their uses. Small rechargeable batteries have been popularly and extensively employed to resolve the complex nature of energy production. There remains, however, a challenge to reduce the technological gap between the power industry and advancing technologies. Green computing has been made possible by blockchain technology. It still considers the energy requirement of technology even though it aims to utilize energy efficiently.

Consider a simple blockchain model in which all users are divided into two groups: trusted and adversarial. To carry out a private attack, The ledger is overturned by malicious users. The total mining rate is β power of all users is assumed to remain constant. Consider an adversarial user β and that $\beta < 1/2$ who has a fraction of "hash power" of (figure 6).

Truthful users assume that all communications are instantaneous, so transmissions are not delayed. Both the private and public chains grow simultaneously after the private attack (visible only to opposing parties) rate of $\beta\lambda$ and $(1 - \beta)\lambda$ respectively. For a private attack to succeed, mining must be random. When k or more trusted blocks are overturned by a private attack (from block B), it is considered successful. To accomplish this, adversarial users must mine more blocks over a long time than authorized users. Take the Genesis block as the starting point of the private assault for the sake of simplicity. It is either fortunate for the opponent (mine blocks appear earlier than anticipated) or unlucky (mine blocks appear later than anticipated). It will not be possible to attack otherwise successfully.

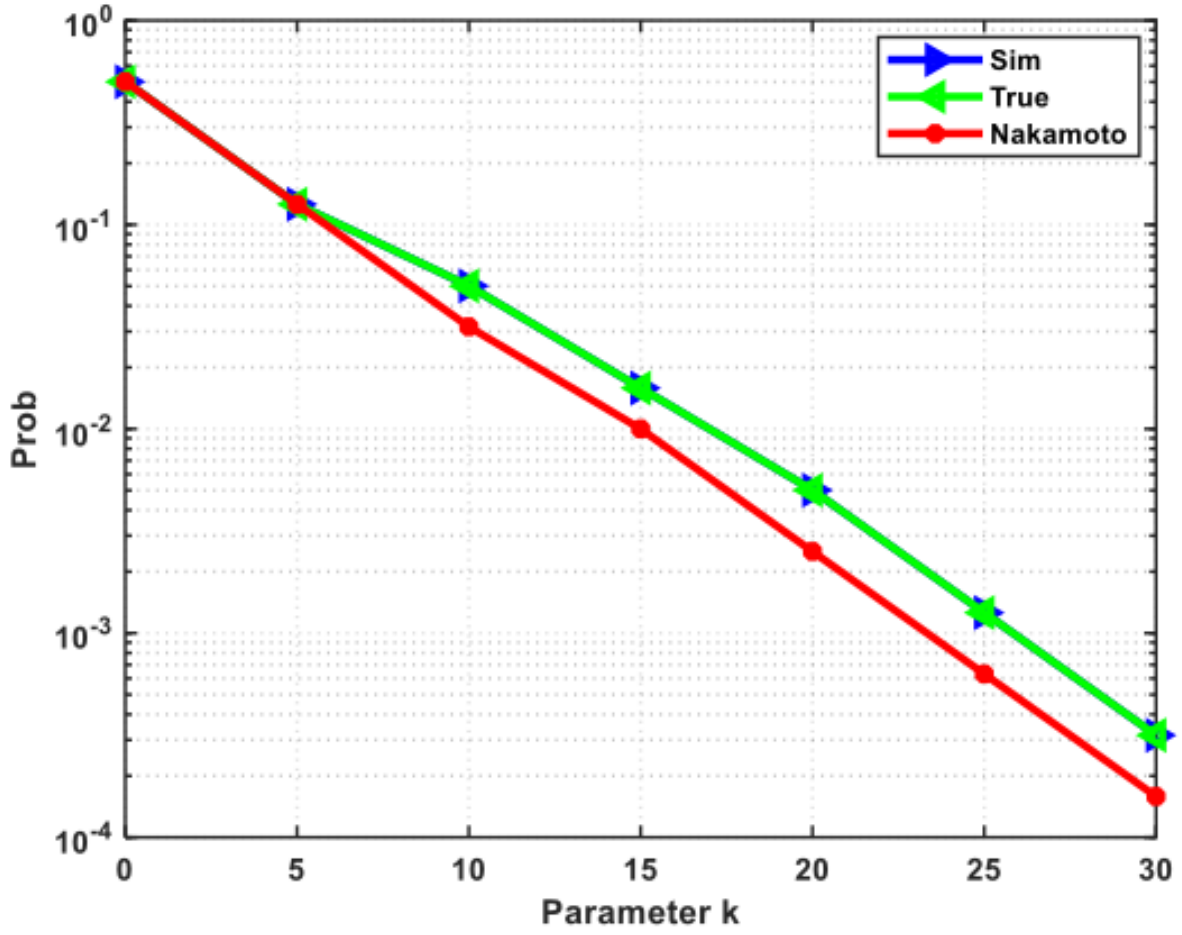

FIGURE 6. Private Attack on (β=0.3)

Trusted blocks are decided randomly by Poisson $((1 - \beta)\lambda T$ distribution in the first T units of time, X_T, which has the value $((1 - \beta)\lambda T$. Likewise, the adversarial block (denoted by Z_T)) should be replaced by B instead of $(1 - \beta)$. $X \sim \ Poisson\ (\lambda)$, is bound to Chernoff

$$P\left(X \geq \lambda + x\right) \leq exp\left(-\frac{x^2}{2\left(\lambda + x\right)}\right) \tag{2}$$

$$P\left(X \geq \lambda - x\right) \leq exp\left(-\frac{x^2}{2\left(\lambda + x\right)}\right) \tag{3}$$

Let $\epsilon \triangleq 1 - 2\beta$. Using (1) for Z_T *with* $x = (\frac{1}{2} - \beta)\lambda T)$ gives

$$P(X_T \geq 0.5\lambda T) \leq exp(-\epsilon^2 \lambda T/4)$$

Using (2) for Z_T *with* $x = (\frac{1}{2} - \beta)\lambda T)$ gives

$$P(X_T \geq 0.5\lambda T) \leq exp(-\epsilon^2 \lambda T/4(1 + 2\epsilon)) \leq exp(-\epsilon^2 \lambda T/12)$$

For any value of T superior to T_0, the probability of Z_T exceeding X_T It can be expressed in the following way (due to the union bound).

$$\sum_{T=T_0}^{\infty} P(Z_T \geq X_T) \leq \sum_{T=T_0}^{\infty} P(Z_T \geq 0.5\lambda T) + P(X_T \leq 0.5\lambda T) \leq \sum_{T=T_0}^{\infty} exp(-\epsilon^2 \lambda T/12) + exp(-\epsilon^2 \lambda T/4) = C(\epsilon, \lambda) exp(-\epsilon^2 \lambda T_0/12$$

ϵ and λ are constants that depend on $C(\epsilon, \lambda)$. Can you recommend a value for T_0?. The time it takes for k trusted blocks to appear should exceed T_0. It is possible to construct T0 in such a way that $\lambda T_0 = k$, implies $(1 - \beta)\lambda T_0 < k$). Boundedness of $X_{T_0} \geq k$ by $exp(-\frac{\beta^2 \lambda T_0}{8})$. With parameter k, a private attack does not have a bounded probability by $exp\left(-\frac{\beta^2 \lambda T_0}{8}\right) + C\left(\epsilon, \lambda\right) exp((-\frac{\epsilon^2 \lambda T_0}{12})$. Replacing λT_0 based on k, it can be seen that this probability decays exponentially with k.

In terms of success likelihood, however, the private attack can be shown to be the worst-case scenario for the most extended chain protocol. The logic indicates that the private attack will follow if any other attack in the probability space succeeds for a specific sample path. A private attack can also be calculated in terms of success probability [30]. This calculation contained a subtle error, first spotted by the author [42].

4. RESULT AND DİSCUSSİON

The distributed consensus network for multi-agent systems is designed and simulated on Network Simulator 3 (NS3). The NS3 is a very popular event simulator. A distributed consensus network under Sybil attacks is being investigated in the proposed work. The proposed work shows the agents' response, security, minor effect, and blockchain-based cryptocurrency. Energy consumption is an issue with Proof of Work. Miners are given a hash code. A hash code of the previous node is also included in the hash code. It is necessary to solve this hash code to add a block to the blockchain. Mining rewards miners with the validation of blocks in the database. Solving the puzzle requires a lot of computational power, so the miners tend to wander around it. A puzzle's difficulty level determines how much emphasis it will receive. However, the power consumption of bitcoin is balanced by its uses. The currency assures a miner to be wealthy enough to afford the computation cost. However, this approach has the disadvantage of not implementing Proof of Work throughout the entire blockchain. However, this approach has the disadvantage of not implementing Proof of Work throughout the entire blockchain. The issue can also be addressed using Proof of Authority (PoA). Nodes can add blockchain notes before transactions take place. Once they have authority, they can make use of Power of Attorney. This allows the selected nodes to have extraordinary power and security since they have permission to do so. In the blockchain itself, sidechains are created.

Energy is efficiently used by Proof of Stake (PoS). Nodes that contribute more to the blockchain are utilized, but not all. Participation will be higher when the stakes are higher. The output of the POS versus time is mentioned in Figure 7.

According to Gartner, blockchain innovation has just hit the peak of the advertising cycle and has entered a period of irritation as people begin to recognize its legitimacy. The common consensus is that passing the time of heightened demand was a significant step forward in blockchain development during the ad period.

Governments and business leaders have now critically assessed blockchain's potential and how it should be integrated into daily operations. Several parts moved at a faster pace than others. The integration of blockchain engineering into day-to-day operations inside large multinational corporations has been formally described, with the bitcoin element being the quickest of the squares.

The blockchain's decentralization and distributed structure is an advantage that makes the miners coordinate and come to a unanimous decision. The proof of work consensus algorithm follows game theory and incentives given to the miners for every action on the blockchain network. The coins put on stake need to be identified; hence, ownership is ensured in

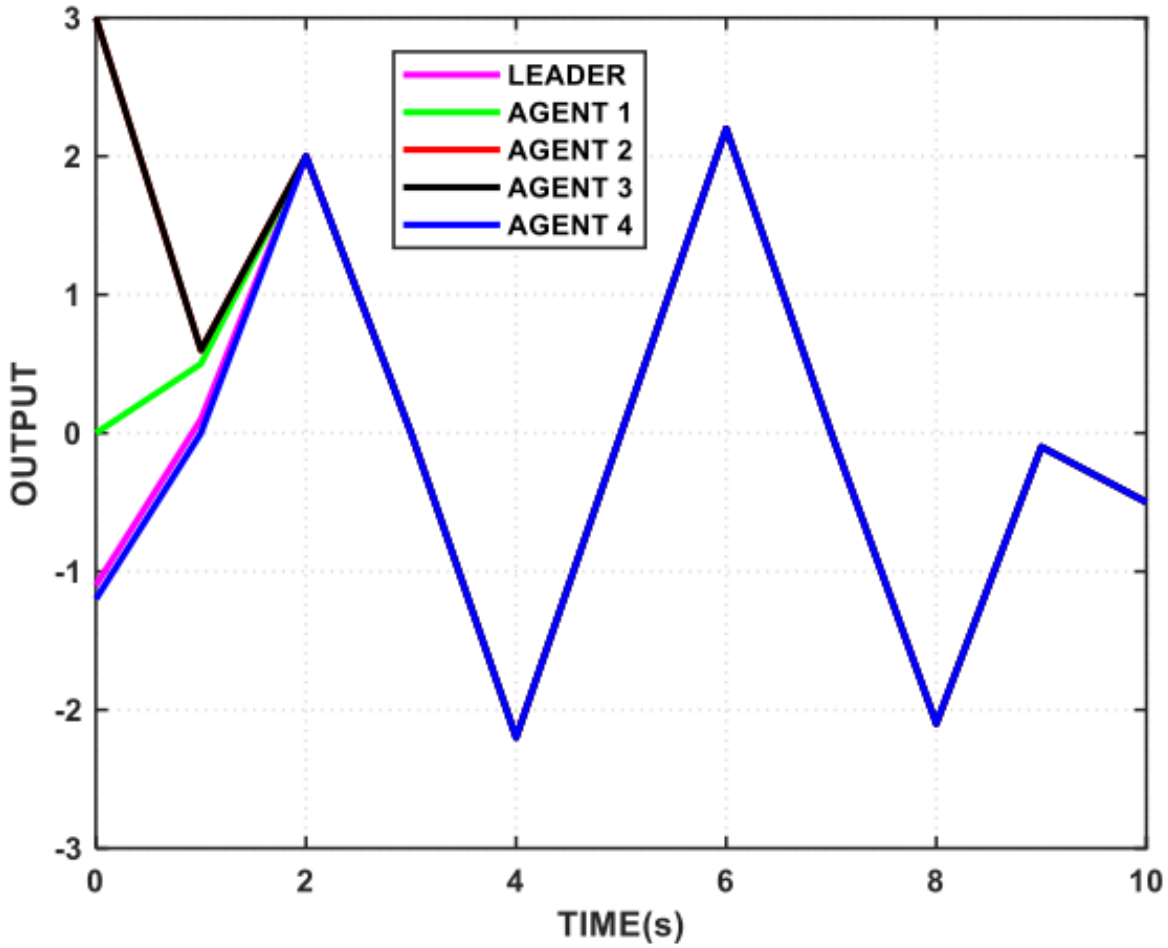

FIGURE 7. The response curves for the leader agent andthe output of Proof of Stake (PoS).

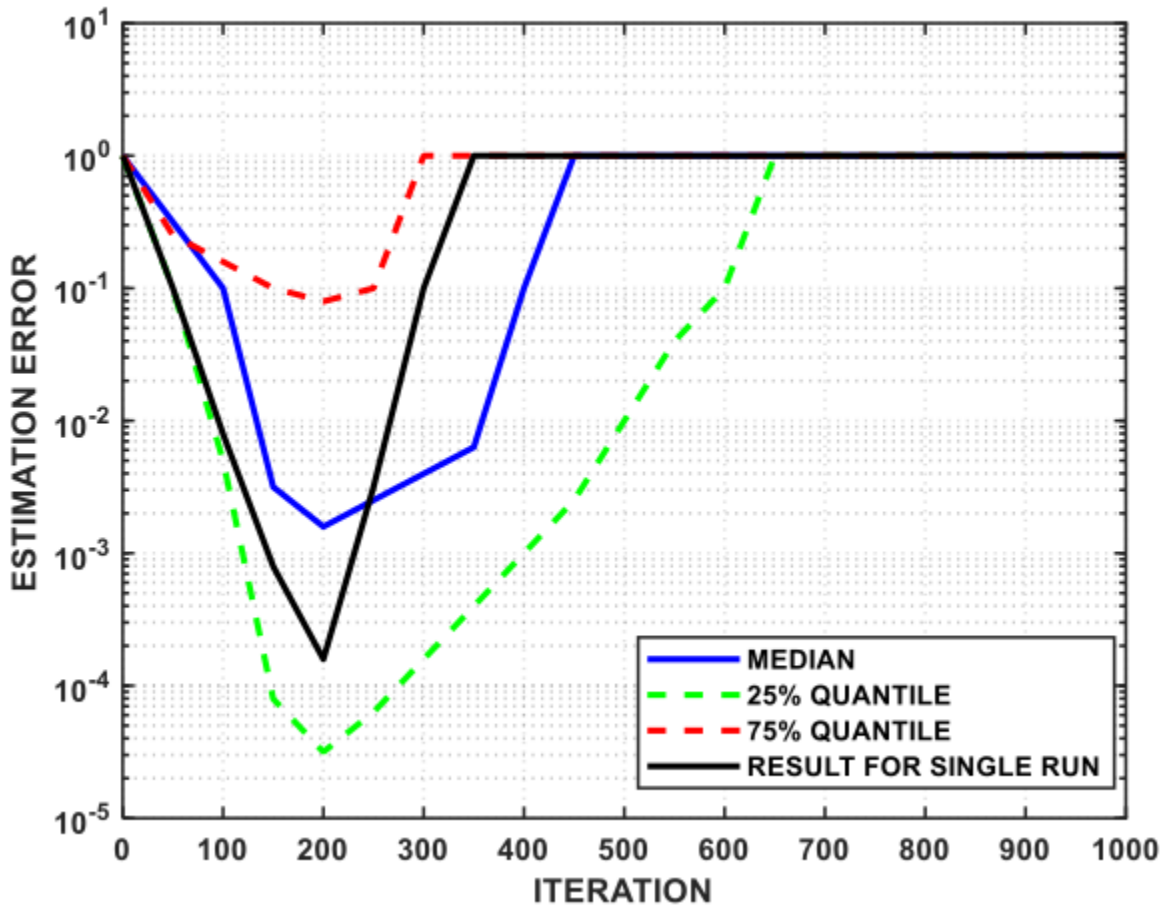

FIGURE 8. The convergence time for different initial conditions with a leader agent and Proof of Stake (PoS)'s mean-squared estimation errors.

the PoS algorithm. The group of miners competing is more in the case of the proof of stake algorithm, and therefore, there are fewer disputes because of transactions. The nodes have cryptocurrency, which puts them at stake.

Figure 8 shows the chain of created nodes in recursive lookups, where one query is directed to the next node, which then queries the next node and the result is returned via each successive node. Here are the simulated results for state block rate (%) and average throughput in transactions/seconds, comparing the traditional and proposed techniques. The average throughput indicates how many transactions are completed per second. Figure 9 shows the distributed network performance: a) State block rate (%) versus block size (MB). (b) Average throughput in transactions per second (tps) versus block interval (second). (c) State block rate (%) versus block interval (seconds). (d)) Average throughput in transactions per second (tps) versus block size (MB).

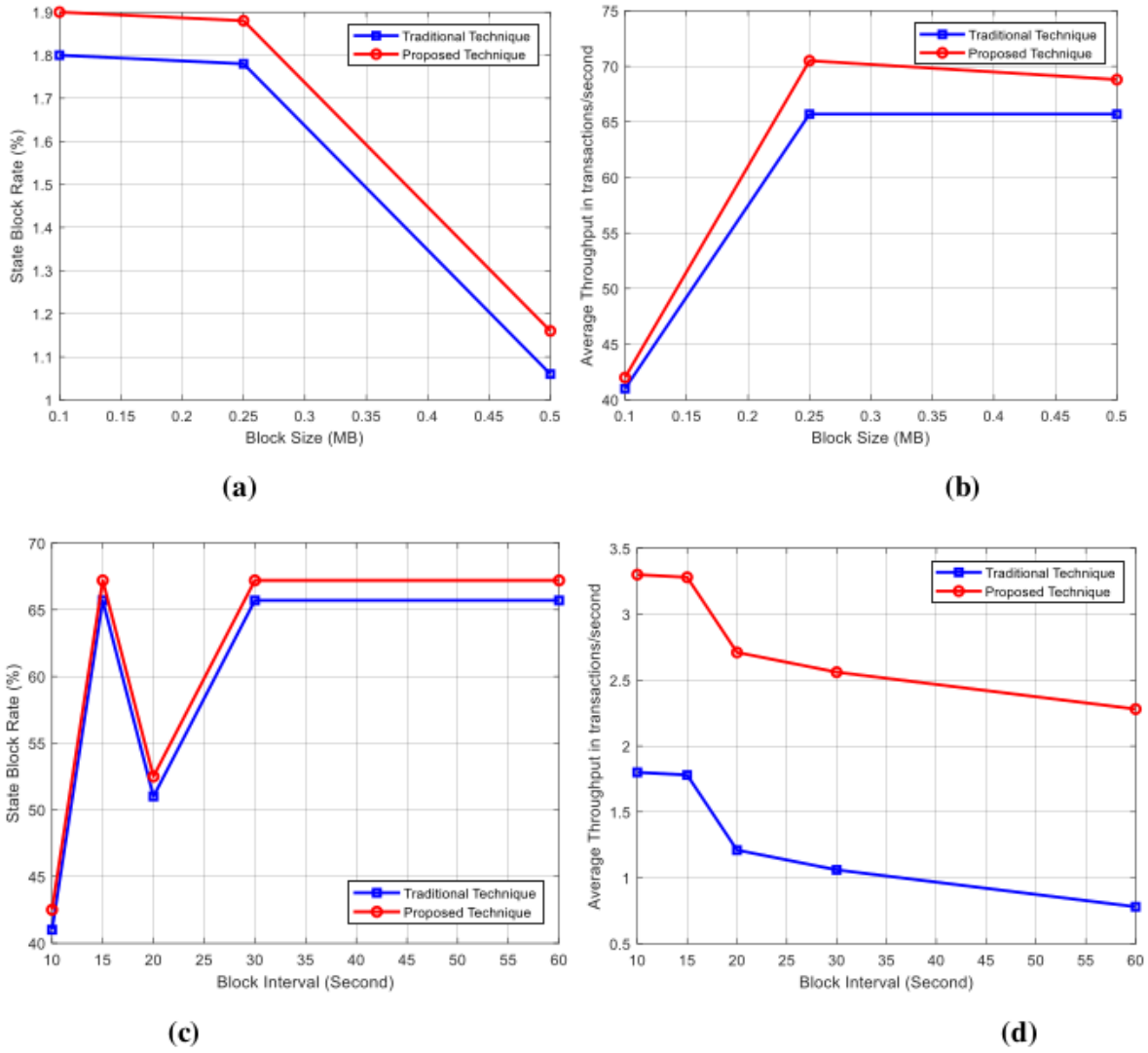

FIGURE 9. Figure 9: Shows the distributed network performance a) State block rate (%) versus block size (MB). (b) A measure of average transaction throughput in transactions per second (tps) versus block intervals (seconds). (c) State block rate (%) versus block interval (seconds). (d)) Average throughput in transactions per second (tps) versus block size (MB).

Identifying whether there is an impact on consensus time based on the number of messages. Simulations, on the other hand, led to an increase in messages. Based on the data shown in Figure 10, the one-message test can be compared with similar tests based on the consensus of four and ten messages. According to this figure, 1000 consensus transactions take 110 minutes each on average. It should be noted that time differences between messages decrease as peers increase. Several factors contribute to delay, according to this discovery. According to this study, the number of peers is more important than the message number in determining system delays.

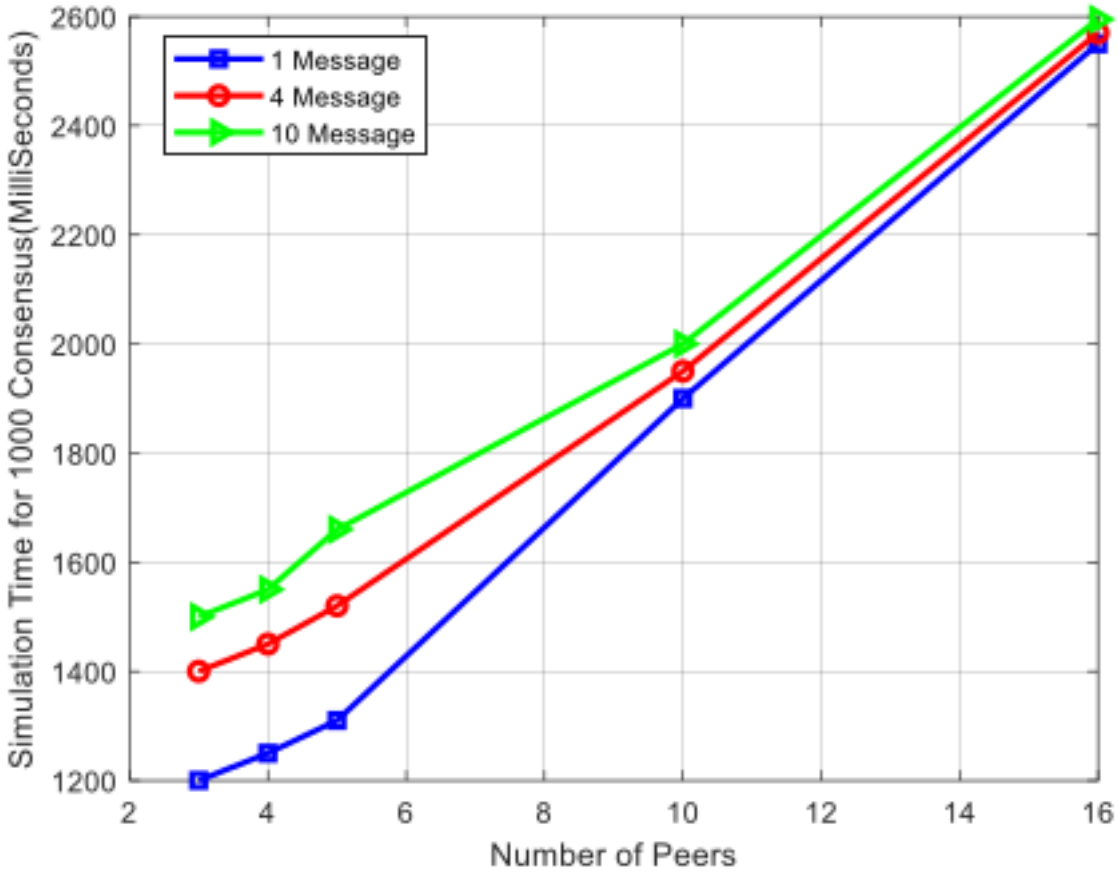

FIGURE 10. Simulation time (Milliseconds) for 1000 transactions versus the number of peers with different messages.

5. CONCLUSION

An agent input protection framework that protects the input of t semi-trusted agents is proposed in the study. On the other hand, the rest of the agents evaluate each other. İnput Because agents know the average information discussed, their inputs are not protected from concurrent leakage. Each distributed average consensus protocol has the same performance without the leakage. Blocks are consistently added to the blockchain, which is a consistent feature of blockchains. The process is the same as adding new miners to the network. If the difficulty level remains constant, a unique miner will take less time to join the network and add new blocks. IoT challenges have been addressed using blockchain-enabled platforms and technologies. Blockchain applications and systems must be tested and evaluated to achieve a practical blockchain deployment for IoT. A critical aspect of our study is evaluating the impact of consensus in congested and contested IoT scenarios to inform practitioners about the right consensus algorithm selection. The performance of the proposed techniques is measured based on the number of peers who estimate the number of messages needed to reach consensus, the state block rate estimation error (%), the throughput average, and the simulation time. The average throughput performance for transactions delivered per second is compared to the traditional protocol.

Regarding average throughput, the proposed protocol performs better than the traditional one. The proposed study can be extended with future network attacks for the Industry 4.0 evaluation. The present model can be applied to the various applications of Industry 4.0, such as Intelligent Transportation Systems, traffic congestion, and data transmission security.

FUNDING

None

ACKNOWLEDGEMENT

None

CONFLICTS OF INTEREST

The author declares no conflict of interest.

REFERENCES

[1] G. Angelo, S. Ferretti, and M. Marzolla, “A blockchain-based flight data recorder for cloud accountability,” *Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems*, pp. 93–98, 2018.

[2] M. Zichichi, M. Contu, S. Ferretti, and G. D. Angelo, “LikeStarter: a Smart-contract based Social DAO for Crowdfunding,” *IEEE INFOCOM 2019-IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS)*, pp. 313–318, 2019.

[3] P. Rani, S. Verma, S. P. Yadav, B. K. Rai, M. S. Naruka, and D. Kumar, “Simulation of the Lightweight Blockchain Technique Based on Privacy and Security for Healthcare Data for the Cloud System,” *Int. J. E-Health Med. Commun. IJEHMC*, vol. 13, no. 4, pp. 1–15, 2022.

[4] Y. Zheng, J. Ma, and L. Wang, “Consensus of Hybrid Multi-Agent Systems,” *IEEE Trans. Neural Netw. Learn. Syst*, vol. 29, no. 4, pp. 1359–1365, 2018.

[5] X. Dong and G. Hu, “Time-Varying Output Formation for Linear Multiagent Systems via Dynamic Output Feedback Control,” *IEEE Trans. Control Netw. Syst*, vol. 4, no. 2, pp. 236–245, 2017.

[6] D. Zhang and G. Feng, “A New Switched System Approach to Leader-Follower Consensus of Heterogeneous Linear Multiagent Systems With DoS Attack,” *IEEE Trans. Syst. Man Cybern. Syst*, vol. 51, no. 2, pp. 1258–1266, 2021.

[7] Y. Shang, “Resilient Consensus for Robust Multiplex Networks with Asymmetric Confidence Intervals,” *IEEE Trans. Netw. Sci. Eng*, vol. 8, no. 1, pp. 65–74, 2021.

[8] P. Rani, “Federated Learning-Based Misbehaviour Detection for the 5G-Enabled Internet of Vehicles,” *IEEE Trans. Consum. Electron*, pp. 1–1, 2023.

[9] D. Wang, N. Zheng, M. Xu, Y. Wu, Q. Hu, and G. Wang, “Resilient privacy-preserving average consensus for multi-agent systems under attacks,” *2020 16th International Conference on Control, Automation, Robotics and Vision (ICARCV)*, pp. 1399–1405, 2020.

[10] G. Wen, Y. Lv, J. Zhou, and J. Fu, “Sufficient and necessary condition for resilient consensus under time-varying topologies,” *2020 7th International Conference on Information, Cybernetics, and Computational Social Systems (ICCSS)*, pp. 84–89, 2020.

[11] Y. Shang, “Resilient consensus of switched multi-agent systems,” *Syst. Control Lett*, vol. 122, pp. 12–18, 2018.

[12] S. Gil, S. Kumar, M. Mazumder, D. Katabi, and D. Rus, “Guaranteeing spoof-resilient multi-robot networks,” *Auton. Robots*, vol. 41, no. 6, pp. 1383–1400, 2017.

[13] P. Rani and R. Sharma, “Intelligent transportation system for internet of vehicles based vehicular networks for smart cities,” *Comput. Electr. Eng*, vol. 105, pp. 108543–108543, 2023.

[14] B. Kailkhura, S. Brahma, and P. K. Varshney, “Data Falsification Attacks on Consensus-Based Detection Systems,” *IEEE Trans. Signal Inf. Process. Netw*, vol. 3, no. 1, pp. 145–158, 2017.

[15] Y. Shang, “Consensus of Hybrid Multi-Agent Systems With Malicious Nodes,” *IEEE Trans. Circuits Syst. II Express Briefs*, vol. 67, no. 4, pp. 685–689, 2020.

[16] P. Rani, N. Hussain, R. A. H. Khan, Y. Sharma, and P. K. Shukla, “Vehicular Intelligence System: Time-Based Vehicle Next Location Prediction in Software-Defined Internet of Vehicles (SDN-IOV) for the Smart Cities,” in *Intelligence of Things: AI-IoT Based Critical-Applications and Innovations* (F. Al-Turjman, A. Nayyar, A. Devi, , and P. K. Shukla, eds.), pp. 35–54, Springer International Publishing, 2021.

[17] A. E. Gencer, S. Basu, I. Eyal, R. V. Renesse, and E. G. Sirer, "Decentralization in bitcoin and ethereum networks," in *Financial Cryptography and Data Security: 22nd International Conference*, pp. 439–457, Springer, 2018.
[18] P. Maymounkov, D. Mazières, and Kademlia, "A Peer-to-Peer Information System Based on the XOR Metric," in Peer-to-Peer Systems," *Lecture Notes in Computer Science*, vol. 2429, pp. 53–65, 2002.
[19] Y. Xiao, N. Zhang, W. Lou, and Y. T. Hou, "A Survey of Distributed Consensus Protocols for Blockchain Networks," *IEEE Commun. Surv. Tutor*, vol. 22, no. 2, pp. 1432–1465, 2020.
[20] B. Bhola, "Quality-enabled decentralized dynamic IoT platform with scalable resources integration," *IET Commun*, 2022.
[21] N. Kumar, P. Rani, V. Kumar, S. V. Athawale, and D. Koundal, "THWSN: Enhanced energy-efficient clustering approach for three-tier heterogeneous wireless sensor networks," *IEEE Sens. J*, vol. 22, no. 20, 2022.
[22] M. Faheem, G. Fizza, M. W. Ashraf, R. A. Butt, M. A. Ngadi, and V. C. Gungor, "Big Data acquired by Internet of Things-enabled industrial multichannel wireless sensors networks for active monitoring and control in the smart grid Industry 4.0," *Data Brief*, vol. 35, pp. 106854–106854, 2021.
[23] G. Wood, "Polkadot: Vision for a heterogeneous multi-chain framework," *White Pap*, vol. 21, no. 2327, pp. 4662–4662, 2016.
[24] E. Buchman *Tendermint: Byzantine fault tolerance in the age of blockchains*, 2016.
[25] J. Dilley, A. Poelstra, J. Wilkins, M. Piekarska, B. Gorlick, and M. Friedenbach, "Strong federations: An interoperable blockchain solution to centralized third-party risks," *ArXiv Prepr*, 2016.
[26] S. Thomas and E. Schwartz *A protocol for interledger payments*, 2015.
[27] C. M. Li, T. Hwang, and N. Y. Lee, "Threshold-multisignature schemes where suspected forgery implies traceability of adversarial shareholders," in *Advances in Cryptology-EUROCRYPT'94: Workshop on the Theory and Application of Cryptographic Techniques*, vol. 13, pp. 194–204, Springer, 1994.
[28] A. Kiayias, N. Lamprou, and A. P. Stouka, "Proofs of Proofs of Work with Sublinear Complexity," in *Financial Cryptography and Data Security* (J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, , and K. Rohloff, eds.), vol. 9604, pp. 61–78, Springer, 2016.
[29] A. Kiayias, A. Miller, and D. Zindros, "Non-interactive proofs of proof-of-work," in *Financial Cryptography and Data Security: 24th International Conference*, vol. 2020, pp. 505–522, Springer, 2020.
[30] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Bus. Rev*, 2008.
[31] V. Buterin and E. White 2015.
[32] S. Zhang and J. H. Lee, "Analysis of the main consensus protocols of blockchain," *ICT Express*, vol. 6, no. 2, pp. 93–97, 2020.
[33] S. Bouraga, "A taxonomy of blockchain consensus protocols: A survey and classification framework," *Expert Syst. Appl*, vol. 168, pp. 114384–114384, 2021.
[34] S. Küfeoğlu and M. Özkuran, "Bitcoin mining: A global review of energy and power demand," *" Energy Res. Soc. Sci*, vol. 58, pp. 101273–101273, 2019.
[35] N. Stifter, A. Judmayer, and E. Weippl, "Revisiting practical byzantine fault tolerance through blockchain technologies," *Secur. Qual. Cyber-Phys. Syst. Eng. Forewords Robert M Lee Tom Gilb*, pp. 471–495, 2019.
[36] S. J. Lukasik, "Protecting users of the cyber commons," *Commun. ACM*, vol. 54, no. 9, pp. 54–61, 2011.
[37] A. V. Uzunov, E. B. Fernandez, and K. Falkner, "Securing distributed systems using patterns: A survey," *Comput. Secur*, vol. 31, no. 5, pp. 681–703, 2012.
[38] M. Conti, E. S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surv. Tutor*, vol. 20, no. 4, pp. 3416–3452, 2018.
[39] N. Hussain, P. Rani, H. Chouhan, and U. S. Gaur, "Cyber Security and Privacy of Connected and Automated Vehicles (CAVs)-Based Federated Learning: Challenges, Opportunities, and Open Issues," in *EAI/Springer Innovations in Communication and Computing* (F. L. for IoT Applications, S. P. Yadav, B. S. Bhati, D. P. Mahato, , and S. Kumar, eds.), pp. 169–183, Springer International Publishing, 2022.
[40] P. Lapsley, "Phreaking out ma bell," *IEEE Spectr*, vol. 50, no. 2, pp. 30–35, 2013.
[41] J. R. Douceur, "The sybil attack," *International workshop on peer-to-peer systems*, pp. 251–260, 2002.
[42] M. Rosenfeld, "Analysis of hashrate-based double spending," *ArXiv Prepr*, 2014.