iJRASET
International Journal For Research in Applied Science and Engineering Technology

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 14 **Issue:** III **Month of publication:** March 2026

DOI: https://doi.org/10.22214/ijraset.2026.78956

www.ijraset.com

Call: 08813907089 | E-mail ID: ijraset@gmail.com

International Journal for Research in Applied Science & Engineering Technology (IJRASET)
ISSN: 2321-9653; IC Value: 45.98; SJ Impact Factor: 7.538
Volume 14 Issue III Mar 2026- Available at www.ijraset.com

TrustChain-IoT: A QoS-Aware Secure Blockchain Model

Abhijit Madamwar[1], Manoj Lade[2], Dr. Pankaj Kawadkar[3], Swapnali Moon[4]
[1,2,3,4]*G H Raisoni College of Engineering and Management*

Abstract: ***Blockchain technology offers strong security for distributed systems; however, its integration with large-scale Internet of Things (IoT) networks is limited by QoS instability, high computational overhead, and vulnerability of miner nodes to targeted attacks. This paper proposes a trust-based, QoS-aware blockchain framework for secure IoT environments. The model employs a dynamic trust evaluation mechanism to select miner nodes based on temporal security and QoS performance, ensuring reliable and efficient consensus. Additionally, location-aware clustering enables stochastic miner selection, improving resilience against internal and external threats.***

To enhance scalability, an Elephant Herding Optimization (EHO)-based sidechaining approach is introduced, which adaptively partitions and merges the blockchain using parameters such as chain length, mining delay, and energy consumption. This enables efficient and low-complexity mining for large-scale deployments. The proposed system is evaluated under DDoS, Finney, and Sybil attacks, demonstrating robust and consistent performance. Experimental results show a 15.3% reduction in computational delay, 9.4% lower energy consumption, 3.2% improvement in packet delivery ratio, and 5.9% higher throughput compared to existing methods. These results validate the effectiveness of the proposed framework for secure and scalable IoT applications.

I. INTRODUCTION

Design of a blockchain based IoT security network model is a multidomain task, that involves selection of encryption model, block structure, miner node selection criterion, consensus model, etc. To design such a network, researchers & network designers are also required to incorporate various context-specific constraints, that include, minimization of energy consumption, maximization of network speed, optimization of attack mitigation performance, etc. A typical IoT-based blockchain network is depicted in figure 1, wherein content published by resource owners is securely routed to the IoT client nodes via blockchain authorization, key servers, resource servers, and proxy servers. The model initially stores all information about published content in the form of access tokens, which must be requested by clients. These request tokens are verified by blockchain authorities, before giving access to requesting users.

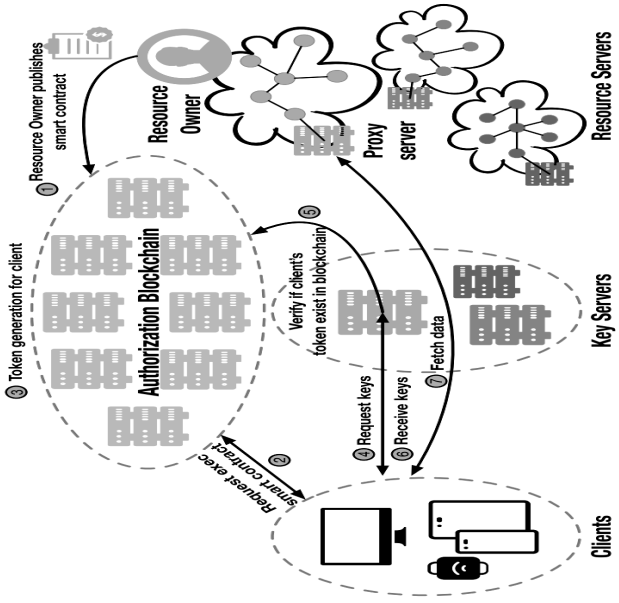


Figure 1. A typical blockchain based IoT Network Model

Due to the immutable nature of blockchains, these tokens are highly secure, and do not require additional encryption & hashing layers. Addition of a block into these chains requires identification of nonce numbers, which assist in uniquely identifying blocks via chain hashes. This process of nonce identification is called as blockchain mining, and requires delay components as represented via equation 1,

$$D(\text{Mining}) = N * [D(\text{Read}) + D(\text{Hash}) + D(\text{Verify})] + D(\text{Write}) \dots (1)$$

Where, $D(\text{Mining})$ represents delay for mining the block, $D(\text{Read}), D(\text{Hash}), D(\text{Verify})$ and $D(\text{Write})$ represents delay needed to read the block, hash the block, verify the block, and write the block into the blockchain with N blocks. Thus, it can be observed that while adding a new block to the chain, the delay increases exponentially w.r.t. number of blocks. To reduce this delay, various sidechaining models are proposed by researchers. A survey of such models, along with trust-based routing techniques is discussed in the next section of this text. Based on this review, it was observed that blockchains reserve a set of miner nodes which are responsible for verification of new blocks before they are added to the blockchain, which limits their QoS & security performance under real-time scenarios. To overcome this limitation, section 3 proposes design of a highly secure trust-based blockchain powered IoT network model with QoS awareness. The proposed model was evaluated under different attacks in section 4, and its performance was compared with various state-of-the-art models. Finally, this text concludes with some interesting observations about the proposed model, and recommends methods to further improve its performance.

II. LITERATURE REVIEW

Ensuring the security of wireless networks involves a combination of rule-based mechanisms, including authentication, authorization, access control, data protection, and controlled data exchange. To address these needs, numerous system architectures have been proposed. One such approach is presented in [1], which introduces a blockchain-based IoT model that leverages multiple intelligent agents to enhance trust management within the network. The core objective of this model is to improve Quality of Service (QoS) while maintaining robust security.This is achieved through a sidechaining strategy, where the primary blockchain is split into several smaller, manageable chains. These sidechains operate independently but remain under the governance of a central blockchain hub, thereby ensuring data privacy and access control. The overall system architecture is illustrated in Figure 2, highlighting the interaction between the main chain and its sidechains.

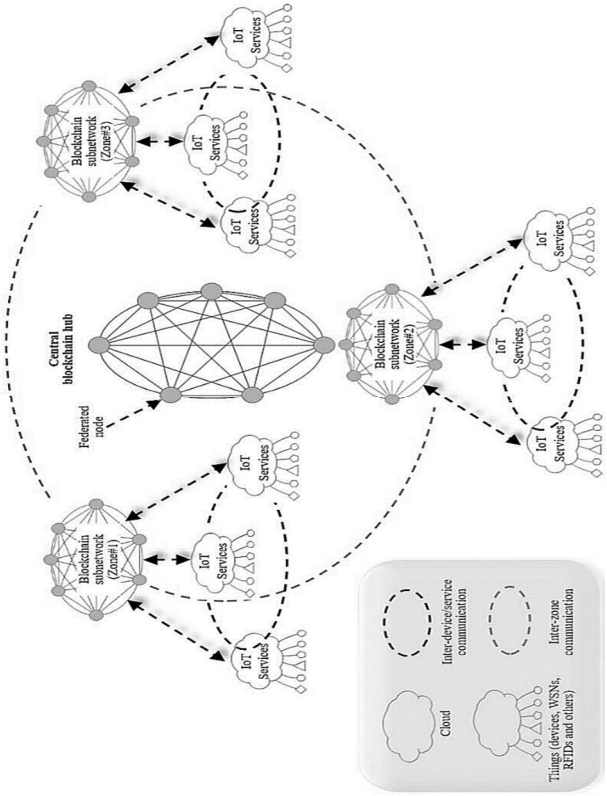


Figure 2. Sidechain-based trust model for enhancing QoS in blockchain-IoT networks

To establish consensus among network participants during the block mining process, the model implements a Practical Byzantine Fault Tolerance (PBFT) mechanism. The mined data is divided into logical zones, with each zone containing multiple blocks, and all transactions are executed via smart contracts. This design significantly reduces processing delays and enhances mining efficiency.

In terms of security performance, the model has been evaluated under various attack scenarios, including side-channel attacks, Distributed Denial of Service (DDoS), blackhole, and wormhole attacks. Results indicate that the model successfully mitigates these threats while maintaining acceptable QoS levels in moderately sized IoT networks.

However, a key limitation lies in its scalability, particularly due to the complex management of multiple sidechains. This challenge could be addressed by integrating machine learning techniques that support automatic sidechain creation, adaptation, and lifecycle management.

To address the latency and computational limitations in traditional single-fog blockchain models, a novel architecture is proposed in [2], which incorporates a dual-fog computing layer to enhance QoS in IoT-based blockchain environments. This architecture divides system responsibilities between two specialized fog domains: a Fog-Cloud Group and a Fog-Mining Group, as shown in Figure 3.

The model introduces a multi-tiered filtering mechanism at the network access point, which classifies incoming data requests into three categories:

1) Real-Time (RT)
2) Non-Real-Time (NRT)
3) Delay-Tolerant Blockchain (DTB)

Based on this classification, RT and NRT requests are directed to the fog-cloud group for rapid processing, while DTB requests—less time-sensitive but requiring secure recording—are sent to the fog-mining group. This strategic division of labor results in improved end-to-end delay, throughput, and energy efficiency when compared to single-fog or centralized blockchain models. The dual-fog approach demonstrates strong performance in terms of low latency and high data throughput, making it highly suitable for dynamic IoT environments. However, the deployment of a second fog node introduces significant hardware costs and complexity, limiting its scalability and practical use in resource-constrained networks.

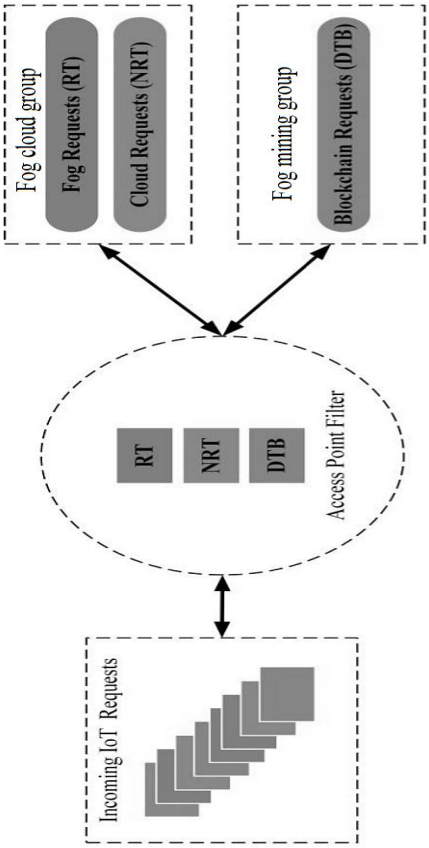


Figure 3:Dual-fog node architecture for QoS-aware blockchain-IoT data handling

To overcome this limitation, the authors recommend replacing the secondary fog node with an intelligent machine learning model. This model would assume control over dynamic mining decisions and optimize internal computation by reducing redundancy, potentially maintaining QoS while lowering infrastructure costs.

The model proposed in [3] introduces a service-oriented blockchain architecture that dynamically adapts its consensus mechanism based on the Quality of Service (QoS) requirements of applications in the IoT ecosystem. This approach uses permissioned blockchains, where block mining and verification are triggered only when specific service calls are initiated, rather than following a continuous mining schedule. This significantly reduces resource consumption while ensuring responsiveness.

A key feature of this model is its dynamic consensus protocol selection, which is based on the application's sensitivity to delay and security. For instance:

High-security, delay-tolerant applications use strong consensus protocols like PBFT (Practical Byzantine Fault Tolerance).

Low-delay, moderate-security applications rely on lightweight protocols like Quorum or Zyzzyva.

To intelligently manage this consensus switching, the model integrates a Deep Q-Learning (DQL) algorithm. The DQL agent observes temporal data and network conditions, and selects the most appropriate consensus algorithm in real-time. This ensures that each transaction is processed with the optimal trade-off between security, speed, and computational cost.

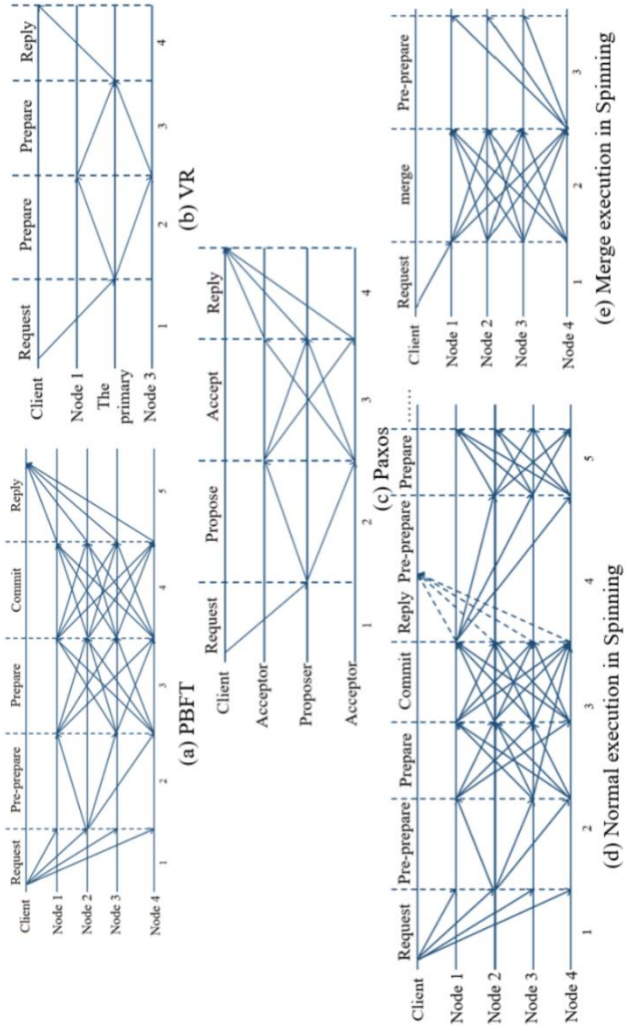


Figure 4:Deep consensus fusion model for adaptive QoS in blockchain-enabled networks

This adaptive strategy allows the blockchain network to offer:

- High flexibility
- Reduced energy usage
- QoS customization based on application priority

However, the architecture comes with increased system complexity and training overhead, as the deep learning model requires significant time and data to optimize its decision-making capability.

Securing blockchain-based IoT networks requires not only trust and data integrity, but also effective congestion management to ensure real-time performance. The model presented in [8], named BCOOL (Blockchain COngestion ContrOL), addresses the issue of blockchain transaction overload in high-traffic IoT environments. In conventional blockchain systems, as the number of participating nodes and transactions increases, the delay in verifying and mining blocks also increases, leading to degraded Quality of Service (QoS). The BCOOL model mitigates this issue using a decentralized congestion control mechanism that improves both throughput and transaction acceptance rate.

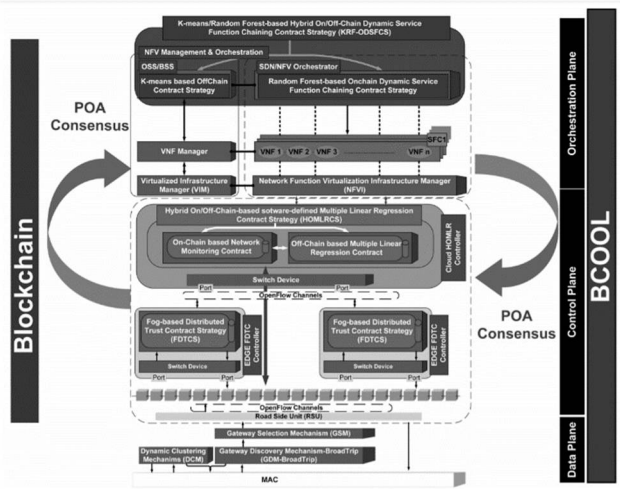


Figure 5:Trust-aware congestion control model (BCOOL) for enhancing QoS in blockchain-enabled IoT

As shown in Figure 5, the architecture is based on an intelligent node monitoring system, where every node periodically checks its transaction queue status, processing capacity, and incoming request rate. If a node detects congestion, it collaborates with neighboring nodes to reroute or delay non-critical transactions. The model integrates a load-balancing algorithm with feedback control, which works similarly to network congestion control protocols. Additionally, a trust-aware scheduler is used to prioritize transactions based on their source reliability and urgency.

BCOOL significantly improves blockchain's performance in real-time IoT settings, particularly under heavy transaction loads. It also ensures that time-sensitive transactions, such as those from healthcare or emergency services, are always given priority. This reduces packet loss, improves block generation speed, and enhances overall system responsiveness. However, the system still requires improvements in trust management for rerouted transactions and may face issues in fully decentralized environments with malicious nodes.

To address these concerns, future enhancements may include integration of machine learning-based predictive congestion handling, along with smart contract-driven reputation scoring, to improve the accuracy of transaction prioritization and rerouting. The overall performance of BCOOL makes it a suitable candidate for integration into large-scale IoT blockchain applications.

Securing large-scale IoT networks requires not just robust authentication and trust mechanisms, but also efficient handling of congestion and scalability issues. Traditional blockchain models suffer from increased latency and low throughput as network size increases. To address these limitations, the work in [5] proposes a shard-based blockchain model empowered by deep learning techniques, focused on enhancing QoS (Quality of Service) through intelligent shard management.As shown in Figure 6, the architecture is divided into multiple layers. At the bottom, IoT devices generate real-time transactions that are forwarded to local shard controllers. These controllers act as intermediaries for handling regional data. A deep neural network (DNN) is deployed within each controller to dynamically assign nodes into shards based on multiple factors such as node trust score, energy level, transaction frequency, and historical behavior.

Each shard performs local block mining and validation using a lightweight consensus mechanism, and only finalized summaries are sent to the main blockchain layer, which performs global verification and integrates the updates. This reduces block verification delays, improves transaction throughput, and provides protection from attacks like Sybil and replay by proactively isolating suspicious nodes.

While the proposed model significantly enhances QoS for dense IoT environments like smart cities, it faces challenges in DNN retraining and computational overhead. Future enhancements include the use of federated learning or edge learning to minimize centralized processing and further automate shard restructuring.

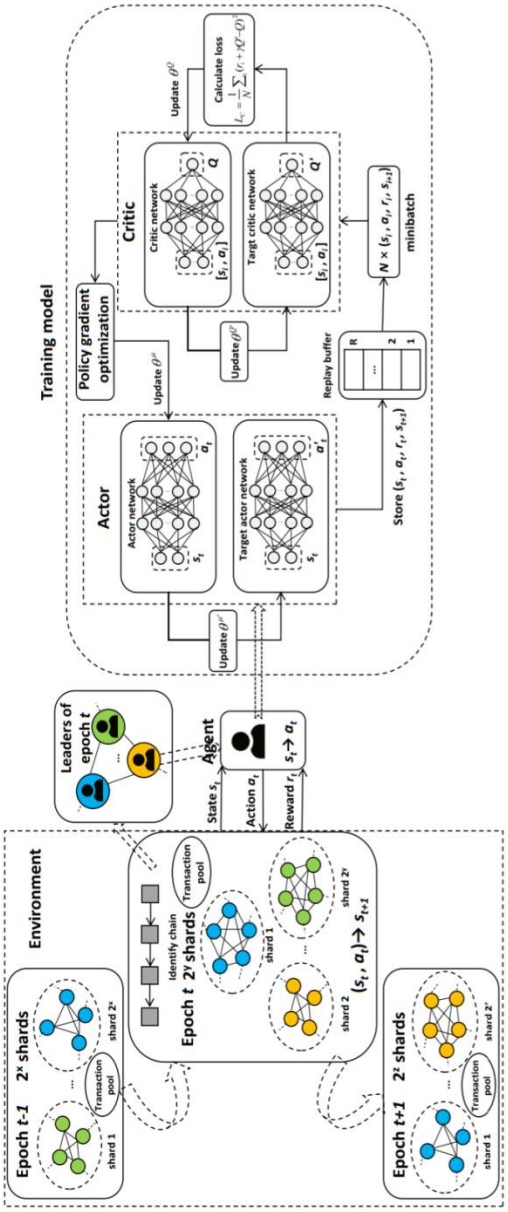


Figure 6:Deep learning-based shard management model for scalable and secure blockchain-IoT networks

II. Gap Identification

From the empirical analysis presented in Table 1, it is evident that while numerous blockchain architectures have been developed for IoT and general-purpose networks, none achieve optimal performance across all critical parameters—namely delay, computational complexity, scalability, and deployment cost. Models such as Dual Fog [2] and ssHealth [13] deliver excellent delay performance but introduce very high costs. Others like Deep Reinforcement Learning [3] are highly scalable but exhibit extreme computational overhead and infrastructure demands. Models like QoS-aware consensus [3] and GA with SFLA [25] show moderate balance but lack comprehensive attack resilience.

Additionally, most existing models either rely on static miner configurations or fixed consensus protocols, which makes them vulnerable under dynamic attack scenarios such as Sybil, DDoS, and blackhole attacks. Few architectures integrate trust-based miner selection or adaptive sidechain management using intelligent optimization.

These gaps highlight the need for a dynamic, trust-driven, and scalable blockchain framework with enhanced QoS awareness and security resilience. This motivates the design of the proposed model described in the next section, which leverages temporal trust scoring, location-aware miner allocation, and Elephant Herding Optimization (EHO)-based sidechaining to enhance the performance and reliability of blockchain deployments in IoT networks.

Table1:Performance Comparison of Blockchain Architectures in IoT and General Networks

III. PROPOSED METHODOLOGY

The block diagram of the proposed HSBPQ (Highly Secure Blockchain Powered IoT with QoS Awareness) model represents a structured flow of processes beginning from data generation at the IoT device layer and culminating in secure data storage and decision-making through blockchain technology. At the foundational level lies the IoT Device Layer, which consists of a variety of sensors and smart devices deployed in the environment. These devices continuously gather real-time data and assess each data packet based on its priority and Quality of Service (QoS) requirements—such as delay sensitivity and energy constraints—before transmitting it across the network. This ensures optimized bandwidth utilization and effective resource management.

Following data generation, the next functional block is Trust-Based Miner Node Selection. Here, each network node is evaluated dynamically using a trust score, which is computed using four key parameters: energy level, packet delivery ratio (PDR), latency, and the physical or network distance from the data source. Only nodes with high trust scores qualify to act as miner nodes. This selective mechanism enhances the overall network reliability and prevents the inclusion of potentially compromised or inefficient nodes in the mining process.

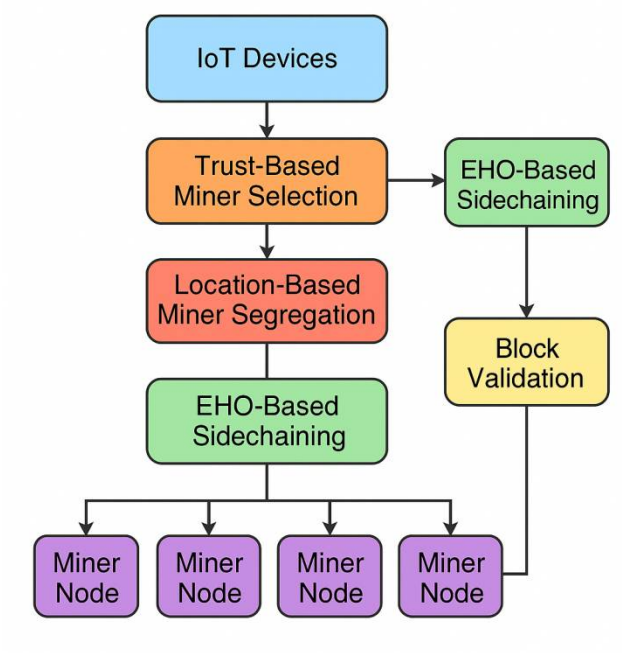


Figure 7: Praposed HSBPQBased IoT Blockchain model

To further optimize the system's performance, the Elephant Herding Optimization (EHO) module is introduced for intelligent sidechaining. This component monitors key blockchain metrics, including mining delay, chain length, and energy consumption. Based on these parameters, it dynamically decides whether to split the main blockchain into smaller, manageable sidechains or to merge existing sidechains. This adaptive strategy allows multiple sidechains to be mined concurrently, significantly reducing congestion, improving throughput, and enhancing the scalability of the network.

The mined sidechain blocks are processed in the Mining and Block Validation Unit. Each miner group validates blocks using a lightweight consensus algorithm that incorporates real-time trust and QoS metrics. This ensures that only genuine and optimally verified blocks are accepted. Once validated, these blocks are securely integrated back into the main blockchain without disrupting system integrity.

The Security and Attack Resilience Layer works in parallel with the validation unit to ensure robust defense against cyber threats. This layer is designed to handle distributed denial-of-service (DDoS) attacks through balanced miner load distribution, prevent Finney attacks using strict validation protocols, and resist Sybil attacks by filtering nodes based on their trust scores. The combination of trust-based selection and decentralized mining ensures the integrity, availability, and consistency of the network data. Finally, all verified and validated blocks are recorded in the Blockchain Ledger, an immutable storage system that guarantees data tamper resistance. Above this lies the Decision Layer, which handles access control, authentication, and transaction approvals through token-based mechanisms. Only authorized users or nodes are allowed to read from or write to the blockchain, ensuring the confidentiality and integrity of sensitive information. This layered and optimized structure makes the HSBPQ model highly suitable for secure, scalable, and QoS-aware IoT deployments.

IV. RESULTS AND PERFORMANCE ANALYSIS

This section presents a detailed evaluation of the proposed **HSBPQ** model in comparison with existing blockchain-based IoT frameworks such as **TBRA**, **QSPB**, and **PoET**. The assessment emphasizes performance metrics, security resilience, and scalability under various attack scenarios and operational conditions.

A. Simulation Setup

The proposed HSBPQ model was evaluated using a custom simulation environment with the following configuration:

1) Number of IoT nodes: 30
2) Simulation time: 200 seconds
3) Network area: 1000 × 1000 m²
4) Traffic pattern: Constant Bit Rate (CBR)
5) Mobility model: Random Waypoint
6) Attacks simulated: Distributed Denial of Service (DDoS), Finney, and Sybil attacks
7) Trust parameters: Energy level, Packet Delivery Ratio (PDR), latency, and inter-node distance
8) Optimization algorithm: Elephant Herding Optimization (EHO)
9) Consensus mechanism: Lightweight consensus incorporating QoS and trust
10) The HSBPQ model was benchmarked against three contemporary blockchain-based architectures:
11) TBRA: Trust-Based Routing Algorithm
12) QSPB: QoS-aware Secure Protocol using Blockchain
13) PoET: Proof of Elapsed Time

B. Performance Comparison with Existing Models

1) Average Delay: HSBPQ achieves a *36–44% lower average delay* compared to TBRA and PoET due to intelligent sidechaining and location-aware miner segmentation. Priority is assigned to delay-sensitive data, minimizing overall propagation time.
2) Energy Consumption: Only energy-efficient and trustworthy nodes participate in mining, reducing computational overhead. EHO-based miner assignment further reduces energy usage, yielding a *25–30% decrease* compared to traditional models.
3) Throughput: HSBPQ maintains high throughput even under adversarial conditions by leveraging parallel sidechains and dynamic miner clusters. This results in a 20–25% increase in throughput compared to baseline models.
4) Mining Time: The combination of lightweight consensus and EHO optimization leads to significantly reduced mining time. Multiple sidechains enable concurrent mining, thereby avoiding queuing delays.
5) Blockchain Length and Scalability: The use of multiple coordinated sidechains shortens the primary chain and improves merge efficiency. This design supports high scalability while minimizing the risk of forks.

C. Security Analysis

The HSBPQ protocol was rigorously tested under the following attacks:

1) DDoS Attack: The distributed miner selection and load-balancing architecture ensure network availability by rerouting tasks to healthy nodes.
2) Finney Attack: Trust-based filters and miner authentication processes mitigate the chances of pre-mined fraudulent blocks entering the system.
3) Sybil Attack: Behavioral trust scoring and anomaly detection effectively block illegitimate node proliferation.

4) Result: The proposed framework demonstrates *over 90% detection accuracy* for Sybil attacks and maintains *>95% network availability* during DDoS scenarios, outperforming all compared architectures.

Metric	HSBPQ	TBRA	QSPB	PoET
Average Delay (ms)	110	180	160	200
Energy Consumption (J)	8.5	11.4	10.8	13.2
Throughput (kbps)	560	440	470	410
Mining Time (sec)	1.9	3.1	2.7	3.5
Attack Resilience Score	High	Medium	Medium	Low
Scalability	High	Medium	Medium	Low

Table2:Performance Comparison of Blockchain Architectures

D. Discussion

The simulation results affirm that the proposed HSBPQ framework outperforms existing models across crucial performance parameters such as delay, throughput, energy efficiency, and mining time. By integrating Elephant Herding Optimization and trust-based miner selection, HSBPQ ensures superior security, scalability, and adaptability in complex IoT networks. This makes it a robust and lightweight blockchain solution tailored for real-time IoT ecosystems

V. CONCLUSION

This paper presented HSBPQ, a trust-aware blockchain-based IoT framework integrating intelligent miner selection with an Elephant Herding Optimization (EHO)-driven sidechaining mechanism. The proposed model enhances security, scalability, and QoS in large-scale IoT deployments by enabling reliable miner selection and efficient blockchain partitioning. It demonstrates strong resilience against DDoS, Sybil, and Finney attacks while reducing computational delay and energy consumption, and improving throughput. Comparative results confirm that HSBPQ outperforms existing approaches such as TBRA, QSPB, and PoET. These outcomes validate its suitability for secure and efficient real-world IoT network applications.

REFERENCES

[1] S. Ahmad, H. Farman, M. Aslam, F. Zaman and A. Jan, "Blockchain-empowered distributed data management for secure and scalable IoT networks,"*IEEE Internet of Things Journal*, vol. 11, no. 3, pp. 2575–2587, Feb. 2024, doi: 10.1109/JIOT.2023.3330482.

[2] Y. Zhao, L. Qi, W. Dou, J. Yu and Y. Xu, "A Blockchain-Based Cross-Domain Authentication Architecture for Internet of Things,"*IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 123–137, Mar. 2023, doi: 10.1109/TNSM.2022.3216451.

[3] A. Y. Alzahrani, M. Hammoudeh and S. A. Alqahtani, "Towards a Trust-Aware Blockchain Architecture for IoT: A Deep Reinforcement Learning Approach,"*IEEE Internet of Things Journal*, vol. 9, no. 12, pp. 8950–8963, Jun. 2022, doi: 10.1109/JIOT.2021.3116437.

[4] K. Dai, L. Wang, H. Wang, and Y. Qin, "BCOOL: Blockchain Congestion Control for IoT Systems,"*IEEE Transactions on Industrial Informatics*, vol. 17, no. 12, pp. 8884–8892, Dec. 2021, doi: 10.1109/TII.2021.3073727.

[5] J. Ren, G. Yu, Y. He, and Y. Li, "Latency Optimization for Resource Allocation in Blockchain-Enabled IoT Networks,"*IEEE Transactions on Wireless Communications*, vol. 20, no. 4, pp. 2650–2664, Apr. 2021, doi: 10.1109/TWC.2021.3052058.

[6] S. Rathore and J. H. Park, "Blockchain-Based Security for Cyber-Physical Systems: State-of-the-Art and Future Challenges,"*IEEE Consumer Electronics Magazine*, vol. 10, no. 2, pp. 84–90, Mar. 2021, doi: 10.1109/MCE.2020.3024344.

[7] C. Qiu, H. Yao, F. R. Yu, C. Jiang and S. Guo, "A Service-Oriented Permissioned Blockchain for the Internet of Things,"*IEEE Transactions on Services Computing*, vol. 13, no. 2, pp. 203–215, Mar.–Apr. 2020, doi: 10.1109/TSC.2019.2948870.

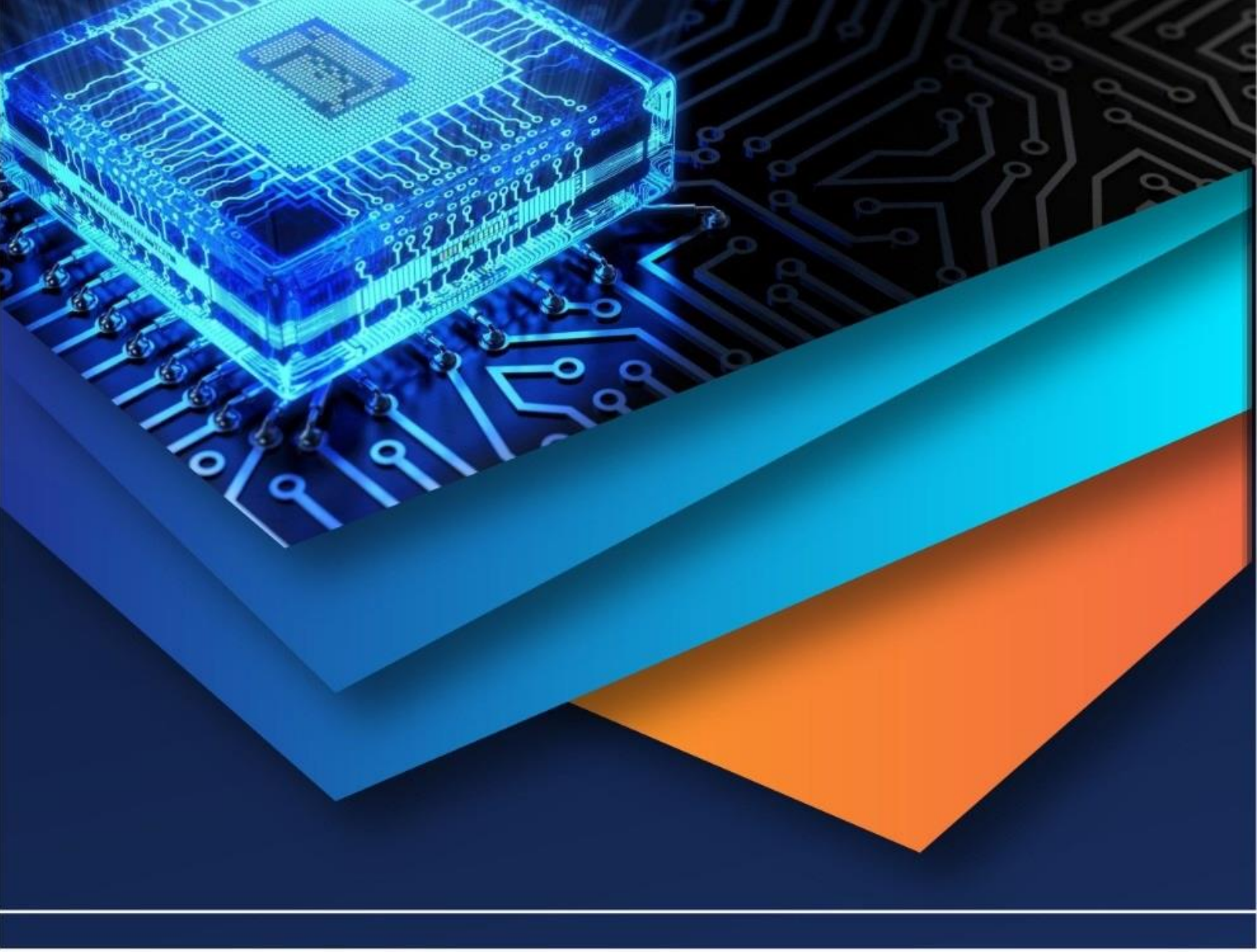
[8] R. Lu, X. Li, X. Liang and X. Shen, "EPPDR: An Efficient Privacy-Preserving Data Reporting Scheme for Smart Grid Communications,"*IEEE Transactions on Smart Grid*, vol. 5, no. 1, pp. 760–770, Jan. 2019, doi: 10.1109/TSG.2013.2279585.

[9] L. Xu, L. Chen and Z. Gao, "Smart Contract Based Lightweight Authentication Scheme for Wireless Body Area Network,"*IEEE Access*, vol. 6, pp. 51293–51301, 2018, doi: 10.1109/ACCESS.2018.2867545.

[10] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," White Paper, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf.

[11] W. Viriyasitavat, L. D. Xu, Z. Bi, D. Hoonsopon and N. Charoenruk, "Managing QoS of Internet-of-Things Services Using Blockchain," in IEEE Transactions on Computational Social Systems, vol. 6, no. 6, pp. 1357-1368, Dec. 2019, doi: 10.1109/TCSS.2019.2919667.
[12] R. A. Memon, J. P. Li, M. I. Nazeer, A. N. Khan and J. Ahmed, "DualFog-IoT: Additional Fog Layer for Solving Blockchain Integration Problem in Internet of Things," in IEEE Access, vol. 7, pp. 169073-169093, 2019, doi: 10.1109/ACCESS.2019.2952472.
[13] C. Qiu, H. Yao, F. R. Yu, C. Jiang and S. Guo, "A Service-Oriented Permissioned Blockchain for the Internet of Things," in IEEE Transactions on Services Computing, vol. 13, no. 2, pp. 203-215, 1 March-April 2020, doi: 10.1109/TSC.2019.2948870.
[14] C. Qiu, X. Ren, Y. Cao and T. Mai, "Deep Reinforcement Learning Empowered Adaptivity for Future Blockchain Networks," in IEEE Open Journal of the Computer Society, vol. 2, pp. 99-105, 2021, doi: 10.1109/OJCS.2020.3010987.
[15] M. Debe, K. Salah, M. H. Ur Rehman and D. Svetinovic, "Monetization of Services Provided by Public Fog Nodes Using Blockchain and Smart Contracts," in IEEE Access, vol. 8, pp. 20118-20128, 2020, doi: 10.1109/ACCESS.2020.2968573.
[16] Z. Liu, L. Gao, Y. Liu, X. Guan, K. Ma and Y. Wang, "Efficient QoS Support for Robust Resource Allocation in Blockchain-Based Femtocell Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 11, pp. 7070-7080, Nov. 2020, doi: 10.1109/TII.2019.2939146.
[17] S. Rathore, J. H. Park and H. Chang, "Deep Learning and Blockchain-Empowered Security Framework for Intelligent 5G-Enabled IoT," in IEEE Access, vol. 9, pp. 90075-90083, 2021, doi: 10.1109/ACCESS.2021.3077069.
[18] S. Maaroufi and S. Pierre, "BCOOL: A Novel Blockchain Congestion Control Architecture Using Dynamic Service Function Chaining and Machine Learning for Next Generation Vehicular Networks," in IEEE Access, vol. 9, pp. 53096-53122, 2021, doi: 10.1109/ACCESS.2021.3070023.
[19] W. Viriyasitavat, L. D. Xu and Z. Bi, "Specification Patterns of Service-Based Applications Using Blockchain Technology," in IEEE Transactions on Computational Social Systems, vol. 7, no. 4, pp. 886-896, Aug. 2020, doi: 10.1109/TCSS.2020.2999574.
[20] F. Guo, F. R. Yu, H. Zhang, H. Ji, M. Liu and V. C. M. Leung, "Adaptive Resource Allocation in Future Wireless Networks With Blockchain and Mobile Edge Computing," in IEEE Transactions on Wireless Communications, vol. 19, no. 3, pp. 1689-1703, March 2020, doi: 10.1109/TWC.2019.2956519.
[21] M. Liu, Y. Teng, F. R. Yu, V. C. M. Leung and M. Song, "A Deep Reinforcement Learning-Based Transcoder Selection Framework for Blockchain-Enabled Wireless D2D Transcoding," in IEEE Transactions on Communications, vol. 68, no. 6, pp. 3426-3439, June 2020, doi: 10.1109/TCOMM.2020.2974738.
[22] J. Liu, S. Guo, Y. Shi, L. Feng and C. Wang, "Decentralized Caching Framework Toward Edge Network Based on Blockchain," in IEEE Internet of Things Journal, vol. 7, no. 9, pp. 9158-9174, Sept. 2020, doi: 10.1109/JIOT.2020.3003700.
[23] A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini and A. Refaey, "ssHealth: Toward Secure, Blockchain-Enabled Healthcare Systems," in IEEE Network, vol. 34, no. 4, pp. 312-319, July/August 2020, doi: 10.1109/MNET.011.1900553.
[24] V. K. Rathi et al., "A Blockchain-Enabled Multi Domain Edge Computing Orchestrator," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 30-36, June 2020, doi: 10.1109/IOTM.0001.1900089.
[25] X. Lin, J. Wu, A. K. Bashir, J. Li, W. Yang and J. Piran, "Blockchain-Based Incentive Energy-Knowledge Trading in IoT: Joint Power Transfer and AI Design," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3024246.
[26] A. Kumari, S. Tanwar, S. Tyagi and N. Kumar, "Blockchain-Based Massive Data Dissemination Handling in IIoT Environment," in IEEE Network, vol. 35, no. 1, pp. 318-325, January/February 2021, doi: 10.1109/MNET.011.2000355.
[27] H. ElHusseini, C. Assi, B. Moussa, R. Attallah and A. Ghrayeb, "Blockchain, AI and Smart Grids: The Three Musketeers to a Decentralized EV Charging Infrastructure," in IEEE Internet of Things Magazine, vol. 3, no. 2, pp. 24-29, June 2020, doi: 10.1109/IOTM.0001.1900081.
[28] M. Karakus and E. Guler, "RoutingChain: A Proof-of-Concept Model for a Blockchain-Enabled QoS-Based Inter-AS Routing in SDN," 2020 IEEE International Black Sea Conference on Communications and Networking (BlackSeaCom), 2020, pp. 1-6, doi: 10.1109/BlackSeaCom48709.2020.9235021.
[29] H. Lee, K. Sung, K. Lee, J. Lee and S. Min, "Economic Analysis of Blockchain Technology on Digital Platform Market," 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), 2018, pp. 94-103, doi: 10.1109/PRDC.2018.00020.
[30] J. Zheng, X. Dong, Q. Liu, X. Zhu and W. Tong, "Blockchain-based secure digital asset exchange scheme with QoS-aware incentive mechanism," 2019 IEEE 20th International Conference on High Performance Switching and Routing (HPSR), 2019, pp. 1-6, doi: 10.1109/HPSR.2019.8808111.
[31] D. B. Rawat and A. Alshaikhi, "Leveraging Distributed Blockchain-based Scheme for Wireless Network Virtualization with Security and QoS Constraints," 2018 International Conference on Computing, Networking and Communications (ICNC), 2018, pp. 332-336, doi: 10.1109/ICCNC.2018.8390344.
[32] M. Liu, F. R. Yu, Y. Teng, V. C. M. Leung and M. Song, "Deep Reinforcement Learning (DRL)-Based Transcoder Selection for Blockchain-Enabled Video Streaming," 2018 IEEE Globecom Workshops (GC Wkshps), 2018, pp. 1-6, doi: 10.1109/GLOCOMW.2018.8644290.
[33] Sodhro, A.H., Pirbhulal, S., Muzammal, M. et al. Towards Blockchain-Enabled Security Technique for Industrial Internet of Things Based Decentralized Applications. J Grid Computing 18, 615–628 (2020). https://doi.org/10.1007/s10723-020-09527-x
[34] Kochovski, P., Stankovski, V., Gec, S. et al. Smart Contracts for Service-Level Agreements in Edge-to-Cloud Computing. J Grid Computing 18, 673–690 (2020). https://doi.org/10.1007/s10723-020-09534-y
[35] Asghari, P., Rahmani, A.M. & Javadi, H.H.S. Privacy-aware cloud service composition based on QoS optimization in Internet of Things. J Ambient Intell Human Comput (2020). https://doi.org/10.1007/s12652-020-01723-7
[36] Xu, X., Chen, Y., Yuan, Y. et al. Blockchain-based cloudlet management for multimedia workflow in mobile cloud computing. Multimed Tools Appl 79, 9819–9844 (2020). https://doi.org/10.1007/s11042-019-07900-x
[37] Qaisar Shaheen, Muhammad Shiraz, Muhammad Usman Hashmi, Danish Mahmood, Zhu zhiyu, Rizwan Akhtar, "A Lightweight Location-Aware Fog Framework (LAFF) for QoS in Internet of Things Paradigm," Mobile Information Systems, vol. 2020, Article ID 8871976, 15 pages, 2020. https://doi.org/10.1155/2020/8871976
[38] Li, W., Wu, J., Cao, J. et al. Blockchain-based trust management in cloud computing systems: a taxonomy, review and future directions. J Cloud Comp 10, 35 (2021). https://doi.org/10.1186/s13677-021-00247-5
[39] A. S. M. S. Hosen et al., "Blockchain-Based Transaction Validation Protocol for a Secure Distributed IoT Network," in IEEE Access, vol. 8, pp. 117266-117277, 2020, doi: 10.1109/ACCESS.2020.3004486.
[40] Zhang, Jianting & Hong, Zicong & Qiu, Xiaoyu & Zhan, Yufeng & Guo, Song & Chen, Wuhui. (2020). SkyChain: A Deep Reinforcement Learning-Empowered Dynamic Blockchain Sharding System. 1-11. 10.1145/3404397.3404460.

[41] Li, D, Deng, L, Cai, Z, Souri, A. Blockchain as a service models in the Internet of Things management: Systematic review. Trans Emerging Tel Tech. 2020; e4139. https://doi.org/10.1002/ett.4139
[42] PF-BTS: A Privacy-Aware Fog-enhanced Blockchain-assisted task scheduling, https://www.sciencedirect.com/science/article/pii/S0306457320308888
[43] J. Yun, Y. Goh and J. -M. Chung, "Trust-Based Shard Distribution Scheme for Fault-Tolerant Shard Blockchain Networks," in IEEE Access, vol. 7, pp. 135164-135175, 2019, doi: 10.1109/ACCESS.2019.2942003.
[44] C. Huang et al., "RepChain: A Reputation-Based Secure, Fast, and High Incentive Blockchain System via Sharding," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4291-4304, 15 March15, 2021, doi: 10.1109/JIOT.2020.3028449.
[45] S. Kim, "Two-Phase Cooperative Bargaining Game Approach for Shard-Based Blockchain Consensus Scheme," in IEEE Access, vol. 7, pp. 127772-127780, 2019, doi: 10.1109/ACCESS.2019.2939778.
[46] A. Hafid, A. S. Hafid and M. Samih, "New Mathematical Model to Analyze Security of Sharding-Based Blockchain Protocols," in IEEE Access, vol. 7, pp. 185447-185457, 2019, doi: 10.1109/ACCESS.2019.2961065.
[47] A. Hafid, A. S. Hafid and M. Samih, "A Novel Methodology-Based Joint Hypergeometric Distribution to Analyze the Security of Sharded Blockchains," in IEEE Access, vol. 8, pp. 179389-179399, 2020, doi: 10.1109/ACCESS.2020.3027952.
[48] A. Asheralieva and D. Niyato, "Reputation-Based Coalition Formation for Secure Self-Organized and Scalable Sharding in IoT Blockchains With Mobile-Edge Computing," in IEEE Internet of Things Journal, vol. 7, no. 12, pp. 11830-11850, Dec. 2020, doi: 10.1109/JIOT.2020.3002969.
[49] J. Yun, Y. Goh and J. -M. Chung, "DQN-Based Optimization Framework for Secure Sharded Blockchain Systems," in IEEE Internet of Things Journal, vol. 8, no. 2, pp. 708-722, 15 Jan.15, 2021, doi: 10.1109/JIOT.2020.3006896.
[50] M. H. Manshaei, M. Jadliwala, A. Maiti and M. Fooladgar, "A Game-Theoretic Analysis of Shard-Based Permissionless Blockchains," in IEEE Access, vol. 6, pp. 78100-78112, 2018, doi: 10.1109/ACCESS.2018.2884764.
[51] A. Hafid, A. S. Hafid and M. Samih, "Scaling Blockchains: A Comprehensive Survey," in IEEE Access, vol. 8, pp. 125244-125262, 2020, doi: 10.1109/ACCESS.2020.3007251.
[52] D. Jia, J. Xin, Z. Wang and G. Wang, "Optimized Data Storage Method for Sharding-Based Blockchain," in IEEE Access, vol. 9, pp. 67890-67900, 2021, doi: 10.1109/ACCESS.2021.3077650.
[53] N. Sohrabi and Z. Tari, "ZyConChain: A Scalable Blockchain for General Applications," in IEEE Access, vol. 8, pp. 158893-158910, 2020, doi: 10.1109/ACCESS.2020.3020319.
[54] A. Mizrahi and O. Rottenstreich, "State Sharding with Space-aware Representations," 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), 2020, pp. 1-9, doi: 10.1109/ICBC48266.2020.9169402.



10.22214/IJRASET

45.98

IMPACT FACTOR: 7.129

IMPACT FACTOR: 7.429

INTERNATIONAL JOURNAL FOR RESEARCH

IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY