Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

Optimizing Blockchain Scalability and IoT Security: A Multi-Objective Performance Framework

Anjana Rani [1], Monika Saxena [2]
[1] *Banasthali Vidyapith, Tonk District, Rajasthan, India. Email: anjanarani2814@gmail.com*
[2] *Banasthali Vidyapith, Tonk District, Rajasthan, India. Email: smonika@banasthali.in*

ARTICLE INFO

Received: 18 Dec 2024

Revised: 21 Feb 2025

Accepted: 28 Feb 2025

ABSTRACT

In this paper, a lightweight blockchain-based security framework for IoT networks that easily mitigates security, scalability, and data integrity issues is proposed. The framework associated with this paper integrates the hybrid consensus mechanism (DPoS + PBFT) and the hybrid cryptographic hashing approach (SHA-256 and ECC) to optimize both security and performance. The framework is implemented in a python based blockchain that employs IoT generated transactional data and is evaluated based on the performance parameters like latency, throughput, consensus delay, computational speed and also memory usage. Experimental results demonstrate that the hybrid consensus approach used in this framework achieves better performance metrics compared to the traditional consensus algorithms like PoW, PoS. hybrid hashing approach allows to achieve additional security with the same computational costs. The result shows that the potential of the proposed framework as a secure, scalable and energy solution in the context of real time IoT networks, and the future scope will include the autonomous deployment in the real-world, AI integration for Anomaly detection, and enhanced optimization for large IoT datasets.

Keywords: Blockchain, IoT, consensus algorithms, SHA-256, ECC

INTRODUCTION

The application of blockchain to the IoT has potential solutions to the challenges of security, scalability as well as efficiency. Decentralization is a critical aspect given the numbers of growing IoT devices and the requirements of data integrity, secure communication, and the scalable consensus mechanisms faced by IoT networks up to October 2023 [1]. Because of the decentralized and cryptographic characteristics of blockchain technology, it can serve as a good alternative since conventional security solutions are not suitable to the challenges raised by the decentralized and resource-constrained nature of IoT devices [2].

Proof-of-Work (PoW) and Proof-of-Stake (PoS) blockchain consensus mechanisms experience scalability limitations and significant computational demands which prevent them from functioning effectively in real-time IoT applications [3]. The latest studies focus on developing lightweight security solutions based on blockchain that integrate hybrid consensus approaches together with optimized cryptographic methods to boost performance. IoT environments benefit from blockchain networks that achieve enhances throughput and low latency through the use of hybrid consensus algorithms. The hybrid hashing algorithm achieves an acceptable compromise between security performance levels according to the study [4] [5] [6].

The research proposes a multi-objective optimization strategy to improve blockchain scalability while strengthening IoT network security. The proposed architecture achieves optimum security speed and resource efficiency through a hybrid consensus mechanism of DPoS and PBFT combined with a dual cryptographic hashing approach of SHA-256 and ECC. This security method improves blockchain IoT capabilities by building upon previous research to address essential performance and scalability issues [7] [8].

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

This paper presents extensive simulations and evaluations that examine various consensus approaches and hashing algorithms to determine their effects on IoT security as well as scalability [9].

The rest of the paper is organized as follows: Section 2 covers literature review on blockchain-enabled IoT security. Section 3 describes the Proposed hybrid security models, including consensus process and hashing methods. Section 4 provides the experimental results which include parameters like latency, throughput, consensus speed, computational delay and memory usage. Section 5 concludes the paper and also provides the future work.

RELATED WORK

Recent years have seen growing interest in combining blockchain technology with IoT due to blockchain's capability to enhance security measures along with the privacy of data and its integrity. The implementation of this technology remains limited due to multiple obstacles including processing complexity alongside scalability restrictions and high memory usage. Fu et al. [10] introduces a blockchain powered decentralized remote IoT access systems (RS-IoT) which removes the requirement for trusted third parties and safeguards IoT devices from zero-day attacks. Their approach takes advantage of blockchain's immutability and decentralization features to improve the security of IoT, which also decrease the risk of cyber-attacks. Similarly, Alamri et al. [11] examined numerous security challenges in IoT and highlighted the capacity of blockchain to handle the authentication, data integrity, and also access control challenges. This study also identifies security threats like MiTM and DoS attacks and also suggested that blockchain-based access control methods significantly improve the security of IoT devices.

Despite the security benefits of blockchain technology, challenges related to processing speed of transactions and resource consumption is also presented by blockchain, and also makes it difficult to implement it in the IoT resource constrained environment. Brotsis et al. [12] compared the performance of various blockchain designs like Ethereum, Hyperledger fabric, and IOTA, and also provide conclusion that permissioned blockchain methods are suitable for IoT applications because of its lower computing costs and speedy consensus procedures. And, to address the issues related to scalability, Rahman et al. [1] investigated the hybrid blockchain consensus algorithms like Delegated Proof-of-Stake (DPoS) and Practical Byzantine Fault Tolerance (PBFT). They find that such hybrid models strike a perfect balance between security, efficiency as well as energy consumption, which makes the integration of blockchain technology easier with the IoT environment.

Because of these findings, there is an increasing demand for multi-objective optimization frameworks that may improve both blockchain security as well as scalability in ioT applications. Current research shows that by combining the hybrid consensus methods with lightweight cryptographic hashing algorithms, might improve the blockchain performance for IoT applications.

PROPOSED FRAMEWORK

In this section, a blockchain-based lightweight security architecture for IoT networks is proposed. This framework uses a hybrid consensus method of DPoS + PBFT and a hybrid hashing algorithm of SHA256 + ECC, to enhance the data security, integrity as well as efficiency while lowering the computational cost. The suggested method aims to tackle the critical IoT security concerns such as manipulation of data, verification, and scalability [10] [11].

3.1 System Architecture

The proposed framework consists of four primary layers:

- **Data Acquisition Layer:** This layer is useful in gathering the real-time IoT generated data from the supply chain datasets, and the data gathered from the dataset is hashed before it is stored in the blockchain ledger [11].
- **Blockchain Layer**: A multi-consensus blockchain that uses Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof of Stake (DPoS), and practical Byzantine Fault Tolerance (PBFT) is implemented to evaluate the performance. SHA256 assures the immutability in the transactions and ECC allows for the efficient authentication [12].

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

- **Layer of Security and Validation:** Hybrid Hashing Approach of SHA256 and ECC strikes a balance between security as well as computational efficiency, and transactional validation guarantees the low latency and good throughput by using the hybrid consensus approach of DPoS and PBFT together [1].
- **Performance Evaluation Layer:** This layer is useful in measuring the latency, throughput, consensus delay, computational speed and memory usage to determine the optimal solution for the challenges.

IMPLEMENTATION METHODOLOGY

To achieve the above proposed research objectives following methodology is going to use.

Step 1: Data Analysis: The supply chain dataset containing the IoT generated Transaction records is analyzed and loaded and after that the key attributes are extracted from the dataset. Next step is to normalized and to clean the data by handling the duplicate, missing and incorrect formats [13].

Step 2: Hybrid Hashing Approach: SHA-256 is implemented for cryptographic security, which ensures the data immutability, while with the help of ECC a secure authentication is provided with minimal computational overhead. By combining both hashing algorithm a hybrid hash function is created that help to balance the security as well as efficiency. The hashed transactions are then structured and stored before inserting in the blockchain, and also ensures the data integrity and protection against tampering.

Step 3: Blockchain Development: A python-based blockchain architecture is designed by using the necessary components, which includes, genesis block, a structured block format which contains a timestamp, hash, previous hash, transactions, and nonce, and a transaction pool to store new transactions before validating the transaction. The blockchain thus implements the creation and linking of blocks, which ensures that each and every new block is connected securely by using the hashed data of transaction. In addition to this, a Python-based API is developed to enable the submission and retrieval of transaction, that allows the efficient interaction within the blockchain network.

Step 4: Implemetation of Hybrid Consensus Mechanism: PoW, PoS, DPoS, PBFT these are the consensus algorithms that are integrated for performance comparison, with DPoS + PBFT are selected for better efficiency and security. DPoS ensures the fast delegate-based validation, reduces the overhead, while on the other side, byzantine fault tolerance is ensured by using PBFT, and secures the transaction finalization. This hybrid approach of consensus algorithms enhances the scalability, security, and the consensus efficiency in IoT networks [14] [15].

Step 5: Smart Contract Integration: To automate the transaction validation and security within a blockchain network a Python-based smart contracts are developed. Predefined security conditions are implemented by using these contracts, such as verifying the hashed data before adding it to the blockchain network, which ensures that only valid transactions are recorded. After the deployment these contracts will verify the transactions by enhancing the security, efficiency, and trust within the IoT network [16].

Step 6: Simulation of Blockchain Network: A blockchain network is thus simulated to evaluate its performance under different cryptographic configurations that includes SHA-256, ECC, and a hybrid SHA-256 and ECC. Transactions are processed under each and every configuration, and then performance metrics are analyzed so that efficient setup to secure the IoT transactions is determined.

Step 7: Performance Evaluation: The blockchain framework is thus assessed on the basis of performance parameters, latency, throughput, consensus delay, computational speed and memory usage. A comparative analysis of PoW, PoS, DPoS, and PBFT is done to identify the suitable consensus mechanism and hashing combination for IoT security.

PERFORMANCE EVALUATION

To test the efficiency, reliability, and scalability of the blockchain-based security model for IoT networks by conducting a comprehensive performance evaluation. Under different configurations, the system is subjected to the test which compares the performance of PoW, PoS, DpoS, and PBFT in combination with various kinds of hash

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

functions of SHA-256 and ECC. They include latency, throughput, consensus delay, computations speed, and memory usage to judge the efficiency of blockchain for IoT networks [10].

5.1 Evaluation Metrics:

The system's performance is analyzed using the performance metrics as follows:

- **THROUGHPUT (Transactions per second):** This metric measures the speed or power of the system. Throughput is the product of network capacity and the maximum number of simultaneous transactions that can be performed [11].
- **Latency:** The average time a transaction sits in the queue before it is validated and approved by the validators. The latency is what makes a system responsive and thus, suitable for real time processing in space and time-sensitive IoT applications [12].
- **Consensus Delay:** The average time the network nodes spend to agree upon the validity of the transaction, and it is dependent on the consensus methods used [1].
- **Computational Speed**: The rate at which transactions are processed, measured in operations per second. This metric helps in assessing the overall transaction handling the efficiency of the system [13].
- **Memory Usage**: This metric will keep the track of peak RAM consumption during system execution, determining the feasibility of deploying blockchain in resource-constrained IoT environments [14].

5.2 Experimental Setup

The blockchain-based IoT security framework is implemented in python, using a supply chain dataset that includes transactional details. The experiment simulates multiple blockchain nodes and executes transactions under different configurations to assess the performance of system [17].

- **Consensus Mechanism Testing**: Transactions are validated using different consensus mechanisms – PoW, PoS, DPoS, and PBFT – to compare their efficiency. In addition to this, a hybrid consensus approach (DPoS + PBFT) is tested to evaluate its suitability for real-time IoT applications.
- **Hashing Algorithm Testing:** Transactions are hashed using SHA-256, ECC, and the hybrid methods (SHA-256 + ECC). The impact of each hashing technique on both security and processing speed is analyzed to identify the optimal solution for the IoT environment.

5.3 Results and Analysis

The result of the proposed framework shows that the Hybrid approach of DPoS + PBFT with SHA-256 + ECC is the most efficient and secure combination for blockchain based IoT security. As shown in Table 1 below, this hybrid approach achieves:

- High throughput and low latency, which makes it ideal for real-time IoT applications.
- Also reduced computational overhead compared to PoW, enabling the deployment on the resource-constrained IoT devices.
- Strong security with SHA-256 + ECC, which prevents the unauthorized access while optimizing the processing speed.

Table 1: Result of Proposed Framework

Approach	Latency	Throughput	Consensus Delay	Computational Speed	Memory Usage
HYBRID (DPoS + PBFT + SHA256 + ECC)	0.003693 sec	270.81 transactions/sec	0.000005 sec	11246.50 operations/sec	5.03 KB

Journal of Information Systems Engineering and Management
2025, 10(40s)
e-ISSN: 2468-4376
https://www.jisem-journal.com/

Research Article

CONCLUSION AND FUTURE WORK

The rapid growth of IoT networks demands advanced security and scalability solutions to secure both transactional data as well as communications between devices. This paper responds by introducing a lightweight blockchain-enabled security framework that blends hybrid consensus mechanisms (DPoS + PBFT) along with a combined cryptographic hashing approach (SHA-256 + ECC). The objective here is to augment the security, performance, and energy efficiency in blockchain-based IoT systems. Moreover, the python-based blockchain network was implemented using the new framework which was not only reliable but was also light in terms of computing data. Tests displayed the fact that very high (approx. 90%) throughput and decreased latency were achieved by the hybrid consensus mechanism, the results also depicted that this hybrid hashing method can increase the speed and accuracy of data integrity and authentication which are completely separate from making the whole process more efficient. In conclusion, the findings of this paper indicate that the proposed blockchain-enabled IoT security framework is a scalable, secure, and efficient solution to IoT security issues. With the help of lightweight cryptographic techniques and hybrid consensus mechanisms, the framework proves to offer real-time protection for IoT data without incurring huge computational costs.

FUTURE WORK

Even though the proposed framework improves blockchain scalability and security for IoT networks, there is still need for an upgrade. Subsequent experiments should try to assess the adaptability through further optimizing the system instead, especially for large-scale IoT environments. Key areas for future work comprise:

Integration with AI for Anomaly Detection: Use AI-based detection techniques to help detect problems in IoT devices in order to increase the system's resistance to threats.

Optimization for Large-Scale IoT Networks: exact transaction confirmation processes could be improved to handle a large Volume of IoT data with less energy usage.

Energy-Efficient Blockchain Solutions: Conduct a study on green blockchain technologies that can support low energy consumption along with high security.

By solving these problems, future security, and efficiency as well as make them for the best for real-world deployments and emerging industrial applications of blockchain-enabled IoT systems.

REFERENCES

[1] Rahman, Z., Yi, X., Khalil, I., & Kelarev, A. (2021). Blockchain for iot: A critical analysis concerning performance and scalability. In *Quality, Reliability, Security and Robustness in Heterogeneous Systems: 17th EAI International Conference, QShine 2021, Virtual Event, November 29–30, 2021, Proceedings 17* (pp. 57-74). Springer International Publishing.

[2] Moudoud, H., Cherkaoui, S., & Khoukhi, L. (2021, June). Towards a scalable and trustworthy blockchain: Iot use case. In *ICC 2021-IEEE International Conference on Communications* (pp. 1-6). IEEE.

[3] Dhieb, N., Ghazzai, H., Besbes, H., & Massoud, Y. (2020, June). Scalable and secure architecture for distributed iot systems. In *2020 IEEE Technology & Engineering Management Conference (TEMSCON)* (pp. 1-6). IEEE.

[4] Haque, E. U., Shah, A., Iqbal, J., Ullah, S. S., Alroobaea, R., & Hussain, S. (2024). A scalable blockchain based framework for efficient IoT data management using lightweight consensus. *Scientific Reports*, *14*(1), 7841.

[5] Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2019). LSB: A Lightweight Scalable Blockchain for IoT security and anonymity. *Journal of Parallel and Distributed Computing*, *134*, 180-197.

[6] Nguyen, D. C., Pathirana, P. N., Ding, M., & Seneviratne, A. (2021). Secure computation offloading in blockchain based IoT networks with deep reinforcement learning. *IEEE Transactions on Network Science and Engineering*, *8*(4), 3192-3208.

[7] Bulgakov, A. L., Aleshina, A. V., Smirnov, S. D., Demidov, A. D., Milyutin, M. A., & Xin, Y. (2024). Scalability and Security in Blockchain Networks: Evaluation of Sharding Algorithms and Prospects for Decentralized Data Storage. *Mathematics*, *12*(23), 3860.

[8] Yu, Y., Li, Y., Tian, J., & Liu, J. (2018). Blockchain-based solutions to security and privacy issues in the internet of things. *IEEE Wireless Communications*, *25*(6), 12-18.
[9] Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., ... & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *Ieee Access*, *7*, 22328-22370.
[10] Fu, C., Zeng, Q., & Du, X. (2019). Towards Efficient Integration of Blockchain for IoT Security: The Case Study of IoT Remote Access. *arXiv preprint arXiv:1912.00264*.
[11] Alamri, M., Jhanjhi, N. Z., & Humayun, M. (2019). Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review. *Int. J. Comput. Sci. Netw. Secur*, *19*(1), 244-258.
[12] Brotsis, S., Limniotis, K., Bendiab, G., Kolokotronis, N., & Shiaeles, S. (2021). On the suitability of blockchain platforms for IoT applications: Architectures, security, privacy, and performance. *Computer Networks*, *191*, 108005.
[13] Yuan, Y., & Wang, F. Y. (2018). Blockchain and cryptocurrencies: Model, techniques, and applications. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *48*(9), 1421-1428.
[14] Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.
[15] Wang, J., Chen, J., Ren, Y., Sharma, P. K., Alfarraj, O., & Tolba, A. (2022). Data security storage mechanism based on blockchain industrial Internet of Things. *Computers & Industrial Engineering*, *164*, 107903.
[16] Wu, J., & Tran, N. K. (2018). Application of blockchain technology in sustainable energy systems: An overview. *Sustainability*, *10*(9), 3067.
[17] Latif, S., Idrees, Z., Ahmad, J., Zheng, L., & Zou, Z. (2021). A blockchain-based architecture for secure and trustworthy operations in the industrial Internet of Things. *Journal of Industrial Information Integration*, *21*, 100190.