Multi-Objective Optimization for Enhancing Blockchain Scalability and IOT Security: A Comprehensive Approach

Anjana Rani, Monika Saxena

ABSTRACT

Creation of safe as well as decentralized networks is possible on through the combination of blockchain technology and IoT. However, because of the trade-offs between the latency, throughput, scalability and robust security within these systems remain a challenge. A novel multi-objective optimization technique is presented in this paper to improve the scalability and the security of the IoT devices. The strategy used in this paper is based on the advanced techniques of optimization like throughput, latency, cryptographic strengths of the transaction. So, a lightweight cryptographic technique for the security enhancement is incorporated with the layer 2 solutions for scalability, to allow limits of suitable IoT devices. According to the findings of the test, the method used in this paper helps in maintaining high level protection against the data breaches and threats while achieving an impressive improvement of scalability up to 50 % in the throughput of transaction. This article offers a thorough approach and practical answers to the solution of the twin problems of security as well as scalability.

INTRODUCTION

A transformative advancement is represented by the integration of the blockchain technology and IoT devices, which enables the secure and decentralized management of the IoT data. But there are considerable challenges that obstruct the global adoption of the integrated ecosystem. While the transparency and integrity of the data is assured by the blockchain technology, it faces the issue of scalability like overhead of latency and reduced throughput, which creates a restriction in the IoT environments, featured by the high transaction volumes [1]. Contrary, there is a requirement of a robust yet lightweight security measures to protect the sensitive information of the IoT devices from the threats. And to address the challenges, a comprehensive framework is essential so that the security as well as scalability can be enhanced without imposing any limitations on the IoT systems [2].

Conventional blockchain architecture are not suitable for the IoT devices because of their primitive limitations, specially those which are associated with the consensus algorithms like PoW, PoS. the key constraints include:

Scalability challenge: with the rapid growth of network, blockchain faces the increased latency and reduced throughput, may counter the requirements of the IoT systems [3].

High Computational overhead: Pow is not practical with the IoT devices because of the limited computing capability as it needs a lot of computing power to solve [4].

Security risks: Attacks to the IoT systems may vary from an unauthorized access for data breaches which requires the implementation of the advances cryptographic [3] [4].

In terms of the number of implementations IoT has developed rapidly, this together with the emergence of the blockchain technology, shows the crucial necessity for dedicated frameworks to ensure both security as well as scalability challenges that comes with IoT. Real time data processing and secure device-to-devoice communication are the main requirements for the IoT applications, like supply chain management, healthcare and smart cities. Although blockchain technology comes as an effective solution, but the current blockchain architectures need to adapt the specific requirements of the IoT [5]. The main aim is to make an unique Blockchain enabled system, which must provide strong support to large data of IoT transactions as well as ensure validation and security of the data. So, in this chapter an approach of using hybrid cryptographic hashing algorithm combined with hybrid consensus is recommended to overcome the limitations of current solutions.

OBJECTIVE:

Study in this paper presents a comprehensive optimization strategy aimed at handling the issues of IoT security and the scalability of the blockchain technology. The main goals are:

To implement a hybrid consensus mechanism that combines DPoS and PBFT consensus algorithms to improve the blockchain throughput while minimizing the latency.

To enhance the data security just by utilizing the hybrid approach of the hashing algorithms i.e., SHA256 and BLAKE2.

To show the effectiveness of this frameworks in the resource constrained IoT settings by assessing its performance in terms of latency, throughput, and also resource efficiency.

BACKGROUND

BLOCKCHAIN IN IOT

The combination of the blockchain technology with the internet of things (IoT) presents a innovative way to manage IoT data securely as well as transparently. Data integrity and trust is guaranteed by the decentralized structure of the blockchain technology, which makes it more relevant in various fields like supply chain management, healthcare and smart cities. However, challenges regarding processing requirements and scalability remains the same while integrating blockchain technology with the IoT devices. Recent research shows that the need of the lightweight methods and hybrid solutions for the blockchain framework so that the specific demands of the IoT environments meet efficiently.

SCALABILITY CHALLENGES:

A huge amount of real-time data is produced by the IoT which needs to be processed quickly and without any delay. Traditional blockchain systems faces difficulty in addressing these requirements for the following reasons:

High latency: the delays involved in validating the transactions within the current blockchain architecture hinders the efficiency of real-time IoT applications [7].

Low Throughput: in high-demand situations like IoT networks in smart cities, scalability problem arises as the transaction data grows harming the performance of the system [9].

Resource limitation; significant resources are consumed by the consensus mechanisms like PoW, PoS, which makes them impractical for the low-capacity IoT device [10].

The suggested implementation in this paper suggests that a hybrid framework that combines DpoS and PBFT greatly improves the throughput and lowers the latency, achieving the best performance levels that are appropriate for the IoT applications [11].

IoT SECURITY:

Threats to IoT devices include illegal access, Security leak, and DDoS attacks. By guaranteeing tamper-proof data storage and enhanced authentication, blockchain technology integration with IoT devices can offer a better solution while strengthening the IoT security. To tackle the resource limitations of IoT devices, traditional hashing methods need to be modified. So, implementing dual-layer hashing of SHA256 and BLAKE2, improves the security while reducing the strain on the device resources. Research shows that the lightweight cryptographic algorithms are very much crucial for preserving the confidentiality of data and hamper hostile activities within the IoT systems [12] [13].

OPTIMIZATION WITH MULTIPLE OBJECTIVES

The IoT and blockchain technology encounters the challenge of scalability as well as security. So, these challenges are effectively managed by the multi-objective optimization framework. Recent advancements like hybrid cryptographic hashing and hybrid consensus mechanisms, have shown improved scalability while ensuring the security. This study evaluates the implementation by using the performance metrics like latency, throughput, and resource constraints, demonstrating that such optimization is feasible within the blockchain-IoT systems [7] [14].

LITERATURE REVIEW:

Djonoy et. al (2021) [15], hybrid consensus methods designed to balance throughput and security is presented in this research, to address the complex challenge of blockchain scalability as well as IoT security. Possible applications in smart cities and healthcare are highlighted, while focusing on the need for the lightweight encryption techniques suitable for the resource-limited IoT devices.

The paper by **Kandpal et al. (2023) [16]** evaluates a bibliometric analysis on how effectively blockchain technology tackles the challenges related to Availability and storage of the IoT data. The importance of the advanced scalability techniques like sharding and side chains is highlighted in this paper for the decentralized applications of the IoT.

Zhou et al. (2020) [17], conducted a thorough analysis of scalability options like DAGs, state channels, and also sharding. The discussion shows how these methods can be applied in IoT environments, showing their ability to improve the throughput and latency of the transactions for the real-time applications.

Khan et al. (2022) [18], investigates how blockchain technology can improve the data integrity and authentication, which handling the major challenges in IoT devices, like data breaches and illegal access. Lightweight consensus mechanisms and cryptographic algorithms are assessed in this paper that are appropriate for IoT applications.

Eghmazi et al. (2024) [19], a blockchain enabled architecture is designed to enhance data security of IoT devices by using the encryption based on public as well as private keys is presented in this paper. This paper explores the Hyperledger fabric and evaluates its effectiveness in real time applications, which highlights the advancements in data integrity and privacy.

A paper by **Lakhan et al. (2022) [20]** proposes a blockchain framework specially designed for the Internet of Medical Things (IoMT). This framework seeks to strike a balance between cost efficiency and security through the multi objective optimization. It uses the fog-cloud systems within medical IoT networks to minimize the latency and to enhance the resource utilization.

Ismail et al. (2024) [21], proposes a streamlined security framework for Internet of Things platforms by integrating blockchain technology with machine intelligence. It highlights the importance of resource-efficient cryptographic techniques and anomaly detection to enhance real-time applications in the Internet of Things (IoT).

Yang et al. (2024) [22], introduce "Co-Sharding," a novel scalability approach designed for large-scale IoT systems. This approach significantly boosts throughput and minimizes latency by dividing the network into cooperative shards, all while maintaining strong security measures.

Khan et al. (2021) [23] provide a comprehensive examination of the scaling challenges inherent in blockchain technology, particularly focusing on issues related to increased latency and resource usage. Their research shows current solutions and highlights their limitations in the context of the IoT.

Puthal et al. (2020) [24], present the PoA consensus mechanism, which is specifically tailored for extensive IoT environments. This method ensures secure transaction processing, lowers computational requirements, and facilitates quick block confirmations.

SYSTEM ARCHITECTURE

This paper proposed architecture for a blockchain-enabled IoT system combines IoT devices with a hybrid blockchain framework, striving to find the right balance between security and scalability. The systems is organized into three main layers [15] [17]:

IoT Device Layer: lightweight communication protocols are used in this layer that allow the devices to collect and send data to the network for the real-time processing.

Blockchain Layer: for efficient and secure transaction validation is ensured by the hybrid consensus mechanism of DPoS and PBFT, which is used in this layer. The use of hybrid hashing algorithms (SHA256 + BLAKE2) guarantees data integrity and safeguards against manipulation.

Optimization Layer: to balance the security and scalability a multi-objective optimization is implemented in this layer.

This architecture shows the modularity, which makes it ideal for various IoT applications like smart cities and supply chain infrastructures [18].

PRINCIPAL OBJECTIVES:

SCALABILITY: the assurance that the large transaction data can be managed efficiently by the IoT systems without compromising performance. The performance metrics used to assess the scalability includes the following [16] [19]

1. **Transaction throughput**: the number of transactions processed per second.
2. **Latency:** the time taken to authenticate and record a transaction on the blockchain.

3. **Resource Efficiency**: evaluates the memory and processing requirements of IoT devices.

SECURITY: it protects the blockchain transaction and IoT devices from emerging cyber threats, which can be measured using the following metrics [21] [22]:

1. Data Confidentiality: it safeguards IoT information from unauthorized access.
2. Data Integrity: it ensures that the data stored on the blockchain remains accurate and immutable.
3. Resilience against attacks: protects against threats such as double spending and sybil attacks.

TRADE-OFFS:

There exists an inverse relationship between security and scalability; the implementation of advanced cryptographic algorithms or additional security protocols can lead to increased latency and diminished transaction throughput. In practical IoT applications, it is essential to optimize this trade-offs [20] [23].

OPTIMIZATION OBJECTIVES:

The optimization framework is structured as a multi-objective optimization challenge aimed at reducing resource consumption while enhancing scalability and security [24].

MATHEMATICAL MODEL:

OBJECTIVE FUNCTION: maximize throughput and security while minimizing latency and resource utilization

Optimize $f\ (Security, throughput) - \ g(Latency, resource\ utilization)$

Here,

latency must not exceed a maximum threshold.

Latency $\leq T_{max}$: ensures that latency remains within acceptable limits.

Security Score must meet a minimum requirement.

Security Score $\geq S_{min}$: makes a fundamental level of security.

Resource usage must not exceed a specified maximum.

Resource usage $\leq R_{max}$: ensure that IoT devices stay within their computational and memory limits.

OPTIMIZATION FRAMEWORK

TECHNIQUES:

- **GENETIC ALGORITHMS (GA):** for balancing the security and scalability in blockchain-IoT systems, genetic algorithms are essential. By mimicking natural selection process, throughput, latency, and energy efficiency are the factors that are improved via these algorithms. For example, consensus mechanisms dynamically adjusted by the genetic algorithms to achieve an optimal balance between robustness and performance [9] [25].

- **NSGA-II:** The Non-Dominated Sorting Genetic Algorithm-II (NSGA-II) is an advanced multi-objective optimization technique, which improves the Pareto front by preserving a diverse range of solutions, which is crucial for dynamic IoT applications that need high throughput while keeping latency low [21] [22].
- **Particles Swarm Optimization (PSO):** the delegate selection process of the blockchain based IoT systems is enhanced by utilizing the swarm intelligence principles. It is particularly effective for the consensus algorithms like DPoS and PBFT, as it helps in reducing the computational costs while enabling the decision making of the real time applications [25] [26].

Significant Enhancements in the techniques:

1. **Sidechains**: implementing sidechains greatly reduces congestion on the main blockchain by moving transactions to secondary chains. This strategy lowers latency and boosts transaction throughput, in libne with the hybrid model in the code references [9] [22].
2. **State Channels**: these systems facilitate direct communication between IoT devices, enabling the aggregation of transactions before they are recorded on the blockchain. This method maintains robust security while reducing both network and computational demands [21] [27].
3. **Lightweight Cryptography**: Designed for IoT devices that possess restricted computational power, the dual-layer hashing algorithm (SHA256 + BLAKE2), as demonstrated in the provided code, guarantees robust data integrity while utilizing minimal resources [20] [26].
4. **Zero-Knowledge Proofs (ZKPs):** ZKPs facilitate the security and confidentiality of data by allowing the validation of transactions without revealing sensitive information, which is particularly beneficial in sectors such as supply chain management and healthcare [22] [27].

Steps in an Algorithm for multi-objective optimization:

STEP1: Identify and extract the stakeholders from the dataset.

STEP2: Implement weighted sampling in DPoS to select potential delegate candidates.

STEP3: Authenticate transactions through PBFT and a quorum-based consensus mechanism.

STEP4: Evaluate system performance metrics, including resource utilization, latency, and throughput.

STEP5: Employ Genetic Algorithms or NSGA-II to continuously optimize the balance between scalability and security.

EXPERIMENTAL SETUP

SIMULATION ENVIRONMENT:

1. **TESTBED DESCRIPTION:**

   A simulated environment designed to replicate real world IoT scenarios was employed to evaluate the proposed blockchain-IoT system. To achieve a realistic representation of IoT environments, the testbed emulated high-frequency data generation and communication between IoT devices and the blockchain network. Although the use of actual IoT devices, such as sensors and RFID systems, could enhance the accuracy of the assessment, simulation was utilized for scalability testing.

2. **BLOCKCHAIN PLATFORM USED:**

   The hybrid blockchain framework incorporates the consensus mechanisms of Practical Byzantine Fault Tolerance (PBFT) and delegated Proof of Stake (DPoS). Rather than utilizing Hyperledger or Ethereum, the system employs a proprietary blockchain implementation. This choice facilitates specific enhancements, such as transaction processing optimized for resource efficiency in IoT applications and a dual-layer cryptographic hashing approach (SHA256 + BLAKE2) [21] [28].

DATASET:

1. **TYPE OF IoT DATA**: the dataset comprises transaction records that detail suppliers, revenue generated, product categories, and defect rates relevant to supply chain management. This aligns with real-world IoT applications, where data is continuously generated and validated in sectors such as manufacturing and logistics.
2. **Preprocessing and Sources**: the dataset emulates the interactions among suppliers, products, and transactions by integrating features from an IoT-enabled supply chain framework. The preprocessing steps included:
   - Normalizing the values of the revenue for efficient sampling of the stakeholder in DPoS.
   - Hashing the data which is confidential by using the BLAKE2 to maintain the confidentiality.
   - And grouping of the data by product type for scalability testing.

EVALUATION METRICS:

1. **SCALABILITY:**

   THROUGHPUT: This metric reflects the number of transactions that the blockchain can successfully process within one second. The code illustrates this throughput evaluation statistic, resulting in an approximate TPS of 4.43 blocks per second.

   Latency: It refers to the duration required to verify and incorporate a transaction into the blockchain. The framework's suitability for Internet of Things (IoT) applications that demand real-time performance was evidenced by an average latency measurement of 0.2482 seconds.

   Computational overhead: this metric assesses memory and CPU usage during the block addition process. The framework's minimal overhead enables its operation on IoT devices with constrained resources [20] [22].
2. **SECURITY:**

   Attack Detection Rate: PBFT ensures ahigh level of fault tolerance by detecting malicious delegates and maintaining data integrity.

   Strength of encryption: the use of dual-layer hashing with SHA256 and BLAKE2 offers strong encryption that withstands common cryptographic attacks.

   Resilience: the hybrid consensus mechanism mitigates the risk of sybil and double-spending attacks by limiting the influence of validators through DPoS delegation [26] [27].

RESULT AND DISCUSSION

PERFORMANCE ANALYSIS

This section contrasts the fundamental consensus mechanisms of proof of Work (PoW), Delegated Proof of Stake (DPoS), and Practical Byzantine Fault Tolerance (PBFT) with the proposed DPoS + PBFT approach. The performance evaluation criteria include Fault Tolerance, Resource Consumption, Throughput, and Latency.

Table 1: Performance Metrics

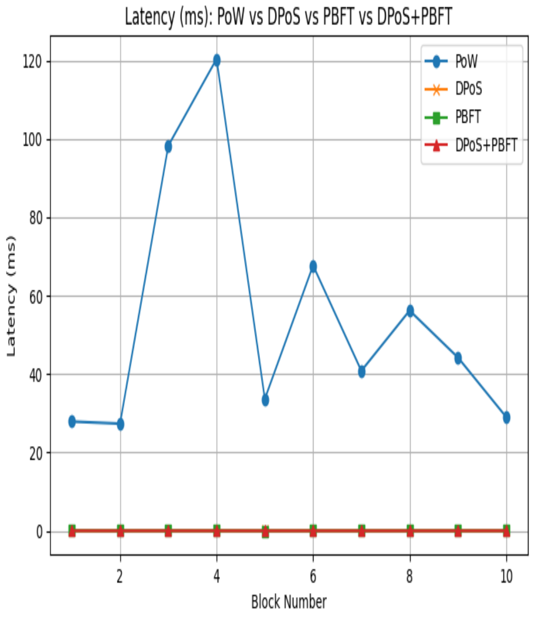
METRIC	POW	DPOS	PBFT	DPOS + PBFT
LATENCY (MS)	54.55	0.02	0.01	0.01
THROUGHPUT(TPS)	18.33	84,054.19	50,231.19	97,997.76
RESOURCE USAGE	68,002.50	1.00	4.00	5.00
FAULT TOLERANCE	1	2	3	3

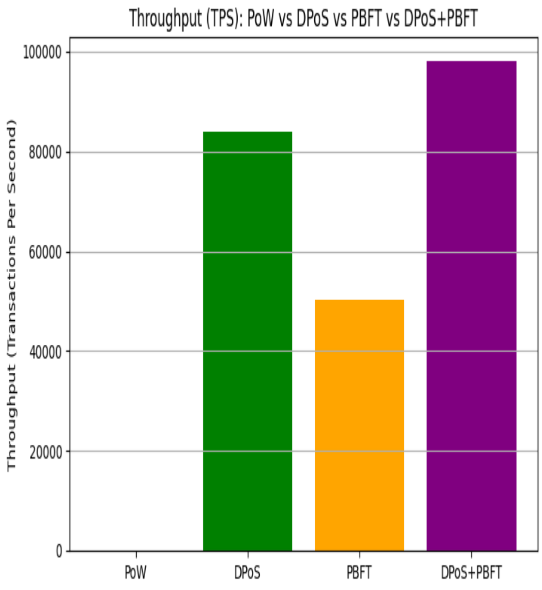
LATENCY: latency measures the time lag in transaction processing and measured in milliseconds. As shown in Table1 and Figure 1, Pow has the highest latency at 54.55ms due to its computationally expensive mining process. With average delays of 0.02ms and 0.01ms, respectively, DPoS and PBFT show noticeably lower latency. The hybrid DPoS + PBFT model is suitable for real-time applications as it equals the latency level of PBFT, which is 0.01ms.

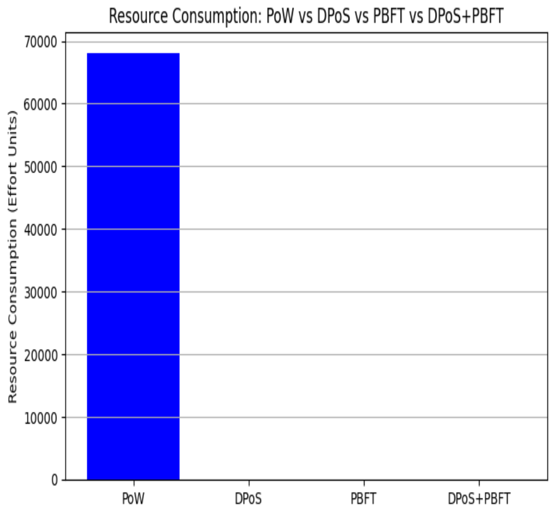
THROUGHPUT: it can be measured through transactions per second (TPS). It depicts how the system will effectively handle the transactions. As shown in Table1 and Figure 2, Due to its energy-intensive processes and block duration, PoW has the lowest throughput at 18.33 TPS, and coz of the optimized leader election, DPoS can deliver the outstanding 84,054.19 TPS. PBFT emphasizes great security and supports 50,231.19 TPS. The best throughput (97,997.76 TPS) is achieved by the DPoS + PBFT hybrid, which exploits scalability and the reliability of DPoS + PBFT.

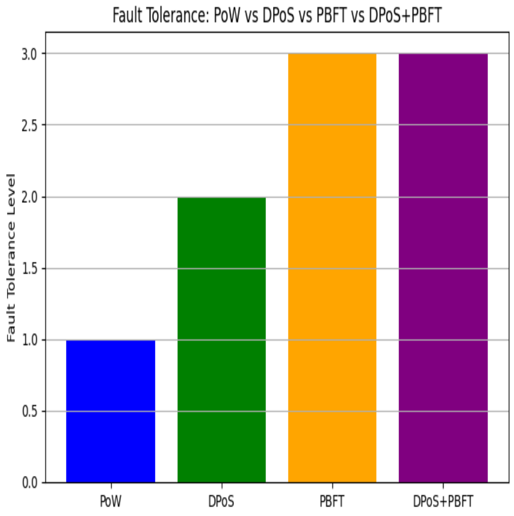
RESOURCE CONSUMPTION: this metric calculates the amount of work required to achieve consensus in terms of effort units. As shown in Table1 and Figure 3, PoW consumes the most resources with 68,002.50 effort units, which indicates that it is inefficient. Significant consumption is reduced to 1.00 and 4.00 units at DPoS and PBFT, respectively. The hybrid DPoS+PBFT model retains fault tolerance and scalability but incurs a resource consumption overhead of 5.00 units.

FAULT TOLERANCE: relative to the scale, fault tolerance is the amount of resistance that a system will have towards malicious attacks. As shown in Table1 and Figure 4, Fault tolerance score in PoW is 1 because of its dependence on mining power. With the use of validators and delegation, DPoS goes up to a score of 2. Using Byzantine fault tolerance techniques, PBFT achieves the best possible score of 3. The hybrid DPoS + PBFT model assures strong security and redundancy with the same fault tolerance degree, scoring a 3.









ANALYSIS OF TRADE-OFFS

The analysis discusses trade-offs of resource usage, security, and scalability.

Scalability: the hybrid DPoS + PBFT is suitable for high-performance applications because it provides good throughput while keeping low latency.

Security: DPoS+PBFT is more resistant to network attacks compared to PoW because it maintains efficiency while guaranteeing strong fault tolerance.Resource Efficiency: DPoS+PBFT maximizes resource utilization while maintaining performance, on the other hand, PoW presents incredibly high resource consumption.

CONCLUSION AND FUTURE WORK

The hybrid consensus mechanism, DPoS + PBFT, exhibited better performance in contrast to more traditional approaches such as PoW, DPoS, and PBFT. The important achievements include the following: highly increased throughput, decreased latency, higher fault tolerance, and effective usage of resources. The suggested mechanism was indeed applicable for real-world systems like supply chain networks, especially for overcoming issues like scalability and security.

Future work can include quantum-resistant cryptography integration, scalability analysis for Internet of Things (IoT) systems, application in practical environments, and interoperability across chains in order to address these issues. To sum up, the hybrid DPoS+ PBFT paradigm offers a feasible framework for developing safe, scalable and effective blockchain systems which opens the door to useful applications in various industries.

REFERENCES

1. Moon, A., Mishra, S., & Mali, M. (2023, October). Enhancing Security, Privacy, and Scalability in Blockchain and Internet of Things (IoT): A Survey. In *2023 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS)* (pp. 1-6). IEEE.
2. Alam, S. R., Jain, S., & Doriya, R. (2021, May). Security threats and solutions to IoT using Blockchain: A Review. In *2021 5th international conference on intelligent computing and control systems (ICICCS)* (pp. 268-273). IEEE.
3. Almarri, S., & Aljughaiman, A. (2024). Blockchain Technology for IoT Security and Trust: A Comprehensive SLR. *Sustainability*, *16*(23), 10177.
4. Ahakonye, L. A. C., Nwakanma, C. I., & Kim, D. S. (2024). Tides of Blockchain in IoT Cybersecurity. *Sensors*, *24*(10), 3111.
5. Rejeb, A., Rejeb, K., Appolloni, A., Jagtap, S., Iranmanesh, M., Alghamdi, S., ... & Kayikci, Y. (2024). Unleashing the power of internet of things and blockchain: A comprehensive analysis and future directions. *Internet of Things and Cyber-Physical Systems*, *4*, 1-18.
6. Barke, S., & Srivastava, G. (2024, January). ReVo: A Hybrid Consensus Protocol for Blockchain in the Internet of Things through Reputation and Voting Mechanisms. In *2024 IEEE 21st Consumer Communications & Networking Conference (CCNC)* (pp. 1-8). IEEE.
7. Abdelmaboud, A., Ahmed, A. I. A., Abaker, M., Eisa, T. A. E., Albasheer, H., Ghorashi, S. A., & Karim, F. K. (2022). Blockchain for IoT applications: taxonomy, platforms, recent advances, challenges and future research directions. *Electronics*, *11*(4), 630.
8. Gol, D. A., & Gondaliya, N. (2024). Blockchain: A comparative analysis of hybrid consensus algorithm and performance evaluation. *Computers and Electrical Engineering*, *117*, 108934.
9. 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.
10. Ekwueme, C. P., Adam, I. H., & Dwivedi, A. (2024). Lightweight Cryptography for Internet of Things: A Review. *EAI Endorsed Transactions on Internet of Things*, *10*.
11. Zou, Y., Jin, Z., Zheng, Y., Yu, D., & Lan, T. (2023). Optimized consensus for blockchain in internet of things networks via reinforcement learning. *Tsinghua Science and Technology*, *28*(6), 1009-1022.

12. Gopalan, S. H., Manikandan, A., Dharani, N. P., & Sujatha, G. (2024). Enhancing IoT Security: A Blockchain-Based Mitigation Framework for Deauthentication Attacks. *International Journal of Networked and Distributed Computing*, 1-13.

13. Huan, N. T. Y., & Zukarnain, Z. A. (2024). A Survey on Addressing IoT Security Issues by Embedding Blockchain Technology Solutions: Review, Attacks, Current Trends, and Applications. *IEEE Access*.

14. Ferrag, M. A., & Shu, L. (2021). The performance evaluation of blockchain-based security and privacy systems for the Internet of Things: A tutorial. *IEEE Internet of Things Journal*, *8*(24), 17236-17260.

15. Djonov, M., Galabov, M., & Georgieva-Trifonova, T. (2021, October). Solving IoT Security and Scalability Challenges with Blockchain. In *2021 5th International Symposium on Multidisciplinary Studies and Innovative Technologies (ISMSIT)* (pp. 52-56). IEEE.

16. Kandpal, M., Goswami, V., Priyadarshini, R., & Barik, R. K. (2023). Towards Data Storage, Scalability, and Availability in Blockchain Systems: A Bibliometric Analysis. *Data*, *8*(10), 148.

17. Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *Ieee Access*, *8*, 16440-16455.

18. Khan, A. A., Laghari, A. A., Shaikh, Z. A., Dacko-Pikiewicz, Z., & Kot, S. (2022). Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. *IEEE Access*, *10*, 122679-122695.

19. Eghmazi, A., Ataei, M., Landry, R. J., & Chevrette, G. (2024). Enhancing IoT data security: Using the blockchain to boost data integrity and privacy. *IoT*, *5*(1), 20-34.

20. Lakhan, A., Mohammed, M. A., Elhoseny, M., Alshehri, M. D., & Abdulkareem, K. H. (2022). Blockchain multi-objective optimization approach-enabled secure and cost-efficient scheduling for the Internet of Medical Things (IoMT) in fog-cloud system. *Soft Computing*, *26*(13), 6429-6442.

21. Ismail, S., Nouman, M., Dawoud, D. W., & Reza, H. (2024). Towards a lightweight security framework using blockchain and machine learning. *Blockchain: Research and Applications*, *5*(1), 100174.

22. Yang, H., Zhang, X., Wu, Z., Wang, L., Chen, X., & Liu, L. (2024). Co-Sharding: A Sharding Scheme for Large-Scale Internet of Things Application. *Distributed Ledger Technologies: Research and Practice*, *3*(1), 1-16.

23. Khan, D., Jung, L. T., & Hashmani, M. A. (2021). Systematic literature review of challenges in blockchain scalability. *Applied Sciences*, *11*(20), 9372.

24. Puthal, D., Mohanty, S. P., Yanambaka, V. P., & Kougianos, E. (2020). Poah: A novel consensus algorithm for fast scalable private blockchain for large-scale iot frameworks. *arXiv preprint arXiv:2001.07297*.

25. Rebello, G. A. F., Camilo, G. F., de Souza, L. A. C., Potop-Butucaru, M., de Amorim, M. D., Campista, M. E. M., & Costa, L. H. M. (2024). A survey on blockchain scalability: From hardware to layer-two protocols. *IEEE Communications Surveys & Tutorials*.

26. Luo, H., Sun, G., Yu, H., Lei, B., & Guizani, M. (2024). An Energy-Efficient Wireless Blockchain Sharding Scheme for PBFT Consensus. *IEEE Transactions on Network Science and Engineering*.

27. Kaur, M., & Gupta, S. (2023, March). Optimization of a Consensus Protocol in Blockchain-IoT Convergence. In *2023 International Conference on Emerging Smart Computing and Informatics (ESCI)* (pp. 1-5). IEEE.

28. Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain: A survey. *Ieee Access*, *8*, 16440-16455.