

Paper Type: Original Article

Blockchain-Enhanced Internet of Thing Networks for Data Privacy

Vanshika Rani* 

Department of Computer Science Engineering, KIIT University, Bhubaneswar, India; 22053998@kiit.ac.in.

Citation:

Received: 26 October 2023
Revised: 24 January 2024
Accepted: 28 February 2024

Rani, V. (2024). Blockchain-enhanced internet of thing networks for data privacy. *Metaverse*, 1(2), 93-101.

Abstract


The Internet of Things (IoT) continues to revolutionize industries by interconnecting billions of devices, but this growth comes with critical challenges related to data privacy and security. Traditional centralized systems for managing IoT data are prone to cyberattacks, data tampering, and breaches, raising concerns about user privacy. Blockchain, a decentralized, tamper-resistant technology, offers a promising solution to these challenges. By integrating blockchain with IoT, data integrity can be ensured through transparent, immutable records. This paper examines how blockchain can enhance IoT networks by improving data privacy, security, and scalability. Case studies from blockchain-based IoT implementations and mathematical models for transaction time and network efficiency are explored.


Keywords: Internet of things, Blockchain, Data privacy, Security, Scalability.

1 | Introduction

The exponential rise in connected IoT devices, projected to surpass 75 billion by 2025, has opened up numerous possibilities for smart industries, health, agriculture, and home automation. Despite these advantages, IoT systems face significant security risks due to their centralized architecture, which creates a single point of failure. Data privacy is particularly at risk as many IoT devices lack sophisticated security mechanisms, making them vulnerable to unauthorized access [1–4].

Blockchain, a decentralized ledger technology, emerged as a transformative tool to address these risks [5], [6]. First introduced as the backbone of cryptocurrencies like Bitcoin, blockchain ensures data immutability and transparency. By leveraging a consensus mechanism, blockchain verifies and records transactions across multiple nodes, making it highly resistant to cyberattacks. Integrating blockchain with IoT allows

 Corresponding Author: 22053998@kiit.ac.in

 10.22105/metaverse.v1i2.55



Licensee System Analytics. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<http://creativecommons.org/licenses/by/4.0>).

decentralized management of data transactions, ensuring that no single entity has control over the network [7–9]. This integration is poised to offer unparalleled security, privacy, and transparency in IoT systems.

1.1 | Variables and Equations

Several key variables and equations help analyze IoT system performance, particularly in terms of data privacy, transaction time, and overall network efficiency, in the context of blockchain-enhanced IoT networks.

Variables

D = Data size generated by the IoT device (in kilobytes, KB).

B = Blockchain block size (in kilobytes, KB).

N = Number of nodes participating in the blockchain network.

T = Time to verify a block (in seconds).

T latency = Latency in the blockchain network (in seconds).

R = Data transmission rate (in kilobytes per second, KB/s).

S encryption = Encryption strength (bits).

P block = Processing power of each node (in operations per second).

These variables form the basis for modeling blockchain's impact on IoT network performance, particularly in terms of data transmission time, verification time, and security.

Equations

Transaction time equation: the total time required for a data transaction to be verified on the blockchain is primarily determined by the size of the data, the number of nodes, and the time taken to verify each block:

$$T_{\text{transaction}} = D \times B / N \times T,$$

where transaction is the total transaction time for the data to be verified across the blockchain.

- I. D is the data size generated by the IoT device.
- II. B is the block size of the blockchain.
- III. N is the number of nodes verifying the transaction.
- IV. T is the time taken to verify one block.

This equation suggests that increasing the number of nodes (N) or reducing the block size (B) can help reduce the overall transaction time.

Latency in blockchain network

The latency in a blockchain network can be modeled as;

$$T_{\text{latency}} = D / R,$$

where

Tlatency is the network latency for transmitting data.

D is the data size.

R is the data transmission rate.

This equation helps quantify how quickly data can be transmitted over the network before blockchain verification takes place.

Blockchain security and processing equation

The security of the blockchain network, particularly of IoT devices, can be influenced by the encryption strength and the processing power of nodes:

$$S_{\text{blockchain}} = S_{\text{encryption}} \times N / P_{\text{block}},$$

where

$S_{\text{blockchain}}$ represents the security level of the blockchain network.

$S_{\text{encryption}}$ is the strength of encryption (measured in bits).

N is the number of nodes participating in the verification process.

P_{block} is the processing power of each node.

This equation indicates that stronger encryption or a higher number of nodes enhances the security of the blockchain, but higher encryption strength also requires more processing power.

Energy consumption for blockchain verification

Given the energy-intensive nature of blockchain consensus mechanisms, the energy consumption for verifying a block can be modeled as follows:

$$E_{\text{verification}} = P_{\text{block}} \times T,$$

where

$E_{\text{verification}}$ is the energy consumed for verifying a single block.

P_{block} is the processing power of the node.

T is the time taken to verify the block

2 | Blockchain in Internet of Thing: Data Privacy and Security

2.1 | Internet of Thing Data Privacy Challenges

IoT devices are designed to continuously collect, transmit, and process data, often containing sensitive personal and operational information. In centralized networks, the control over this data typically resides with a third-party service provider, creating concerns over trust and unauthorized data usage. These issues are magnified in smart environments where devices like cameras, health monitors, and personal assistants gather real-time data.

The current security protocols used in IoT networks—such as firewalls and encryption—are inadequate when faced with sophisticated cyberattacks or internal threats. Moreover, the complexity and heterogeneity of IoT devices, combined with their limited computational resources, make it difficult to implement robust security measures.

2.2 | Blockchain as a Solution to Data Privacy

Blockchain's decentralized nature ensures that no central authority has control over the data, which is recorded on a tamper-resistant ledger [10]. This not only increases transparency but also prevents unauthorized manipulation of data. Each transaction or data entry on the blockchain is cryptographically signed, and network-wide consensus is required before it is added to the blockchain. As a result, hackers would need to gain control of the majority of nodes to alter any data, making attacks highly impractical and expensive.

Blockchain also supports user anonymity through pseudonymous addresses. In a blockchain-IoT system, device identities are tied to cryptographic keys rather than personal information, reducing the risk of data breaches related to user identity.

3 | Blockchain Integration Models for Internet of Thing

3.1 | Public Blockchains in Internet of Thing

Public blockchains, such as ethereum, allow anyone to participate in the network. This model is highly decentralized and secure, making it suitable for applications where trust in a centralized authority is absent. However, the major drawback of public blockchains is scalability. As the number of IoT devices and transactions grows, the public blockchain network faces challenges in processing transactions quickly due to its consensus mechanisms like Proof of Work (PoW) [11].

A recent study by Christidis and Devetsikiotis explored how Ethereum's smart contract capabilities could be leveraged to automate secure data transactions in IoT devices [12]. Although Ethereum successfully facilitated secure transactions, scalability, and latency issues arose as the network grew. Transaction verification times extended up to 30 minutes, making it unsuitable for time-sensitive IoT applications.

3.2 | Private Blockchains in Internet of Thing

In contrast, private blockchains restrict participation to pre-approved entities, which can improve network efficiency and reduce transaction verification times. Private blockchains are more suitable for enterprise-level IoT applications where high throughput and low latency are required, such as in supply chain management or smart cities. IBM's Hyperledger Fabric was deployed in smart grids to transmit energy consumption data from IoT-enabled smart meters securely. The blockchain provided a transparent, tamper-proof ledger of all energy transactions, reducing fraud and ensuring data privacy. The smart grid implementation reported a transaction verification time of less than 5 seconds.

4 | Mathematical Model: Blockchain Transaction Efficiency in Internet of Thing Networks

Blockchain and IoT integration can be evaluated mathematically by measuring the time taken for a data transaction to be verified and added to the blockchain.

4.1 | Variables and Equations

The following factors determine the efficiency of blockchain in IoT:

D: Data size (KB).

N: Number of nodes in the blockchain.

T: Time to verify a block (seconds).

B: Block size (KB).

Transaction time equation:

The transaction time $T_{\text{transaction}}$ for IoT data can be modeled as

$$T_{\text{transaction}} = D \times \frac{B}{N} \times T,$$

where

$T_{\text{transaction}}$ represents the time for a data transaction to be verified across the blockchain network.

D is the data size generated by the IoT device.

B is the size of each blockchain block.

N is the number of nodes validating the transaction.

T is the average time taken by each node to verify a block.

5 | Discussion

From this equation, we can infer that increasing the number of nodes or decreasing the block size can significantly reduce the transaction time. However, reducing the block size too much may increase the frequency of transactions, which can overwhelm the network. Thus, an optimal balance must be found between these variables to ensure efficiency.

5.1 | Limitations and Future Directions

While blockchain holds great potential for enhancing data privacy in IoT networks, several limitations need to be addressed:

- I. Scalability: Public blockchains struggle to process many transactions in real-time, a critical requirement for IoT applications.
- II. Energy consumption: The energy consumption associated with blockchain verification processes, especially in PoW systems, can be high. This is not ideal for IoT devices, many of which are low-power.
- III. Latency: Blockchain's inherent latency, due to the consensus mechanisms, may affect real-time IoT applications like autonomous vehicles.

5.2 | Future Research

Future research should focus on integrating more energy-efficient consensus mechanisms, such as Proof of Stake (PoS) or Delegated Proof of Stake (DPoS), to improve blockchain's scalability for IoT applications. Additionally, hybrid models combining centralized and decentralized systems could offer a practical solution, balancing the need for security and efficiency.

6 | Conclusion

Blockchain technology offers a transformative approach to addressing the critical challenges of data privacy and security in IoT networks. By decentralizing control and ensuring transparency through its immutable ledger, blockchain enhances the overall trust in IoT systems, reducing the risk of data tampering and unauthorized access. This paper has demonstrated how blockchain can improve the privacy of IoT-generated data by preventing single points of failure, ensuring data integrity, and allowing only authorized entities to access sensitive information.

The mathematical models provided in this research further illustrate how blockchain integration impacts IoT performance, particularly in terms of transaction time, latency, security, and energy consumption. These models highlight the need to balance key variables such as block size, the number of network nodes, and encryption strength to optimize blockchain IoT systems.

Despite its advantages, blockchain implementation in IoT still faces limitations, particularly around scalability and energy efficiency. Public blockchains like Ethereum struggle with transaction throughput and latency, making them less suitable for large-scale, real-time IoT applications. However, private or consortium blockchains provide a more viable alternative, offering higher efficiency and faster transaction times.

Moving forward, ongoing research into more scalable consensus mechanisms (such as PoS) and hybrid blockchain architectures could address these challenges. By exploring these innovations, blockchain can become a crucial tool in securing IoT networks and ensuring data privacy while maintaining scalability and

performance for the massive amounts of data generated by IoT devices. In conclusion, blockchain holds immense potential to transform IoT into a more secure and privacy-focused technology ecosystem, but further advancements are needed to realize its capabilities fully.

Acknowledgments

I would like to express my gratitude to the KIIT faculty, especially the IoT research group, for their valuable input throughout this study. I also extend my thanks to my colleagues for their constructive feedback and for providing the necessary resources to conduct this research.

Author Contribution

The sole author was responsible for all aspects of this research, including the conceptualization and design of the study, data collection, analysis, and interpretation of the results. The author also wrote the entire manuscript, conducted the literature review, developed the mathematical models, and prepared the figures and tables. The author carried out all revisions and finalizations of the paper independently.

Funding

This research received no external funding.

Data Availability

The data generated or analyzed during this study, including raw datasets, experimental results, and any supporting material, are not publicly available due to privacy concerns and restrictions related to the nature of the research. However, these materials can be provided by the author upon reasonable request for academic and research purposes. Any interested parties who wish to access the data for further analysis or replication of the study may contact the author at 22053998@kiit.ac.in. Reasonable requests will be considered, and appropriate data-sharing agreements will be established to ensure privacy and confidentiality guidelines compliance.

Conflicts of Interest

The author declares that there are no conflicts of interest regarding the publication of this paper. No financial, personal, or professional influence could have affected the research, its outcomes, or the integrity of the findings presented in this work.

References

- [1] Shafiq, M., Gu, Z., Cheikhrouhou, O., Alhakami, W., & Hamam, H. (2022). The rise of “internet of things”: Review and open research issues related to detection and prevention of IoT-based security attacks. *Wireless communications and mobile computing*, 2022(1), 8669348. <https://doi.org/10.1155/2022/8669348>
- [2] Shahid, J., Ahmad, R., Kiani, A. K., Ahmad, T., Saeed, S., & Almuhaideb, A. M. (2022). Data protection and privacy of the internet of healthcare things (IoHTs). *Applied sciences*, 12(4), 1927. <https://doi.org/10.3390/app12041927>
- [3] Aqeel, M., Ali, F., Iqbal, M. W., Rana, T. A., Arif, M., & Auwul, M. R. (2022). A review of security and privacy concerns in the internet of things (IoT). *Journal of sensors*, 2022(1), 5724168. <https://doi.org/10.1155/2022/5724168>
- [4] Barik, B., Kar, D., Parida, S., Aeron, D., Mohapatra, H., & Mishra, S. R. (2024). Ensuring security and privacy in IoT ecosystems: A comprehensive approach. *Journal of network security computer networks*, 10(2), 50–66. <https://B2n.ir/j85299>
- [5] Anthony Jnr, B. (2023). Distributed ledger and decentralised technology adoption for smart digital transition in collaborative enterprise. *Enterprise information systems*, 17(4), 1989494. <https://doi.org/10.1080/17517575.2021.1989494>

- [6] Singh, D. S. (2024). Decentralized finance (DeFi): Exploring the role of blockchain and cryptocurrency in financial ecosystems. *International research journal of modernization in engineering technology and science*, 5. <https://www.doi.org/10.56726/IRJMETS48585>
- [7] Al Sadawi, A., Hassan, M. S., & Ndiaye, M. (2021). A survey on the integration of blockchain with IoT to enhance performance and eliminate challenges. *IEEe access*, 9, 54478–54497. <https://doi.org/10.1109/ACCESS.2021.3070555>
- [8] Rahman, M. S., Chamikara, M. A. P., Khalil, I., & Bouras, A. (2022). Blockchain-of-blockchains: An interoperable blockchain platform for ensuring IoT data integrity in smart city. *Journal of industrial information integration*, 30, 100408. <https://doi.org/10.1016/j.jii.2022.100408>
- [9] Habib, G., Sharma, S., Ibrahim, S., Ahmad, I., Qureshi, S., & Ishfaq, M. (2022). Blockchain technology: Benefits, challenges, applications, and integration of blockchain technology with cloud computing. *Future internet*, 14(11), 341. <https://doi.org/10.3390/fi14110341>
- [10] Dong, S., Abbas, K., Li, M., & Kamruzzaman, J. (2023). Blockchain technology and application: An overview. *PeerJ computer science*, 9, e1705. <https://doi.org/10.7717/peerj-cs.1705>
- [11] Sapra, N., Shaikh, I., & Dash, A. (2023). Impact of proof of work (PoW)-based blockchain applications on the environment: A systematic review and research agenda. *Journal of risk and financial management*, 16(4), 218. <https://doi.org/10.3390/jrfm16040218>
- [12] Christidis, K., & Devetsikiotis, M. (2016). Blockchains and smart contracts for the internet of things. *IEEE access*, 4, 2292–2303. <https://doi.org/10.1109/ACCESS.2016.2566339>

Appendix A

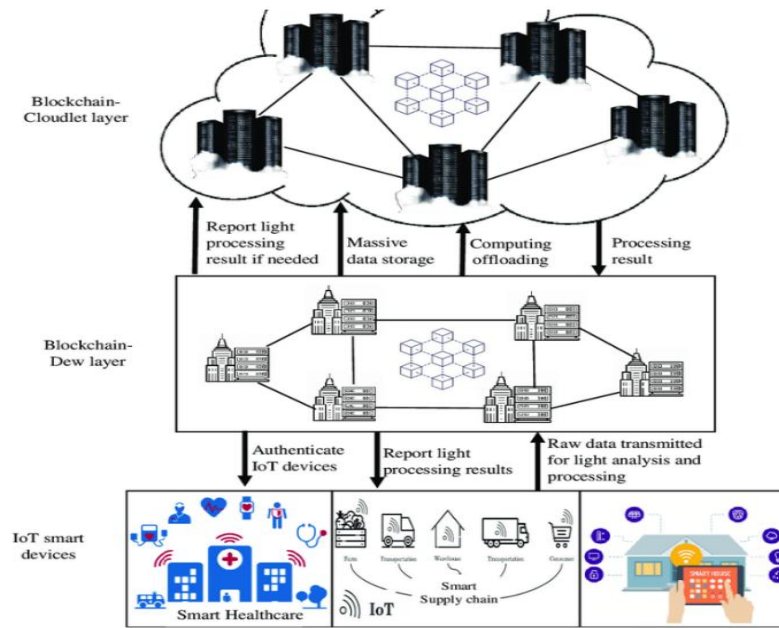


Fig. A1. Architecture of blockchain-enhanced IoT network.

Appendix B

Table B1. Table of key terms.

Term	Definition
Blockchain	A decentralized, distributed ledger technology that records transactions across many computers.
IoT	A network of interconnected devices that communicate and exchange data with each other.
Smart contract	Self-executing contracts with the terms of the agreement directly written into code.
Consensus mechanism	A process used to achieve agreement on a single data value among distributed systems.
Decentralization	Distribution of authority away from a central entity, reducing the risk of data tampering.

Appendix C

Table C1. Mathematical model variables.

Variable	Description
D	Data size generated by the IoT device (in KB)
B	Blockchain block size (in KB)
N	Number of nodes participating in the blockchain network
T	Time to verify a block (in seconds)
Tlatency	Latency in the blockchain network (in seconds)
R	Data transmission rate (in KB/s)
Sencryption	Encryption strength (in bits)
Pblock	Processing power of each node (in operations per second)

Appendix D

Table D1. Sample data for analysis.

Device ID	Data Generated (KB)	Timestamp	Status
IoT_001	50	2024-10-01 12:00:00	Active
IoT_002	30	2024-10-01 12:01:00	Active
IoT_003	45	2024-10-01 12:02:00	Inactive
IoT_004	20	2024-10-01 12:03:00	Active
IoT_005	60	2024-10-01 12:04:00	Active