

A Review of Blockchain-Based Solutions to Internet of Things (IoT) Security Challenges

Joni^{1*}, ShuchitaUpadhyaya², MonikaPoriye³, and NaveenSharma⁴

^{1,2,3}Department of Computer Science & Applications, Kurukshetra University, Kurukshetra

⁴Department of Computer Science and Engineering, HMR Institute of Technology and Management, GGSIP University, Delhi

*2228phd.joni@kuk.ac.in

* Corresponding author

doi: <https://doi.org/10.21467/proceedings.7.6.55>

Abstract

The Internet of Things (IoT) is the collaboration of computation, networking, and physical objects. This physical object is combined within a network that shares information between connected devices via the Internet. In today's era, IoT technology is used in almost all fields smart homes, smart cities, distributed grid systems, intelligent transportation systems, and healthcare. But the centralized architecture used in the Internet of Things for connecting and communicating via the Internet produces a threat to the security and privacy of the most sensitive data, which requires a decentralized system. Blockchain is the most emerging technology that provides solutions to modern IoT-based applications and provides a secure, reliable, and efficient computing framework. The intrinsic interior consensus algorithm and distributed storage address the issues that arise in IoT applications. This paper discusses the security challenges in IoT-based systems, a systematic review of blockchain as a solution to the IoT-based problem, and the challenges that occur in the collaboration of Blockchain with IoT.

Keywords: Internet of Things, Blockchain, and Security.

1 Introduction

The Internet of Things was coined by Kevin Ashton in 1999. At that period, it was not so popular, but it gained popularity after Gartner integrated IoT with its "new emerging technologies" in 2011 [1]. In 2022, around 29 billion devices are forecasted, where the count of devices related to IoT was around 18 billion, which is half of all the total devices forecasted, which automatically explains the global momentum that IoT gained. With the increasing and easy access to Internet connectivity in every area, whether it is related to healthcare, transportation, or many other sectors, there is a demand for making everything smart and intelligent, which is the biggest reason for the growing popularity of the Internet of Things. It consists of physical objects enabled by the Web that are interrelated to each other, communicate, process, and transfer data over the Internet [2]. As IoT systems have grown in scale and complexity, they have faced challenges related to communication transactions, security, and data analysis. Blockchain is emerging as a crucial component to tackle these problems. The concept of IoT was introduced in the early 2000s, although it gained popularity in the following decade. IoT encompasses a wide spectrum of applications such as smart homes, smart healthcare, smart cameras, smart cities, and wearable devices, to industrial automation. These applications share a common goal: to use data from various devices to make informed decisions and streamline processes. Blockchain's distributed ledger system offers a tamper-resistant and decentralized framework for recording transactions. Smart contracts in blockchain are self-executing contracts that automatically execute when specific conditions are met. For example, a blockchain-based smart contract constructed on predefined rules makes a payment to a supplier after a shipment of goods is received and verified by IoT sensors. Security is a paramount concern in IoT, which gives the potential consequences of data violations and malicious attacks. IoT devices are usually vulnerable consequent their limited processing power and memory, making them attractive targets for cybercriminals. Blockchain's decentralization cryptographic technique significantly enhances security by protecting data integrity, reducing the threat of unauthorized accessibility, and ensuring traceability.



2 Security Concerns in Internet of Things

Security concerns in IoT, particularly concerning authentication and authorization, are paramount for ensuring the integrity, confidentiality, and availability of IoT systems and data [3]. Figure 1 defines some important security aspects in IoT. Authentication involves verifying the identity of users and devices attempting to access IoT resources, including challenges related to device identity validation, secure key management, and user authentication, especially in user-interaction-based IoT systems like smart homes. In authorization, focus

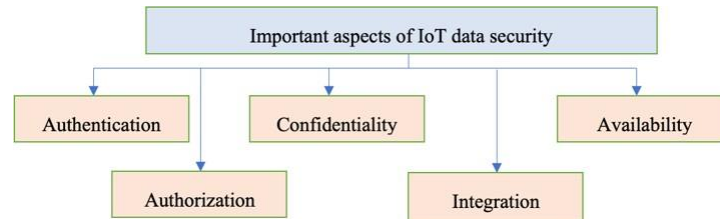


Fig. 1. Security Concept in IoT

is on defining and enforcing access control policies, addressing issues such as granular access control for different devices, dynamic authorization in fluctuating IoT environments, and secure data sharing among multiple devices and users. Blockchain technology, in this context, plays a critical role by providing a tamper-resistant ledger for device identities, ensuring the secure storage and management of cryptographic keys, facilitating transparent, immutable access control rules, and validating and tracking data sharing agreements. The intrinsic interior consensus algorithm and dispersed storage solve the problems that occur in IoT applications.

3 Blockchain as a Solution to the IoT (Internet of Things) Problem

Blockchain with IoT is a new automation that provides a decentralized, immutable, distributed, and digital ledger that records the transactions among IoT devices. In the blockchain digital ledger contains records that are used to record transactions among many computers, so that if any computer wants to change, it cannot be done without their members. The Internet of Things defines the physical objects that are smart devices with processing ability, sensors, software, and actuators that can connect and share data among the devices. The idea of blockchain with IoT provides a method to process the data securely among the Internet of Things. Blockchain is an open-source platform that is publicly opened for every communication. Blockchain technology used by the IoT for secure transmission among IoT devices in diverse environments. The work on blockchain was started in the 1990s when S. Haber and W. S. Stornetta started work for securing the data in blocks (like linked list) [4].

4 Overview of Blockchain

Blockchain is a series of blocks, which hold the information of all the transactions like convention public ledger [5]. Block connected to the previous one by the hash value of the previous block, which is the parent block. The first block is the genesis block without any parent block. All incoming transactions are stored in the transaction pool. Now, the nodes need to verify these transactions based on predefined criteria. Verification also solves the problem of double-spending. In double spending same input amount is used for two or more different transactions [6]. After the verification is done by the miners, the transaction is included in the block. The nodes that mine the blocks are called miners [7]. Figure 2 defines the transaction verification in blockchain.

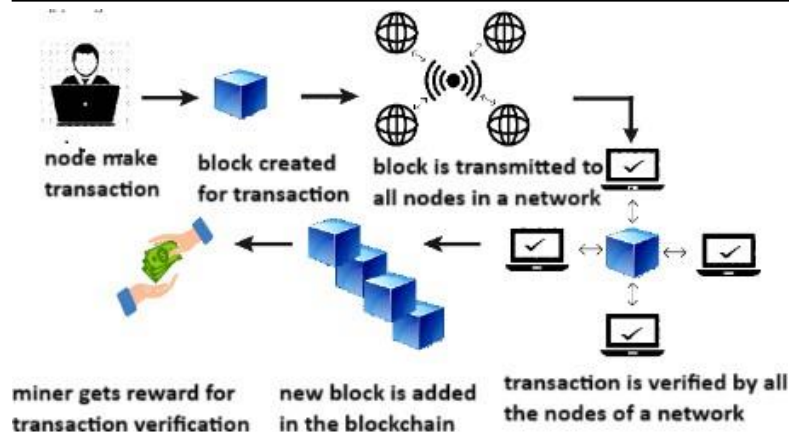


Fig. 2. Transaction Verification in Blockchain

5 Related work

Table 1: Summary of related work with their research gap and proposed solutions

Author	Year	Methodology Used	Research Gap	Proposed Solution
Ouaddah et al. [8]	2017	Introduced a privacy-preserving access control model based on blockchain technology for IoT environments. Addressed access control and privacy challenges.	Data security and access control in IoT.	Utilize blockchain's tamper-proof ledger and decentralization to develop an access control framework that enhances security and privacy for IoT applications.
Roy et al. [9]	2019	Proposed a QoS-based secure transaction structure for IoT using blockchain mechanisms. Ensured data integrity, privacy, and quality of service.	Efficiency of IoT-assisted healthcare systems.	Ensure data integrity, privacy, and QoS in IoT deployments by incorporating blockchain technology for secure and efficient transactions.
Indumathi et al. [10]	2020	Explored blockchain applications in healthcare for uninterrupted, user-friendly services, emphasizing ubiquitous healthcare accessibility.	Ubiquitous healthcare accessibility.	Harness blockchain capabilities to transform healthcare delivery into a seamless, patient-centric experience.
Qiu et al. [11]	2020	Introduced a collective Q-learning model with blockchain assistance to optimize IoT networking dynamics.	IoT network dynamics.	Use blockchain's transparency and security to enhance networking strategies and optimize IoT ecosystems.
Shammar et al. [12]	2021	Conducted a comprehensive survey exploring IoT and blockchain integration with a focus on critical security aspects.	Security concerns in IoT blockchain integration.	Address security issues by evaluating mechanisms and approaches tailored for IoT-blockchain integration, enhancing overall system security.

Singh et al. [13]	2022	Merged Federated Learning and blockchain to ensure the confidentiality and security of healthcare data.	Privacy preservation in healthcare data.	Safeguard patient privacy and enable secure data sharing in healthcare systems through Federated Learning and blockchain technology.
Vairagade and SH [14]	2022	Explored innovative techniques for optimizing network resources and improving IoT system performance using ML and blockchain.	Performance optimization in blockchain-powered IoT.	Combine blockchain and machine learning algorithms to enhance QoS and overall performance in IoT environments.
Sharma et al. [15]	2023	Applied blockchain in IoT-enabled healthcare systems, focusing on privacy and security.	Data security and privacy in healthcare systems.	Use blockchain to reinforce the confidentiality and integrity of healthcare records, improving trustworthiness in IoT-enabled healthcare.
Almarri et al. [16]	2024	Investigated blockchain features (immutability, decentralization, integrity) to address IoT security and scalability issues.	Scalability and security issues in IoT blockchain integration.	Add a new layer before blockchain-IoT integration to resolve scalability and improve data protection.
Mohanta et al. [17]	2024	Focused on decentralized blockchain consensus protocols, ensuring data integrity and preventing unauthorized access.	High energy consumption in Proof-of-Work consensus.	Employ energy-efficient algorithms like Practical Byzantine Fault Tolerance or Ripple to reduce energy consumption.
Maurya et al. [18]	2025	Proposed an integration of machine learning and blockchain for decision-making in IoT environments.	Complex and costly ML-blockchain integration with low throughput and latency.	Utilize deep neural networks as a better alternative to improve efficiency, throughput, and decision-making in IoT systems.

6 Opportunities of IoT with Blockchain

Combining BC with IoT creates many opportunities for both of them. Let's discuss some opportunities here, as shown in Figure 3.

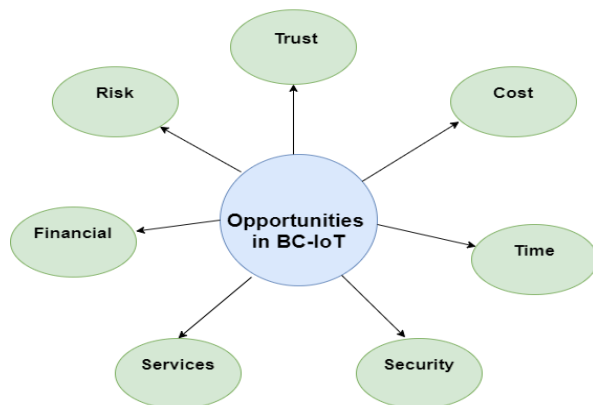


Fig. 3. Opportunities of blockchain with IoT

6.1 Make the Trust among the partners

The integration of these techniques creates trust between the parties that are connected in the network. Because every transaction is verified by the prospector, so that verified devices interact in the network and then are allowed to get into BC [19].

6.2 Cost Reduction

This technique also reduces the cost between the devices because it allows direct interaction among the parties. It removes all the mediator nodes between the receiver and sender. It allows direct communication [20].

6.3 Time Reduction

This technique also reduces a lot of time. Because it allows the single version data verification among the stakeholders, and the time used for transaction verification is reduced from days to seconds [21].

6.4 Social Services

It also provides better services for all public and social devices that are connected. All devices can communicate and share data among themselves.

6.5 Security

Blockchain uses the Distributed Ledger technique, where every node holds a replica of the original chain, which makes the network more functional even though lots of nodes fail. It provides privacy among the connected nodes. It is difficult for the attackers to understand the data on one node because the copies of data are stored across multiple nodes that the attackers can't access in a unit time [22].

6.6 Financial Services

Blockchain technology also makes financial services more transparent. It allows for the transfer of funds with security without a mediator. It also reduces the transfer cost and time.

6.7 Risk control

Blockchain technique plays an important role in analyzing the risk. After analyzing the risk, it also tries to minimize the risk from the failure of resources and transactions.

7 Challenges in blockchain–IoT integration

This section discusses the challenges that occur in the collaboration of blockchain in IoT. Blockchain was designed for high-profile devices that need more software and hardware for securing transactions. But in the IoT, some devices are very small, but require huge amounts of data for processing. Challenges are defined here.

7.1 Storage capacity and scalability

In BC, the blockchain is always growing. So, it can hang out due to its heavy transaction. Because the size of Ethereum and Bitcoin is 400 and 150, respectively, that requires a huge amount of storage. Ethereum can process 20 transactions/second. But network-based applications like Visa and PayPal require 2000 and 170, respectively, as their throughput. Although only a fully validated transaction can be stored in the chain, the storage requirement is feasible. As the block size is growing, it requires more resources, which reduce the system capacity and also degrades the system performance.

7.2 Lack of skills

Blockchain technology is transforming the whole world. Not everyone is familiar with this technology. So, blockchain requires training the people is a challenging task.

7.3 Integration and Discovery

The blockchain technology was not specifically designed for IoT devices. So, it is difficult to discover the IoT-connected devices with the blockchain. So IoT devices can find other devices, but can't find and integrate the blockchain with other devices.

8 Conclusion

In the present revolution era, IoT systems are evolving quickly, but their security issues are also increasing. The vital challenge in IoT arises due to its centralized architecture. Blockchain technology, which is a decentralized approach, is the solution to these problems. Blockchain and its inherent nature, transparency, distributed data storage, immutability, trustworthy and consensus algorithm can be applied to make reliability and robustness in IoT systems. A blockchain-based distributed idea removes the problem of single-point failure, providing efficient data security and transparency between transactions. Blockchain's peer-to-peer nature removes the third-party need that reduces cost, time, and delivers accurate information between connected devices in real time in an IoT system. So, the use of blockchain in IoT can be more beneficial in the future. But still, there are some challenges of IoT integration with blockchain, such as scalability and storage issues that can be resolved in the future by adding a layer such as IPFS (Interplanetary File System) or other techniques of data compression that require less storage before blockchain and IoT integration.

Compliance with Ethical Standards The authors have no conflicts of interest to declare. All the co-authors have seen and agree with the contents of the manuscript, and there is no financial interest to report. Each author has made substantial contributions to the conception or design of the work or the acquisition, analysis, or interpretation of data.

References

- [1] E. B. Bayarcelik and H. B. Bumin Doyduk, "Digitalization of business logistics activities and future directions," *Digital Business Strategies in Blockchain Ecosystems: Transformational Design and Future of Global Business*, pp. 201–238, 2020.
- [2] M. D. Ilić, L. Xie, U. A. Khan, and J. M. Moura, "Modeling of future cyber-physical energy systems for distributed sensing and control," *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, vol. 40, no. 4, pp. 825–838, 2010.
- [3] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gan-domi, "Addressing security and privacy issues of IoT using blockchain technology," *IEEE Internet of Things Journal*, vol. 8, no. 2, pp. 881–888, 2020.
- [4] S. Haber and W. S. Stornetta, *How to time-stamp a digital document*. Springer, 1991.
- [5] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*. IEEE, 2017, pp. 557–564.
- [6] G. O. Karame, E. Androulaki, and S. Capkun, "Double-spending fast payments in bitcoin," in *Proceedings of the 2012 ACM conference on Computer and communications security*, 2012, pp. 906–917.
- [7] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proceedings of WEIS*, vol. 2013, no. 11. Citeseer, 2013.
- [8] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in iot," in *Europe and MENA cooperation advances in information and communication technologies*. Springer, 2017, pp. 523–533.
- [9] D. G. Roy, P. Das, D. De, and R. Buyya, "Qos-aware secure transaction framework for internet of things using blockchain mechanism," *Journal of Network and Computer Applications*, vol. 144, pp. 59–78, 2019.
- [10] J. Indumathi, A. Shankar, M. R. Ghalib, J. Gitanjali, Q. Hua, Z. Wen, and X. Qi, "Block chain based internet of medical things for uninterrupted, ubiquitous, user- friendly, unflappable, unblemished, unlimited health care services (bc iomt u 6 hcs)," *IEEE Access*, vol. 8, pp. 216 856–216 872, 2020.
- [11] C. Qiu, X. Wang, H. Yao, J. Du, F. R. Yu, and S. Guo, "Networking integrated cloud-edge-end in iot: A blockchain-assisted collective q-learning approach," *IEEE Internet of Things Journal*, vol. 8, no. 16, pp. 12 694–12 704, 2020.
- [12] E. A. Shammam, A. T. Zahary, and A. A. Al-Shargabi, "A survey of iot and blockchain integration: Security perspective," *IEEE Access*, vol. 9, pp. 156 114– 156 150, 2021.
- [13] S. Singh, S. Rathore, O. Alfarraj, A. Tolba, and B. Yoon, "A framework for privacy- preservation of iot healthcare data using federated learning and blockchain tech- nology," *Future Generation Computer Systems*, vol. 129, pp. 380–388, 2022.
- [14] R. S. Vairagade and B. SH, "Enabling machine learning-based side-chaining for improving qos in blockchain-powered iot networks," *Transactions on Emerging Telecommunications Technologies*, vol. 33, no. 4, p. e4433, 2022.
- [15] P. Sharma, S. Namasudra, N. Chilamkurti, B.-G. Kim, and R. Gonzalez Crespo, "Blockchain-based privacy preservation for iot-enabled healthcare system," *ACM Transactions on Sensor Networks*, vol. 19, no. 3, pp. 1–17, 2023.
- [16] S. Almarri and A. Aljughaiman, "Blockchain technology for iot security and trust: a comprehensive slr," *Sustainability*, vol. 16, no. 23, p. 10177, 2024.
- [17] B. K. Mohanta, M. K. Dehury, P. K. Solleti, and S. S. Panda, "Decentralized consensus protocol for securing iot networks using blockchain technology," in *2024 8th International Conference on I-SMAC (IoT in Social, Mobile,*

- Analytics and Cloud*)(I-SMAC). IEEE, 2024, pp. 81–87.
- [18] V. Maurya, V. Rishiwal, M. Yadav, M. Shiblee, P. Yadav, U. Agarwal, and R. Chaudhry, “Blockchain-driven security for iot networks: State-of-the-art, challenges and future directions,” *Peer-to-Peer Networking and Applications*, vol. 18, no. 1, pp. 1–35, 2025.
- [19] R. Kumar and R. Sharma, “Leveraging blockchain for ensuring trust in iot: A survey,” *Journal of King Saud University-Computer and Information Sciences*, vol. 34, no. 10, pp. 8599–8622, 2022.
- [20] F. Lombardi, L. Aniello, S. De Angelis, A. Margheri, and V. Sassone, “A blockchain-based infrastructure for reliable and cost-effective iot-aided smart grids,” 2018.
- [21] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, “Blockchain-based secure time protection scheme in iot,” *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671–4679, 2018.
- [22] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, “Blockchain for iot security and privacy: The case study of a smart home,” in *2017 IEEE international conference on pervasive computing and communications workshops (PerCom work-shops)*. IEEE, 2017, pp. 618–623.