Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly
DOI: http://doi.org/10.65568/gujes.2025.010204

Blockchain as a Solution for Internet of Things Security: a Survey

Aisha Elzegr [1] [*], Kheriya Alhaddar [2] , Somaya H. Alshebani [3]

[1] Computer Science Department, High Institute of Science and Technology, ElKhoms, *elzegraisha@gmail.com*
[2] Dept. of Electrical and Computer Eng.. Faculty of Engineering, Almergib Univ. kfalhadar@elmergib.edu.ly
[3] Electrical Eng. Department. High Institute of Science and Technology, , eng.somayahassan@gmail.com

[*]*Corresponding author elzegraisha@gmail.com*

Received: 11 Aug 2025	Accepted: 20 Aug 2025	Published: 06 Sep 2025

Abstract

The Internet of Things (IoT) has revolutionized device interactions, enabling automation and connectivity, but security and trust issues have hindered its widespread adoption. Blockchain technology is seen as the optimal way to address these difficulties due to its immutable and decentralized characteristics. This article examines the capacity of blockchain technology to mitigate significant security and trust issues in the expanding IoT environment. This study conducts a thorough literature analysis to analyses how the decentralised, irreversible, and transparent characteristics of blockchain enhance security and trust in IoT networks. This study analyse and classify prevalent security concerns pertaining to the IoT layered architecture. Additionally, catalogue and illustrate the most common challenges in both blockchain networks and IoT network during the integration, and the advantages of this combination between those two technologies. Furthermore, the limitation of blockchain with some IoT application.

Keywords: *The IoT, Blockchain, The Integration between IoT and blockchain.*

1. Introduction

Blockchain technology is a revolutionary innovation capable of altering numerous domains, including the Internet of Things (IoT). The swift expansion of the IoT ecosystem has rendered security and trust the foremost concerns confronting this interconnected network of devices. Dependence solely on conventional procedures is inadequate to safeguard the IoT against these difficulties, including ensuring proper authentication and preserving data integrity(1)(3). In blockchain technology main key features has improved security, transparency, and efficiency of data management and transactions which are: Distributed ledgers / Public key cryptography/ Immutable record/ Smart contracts, also, There is an important strength point in this technology, which is that each node can obtain a private copy of the distributed ledgers.(3).

Moreover, blockchain employs cryptographic techniques to provide data security and immutability, which are maintained within a distributed ledger that guarantees the absence of a central authority over the data, thereby mitigating the danger of fraud and promoting transparency and decentralisation (1)-(3).This paper posits blockchain as an ideal solution to increase the security and reliability of IoT through enhanced transparency, decentralisation, and diminished manipulation.

This study is based on three major points: first, the difficulties associated with IoT-layered infrastructures and how blockchain technology can address these issues, secand, the advantages of integrating IoT networks within blockchain technology, third, the five keys challenges in integrating blockchain technology within IoT networks. This study also contributes to existing research by compiling relevant information from the current literature in a manner that will assist future readers in obtaining the necessary insights from a single brief article.

This paper is structured as follows, The introduction –Motivation- The Internet of Things- Blockchain technology –related work- IoT architecture- Combining blockchain with IoT - Challenges of this integration - Summarize the key findings. The objective of this paper is to consolidate pertinent information from current literature in a manner that aids future readers in obtaining necessary insights from a single article.

2. Blockchain Technology

A blockchain is a series of blocks that are cryptographically linked and generated by nodes. Each block contains a header, relevant transaction data for protection, and supplemental security metadata such as the identity of the creator, the last block number, and the signature.(7). A blockchain enables "decentralised consensus" using a distributed ledger, this system functions as a distributed database that maintains an ever-increasing list of records while simultaneously preventing any retrospective changes or tampering with those records. Blockchains are inherently resistant to alterations to the underlying data; hence, they are regarded as a tamper-proof, incorruptible, decentralised digital record for economic or logical transactions pertaining to nearly any asset of value (8).

A. Blockchain Key Characteristics

- It permanently records transaction data in a chain (distributed ledger).
- It prohibits any alterations to the data or the chain following block acceptance.
- It offers secure storage of historical data that is resistant to tampering.
- Modifying data after it has been stored on the unchangeable blockchain is forbidden.
- Every block incorporates the hash value of its predecessor; consequently, any modification to a block undermines all subsequent blocks in the chain.(9)(4)

B. Blockchain system

The blockchain technology is perceived as a chronological ledger of transactions, where each block is sequentially connected to others and permanently recorded over a peer-to-peer networks (2). The system implements a unique coding assurance for every transaction. Participants utilise the system to uphold an encrypted ledger of each transaction inside a decentralised framework, enhancing security and accessibility, and enabling all participants, particularly those without mutual trust, to authenticate records and transactions(1). The system has significant scalability and high adaptability, and it does not necessitate any additional intermediates (5). Figure 1 illustrates the functionality of blockchain technology in safeguarding data integrity.

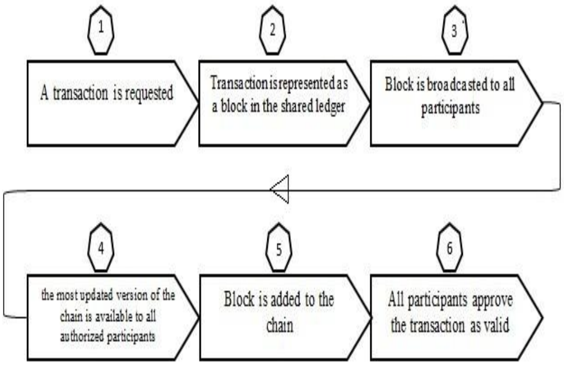
1
A transaction is requested
2
Transaction is represented as a block in the shared ledger
3
Block is broadcasted to all participants
4
the most updated version of the chain is available to all authorized participants
5
Block is added to the chain
6
All participants approve the transaction as valid

Fig.1. the functionality of blockchain

3. Related Work

The Internet of Things profoundly influences daily life, prompting scholars to engage in contributions. Numerous polls offer insights into the complexity of the IoT ecosystem, the obstacles encountered, and the security dangers present. We examined multiple studies to delineate the challenges faced by IoT. The papers (1)-(3) analyse the security threats associated with IoT. The articles analysed various attack types, including spoofing and distributed denial-of-service (DDoS) assaults, which present significant threats to IoT devices and networks.

The findings emphasise the necessity of establishing comprehensive security rules and recommendations to successfully minimise these threats. assaults, protocol-oriented assaults, host-centric assaults. Articles (4)(5)(2) illustrated the security vulnerabilities within IoT architectural layers and the potential threats. Paper [4] examines security vulnerabilities and methods to exploit these issues in IoT devices. (5)(1)(6) illustrate diverse domains of IoT applications, including smart cities, smart homes, healthcare, education, agriculture, and industry, along with the associated security issues. The architecture and layers of IoT were examined in (2), whereas (7) addressed several uses of blockchain. Numerous studies examined the influence of blockchain on the security of IoT layers, including improvements in data security and privacy, data integrity, and scalability. (1)(2).

Various review articles, including (1), (5), and (2), proposed solutions such as blockchain-based decentralisation techniques. Some publications, such as (1),(13), assert that blockchain provides a conclusive answer to trust-related issues and numerous security concerns. In contrast, (9) argued that Blockchain technology is appropriate for many real-time applications, including tracking, supply chain management, and financial transactions processing, because of its transparent and immutable ledger system. However, it faces challenges related to processing speeds, scalability, and high transaction volumes, which limiting its applicability in all high-frequency real-time contexts. Although it facilitates real-time updates, its decentralised structure and consensus protocols can cause latency that is absent in conventional centralised systems.

Table I Comparative analysis of related works

Source no	Citation	Year	Objectives
[1]	M. A. Obaidat et al.	2024	This study provides an overview of blockchain technologies, their components, features, and secure application methods. It discusses how blockchain can be integrated into IoT infrastructure, its applications, and its security measures. It also explores suitable methods, architectural challenges, consensus protocols, and algorithms for IoT-blockchain integration.
[2]	S. Almarri and A. Aljughaiman	2024	This study investigates the security and trust challenges inside IoT systems, concentrating on the layers of the IoT reference model. It assesses the possibilities of blockchain technology for IoT security, including decentralisation, transparency, and immutability. Additionally, it examines the role of blockchain in the sustainability of IoT, pinpointing integration obstacles and prospective trajectories.
[3]	I. I. A. Barazanchi and W. Hashim	2023	This research presents a blockchain-oriented security solution designed to alleviate security vulnerabilities in IoT networks. The system employs smart contracts to execute fundamental functions such device authentication, data integrity verification, and access control. in order to develop IoT security solutions that enhance device reliability, accelerate speeds, diminish power consumption, minimise connection latency, and optimise network availability.
[4]	S. P.Kumar, et al	2022	This survey article is classifying attacks/vulnerabilities based on items. Also presents the methods of assaults and corresponding countermeasures for each type of attack. The examination of security solutions encompasses not just conventional secret key-based cryptography methods but also includes physical unclonable functions (PUF) and blockchain technologies. It also examines the advantages and disadvantages of each security solution.
[5]	N. T. Y. Huan	2024	This article offers a preliminary examination of the Internet of Things

	and Z. A. Zukarnain		(IoT) and subsequently explores the various security threats and vulnerabilities inherent in the IoT framework, including challenges in IoT architecture. The study presents an overview of blockchain, emphasising its classification and key attributes. Furthermore, this article investigates the imperative of integrating blockchain technology with the Internet of Things (IoT) and reviews blockchain-based IoT applications.
[6]	N. Adhikari and M. Ramkumar	2023	This article explores the architecture of an IoT network, its applications, and the use of blockchain technology in financial transactions and digital payments. It also discusses the security risks associated with IoT, the challenges of integrating IoT with blockchain, and strategies to overcome these issues. The study also explores the integration of IoT with blockchain technology.
[7]	A. K. Tyagi et al.	2023	This study delineates uses of blockchain technology that integrate artificial intelligence (AI) and the Internet of Things (IoT). This paper proposed Integrating blockchain, IoT, and AI will enhance and address the vulnerabilities of the technologies.
[8]	B. K. Mohanta et al.	2020	This article examines the security and privacy issues inherent in the IoT system. Subsequently, in alignment with blockchain technology, this study provides a range of security solutions that come up with the amalgamation of IoT with blockchain technology, together with the impact of blockchain on IoT (advantages and disadvantages).
[9]	D. Puthal	2020	This article discusses which applications are suitable for blockchain implementation and which are not, based on the requirements for real-time auditing.
[10]	V. Hassija et al.	2019	This paper studied security challenges in IoT applications, highlighting emerging technologies like blockchain, fog computing, edge computing, and machine learning to enhance trust and security in IoT applications.
[11]	A. Pieroni, N. et al.	2020	This paper reviews recent Blockchain architectures, compares consensus algorithms, and evaluates convergence between Blockchain and IoT. It explores AI algorithms for Blockchain-based IoT devices.
[12]	A. Chhabra. et al	2024	This survey analyzes privacy factors in blockchain solutions, discussing their applicability in various domains like e-commerce, supply chain, healthcare, and IoT. It highlights Privacy Information Retrieval related issues.
[13]	V.Gugueoth. et al	2023	This paper discusses security threats, Blockchain-based solutions, challenges, consensus protocols, existing security techniques, and evaluation parameters in the integration of Blockchain with IoT.

4. IoT Architecture

The layers or architecture of IoT systematically organize its components and their interactions where it encompasses software, interfaces, protocols, and data flow. Such as, smart devices within an IoT ecosystem gather data, that is subsequently transmitted to the communication protocol. Subsequently, data processing occurs within the cloud, as users engage with the information through applications of the IoT (14)(2)(8). This section introduces a three-layer design for IoT, which serves as a generalised model, as illustrated in Fig 2.

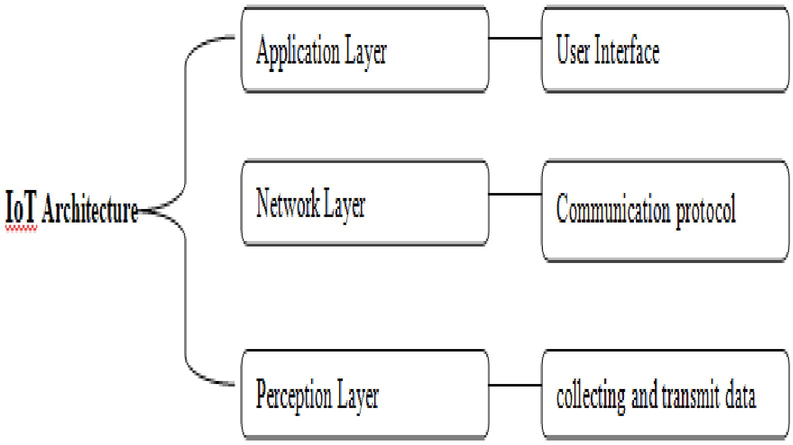

Fig. 2. IoT Architecture

A. The perception Layer

Alternatively referred to as the physical layer. This layer comprises sensors and various collection instruments utilized for information gathering. The primary responsibility of this layer is to gather, process, and transfer information to the network layer. Furthermore, it facilitates collaboration among IoT nodes within local networks(2)(14).

B. Network Layer:

Known as the transport layer, comprises communication protocols like Wi-Fi, Bluetooth, and contains routers, Internet gateways, and switches The main function of this layer is to ensure secure and expedited data transit between layers(20(10)(14).

C. Application Layer

Resides at the apex of the Internet of Things architecture. This layer comprises applications, user interface, data storage system, and additional services for user. The primary responsibility of this layer is to facilitate the interface between the IoT network and the applications that engage with them. That also guarantees the confidentiality, integrity, and availability triad of the data (2)(14).

5. Security Challenges in IoT

The IoT architecture is plagued by numerous security vulnerabilities associated with each tier(8). We must analyse the existing solutions to cybersecurity challenges related to the model of IoT to achieve more systematic, robust, and cohesive understanding of how to safeguard the IoT against various cyberattacks.

The Internet of Things (IoT) comprises a three-tier architecture that emphasises cyber security vulnerabilities and corresponding remedies at each layer. (8),(10). Figure 3 categorizes common IoT security vulnerabilities according to the applications, network, and perception levels, including threats such as man in the middle (MITM) attack, sniffing attack, denial of service (DoS), and routing attack. This layer-wise perspective illustrates that attacks exploit specific places inside the IoT system, underscoring the necessity of security implementation at each layer(10).

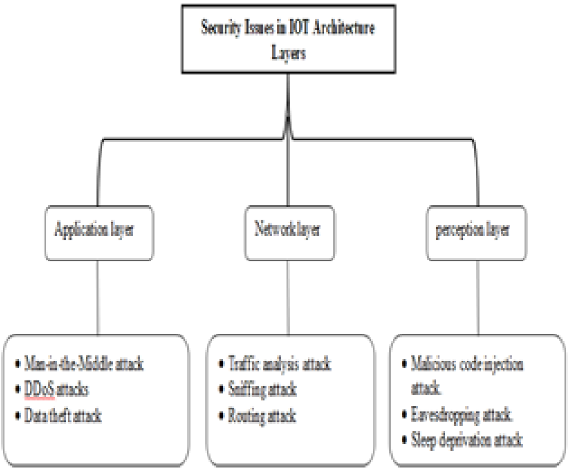
Security Issues in IOT Architecture Layers
Application layer
Network layer
perception layer
• Man-in-the-Middle attack
• DDoS attacks
• Data theft attack
• Traffic analysis attack
• Sniffing attack
• Routing attack
• Malicious code injection attack
• Eavesdropping attack
• Sleep deprivation attack

Fig. 3. IoT attacks across layers.

A. Application Layer Attacks:

The application layer directly engages with and provides services to end user, which makes security threats a major concern in this kind of network (10)(8)(13). The following some major security issues:

- A man-in-the-middle (MITM): attack is a cyberattack wherein hackers illicitly acquire important information by intercepting communication between online devices, such as an end user and web applications(10)(8).
- Distributed denile of service (DDoS) attack: focuses on the data layer of a web application that end users interact with. In this type of attack, the attacker overwhelms the server with an excessive amount of requests beyond its capacity or with malicious requests that significantly increase response latency (8)(13).
- Data theft attack: IoT apps handle sensitive data, making them vulnerable to data theft. Data in move is more susceptible to attack than pasive data, To protect users' personal information, Users may be hesitant to register their personal data on IoT

applications due to potential information theft attack. as a solution for this kind of threats techniques such as encryption, isolation, authentication, and privacy management are employed(8)(13).

B. Network Layer Attacks:

This layer's primary function is to transmit data collected by the sensing layer to the computing unit for processing (8)(10)(13). The following are some major security issues:

- Traffic analysis attack: An assailant can scrutinise network traffic patterns to deduce the content of packets, not with standing their encryption(8)(13).
- Sniffing attack: Sniffing refers to the monitoring and interception of network traffic. Data encryption is an optimal option for protect sensitive information against interception(10)(8).
- Routing attack: In these attacks, malicios nodes within an IoT applications attack the routing pathways to alter during data transmission(8)(10).

C. Perception Layer Attacks:

This layer is the physical layer, equipped with sensors for collecting and gathering information. Also, senses certain physical parameters and recognises other intelligent devices in the surroundings (8)(10)(13), which make it susceptible at attacks such as:

- Malicious Code Injection Attack: The attacker is introducing malicious code into the memory of IoT network nodes, blockchain can solve this issue by use secure authentication process.
- Eavesdropping and Interference: is an attempt to capture and read data delivered over a network without authorization.
- Sleep Deprivation Attacks: Adversary attempts to exhaust the battery of low-powered IoT edge devices.

6. Combining Blockchain with IoT

Current IoT infrastructures are centralised, complicate, and exhibit security vulnerabilities in their connections and data transmission. Data is transmitted from the device to the cloud, where it is analysed and subsequently returned to the IoT devices. As billions of devices are anticipated to integrate into IoT networks in the forthcoming years, this centralised system exhibits significant limitations in scalability, presents numerous vulnerabilities that threating network security, and will incur substantial costs and delays if third parties are required to verify and authenticate every transaction among devices. Blockchain serves as the crucial element to address security, immutability, and reliability issues in the IoT networks. It can facilitate the monitoring of several linked devices, enable transaction processing, and coordinate interactions among devices. This decentralised methodology remove single points of failure, fostering a more robust environment for device operation. Data is safely transmitted across a decentralised, cryptographically protected network, rendering the entire system exceedingly difficult to attack. (8).

A. The Cryptographic Attributes of Blockchain

Blockchain network employs multiple cryptographic techniques to secure data, and regulate access inside IoT networks (5). Furthermore, the cryptographic attributes of blockchain enhance security throughout every layer of IoT architecture (8).

B. Hashing Attribute of Blockchain

A hashing function is a mathematical operation that converts an input signal into a fixed-size string, typically known as a hash value. This deterministic transformation ensures that a certain input produces the identical hash output consistently . Concurrently, it exhibits a unidirectional property, obstructing the recovery of the original input signal from the hash value(1)(13)(5). Table 3expain the major roles of blockchain in securing IoT layers:

Table II The role of blockchain in securing the layers of the IoT

Application Layer	Blockchain enhances this layer by providing immutable and transparent transaction records, that ensure compliance and instill confidence in applications. The key indicators of data reliability are as follows: Hashing can guarantee data validity. Digital signatures guarantee data authenticity(1).
Perception Layer	The incorporation of blockchain improves security by the encryption and hashing of information, hence reducing the likelihood of unauthorised access to data obtained by sensors. Conversely, smart contracts authenticate device IDs to guarantee that only authorised devices engage in data transmission within the IoT ecosystem(1)(4)..
Network Layer	Blockchain employs decentralised and cryptographic mechanisms to secure packet transmission over communication channels, including wireless fidelity WiFi, Bluetooth, and mobile network. Moreover, digital signatures and secure transmission protocols protect against prevalent attack vectors, including (MiTM) attacks and (DDoS) assaults (2)(1)(4).

C. The Impact of Blockchain Combining with IoT

This part delineates the benefits of integrating blockchain networks with IoT ecosystems, which include distributed ledger capability, cryptographic security, consensus mechanisms, decentralised identification, transparency, and auditability. In contrast, IoT devices provide real-time data from sensors, while blockchain ensures data security through a distributed, decentralised, and shared ledger (8).

Table III The advantages of combination

The Advantages of Blockchain Combining with IoT	
Decentralization	Identity management for IoT networks is decentralised on the blockchain, enabling secure identification, authentication, and authorisation for IoT people, entities, or devices. This functionality mitigates identity theft attempts.(2)(1).
Distributed ledgers	The blockchain serves to document IoT data within a decentralised ledger that is immutable and impervious to alteration by unauthorised individuals. This functionality guarantees the traceability and integrity of the data (2)(1).
Data Manipulation	The blockchain technology inhibits data manipulation as it prohibited modifications without the consent of the involved parties. Should any node attempt to do any modification, all inodes will be informed. (2)(1).
Cryptography	Blockchain employs robust cryptographic mechanisms, such as hashing and, digital signatures to safeguard the IoT against exposure to malicious attack (2)(1).
Transparency and Auditability	The immutable nature of the blockchain ledger ensures transparency and auditability, enabling stakeholders to access the complete history of all transactions and activities recorded on the blockchain, hence enhancing trust.(2)(1).
Consensus Mechanism	Blockchain employs a consensus technique to guarantee that all nodes or participants agree on the ledger's state, such as proof of work and proof of stake. This functionality bolsters confidence in IoT data and inhibits unauthorised modifications. (2)(1).

D. Challenges of Blockchain and IoT Combination

The integration of blockchain networks with IoT network presents challenges because of the contrasting amounts of IoT users' data and blockchain data. The blockchain data volume, including Ethereum and Bitcoin, varies from 250GB to 1TB, which is substantial in comparison to IoT devices (11),(12). This inconsistency presents obstacles to the comprehensive implementation of blockchain in IoT devices. A potential option is to use cloud computing for the storage of block data while retaining only hash chains on IoT devices. The adoption of IoT technology serves as an impetus for employing blockchains to ensure secure data transmission within IoT networks. This benefit can address numerous security-related issues. (12) Furthermore, transactions inside a blockchain network are digitally signed. We must equip IoT devices to function and utilise a blockchain (11). Prior to conducting a thorough analysis of the integration between blockchain networks and IoT networks, it is essential to examine various issues and concerns that emerge from this integration. Table 5 shows some of the most common challenges:

Table V The summary of the most common challenges in this combination

Challenges	Blockchain networks	IoT networks
Network size	The heterogeneity of IoT network devices makes integration with blockchain more challenging and complicated. This presents challenges in facilitating communication between blockchain and IoT (1)(2)(13).	Being a network of different devices using different communication techniques to interact with each other, the IoT has a heterogeneous and distributed nature of network (1)(2)(13).
hardware limitation	Hardware limitations in IoT devices hinder the implementation of complex blockchain activities, thereby impacting their performance (1)(2)(13).	The constrained devices in IoT contexts possess limited memory, computing capacity, and resources(1)(2)(13).
speed response	Shows higher latency, potentially affecting response times (2)(13).	Numerous IoT applications necessitate rapid responses, such as emergency alerts in healthcare settings.(1)(2)(13)
security	Cannot fully address security challenges faced by IoT devices, making it unattainable to ensure complete privacy and security (1)-(3).	Need high level of security(1)-(3).
Energy consumption	Require substantial energy(1)-(3).	limited energy capabilities(1)-(3).

E. The limitations of Blockchain

- Signature verification: this process is intricate and time-consuming, where each blockchain transaction must be digitally signed and authenticated utilising a public or private key cryptography framework(1).
- Redundancy: each node must independently traverse and process every intermediate node to reach the target node. Consequently, the redundancy inherent in blockchain technology impacts its performance(3).
- The 51% attack: If 50 persent of nodes in a blockchain network validate a transaction, it is deemed to be true. If more than half the nodes in a network propagate a falsehood, then that lie will be perceived as truth(1).
- Insufficient Technical Knowledge: Despite the growing popularity of Blockchain, many investors remain unaware of the technical terminology(3).

7. Conclusion

Current Internet of Things (IoT) systems have several obstacles, including heterogeneity, inadequate interoperability, resource limitations, and vulnerabilities related to privacy and security. The current emergence of blockchain technologies effectively addresses challenges related to interoperability, privacy, security, traceability, and reliability. This article provided an extensive analysis of the deployment of blockchain in IoT systems and the numerous concerns impacting the security and privacy of IoT data. In this paper, we investigate integrating blockchain with IoT. Moreover, this paper examines the classification of various security concerns in IoT and provides a concise overview of recent research that utilizes blockchain to enhance IoT security. Furthermore, provide a comprehensive survey on the operation of blockchain that is examined comprehensively, including its security and privacy features, consensus methods. This analysis examines the integration of blockchain with IoT, outlining the advantages, problems, security measures, and fietuers such as cryptographic and hashing. This paper suggests that blockchain technology is a promising innovation that might significantly enhance the security and privacy of IoT data, thereby facilitating its expansion across multiple applications. The observed concerns indicate that the implementation of blockchain for IoT remains nascent, necessitating further research to tackle the obstacles and complexities inherent in the integration of blockchain with IoT.

References

[1] M. A. Obaidat, M. Rawashdeh, M. Alja'afreh, M. Abouali, K. Thakur, and A. Karime, “Exploring IoT and Blockchain: A comprehensive survey on security, integration strategies, applications and future research directions,” Big Data and Cognitive Computing, vol. 8, no. 12, p. 174, Nov. 2024, doi: 10.3390/bdcc8120174.

[2] S. Almarri and A. Aljughaiman, “Blockchain Technology for IoT Security and Trust: A Comprehensive SLR,” Sustainability, vol. 16, no. 23, p. 10177, Nov. 2024, doi: 10.3390/su162310177.

[3] I. I. A. Barazanchi and W. Hashim, “Enhancing IoT Device Security through Blockchain Technology: A Decentralized Approach,” Shifra., vol. 2023, pp. 10–16, Feb. 2023, doi: 10.70470/shifra/2023/002.

[4] S. P.Kumar, et al., "Internet of things: Security and solutions survey." Sensors, vol 22, no.19 , p 7433, Sept. 2022.

[5] N. T. Y. Huan and Z. A. Zukarnain, “A survey on addressing IoT security issues by embedding blockchain Technology Solutions: review, attacks, current trends, and applications,” IEEE Access, vol. 12, pp. 69765–69782, Jan. 2024, doi: 10.1109/access.2024.3378592

[6] N. Adhikari and M. Ramkumar, “IoT and Blockchain Integration: Applications, Opportunities, and Challenges,” Network, vol. 3, no. 1, pp. 115–141, Jan. 2023, doi: 10.3390/network3010006.

[7] A. K. Tyagi, S. Dananjayan, D. Agarwal, and H. F. T. Ahmed, “Blockchain—Internet of Things Applications: Opportunities and Challenges for Industry 4.0 and Society 5.0,” Sensors, vol. 23, no. 2, p. 947, Jan. 2023, doi: 10.3390/s23020947.

[8] B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, and A. H. Gandomi, “Addressing security and privacy issues of IoT using blockchain technology,” IEEE Internet of Things Journal, vol. 8, no. 2, pp. 881–888, Jul. 2020, doi: 10.1109/jiot.2020.3008906.

[9] D. Puthal, S. P. Mohanty, E. Kougianos, and G. Das, “When do we need the blockchain?,” IEEE Consumer Electronics Magazine, vol. 10, no. 2, pp. 53–56, Aug. 2020, doi: 10.1109/mce.2020.3015606.

[10] V. Hassija, V. Chamola, V. Saxena, D. Jain, P. Goyal, and B. Sikdar, “A survey on IoT security: application areas, security threats, and solution architectures,” IEEE Access, vol. 7, pp. 82721–82743, Jan. 2019, doi: 10.1109/access.2019.2924045.

[11] A. Pieroni, N. Scarpato, and L. Felli, “Blockchain and IoT Convergence—A systematic survey on technologies, protocols and security,” Applied Sciences, vol. 10, no. 19, p. 6749, Sep. 2020, doi: 10.3390/app10196749.

[12] A. Chhabra, R. Saha, G. Kumar, and T.-H. Kim, “Navigating the Maze: Exploring blockchain privacy and its information retrieval,” IEEE Access, vol. 12, pp. 32089–32110, Jan. 2024, doi: 10.1109/access.2024.3370857.

[13] V. Gugueoth, S. Safavat, S. Shetty, D. Rawat “A review of IoT security and privacy using decentralized blockchain techniques,” computer Science Review, vol. 50, pp. 4-5, Nov 2023, doi.org/10.1016/j.cosrev.2023.100585

[14] N. Rachit, S. Bhatt, and P. R. Ragiri, “Security trends in Internet of Things: a survey,” SN Applied Sciences, vol. 3, no. 1, Jan. 2021, doi: 10.1007/s42452-021-04156-9.