Review Article

IoT security with blockchain: A review

Selami Terazi[1]*, Arafat Şentürk[2]*

[1] Düzce University, Faculty of Engineering, Department of Computer Engineering, Düzce, Türkiye, Orcid ID: 0009-0000-5375-5317, E-mail: selami96641@ogr.duzce.edu.tr
[2] Düzce University, Faculty of Engineering, Department of Computer Engineering, Düzce, Türkiye, Orcid ID: 0000-0002-9005-3565, E-mail: arafatsenturk@duzce.edu.tr,
* Correspondence: arafatsenturk@duzce.edu.tr

(First received September 15, 2023 and in final form December 18, 2023)

Reference: Terazi, S., Şentürk, A. IoT security with blockchain: A review. The European Journal of Research and Development, 3(4), 117-132.

Abstract

The relationship between the Internet of Things (IoT) and Blockchain has emerged to address the challenges of security, data integrity and transparency of IoT devices. Blockchain, with its distributed and decentralized nature, ensures reliable data transmission between IoT devices and security by preventing data manipulation. It also enhances the security and transparency of IoT applications by supporting automated and trusted transactions through smart contracts. In this context, Blockchain plays a critical role in making the IoT ecosystem more reliable and effective. In this study, we review studies that emphasize the importance of Blockchain technology for IoT security and propose various solutions. The proposed solutions include scalable frameworks for secure transactions in dynamic applications, Hyperledger Sawtooth-based frameworks that support secure logging of industrial activities, specialized access control mechanisms such as Trust-Based Access Control Mechanism (TABI), and IoT Cop monitoring framework that offers advanced security features. In addition, blockchain-based access control protocols, authentication systems and security models are aimed at enhancing IoT security. While most of the studies in the literature focus on the current challenges of IoT and Blockchain integration, they also reveal future research opportunities. These studies are briefly mentioned and the necessary ones are expressed in a table. In this way, it is aimed to create the necessary infrastructure for those who will work in this field.

Keywords: IoT, Blockchain, Security

1. Introduction

Nowadays, Internet of Things (IoT) devices are being integrated into our lives at a rapidly increasing rate. Used not only in industrial sectors but also in our daily lives, these devices enable communication between sensors, devices and other objects, creating a smarter and more connected world. Today, billions of IoT devices are in active use, but this number is growing every day and is expected to increase exponentially in the future [1].

For example, the demand for IoT devices is growing rapidly in many areas such as smart home devices used in our daily lives, wearable technologies in the healthcare sector, sensor networks in industrial production and smart agricultural applications in agriculture. As of 2023, there are approximately 15 billion IoT devices worldwide and this number is expected to double by 2030 [1].

However, this growth has brought with it some significant security and data integrity challenges. The use of an increasing number of IoT devices raises new concerns about data security, privacy and integrity. This is where the introduction of Blockchain technology offers significant potential to address these challenges of the IoT ecosystem. This paper examines the critical role of IoT and Blockchain integration, focusing on research to create a secure digital environment in this dynamic future ecosystem.

2. Literature Review

In [2], S. Basudan presents a scalable framework for secure transactions in dynamic applications by combining IoT and Blockchain. Moreover, with dynamic device management and conditional traceability, the DABG protocol offers the potential for fast transaction confirmations, data security and privacy protection. In the future, the integration of federative learning and privacy protection methods is targeted.

When the studies conducted in the field of IoT security are examined, how Blockchain technology is used effectively with IoT devices and which features are utilized are detailed in Tables 1 and 2.

Table 1: Some studies leveraging Blockchain for IoT security

Reference	Security Threats	IoT Applications	Observation
[3]	Self-promoting attack, Bad-mouthing attack, Sybil attack	IoT devices	Hyperledger introduces TABI, a Trust-Based Access Control Mechanism for Edge-IoT Networks,

			leveraging blockchain technology.
[4]	Malicious software or physical attacks	IoT devices	Introducing IoTCop, a blockchain-based IoT monitoring framework. It quickly detects and isolates compromised devices using Hyperledger Fabric and plug-in hardware modules.
[5]	"replay," "impersonation," "man-in-the-middle" and "ephemeral secret leakage (ESL)" attacks.	IoT-enabled smart grid system	Introduces DBACP-IoTSG, a new IoT-enabled smart grid system operating without a Trusted Third Party (TTP). It uses leader election and PBFT consensus for secure block verification and uses ECC encryption for transaction privacy.
[6]	Jamming and impersonation attacks	IoT blockchain network	By studying obfuscation and impersonation attacks against a RAFT-based IoT blockchain network, it proposed a path-loss-based identification method with strong detection rates.
[7]	Eavesdropping attack, replay attack, impersonation attack, and man-in-the-middle attack.	IoT network	It offers a blockchain-based, lightweight authentication solution for IoT that leverages MSR encryption for decentralized and privacy-preserving authentication.
[8]	Malicious attacks	Industrial IoT network	Proposed a secure framework based on trust management and blockchain to deal with problems caused by various levels of malicious devices in industrial IoT networks

Table 2: Blockchain mechanisms for IoT Security

Security areas in IoT	Proposed solutions	Blockchain features
Access control	[3]	Trust-Based Access Control Mechanism for Edge-IoT Networks
	[9]	Smart contracts for access control
	[5]	Respective smart meters (SMs)
	[10]	Organize and manage groups with group key (GK)
	[11]	ABAC grants access based on the qualifications provided by the target
Data integrity	[6]	Applying a binary hypothesis test for transmission node identification
	[8]	
	[12]	
Data confidentiality	[13]	Asymmetric Scalar-product Preserving Encryption (ASPE)
	[14]	Attribute-based security authentication based on Hyperledger Fabric blockchain framework
	[7]	The framework combines blockchain technology with the modular square root algorithm
	[2]	Blockchain-powered IoT with dynamic device management and conditional traceability
	[15]	Blockchain-based model for IoT authentication and security protection.
Data availability	[6]	Stochastic geometry tool

A. Pathak et al [3] focused on the use of Blockchain technology to address security issues in IoT networks, aiming to reduce high computing loads and energy costs with edge computing technology. TABI (see Figure 1), a novel Trust-Based Access Control Mechanism, aims to provide end-to-end security in resource-constrained IoT networks. Furthermore, the mechanism aims to mitigate the impact of malicious IoT users and devices by utilizing access control and trust evaluation mechanisms. TABI's performance shows that it is effective in areas that require low latency and resource efficiency for IoT applications. Future work aims to improve the quality of service and detect malicious IoT devices.

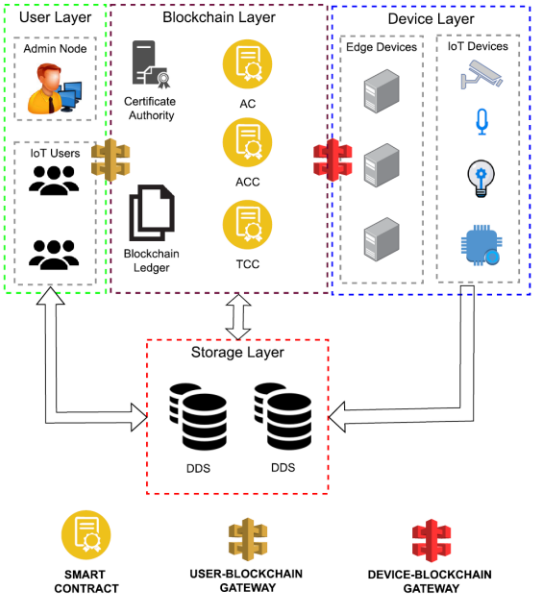

Figure 1: TABI architecture [3].

S. Seshadri et al [4],use IoTCop, a blockchain-based monitoring framework, to secure IoT devices. Unlike traditional servers, IoT devices can be geographically distributed and located close to physical systems, so they face resource constraints despite the complexity of security solutions. The study assumes that a device can be compromised and emphasizes the need to be able to automatically isolate compromised devices. To this end, the use of blockchain to enforce security policies is proposed. Using a permissioned blockchain (Hyperledger Fabric) and additional hardware modules, the proposed framework offers low latency and workload and allows existing IoT devices to join the framework without modification. IoTCop provides a practical and generic solution to protect IoT devices against the malicious attacks listed in Table 3.

Table 3: Common attacks on IoT networks

Attack	Category	Description	Research on defending attack using blockchain
Impersonation attack	Internal/External	Impersonation attack is an attempt by a device to gain unauthorized access to IoT networks by pretending to be another device with a false identity or authorization.	[5], [6], [7]
Man-in-the-Middle attack	Internal/External	Man-in-the-Middle (MitM) attack on IoT networks is a type of attack that enables an attacker to monitor or manipulate communication between IoT devices.	[5], [7]
Bad-mouthing attack	Internal	A bad-mouthing attack is a cyber-attack on IoT networks that aims to discredit other devices with fake or misleading information.	[3]
Replay attack	External	A replay attack is a security threat in IoT networks where a malicious actor attempts to gain unauthorized access by retransmitting or reusing recorded data.	[4], [5], [7]

Sybil attack	Internal/External	Sybil attack is an attempt by an attacker in IoT networks to infiltrate the network by creating a large number of fake devices with fake identities.	[3]
Jamming attack	External	A jamming attack in IoT networks is a type of attack where a hostile device or jammer heavily blocks radio frequencies to disrupt the communication of IoT devices.	[6]
Self-promoting attack	External	In IoT networks, a "self-promoting attack" refers to an attempt by an IoT device to secretly join the network or gain unauthorized access by identifying itself. The device tends to infiltrate the network directly or by exploiting vulnerabilities.	[3]
Eavesdropping attack	External	Eavesdropping is an attack of eavesdropping on IoT networks. Attackers try to access sensitive information by monitoring communication traffic, creating privacy breaches and security vulnerabilities.	[7]
Ephemeral secret leakage (ESL) attack	Internal	In ESL IoT networks, unauthorized leakage of temporary passwords by unauthorized persons or devices represents an insider security breach.	[5]
DDoS	Internal/External	DDoS (Denial of Service) attack on IoT networks is a type of cyber attack in which many IoT devices send a large amount of client traffic to a target in a coordinated manner, causing the target to crash.	[15]

B. Bera et al [5] investigated DBACP-IoTSG, a novel blockchain-based access control protocol for IoT-enabled smart grid systems. DBACP-IoTSG aims at secure data transmission and protection of private data, while offering better security and lower communication overheads than other similar schemes.

Another study [6] considers active (jamming and impersonation) attacks on an IoT blockchain network using the RAFT consensus protocol. In the case of a jamming attack, it evaluates the effects by examining coverage probabilities. In the case of an impersonation attack, it proposes a novel methodology that exploits the path loss of the communication button and aims to minimize the probabilities of false alarms, missed detections and misclassification. The results show that for jamming attack, the threshold value increases, the jammer density decreases the coverage probability, while for impersonation attack, the path loss of the communication button can be used as the device ID and more than 95% detection probability can be achieved for 10 dB link quality.

In another study [7], a blockchain-based secure and lightweight authentication scheme for IoT is proposed. The proposed framework combines blockchain and MSR encryption algorithm to realize a decentralized, privacy-preserving and lightweight authentication system. Furthermore, the security of the proposed scheme is analyzed. The performance of the scheme is evaluated by implementing it on Remix and comparing its computational and communication cost with other schemes.

Proposing a secure framework for the Industrial Internet of Things (IIoT) network, the work [8] addresses the problems caused by malicious devices in the network, using a combination of trust management and blockchain technology. The proposed model determines the legitimacy of each IoT device by calculating its Trust Factor (GF) and is used by the selected Coordinating IoT Device (CID). It also uses a blockchain-based data model to prevent changes in the information of the local database. The approach has achieved a 91% success rate with a wide range of validation for different network sizes and evaluation criteria. This framework provides an effective mechanism for enhancing security in IIoT networks.

H. Liu et al [9] take the characteristics of IoT devices and propose Fabric-IoT, an access control system based on the Hyperledger Fabric blockchain framework, to solve the inadequacy of traditional access control methods in this large-scale IoT environment. The system includes three types of smart contracts: device contract (DC), policy contract (PC), and access contract (AC). Fabric-IoT offers decentralized, fine-grained, and dynamic access control management. The results of two sets of simulation experiments show that Fabric-IoT can maintain high data transmission rate under large-scale demand environment and can effectively reach consensus in a distributed system to ensure data consistency. Future work aims to improve the scalability of Fabric-IoT and support the integration of more IoT applications.

In another study [10], IoT, a network where IoT devices collect data, proposes a model of organizing and managing groups that offers an access control that allows authorized users to access the data in order to reduce the risk of leaking sensitive information. In particular, the cost of key replacement is reduced. Since IoT devices are resource-limited, the lifetime of the network may decrease as the cost of key replacement increases [10] Also, there is a problem when group communication between multiple users is not used. Sensitive information leakage increases when multiple users can easily access all data. To solve this problem, only users who need to share data form a group based on Hyperledger Fabric. The approach groups users with the same group key (GK) and protects sensitive data using secure communication links within the group. Furthermore, for key reissuance, a trusted agent sends a new GK to users within the group. Therefore, the security of data is guaranteed and network lifetime is extended. The results of the performance analysis show that the proposed Hyperledger Fabric-based lightweight group management (H-LGM) method exceeds the existing method in terms of storage cost, latency, and processing time.

Addressing the shortcomings of traditional IoT access control methods, [11] proposes an access control model called ABAC-HLFBC using the Hyperledger Fabric blockchain framework. This model grants access based on the offered features, granting access only to users with features that comply with the relevant access policies. The proposed model is compared with the Fabric-IoT model and shown to be more effective in terms of performance. The study also includes recommendations for future work, including implementing the model over more organizations and channels, security testing, and reliability and performance testing using IoT physical devices. This study is an important resource that highlights the importance and potential of blockchain-based access control. In another study [12], it is emphasized that blockchain has many applications other than cryptocurrency. In particular, the use of blockchain in IoT-based networks needs to be analyzed. It is stated that there are some challenges due to the limited capabilities of IoT devices and the encrypted data-based nature of the blockchain protocol. The study examines how blockchain can contribute to IoT security and shows that a blockchain-based IoT structure is more secure than a traditional IoT structure.

Another study [13] addresses a backdrop where traditional centralized IoT security frameworks may be limited in terms of data storage space, data reliability, scalability, operational costs and liability assessment in an environment where more IoT devices are in constant communication as a result of the rapidly evolving IoT. The study proposes a new key information storage framework based on a small distributed database created by blockchain technology and cloud storage. In order to solve the problems of data reliability, scalability and liability assessment, all encrypted key communication data will be uploaded to the cloud server, but the digests of these data will be saved in a distributed database called "IoT ledger". It also designs the secure search scheme for the "IoT ledger" and utilizes the ASPE approach to guarantee data security and provide an effective search function. It is demonstrated through experiments on synthetic dataset that these proposed schemes are secure and efficient. This framework enables secure and efficient management of IoT data.

Z. Gong-Guo and Z. Wan in [14] propose a security authentication system called IoT-chain in a context where traditional centralized security authentication methods struggle to support security authentication in the IoT environment, given the limited resources and mobility of IoT devices. IoT-chain provides a property-based security authentication system based on the Hyperledger Fabric blockchain framework and implements a security verification method for users. Experiment results show that IoT-chain can sustain high transaction capacity and achieve consensus effectively in distributed systems. Future work can focus on improvements in areas such as consensus efficiency, system performance, and customizability of smart contracts. Table 4 shows consensus mechanisms for Blockchain-based IoT.

Table 4: Consensus mechanisms for blockchain-based IoT

Year	Reference	Name of the mechanism	Features
2023	[2]	Dynamic Application Block Generation (DABG)	• It uses a newly defined group of signature techniques used to achieve anonymity, traceability and non-frameability. • The proposed method has the ability to verify transactions quickly, enabling efficient processing of both urgent and routine application transactions.

2022	[6]	RAFT	• Improves network resilience by addressing disruptive attacks on IoT blockchain networks. • Develops a method for forwarding node identification that utilizes path loss and reduces the risk of impersonation attacks. • Proposes a method for acquiring IoT nodes to identify forwarding nodes, which improves security against impersonation attacks.

D. Li et al [15] propose a blockchain-based authentication and security mechanism by addressing traditional IoT security issues. The proposed system assigns unique identities to devices and securely stores data. With its low cost and additional security advantages, it is suitable for IoT and focuses on the management of IoT data in the future.

E. Shammar et al [16] discuss IoT and blockchain integration from a security perspective. Blockchain has the potential to be used to create a decentralized, trusted and secure environment in the IoT space. However, there are very few papers that explore the complexities of this integration in depth. The study [16] examines blockchain-based IoT security solutions published between 2017 and 2021 and addresses current research topics and trends in this field. The study examines the key issues and challenges of IoT and blockchain integration and reviews the research efforts conducted so far to overcome these challenges.

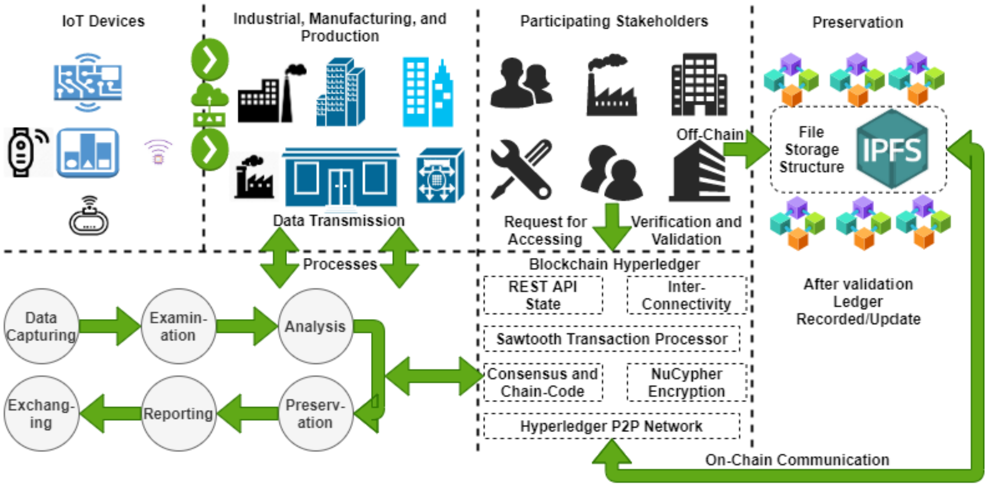

Figure 2: Proposed industrial IoT with blockchain Hyperledger sawtooth-enabled privacy protection and security solution [17].

The study [17], which assesses the current challenges by examining the security applications of Blockchain technology for industrial IoT, proposes a Blockchain Hyperledger Sawtooth-based framework as shown in Figure 2, which supports secure recording and communication of industrial activities. The study presents various protocols and chain codes for fluid industrial device transactions and data transmission.

It is noted that the proposed framework can be implemented as a general-purpose solution in industrial, manufacturing environments. The study examines the combination of industrial IoT and Blockchain technology, offering a promising approach for future applications.

Another study [18] addresses how blockchain technology can be used in the IoT domain and the related security issues. The development of IoT technology has led to significant advances in distributed systems. The blockchain concept requires a decentralized data management system to store and share data and transactions across the network. The study addresses factors that analyze potential security attacks in detail and presents existing solutions that can be taken against these attacks. It also summarizes solutions to enhance blockchain security, presenting the main points that can be used against security vulnerabilities. Finally, the study discusses open issues and future research directions regarding blockchain-IoT systems.

F. Oikonomou et al. [19] propose a Hyperledger Fabric-based blockchain architecture to enhance the security of IoT-based health monitoring systems. This proposal aims to address the problem that IoT devices with limited processing power, storage capacity and battery life cannot support complex transactions. Furthermore, this architecture aims to provide data integrity and availability at local and global level. Future work could include implementing the proposed architecture in a virtual environment and evaluating it in terms of performance metrics such as processing speed, resource consumption, network utilization and latency.

The other study [20] provides important data when addressing the security and authentication of IoT data. First, data analysis was performed with machine learning algorithms to secure IoT data. The experiments selected 15 features from the 80-feature IoTID20 dataset by using algorithms such as Pearson correlation and Logistic Regression. This reduced the computational intensity to achieve fast prediction models. The study also revealed that AdaBoost and Random Forest classifiers have the best performance. AdaBoost had an accuracy of 96.3%, precision of 97.9%, recall of 95% and F1 score of 96.3%. Random Forest has an accuracy of 96.2%, precision of 96.2%, recall of 96.2% and F1 score of 96.2%. It is also shown that IoT data is securely stored using blockchain technology. The blockchain is based on a hashing process where data is verified by trusted nodes using digital signatures and hashing of entries to secure the data. The results also showed a positive relationship between sample size and prediction time. The experiments showed that Decision Tree and Naïve Bayes classifiers gave the best results in time prediction. However, noting that IDS does not have 100% accuracy, it is suggested that IDS should be improved in the future and other blockchain platforms should be investigated.

The study [21], which examines Machine Learning methods in intrusion detection, examines and compares the performance analysis of machine learning methods on the

UNSW-NB15 dataset. The Random Forest algorithm achieved the highest accuracy rate in the tests. In addition, an increase in performance was observed when the number of features was reduced using the reliefF scoring method. In particular, the Neural Network algorithm was found to have the highest accuracy rate after feature selection. Comparing the study with the literature, it is seen that using the reliefF method in feature selection contributes to better results. In future studies, it is aimed to achieve higher accuracy rates by using methods such as Association Rule Extraction and Ensemble Learning.

Another study [22] addresses a blockchain-based approach for IoT security and privacy, emphasizing the challenges of scale and decentralization, which are not feasible in terms of energy and transaction costs. In the smart home case, it proposes a lightweight blockchain (BC) model by eliminating the concepts of Proof of Work (POW) and coins. The paper analyzes the security of the proposed BC-based smart home framework by describing in detail the core components and functionalities of the smart home layer. Simulation results show that the proposed method is low-cost and offers significant security and privacy benefits for low-resource IoT devices.

The work of S. Mohanty et al [23] presents an efficient Lightweight Integrated Blockchain (ELIB) model specifically developed for the Internet of Things (IoT). The ELIB model is implemented in a smart home environment and used as an important example to validate its applicability in various IoT scenarios. The ELIB model provides a structure that leverages a centralized administrator to process every incoming and outgoing request to resource-constrained smart home resources, generating shared keys for data transmission. The presented ELIB model includes three optimizations including a lightweight consensus algorithm, certificate-free (CC) encryption and a Distributed Throughput Management (DTM) scheme. A detailed simulation of different scenarios is performed in terms of processing time, energy consumption and workload. ELIB achieves 50% savings in processing time and a minimum energy consumption of 0.07 mJ compared to the baseline method. The experimental results obtained show that ELIB shows maximum performance under various evaluation parameters.

Another study [24] introduces a Lightweight Scalable Blockchain (LSB) model optimized for IoT. LSB is studied in the smart home scenario and provides security and privacy using a centralized manager for low-resource devices. Optimized with algorithms, LSB is shown to be resilient to attacks after extensive security analysis. Simulations show that LSB offers high performance by reducing bandwidth and processing time. Future work on LSB includes evaluating its real-world performance and investigating its suitability in different application domains.

In [25], M. Du et al. introduce a three-dimensional blockchain architecture called Spacechain, an effective solution for IoT security. Unique data structures and parallel workflows are designed to address heterogeneity and scalability issues. Furthermore, the 3D-GHOST consensus mechanism is proposed to improve security and network performance under high workload. The detailed security analysis and extensive experimental validation demonstrate the performance of Spacechain. Some open security issues are also summarized for future work.

Another study [26] presents IoTchain, a three-tier blockchain-based IoT security architecture developed to enhance IoT security. Designed to provide authentication, access control, privacy protection, lightweight feature, regional node fault tolerance, DDoS resistance and storage integrity, this architecture includes an authentication layer, a blockchain layer and an application layer. We also evaluate the performance of IoTchain and demonstrate its use in a real IoT application.

In another study [27], a lightweight blockchain called Fusion Chain is proposed to increase the security of IoT devices. With the proposed solutions, the size of the blockchain is significantly reduced, low computational power is required by using the PBFT consensus algorithm, and data privacy is ensured with PKI encryption. The experimental results show that Fusion Chain is suitable for IoT devices and can solve the security vulnerabilities of IoT applications such as Mirai botnet and DDoS attacks by ensuring data reliability and integrity. Currently, research is underway on a lightweight blockchain that provides high transaction speed (TPS) on an inter-chain structured blockchain that divides IoT devices into groups using Fusion Chain.

In A. Rajawat et al.'s study [28], a Blockchain-based model is proposed as a solution to data management problems in the healthcare sector. With the SHA256 hashing algorithm used for the security of data obtained from health IoT devices, each data change is securely verified, thereby increasing the security of health data. By applying SHA256 hashing algorithm to each block, the proposed algorithm ensures that the data cannot be modified by malicious sources. Designed in line with the priorities of verifiability, relevance, comprehensiveness, comprehensiveness, uniqueness, robustness, and resistance to coercion, this Blockchain-based model offers several possibilities for future work.

Another study [29] proposes BCSDN-IoT, a new architecture for IoT security that includes a combination of blockchain and SDN. This architecture is developed to address the challenges faced by large-scale IoT networks and to meet new service requirements. The BCSDN-IoT model is designed to build and deploy protections such as threat prevention, data protection and access control, as well as detect network attacks such as cache poisoning/ARP spoofing, DDoS/DoS attacks. This approach focuses on minimizing the attack window time by allowing IoT routers to check the most up-to-date flow rule table when needed. The performance evaluation is based on the effects of the proposed model on scalability, defense effects, accuracy rates and performance.

In [30], M. Hammi et al. propose "Bubbles of Trust", an effective decentralized authentication system for IoT. This approach protects data integrity and accessibility by enabling objects to recognize and authenticate each other. Based on the security advantages of the blockchain, this method provides an environment where objects can trust each other by creating secure virtual regions (bubbles). The results of the study, which presents a real implementation using the C++ language and the Ethereum blockchain, show that it succeeds in meeting IoT security requirements, efficiency and low cost. In the future, it is planned to further optimize this system in areas such as communication, security and energy consumption.

When literature reviews are generally examined, challenges brought by the integration of blockchain and IoT should also be taken into consideration. Table 5 examines these challenges. Issues such as latency, applicability, and scalability are among the foremost challenges in this context.

Table 5: Challenges in integrating blockchain with IoT

References	Key areas	Challenges
[4]	Delay	It takes 1 to 10 minutes to reach consensus
	Resource Constraints	IoT devices may not be suitable for resource-intensive blockchains
	Applicability	It is impractical to assume that all devices support the same blockchain framework
[2]	Efficiency and Scalability	Low blockchain throughput hinders IoT scalability.
	Privacy and Traceability	Balancing anonymity and traceability in IoT blockchain transactions.
	Device Management	IoT mobility challenges decentralized device management on blockchain
[18]	Blockchain Attacks	IoT devices may be exposed to various Blockchain attacks

3. Results

This study examines the integration of IoT and blockchain technologies, offering various solutions for secure transactions. Research conducted in various fields highlights the potential of blockchain in ensuring security and data integrity across a wide range of applications, from industrial IoT to the healthcare sector.

Prominent findings include fast transaction confirmations with the DABG protocol, secure recording of industrial activities with a Hyperledger Sawtooth-based framework, and the provision of secure access control in large-scale IoT environments with solutions like Fabric-IoT.

In conclusion, the findings from the reviewed literature in this study indicate that the integration of blockchain and IoT is a promising area for future secure applications.

References

[1] L. S. Vailshery, "Number of IoT connected devices worldwide 2019-2023, with forecasts to 2030," Statista. Accessed: Nov. 10, 2023. [Online]. Available: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/

[2] S. Basudan, "A Scalable Blockchain Framework for Secure Transactions in IoT-Based Dynamic Applications," *IEEE Open Journal of the Communications Society*, 2023, doi: 10.1109/OJCOMS.2023.3307337.

[3] A. Pathak, I. Al-Anbagi, and H. J. Hamilton, "TABI: Trust-Based ABAC Mechanism for Edge-IoT Using Blockchain Technology," *IEEE Access*, vol. 11, pp. 36379–36398, 2023, doi: 10.1109/ACCESS.2023.3265349.

[4] S. S. Seshadri *et al.*, "IoTCop: A Blockchain-Based Monitoring Framework for Detection and Isolation of Malicious Devices in Internet-of-Things Systems," *IEEE Internet Things J*, vol. 8, no. 5, pp. 3346–3359, Mar. 2021, doi: 10.1109/JIOT.2020.3022033.

[5] B. Bera, S. Saha, A. K. Das, and A. V. Vasilakos, "Designing blockchain-based access control protocol in iot-enabled smart-grid system," *IEEE Internet Things J*, vol. 8, no. 7, pp. 5744–5761, Apr. 2021, doi: 10.1109/JIOT.2020.3030308.

[6] H. M. Buttar, W. Aman, M. M. U. Rahman, and Q. H. Abbasi, "Countering Active Attacks on RAFT-Based IoT Blockchain Networks," *IEEE Sens J*, vol. 23, no. 13, pp. 14691–14699, Jul. 2023, doi: 10.1109/JSEN.2023.3274687.

[7] X. Yang *et al.*, "Blockchain-Based Secure and Lightweight Authentication for Internet of Things," *IEEE Internet Things J*, vol. 9, no. 5, pp. 3321–3332, Mar. 2022, doi: 10.1109/JIOT.2021.3098007.

[8] G. Rathee, F. Ahmad, N. Jaglan, and C. Konstantinou, "A Secure and Trusted Mechanism for Industrial IoT Network Using Blockchain," *IEEE Trans Industr Inform*, vol. 19, no. 2, pp. 1894–1902, Feb. 2023, doi: 10.1109/TII.2022.3182121.

[9] H. Liu, D. Han, and D. Li, "Fabric-iot: A Blockchain-Based Access Control System in IoT," *IEEE Access*, vol. 8, pp. 18207–18218, 2020, doi: 10.1109/ACCESS.2020.2968492.

[10] J. Maeng, Y. Heo, and I. Joe, "Hyperledger Fabric-Based Lightweight Group Management (H-LGM) for IoT Devices," *IEEE Access*, vol. 10, pp. 56401–56409, 2022, doi: 10.1109/ACCESS.2022.3177270.

[11] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "An Attribute-Based Access Control Model for Internet of Things Using Hyperledger Fabric Blockchain," *Wirel Commun Mob Comput*, vol. 2022, 2022, doi: 10.1155/2022/6926408.

[12] R. Kaur and A. Ali, "A Novel Blockchain Model for Securing IoT Based Data Transmission," *International Journal of Grid and Distributed Computing*, vol. 14, no. 1, pp. 1045–1055, Apr. 2021.

[13] H. Zhang, X. Zhang, Z. Guo, H. Wang, D. Cui, and Q. Wen, "Secure and Efficiently Searchable IoT Communication Data Management Model: Using Blockchain as a New Tool," *IEEE Internet Things J*, vol. 10, no. 14, pp. 11985–11999, Jul. 2023, doi: 10.1109/JIOT.2021.3121482.

[14] Z. Gong-Guo and Z. Wan, "Blockchain-based IoT security authentication system," *Proceedings - 2021 International Conference on Computer, Blockchain and Financial Development, CBFD 2021*, pp. 415–418, 2021, doi: 10.1109/CBFD52659.2021.00090.

[15] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," *Proceedings - International Conference on Computer Communications and Networks, ICCCN*, vol. 2018-July, Oct. 2018, doi: 10.1109/ICCCN.2018.8487449.

[16] E. A. Shammar, A. T. Zahary, and A. A. Al-Shargabi, "A Survey of IoT and Blockchain Integration: Security Perspective," *IEEE Access*, vol. 9, pp. 156114–156150, 2021, doi: 10.1109/ACCESS.2021.3129697.

[17] A. Ayub Khan, A. A. Laghari, Z. A. Shaikh, Z. Dacko-Pikiewicz, and S. Kot, "Internet of Things (IoT) Security With Blockchain Technology: A State-of-the-Art Review," *IEEE Access*, vol. 10, pp. 122679–122695, 2022, doi: 10.1109/ACCESS.2022.3223370.

[18] S. Singh, A. S. M. Sanwar Hosen, and B. Yoon, "Blockchain Security Attacks, Challenges, and Solutions for the Future Distributed IoT Network," *IEEE Access*, vol. 9, pp. 13938–13959, 2021, doi: 10.1109/ACCESS.2021.3051602.

[19] F. P. Oikonomou, J. Ribeiro, G. Mantas, J. M. C. S. Bastos, and J. Rodriguez, "A Hyperledger Fabric-based Blockchain Architecture to Secure IoT-based Health Monitoring Systems," *2021 IEEE International Mediterranean Conference on Communications and Networking, MeditCom 2021*, pp. 186–190, 2021, doi: 10.1109/MEDITCOM49071.2021.9647521.

[20] R. Shahin and K. E. Sabri, "A Secure IoT Framework Based on Blockchain and Machine Learning," *International Journal of Computing and Digital Systems*, vol. 11, no. 1, pp. 671–683, 2022, doi: 10.12785/IJCDS/110154.

[21] Y. Türkyilmaz and A. Şentürk, "Saldırı Tespitinde Makine Öğrenmesi Yöntemlerinin Performans Analizi," *Avrupa Bilim ve Teknoloji Dergisi*, vol. 32, no. 32, pp. 107–112, Dec. 2021, doi: 10.31590/EJOSAT.1045551.

[22] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," *2017 IEEE International Conference on Pervasive Computing and Communications Workshops, PerCom Workshops 2017*, pp. 618–623, May 2017, doi: 10.1109/PERCOMW.2017.7917634.

[23] S. N. Mohanty *et al.*, "An efficient Lightweight integrated Blockchain (ELIB) model for IoT security and privacy," *Future Generation Computer Systems*, vol. 102, pp. 1027–1037, Jan. 2020, doi: 10.1016/J.FUTURE.2019.09.050.

[24] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A Lightweight Scalable Blockchain for IoT security and anonymity," *J Parallel Distrib Comput*, vol. 134, pp. 180–197, Dec. 2019, doi: 10.1016/J.JPDC.2019.08.005.

[25] M. Du *et al.*, "Spacechain: A three-dimensional blockchain architecture for IoT security," *IEEE Wirel Commun*, vol. 27, no. 3, pp. 38–45, Jun. 2020, doi: 10.1109/MWC.001.1900466.

[26] Z. Bao, W. Shi, D. He, and K.-K. R. Chood, "IoTChain: A Three-Tier Blockchain-based IoT Security Architecture," Jun. 2018, Accessed: Dec. 02, 2023. [Online]. Available: https://arxiv.org/abs/1806.02008v2

[27] D. Na, S. Park, J. Prieto, and F. De La Prieta, "Fusion Chain: A Decentralized Lightweight Blockchain for IoT Security and Privacy," *Electronics 2021, Vol. 10, Page 391*, vol. 10, no. 4, p. 391, Feb. 2021, doi: 10.3390/ELECTRONICS10040391.

[28] A. S. Rajawat, R. Rawat, K. Barhanpurkar, R. N. Shaw, and A. Ghosh, "Blockchain-Based Model for Expanding IoT Device Data Security," *Advances in Intelligent Systems and Computing*, vol. 1319, pp. 61–71, 2021, doi: 10.1007/978-981-33-6919-1_5/COVER.

[29] Y. Abbassi and H. Benlahmer, "BCSDN-IoT: Towards an IoT security architecture based on SDN and Blockchain," *International journal of electrical and computer engineering systems*, vol. 13, no. 2, pp. 155–163, Feb. 2022, doi: 10.32985/IJECES.13.2.8.

[30] M. T. Hammi, B. Hammi, P. Bellot, and A. Serhrouchni, "Bubbles of Trust: A decentralized blockchain-based authentication system for IoT," *Comput Secur*, vol. 78, pp. 126–142, Sep. 2018, doi: 10.1016/J.COSE.2018.06.004.