SAKARYA UNIVERSITY JOURNAL OF COMPUTER AND INFORMATION SCIENCES
http://saucis.sakarya.edu.tr/
e-ISSN: 2636-8129
Publisher: Sakarya University
Vol. 8, No. 1, 12-26, 2025
DOI: 10.35377/saucis...1607145
RESEARCH ARTICLE

Blockchain-Based IoT Security and Performance Analysis

Selami Terazi[1], **Arafat Şentürk**[1*]

[1]Duzce University, Faculty of Engineering, Department of Computer Engineering, Duzce, Türkiye, ror.org/04ttnw109

Corresponding author:
Arafat Şentürk, Duzce University, Faculty of Engineering, Department of Computer Engineering, Duzce, Türkiye
arafatsenturk@duzce.edu.tr

Article History:
Received: 25.12.2024
Revised: 05.02.2025
Accepted: 27.02.2025
Published Online: 27.03.2025

ABSTRACT
The Internet of Things (IoT) enables devices to connect and exchange data, revolutionizing industries and daily life. However, the rapid growth of IoT devices has introduced significant security challenges, including cyber-attacks, data breaches, and unauthorized access. This study explores the integration of blockchain technology, particularly Hyperledger Fabric, to enhance IoT security. With its permissioned structure and decentralized approach, blockchain ensures secure data storage, integrity, and confidentiality. Hyperledger Fabric's modular architecture offers organizations the flexibility to address these security needs effectively. Using the OPNET simulation tool, the study analyses the performance of IoT networks transmitting blockchain-encrypted packets. Results show that blockchain integration enhances security, strengthens user authentication, and prevents unauthorized access. These findings highlight blockchain's transformative potential for IoT security, offering practical solutions for industrial applications and emphasizing the need for continued research in this critical field.

Keywords: Blockchain, IoT, Cyber security, Hyperledger Fabric, OPNET

1. Introduction

The number of IoT devices is growing rapidly, reaching 17 billion devices worldwide by 2024 [1]. This number is projected to increase to 30 billion by 2030 [1]. These Internet-connected devices range from smart thermostats in homes to complex industrial control systems in factories [2]. In healthcare, for example, IoT devices enable real-time patient monitoring, enabling faster response times and more personalized care [3]. Similarly, IoT systems in manufacturing provide real-time data on machine performance, helping to minimize downtime and increase productivity [4]. The potential of IoT extends to how smart infrastructure can optimize traffic flow, reduce energy consumption and improve public safety [5].

However, this vast interconnected ecosystem also poses significant security risks [6]. Each device connected to the internet represents a potential entry point for cyber-attacks [6]. A study by HP highlighted the widespread security concerns in IoT systems, revealing that 70% of IoT devices are vulnerable to attacks [7]. A notable example of IoT vulnerabilities was the 2016 Mirai botnet attack, in which thousands of compromised IoT devices were used to launch a distributed denial of service (DDoS) attack, bringing down major websites [8]. With IoT devices often deployed without proper security measures in place, the attack surface for potential breaches has expanded significantly [6].

Security challenges in IoT are exacerbated by the limitations of many internet-connected devices [6]. Unlike traditional computing systems, many IoT devices have limited processing power and memory, making it difficult to implement traditional security mechanisms such as firewalls and encryption [9]. This has led to an increasing focus on lightweight cryptography and secure communication protocols adapted for resource-constrained environments [9]. Furthermore, the heterogeneous nature of IoT devices, ranging from simple sensors to complex machines, poses interoperability challenges and complicates security measures across different platforms [9].

In recent years, blockchain technology has emerged as a promising tool for improving IoT security [10]. Originally developed as the technology that created cryptocurrencies such as Bitcoin, blockchain is a decentralized ledger that records transactions across multiple nodes in a network [11]. Its characteristics of transparency, immutability and decentralized control make it an ideal solution for securing IoT systems [12]. Using Blockchain, data generated by IoT devices can be recorded in a hacker-proof manner and data integrity can be ensured [12]. Furthermore, the decentralized nature of Blockchain reduces the risk of single points of failure in the system by eliminating the need for a central authority [10].

Cite as: S. Terazi and A. Şentürk, "Blockchain-based IoT security and performance analysis," *Sakarya University Journal of Computer and Information Sciences,* vol. 8, no. 1, pp. 12-26, 2025, doi: 10.35377/saucis...1607145

Table 1. Blockchain Mechanisms for IoT Security

Reference	Security Threats	IoT Applications	Observation
[20]	Sybil attack, self-promoting attack, bad-mouthing attack.	IoT devices	Hyperledger's TABI is an access control mechanism designed for Edge-IoT networks that builds trust using blockchain technology. This Trust-Based Access Control Mechanism ensures secure and reliable access management, specifically tailored for the unique demands of IoT environments at the network edge.
[21]	Malicious software or physical attacks	IoT devices	IoTCop is an IoT monitoring framework that utilizes blockchain technology for enhanced security. Leveraging Hyperledger Fabric and modular hardware plugins, it swiftly identifies and isolates compromised devices to maintain network integrity.
[22]	"Impersonation," "man-in-the-middle," "ephemeral secret leakage (ESL)," and "replay" attacks.	IoT-enabled smart grid system	DBACP-IoTSG is a newly developed IoT-enabled smart grid system that operates independently of a Trusted Third Party (TTP). It employs leader election and PBFT (Practical Byzantine Fault Tolerance) consensus for secure block verification, while ECC (Elliptic Curve Cryptography) encryption ensures transaction privacy.
[23]	Jamming and impersonation attacks	IoT blockchain network	Through the study of obfuscation and impersonation attacks on a RAFT-based IoT blockchain network, a path-loss-based identification method was proposed, demonstrating strong detection rates against these types of threats.
[24]	Man-in-the-middle attack, eavesdropping attack, impersonation attack, replay attack.	IoT network	This solution provides a lightweight, blockchain-based authentication method for IoT, utilizing MSR encryption to enable decentralized and privacy-preserving authentication.
[25]	Malicious attacks	Industrial IoT network	A secure framework has been proposed that combines trust management with blockchain technology to address issues arising from varying levels of malicious devices in industrial IoT networks. This approach enhances network reliability by effectively managing and mitigating threats posed by compromised devices.

Table 2. Some Studies Leveraging Blockchain for IoT Security

Security areas in IoT	Proposed solutions	Blockchain features
Access control	[20]	TABI Mechanism for Edge-IoT Networks
	[26]	Access Control through Smart Contracts
	[22]	Respective smart meters (SMs)
	[27]	Manage and organize groups using a group key (GK)
	[28]	ABAC grants access based on the qualifications specified by the target
Data integrity	[23]	Applying a binary hypothesis test for identifying transmission nodes.
	[25]	
	[29]	
Data confidentiality	[30]	Asymmetric Scalar-product Preserving Encryption (ASPE)
	[31]	Attribute-based security authentication using the Hyperledger Fabric blockchain framework
	[24]	The framework integrates blockchain technology with the modular square root algorithm
	[19]	IoT powered by blockchain with dynamic device management and conditional traceability
	[32]	Blockchain-based model for IoT authentication and security protection
Data availability	[23]	Stochastic geometry tool

Blockchain can also help address some of the key challenges related to IoT security [12]. For example, it can be used to secure device-to-device communication by establishing trust between devices without relying on a centralized server [12]. This is particularly important for the traditional constrained client-server model [13]. Furthermore, smart contracts (self-executing contracts where the terms of the agreement are written directly into the code) can be used to automate processes in IoT systems, further improving security and efficiency [10]. For example, in supply chain management, smart contracts can reduce the risk of fraud by automatically triggering payments when goods are delivered [14].

Despite its advantages, there are also disadvantages in the integration of blockchain with IoT. One of the biggest issues is scalability [15]. Traditional blockchain networks such as Bitcoin and Ethereum struggle to handle large transaction volumes, making them inefficient for the high data throughput of IoT systems [16]. To address this issue, new blockchain platforms such as Hyperledger Fabric are being developed and offer more efficient consensus mechanisms that can support enterprise-level applications [17]. Additionally, the energy consumption of blockchain networks, especially those based on proof-of-work consensus algorithms, raises sustainability concerns, especially in IoT environments where energy efficiency is critical [18].

2. Related Works

In [19], S. Basudan introduces a scalable framework that integrates IoT with blockchain technology to enable secure transactions in dynamic environments. The framework leverages dynamic device management and conditional traceability through the DABG protocol, offering rapid transaction confirmations, enhanced data security, and privacy protection. Future developments in this framework aim to incorporate federative learning and advanced privacy protection techniques. Table 1 and Table 2 provide a detailed analysis of how blockchain is effectively utilized with IoT devices and the key features involved.

A. Pathak et al. [20] explore the application of blockchain to enhance security in IoT networks, addressing issues such as computational overhead and high energy consumption. By employing edge computing, their proposed Trust-Based Access Control Mechanism (TABI) (see Figure 1) provides a solution for ensuring end-to-end security in IoT networks, particularly those with limited resources. TABI integrates trust evaluation and access control to mitigate risks from malicious devices and users. Its performance indicates suitability for IoT applications requiring low latency and resource optimization. Future research will focus on improving service quality and identifying malicious devices within IoT ecosystems.

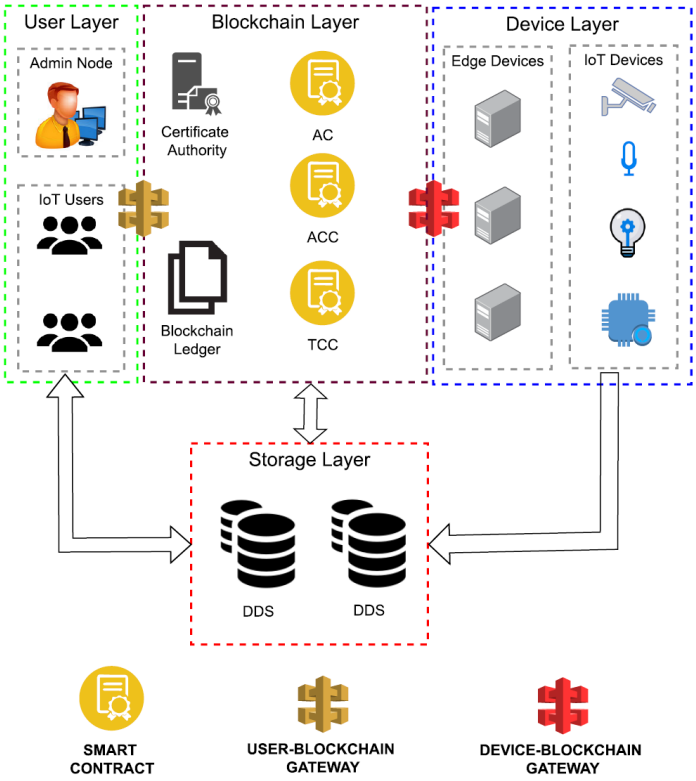


Figure 1. TABI architecture [20]

S. Seshadri et al. [21] present IoTCop, a blockchain-based monitoring framework designed to safeguard IoT devices. Unlike traditional servers, IoT devices are often geographically distributed and close to physical systems, leading to resource limitations despite the need for robust security measures. The study proposes leveraging blockchain technology to enforce security policies, allowing automatic isolation of compromised devices. By utilizing a permissioned blockchain (Hyperledger Fabric) and supplementary hardware modules, the framework delivers low latency and minimal workload while enabling seamless integration of existing IoT devices. Table 3 outlines various malicious attacks that IoTCop protects against.

Table 3. Common Attacks on IoT Networks

Attack	Category	Description	Research on defending attack using blockchain
Impersonation attack	Internal/External	An impersonation attack occurs when a device falsely assumes the identity or authorization of another device to gain unauthorized access to IoT networks.	[22], [23], [24]
Man-in-the-Middle attack	Internal/External	A Man-in-the-Middle (MitM) attack on IoT networks allows an attacker to intercept or alter communication between IoT devices.	[22], [24]
Bad-mouthing attack	Internal	A bad-mouthing attack is a type of cyber-attack on IoT networks where an attacker spreads false or misleading information to discredit other devices.	[20]
Replay attack	External	In a replay attack, a malicious actor attempts to gain unauthorized access to IoT networks by reusing or retransmitting recorded data.	[21], [22], [24]
Sybil attack	Internal/External	A Sybil attack in IoT networks involves an attacker infiltrating the network by generating numerous fake devices, each with a counterfeit identity	[20]

Table 3. (Continued)

Jamming attack	External	A jamming attack in IoT networks occurs when a malicious device or jammer floods radio frequencies, disrupting the communication between IoT devices.	[23]
Self-promoting attack	External	In IoT networks, a "self-promoting attack" involves an IoT device attempting to secretly join the network or gain unauthorized access by falsely identifying itself. The device typically infiltrates the network either directly or by exploiting existing vulnerabilities.	[20]
Eavesdropping attack	External	Eavesdropping is an attack on IoT networks where attackers monitor communication traffic to access sensitive information, creating security vulnerabilities and privacy breaches.	[24]
Ephemeral secret leakage (ESL) attack	Internal	In ESL IoT networks, an insider security breach occurs when unauthorized persons or devices leak temporary passwords without permission.	[22]
DDoS	Internal/External	A DDoS (Denial of Service) attack on IoT networks is a cyber attack where numerous IoT devices collectively send a massive volume of client traffic to a target, overwhelming it and causing a crash.	[32]

A review of literature on blockchain and IoT integration highlights several challenges that must be addressed, such as latency, scalability, and real-world applicability. Table 4 offers an in-depth look at these challenges and their potential impact on IoT security solutions.

Table 4. Challenges in Blockchain Integration with IoT

References	**Key areas**	**Challenges**
[21]	Delay	Consensus is reached within 1 to 10 minutes
	Resource Constraints	Resource-intensive blockchains may not be suitable for IoT devices
	Applicability	Assuming that all devices support the same blockchain framework is impractical
[19]	Efficiency and Scalability	IoT scalability is hindered by low blockchain throughput
	Privacy and Traceability	Balancing traceability and anonymity in blockchain transactions for IoT
	Device Management	Decentralized device management on blockchain faces challenges due to IoT mobility
[12]	Blockchain Attacks	Various Blockchain attacks may expose IoT devices to risks

3. The Proposed Method

This study combines Hyperledger Fabric, a blockchain platform, with OPNET, a network simulation tool. Hyperledger Fabric is used to demonstrate secure data transactions and management in IoT ecosystems, while OPNET simulates network

dynamics and potential vulnerabilities in IoT infrastructures. Together, these tools provide a comprehensive framework for assessing the effectiveness of blockchain in IoT security.

Hyperledger Fabric is an open-source blockchain framework designed to meet the specific needs of businesses by offering high levels of privacy, security and scalability. Unlike public blockchains like Bitcoin and Ethereum, which operate on permissionless networks, Hyperledger Fabric offers a permissioned model, meaning that participants must be identified and verified before they are allowed to join the network [33].

OPNET is a powerful simulation tool used to model and analyze the performance of communication networks, protocols and devices. Originally developed by MIL 3, Inc. and later acquired by Riverbed Technology [34], OPNET allows users to test various network configurations, simulate traffic loads, and evaluate the impact of different network protocols before deploying them in real-world environments [35].

3.1. Hyperledger Fabric Network Setup and Data Operations

First, an outline of the network architecture was created, highlighting the roles and interactions of various components, including organizations, peers and orderer. Next, the Hyperledger Fabric network was run, followed by interactions through Postman. A user was registered and the corresponding token (key) was obtained. Using this token, vehicle registrations were added to the blockchain, each generating a unique transaction ID. The Fabcar.go code serves as an application that demonstrates how to interact with the blockchain network by adding and transacting on sample vehicle/car records [36].

The network diagram shown in Figure 2 illustrates the interaction between the two organizations, the peers each has, and the orderer, which plays a critical role in the consensus process. The process of confirming a transaction within the Hyperledger Fabric network, adding it to the blockchain, and adding new blocks to the existing blockchain is shown in Figure 2 [37].

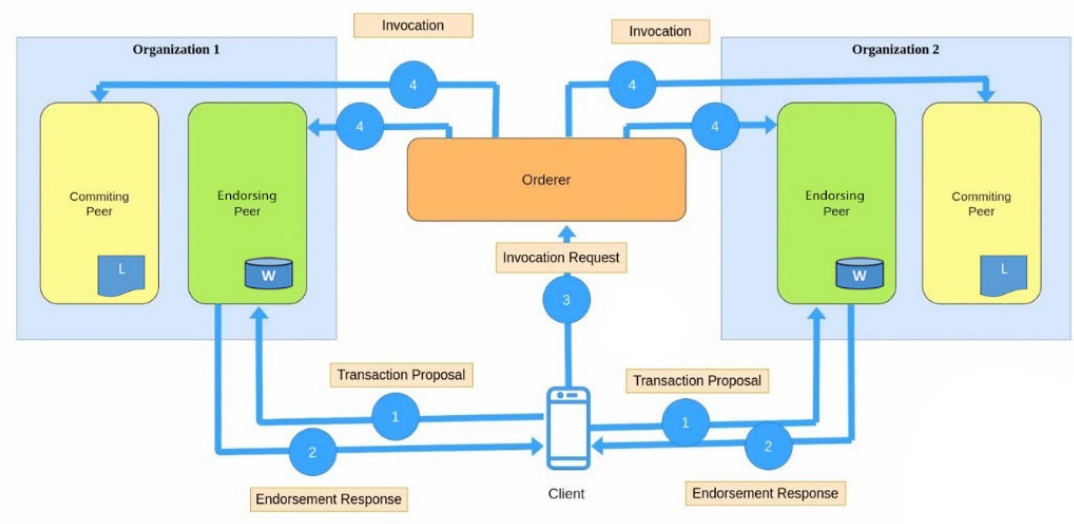


Figure 2. Transaction flow in Hyperledger Fabric [37]

In the Hyperledger Fabric network, organizations represent independent entities that participate in the blockchain network. Each organization operates its own peers, which are responsible for verifying and approving transactions. Approving peers show and approve transaction proposals. When a client submits a transaction proposal, the confirming peers access the world state database (W) to run the chaincode and indicate the transaction. They then generate an acknowledgment response. This response contains simulation results and a signature. The confirmation response is critical to the validity of the transaction and must comply with the network's confirmation policy. Committing peers do not keep a complete ledger; they only evaluate transactions using the current world state database. Committing peers are responsible for validating the confirmed transactions received from the orderer and committing them to the blockchain ledger (L). Once the transactions are verified, they are recorded in the ledger and the world state database is updated accordingly. Committing peers do not show transactions; instead, they perform verification and recording to maintain the integrity of the network and maintain an up-to-date ledger.

The client is the entity in the network that initiates the transaction process. It sends the transaction proposal to the network's confirming peers. After collecting the necessary approvals, it forwards the transaction request to the orderer. The client sends the transaction offer to the confirming peers. For the Confirmation Response, the confirming peers execute the trade offer, generate a confirmation response and send it back to the client.

To make an Invocation Request, the client collects the necessary confirmations and sends an invocation request to the orderer. The orderer queues transactions, creates blocks and distributes them to committing peers. Committing peers verify and commit transactions to the ledger, updating the world state accordingly.

The orderer plays a critical role in ensuring the consistency of the blockchain. It collects confirmed transactions, sorts them into blocks and distributes these blocks to committing peers. By ensuring that all peers receive the same order of transactions, the orderer maintains the integrity of the network. The Raft consensus algorithm is the primary consensus mechanism used in Hyperledger Fabric. Raft is a crash fault tolerant (CFT) consensus protocol that provides deterministic transaction ordering. Unlike Byzantine Fault Tolerant (BFT) algorithms, Raft focuses on scenarios where participants are generally trustworthy. It manages the process of ordering transactions by electing a leader among the orderers. In case the leader fails, a new leader is automatically elected, which ensures a continuous operation without downtime.

To initialize the Hyperledger Fabric network, a command is used that leverages Docker Compose, which helps manage multiple Docker containers. These containers represent different components of the Fabric network, such as peers and orderers, all of which are defined in a YAML configuration file. Channels provide data privacy and segregation by allowing certain participants to communicate and transact privately. Once the configuration of the channel is defined, it is created and peers from different organizations are instructed to join.

In Figure 3, there are two separate channels between organizations, Channel 1 and Channel 2. These channels allow specific organizations to communicate in a secure and private way. Once the channel is established, chaincode is distributed to all peers in the network, as shown in Figure 3. Chaincode is written in languages such as Go or JavaScript and governs how transactions are handled. The process involves packaging the chaincode, uploading it to the peers and obtaining approval from all relevant organizations. After approval, the chaincode becomes active and manages network transactions.

Each step ensures that the network, channels and smart contracts are properly configured and can interact securely and efficiently.

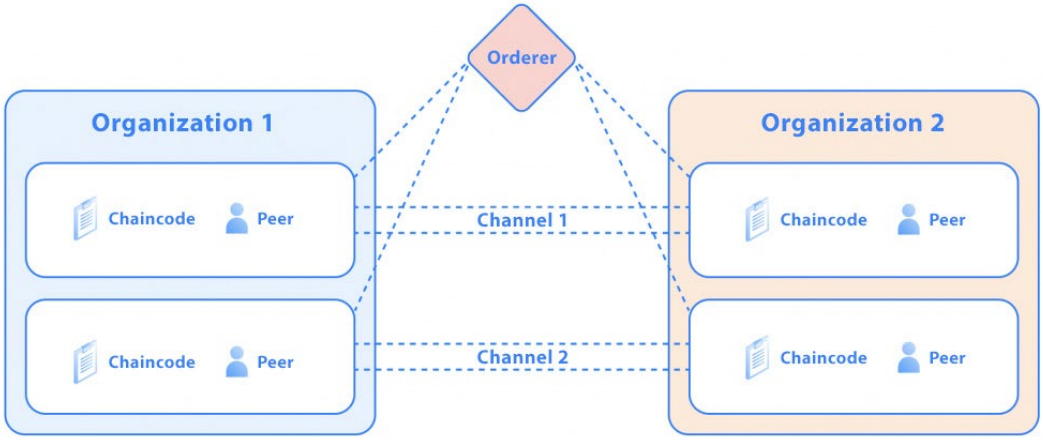


Figure 3. Channels and Chaincode [38]

A block named car is used as an example to add a new block to the system, but this process can be applied to any entity record. In Figure 5, the block named car is shown as an example, the type of data to be registered may vary depending on the system or the user. Clients can register users through the /users API endpoint. This requires providing a username and organization name. Upon successful registration, the system issues a JSON Web Token (JWT) to the client (see Figure 4). This token is required to perform other sensitive operations such as authentication, channel management and chaincode interactions.


```
{
"username": "Selami",
"orgName":"Org1"
}
============================
"message": "Selami enrolled Successfully",
"token": "eyJhbGci0iJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJleHAiOjE3MjQw
MjQzNzksInVzZXJuYW1lIjoiU2VsYW1pIiwib3JnTmFtZSI6Ik9yZzEiLCJpYX
QiOjE3MjM500gzNz1.vQGKB3n6c8cs9IKHW2RPhBzmq6HgXP2b19iLD1Z480"
```


Figure 4. User Enrolling and JWT Generation

This function starts by creating a unique ID for a block named “car” as an instance in the ledger. This instance represents a transaction specifically related to vehicle information. Using the Fabcar.go chaincode, specific data for each vehicle (make, model, color and owner) is recorded within a block.

In the first step, the client application sends a transaction proposal to the Hyperledger Fabric network. This includes a request to create a block for a specific vehicle data. Peer nodes approve this proposal and the transaction is forwarded to the orderer. The orderer merges the approved transaction with other transactions and adds a new block to the chain.


```
{
"fcn":"createCar",
"peers": ["peer0.org1.example.com","peer0.org2.example.com"],
"chaincodeName":"fabcar",
"channelName":"mychannel",
"args":["Araba","Fiat","Egea","Siyah","Selami"]
}
============================
"result": {
"tx_id": "6ff6a238e40f18181db76754d1d74c0ad4cd811fea42e7b2ca@c355dcd3"
}
```


Figure 5. Creating A “car” Eecord

3.2. Network Simulation with OPNET

This section describes in detail the simulation of a ZigBee-based IoT network that mirrors a blockchain environment.

In the simulation scenarios, the ACK mechanism is enabled in many studies in the literature [39] to increase the reliability of the data packets, so it is done in the same way in this study. Also, the simulation time is set to 15 minutes in many studies [40], which is also used in this study.

The metrics selected to evaluate performance are as follows;

- End-to-End Latency (sec): Captures the total time it takes for a data packet to traverse the network from the source device to the destination. It is important for IoT applications, where fast response times are often required, to assess whether data delivery is timely [39].
- Data Traffic Sent (bits/sec): Measures the rate at which data is transmitted from a device in bits per second. Monitoring this metric is essential to understand how much data is being sent over the network. This helps to understand network efficiency and capacity utilization [41].
- Received Data Traffic (bits/sec): Indicates how much data is successfully received per second by ZigBee devices. It helps to evaluate network reliability and packet delivery success [41].
- Throughput (bits/sec): Throughput is the actual rate of successful data transmission over the network. It represents how efficiently the network is being utilized. Throughput is a key indicator of network performance as it reflects how well the network handles data transmission under load [41].

To simulate the IoT environment, the size of the blockchain packets was represented using OPNET's packet size adjustment feature. This has been done previously in the literature [42] [43] and [44]. This assumption is based on the average packet size in the literature, which is approximately 2500 bytes [42]. This size is reflected in OPNET's packet size feature to ensure consistency with simulated blockchain packet transmissions. By adjusting certain parameters, two different scenarios were realized by simulating different network conditions and the results were compared.

4. Experiments

In order to evaluate the performance of IoT networks transmitting packets encrypted using blockchain, four scenarios are realized in pairs. The first scenario tests the operation of the network under low load, while the second scenario examines the responsiveness of the network with more devices. Increasing the number of devices is very important in evaluating the scalability of IoT applications by affecting the performance metrics accepted in the literature such as latency, data traffic and throughput.

For comparison in the scenarios, packets were transmitted directly without the blockchain and encrypted and transmitted using the blockchain. The size of the packets assumed to be encrypted using the blockchain was set to 2500bytes (see Figure 6) based on previous work [42]. The size of packets transmitted without blockchain is set to 512bytes, which is the packet size in standard wireless networks [45].

Figure 6. Blockchain-IoT environment

In the scenarios section, the network structure that transmits packets without blockchain is referred to as “standard” and the network structure that transmits packets encrypted using blockchain is referred to as “using blockchain”.

4.1. Scenario 1 and Scenario 2

In Scenarios 1 and 2, five end devices and one central ZigBee coordinator, a total of six devices were deployed using OPNET as shown in Figure 6 and Figure 7. The number of devices was chosen as five based on [46] and [47]. Because in this section, it was chosen to test the performance of the network at low device density

In scenario 1, packets are transmitted directly on the wireless network without any processing, but in scenario 2, packets are transmitted after being encrypted using blockchain.

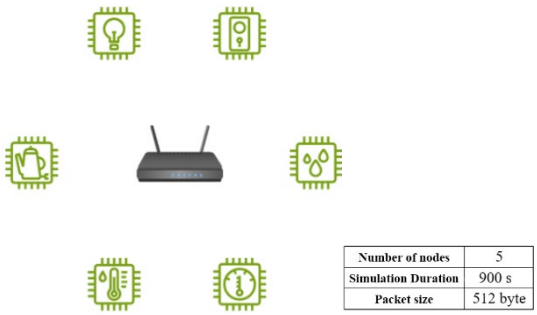


Figure 7. Topology of Scenario 1

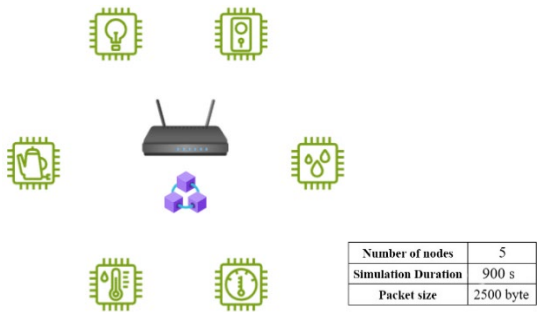
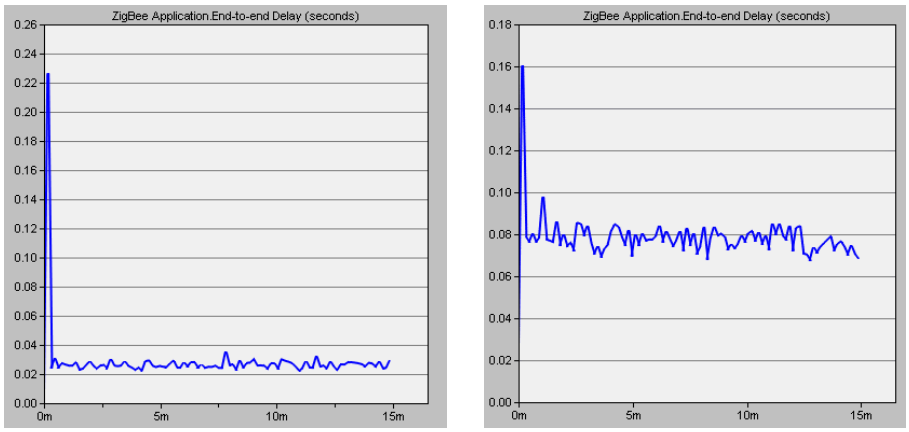


Figure 8. Topology of Scenario 2

As shown in Figure 8, in scenario 1 the end-to-end delay is between 0.02 and 0.04 seconds, while in scenario 2 it is between 0.07 and 0.10 seconds.



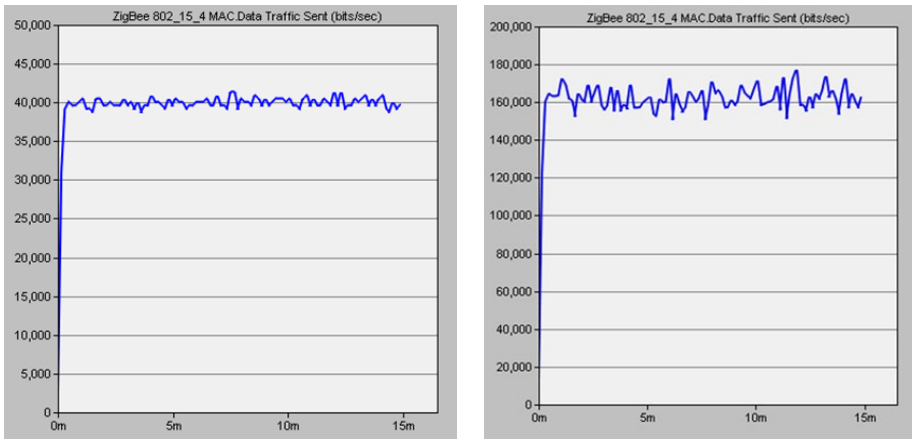
(a) (b)

Figure 9. End-to-End Delay

(a) Scenario 1 - “standard” (b) Scenario 2 - “using blockchain”

As shown in Figure 9, the transmitted data traffic varies between 39,000 bits/sec and 42,000 bits/sec in scenario 1. In scenario 2, these values vary between 150,000 and 180,000 bits/s.

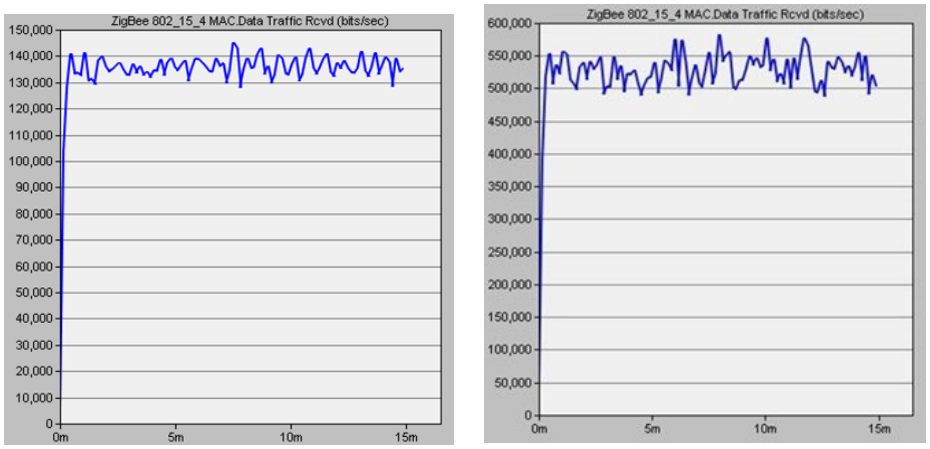
As seen in Figure 10, the received data traffic varies between 130,000 bit/s and 145,000 bit/s in scenario 1. In scenario 2, the received data traffic varies between 500,000 bit/s and 600,000 bit/s.



(a) (b)

Figure 10. Data Traffic Sent

a) Scenario 1 - “standard” (b) Scenario 2 - “using blockchain”

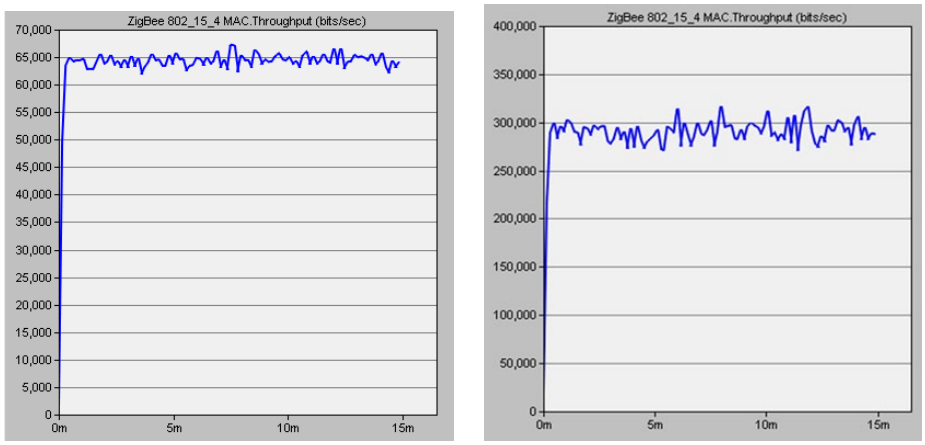


(a) (b)

Figure 11. Received Data Traffic

a) Scenario 1 - “standard” (b) Scenario 2 - “using blockchain”

As shown in Figure 11, the throughput fluctuates between 63,000 bits/sec and 68,000 bits/sec in scenario 1. In scenario 2, the throughput fluctuates between 270,000 and 320,000 bits/sec.



(a) (b)

Figure 12. Throughput

a) Scenario 1 - “standard” (b) Scenario 2 - “using blockchain”

4.2. Scenario 3 and Scenario 4

In Scenarios 3 and 4, as shown in Figure 12 and Figure 13, the network complexity is increased by adding 24 more devices, bringing the total to 29. The choice of the number of devices was based on [46] and [47] and was chosen as 29. This is because it is chosen in this section to test the performance of the network at medium device density.

In scenario 3, packets are transmitted directly on the wireless network without any processing, but in scenario 4, packets are transmitted after being encrypted using blockchain.

In these scenarios, the packet size is set to 2500bytes for packets encrypted using blockchain and 512bytes for standard packets, as in the first two scenarios.

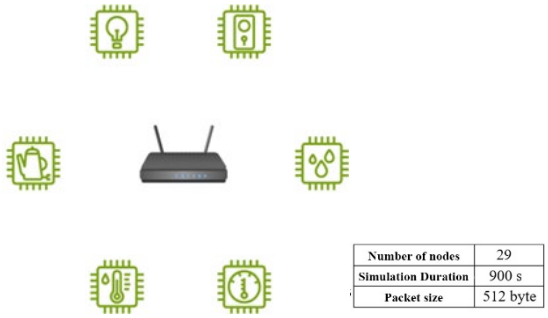


Figure 13. Topology of Scenario 3

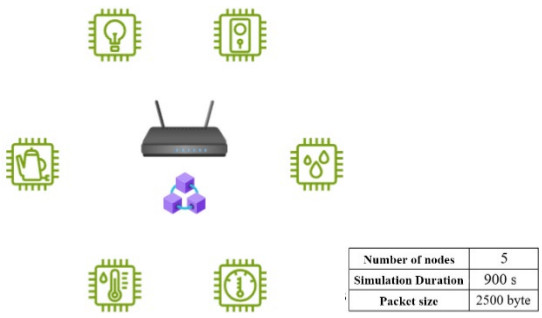
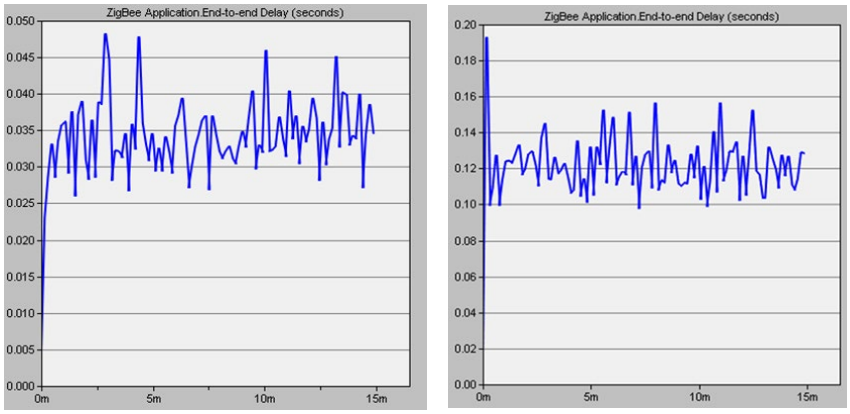


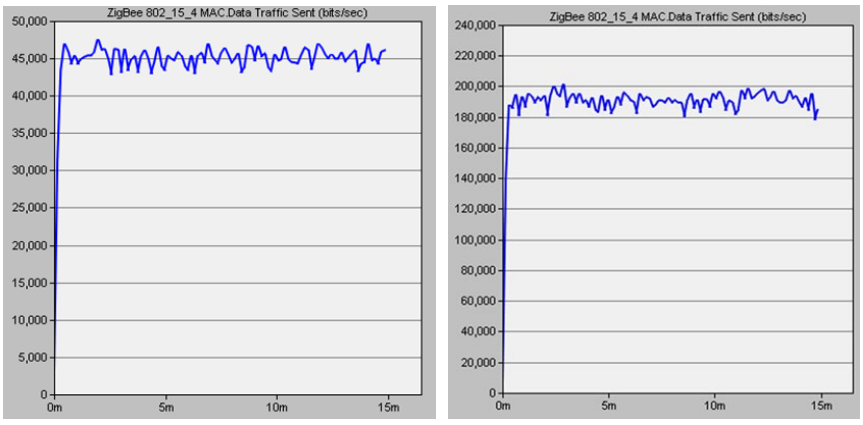
Figure 14. Topology of Scenario 4



(a) (b)

Figure 15. End-to-End Delay

a) Scenario 3 - “standard” (b) Scenario 4 - “using blockchain”



(a) (b)

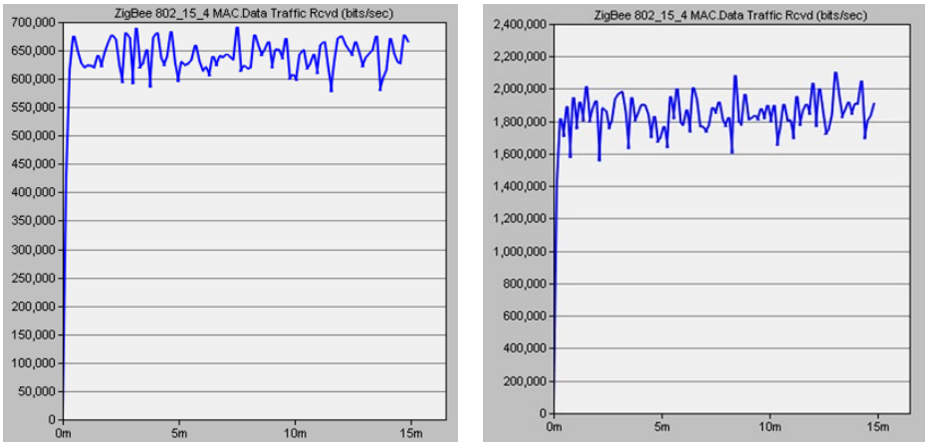
Figure 16. Data Traffic Sent

a) Scenario 3 - “standard” (b) Scenario 4 - “using blockchain”

In Figure 14, the end-to-end delay fluctuates between 0.026 and 0.048 seconds in scenario 3. In scenario 4, it fluctuates between 0.10 and 0.16 seconds.

As shown in Figure 15, the transmitted data traffic varies between 43,000 bits/sec and 47,000 bits/sec in scenario 3. In scenario 4, this value varies between 180,000 and 200,000 bits/s.

As shown in Figure 16, the received data traffic varies between 560,000 bit/s and 700,000 bit/s in scenario 3. In scenario 4, this value varies between 1,600,000 bit/s and 2,100,000 bit/s.

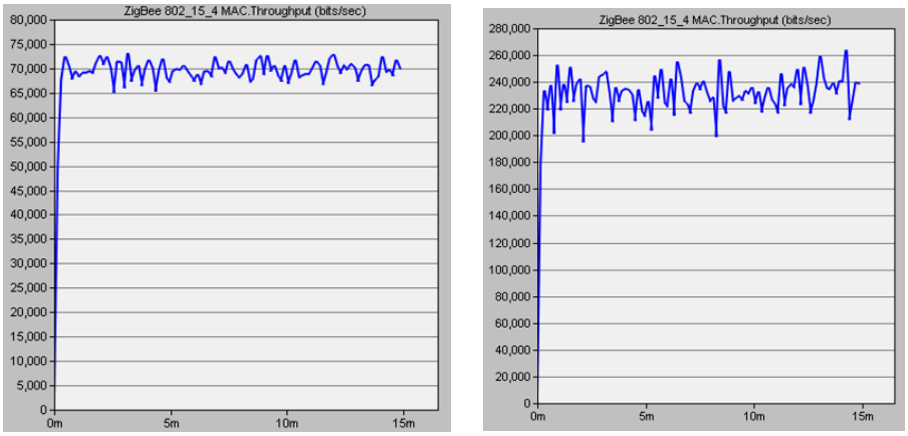


(a) (b)

Figure 17. Received Data Traffic

a) Scenario 3 - “standard” (b) Scenario 4 - “using blockchain”

As shown in Figure 17, throughput varies between 65,000 bits/sec and 73,000 bits/sec in scenario 3. In scenario 4, the throughput varies between 200,000 bits/sec and 260,000 bits/sec.



(a) (b)

Figure 18. Throughput

a) Scenario 3 - “standard” (b) Scenario 4 - “using blockchain”

4.3. Performance Evaluation

The main purpose of the scenarios is to compare the security and performance of packets transmitted directly without blockchain and encrypted and transmitted using blockchain in IoT networks. Blockchain offers an inherently secure system [48]. The security, integrity and confidentiality of the data are secured by the blockchain. However, these security features create some overhead in the performance of the network.

In the first two scenarios, the network that transmits packets encrypted using blockchain is compared with the network that transmits packets without blockchain using a small number of devices. In the first scenario, the networks transmitting packets without blockchain outperformed the networks transmitting packets without blockchain in terms of end-to-end delay, data sent and received, and throughput. For example, the end-to-end delay fluctuated between 0.02 and 0.04 seconds in scenario 1, while it fluctuated between 0.07 and 0.10 seconds in scenario 2 for networks transmitting packets encrypted using

blockchain. Similarly, the data traffic sent varied from 39,000 bits/sec to 42,000 bits/sec in scenario 1 to 150,000 to 180,000 bits/sec in scenario 2.

In scenarios 3 and 4, the number of devices increased, and tests were performed with 29 devices in total. In Scenario 3, the end-to-end delay for networks transmitting packets without blockchain was between 0.026 and 0.048 seconds, while in Scenario 4, the delay for networks transmitting encrypted packets using blockchain was between 0.10 and 0.16 seconds. The data traffic sent and received increased substantially with more devices. In scenario 3, the received data traffic ranged from 560,000 bits/sec to 700,000 bits/sec, while in scenario 4 it ranged from 1,600,000 bits/sec to 2,100,000 bits/sec. This shows that networks transmitting packets encrypted using blockchain generate more data overhead. Similarly, throughput is also higher for networks transmitting packets without blockchain, fluctuating between 65,000 bits/sec and 73,000 bits/sec in scenario 3 and between 200,000 and 260,000 bits/sec in scenario 4.

As a result of these evaluations, it can be seen that networks that transmit packets encrypted using blockchain technology have some disadvantages in terms of performance despite their security advantages. However, in applications where the need for security is critical, the use of blockchain in transmitted packets can be preferred as a secure solution. Table 5 presents a comparison of the four scenarios in terms of key performance metrics.

Table 5. Comparison of Four Scenarios

Metric	**Scenario 1** "standard"	**Scenario 2** "using blockchain"	**Scenario 3** "standard"	**Scenario 4** "using blockchain"
Number of nodes	5	5	29	29
Simulation Duration	900 sec	900 sec	900 sec	900 sec
Packet size	512 bytes	2500 byte	512 bytes	2500 byte
End-to-end delay (average)	0,03 sec	0,08 sec	0,035 sec	0,12 sec
Data traffic sent (average)	40.000 bit/ sec	160.000 bit/ sec	45.000 bit/ sec	190.000 bit/ sec
Data traffic received (average)	137.000 bit/ sec	525.000 bit/ sec	650.000 bit/ sec	1.800.000 bit/ sec
Throughput (average)	64.000 bit/ sec	280.000 bit/ sec	68.000 bit/ sec	230.000 bit/ sec

5. Discussions and Conclusion

In this study, blockchain technology is used to improve IoT security. The process involves setting up a blockchain network, using IoT transactions through simulation, and verifying the results using real-world inspired scenarios. The practical potential of blockchain in IoT environments is to perform actions such as authenticating users, registering, adding and retrieving object records. This secure, decentralized approach strengthens data integrity, making it an ideal solution for IoT systems where sensitive information is frequently exchanged.

One of the findings of the effective use of blockchain is that it ensures transparency and traceability of data. In an IoT environment where devices communicate autonomously, ensuring data accuracy and preventing loss is critical. Blockchain's role as an immutable ledger for these interactions lays a strong foundation for secure IoT networks. Furthermore, the ability to retrieve transaction histories and exchange ownership records in a secure and authenticated manner supports the system's utility in sectors such as logistics, smart cities and connected devices.

In future work, the findings suggest that blockchain has great potential in improving IoT security. However, additional research and testing in more diverse settings is necessary to fully unlock its benefits. Developing a more efficient simulation model and incorporating real-world IoT data and conditions would allow for better performance evaluations. In addition, incorporating machine learning or AI-based approaches to further optimize the network's response to dynamic conditions in IoT networks could increase its applicability.

In conclusion, the combination of blockchain and IoT is advancing the field by offering robust security mechanisms and assurance of data integrity. With further optimization and scalability considerations, blockchain-enabled IoT systems could become the industry standard for secure device communication, data management and automated decision-making.

References

[1] "How Many IoT Devices Are There (2024-2032)." Accessed: Jul. 22, 2024. [Online]. Available: https://www.demandsage.com/number-of-iot-devices/

[2] D. Miorandi, S. Sicari, F. De Pellegrini, and I. Chlamtac, "Internet of things: Vision, applications and research challenges," *Ad Hoc Networks*, vol. 10, no. 7, pp. 1497–1516, Sep. 2012, doi: 10.1016/J.ADHOC.2012.02.016.

[3] A. Zanella, N. Bui, A. Castellani, L. Vangelista, and M. Zorzi, "Internet of things for smart cities," *IEEE Internet Things J*, vol. 1, no. 1, pp. 22–32, Feb. 2014, doi: 10.1109/JIOT.2014.2306328.

[4] I. Lee and K. Lee, "The Internet of Things (IoT): Applications, investments, and challenges for enterprises," *Bus Horiz*, vol. 58, no. 4, pp. 431–440, Jul. 2015, doi: 10.1016/J.BUSHOR.2015.03.008.

[5] L. Woetzel, J. Remes, B. Boland, and K. Lv, "Smart city technology for a more liveable future | McKinsey," Jun. 2018. Accessed: Sep. 13, 2024. [Online]. Available: https://www.mckinsey.com/capabilities/operations/our-insights/smart-cities-digital-solutions-for-a-more-livable-future

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," *Computer Networks*, vol. 76, pp. 146–164, Jan. 2015, doi: 10.1016/J.COMNET.2014.11.008.

[7] HP, "Internet of Things Research Study," 2014.

[8] C. Kolias, G. Kambourakis, A. Stavrou, and J. Voas, "DDoS in the IoT: Mirai and other botnets," *Computer (Long Beach Calif)*, vol. 50, no. 7, pp. 80–84, 2017, doi: 10.1109/MC.2017.201.

[9] R. H. Weber and E. Studer, "Cybersecurity in the Internet of Things: Legal aspects," *Computer Law and Security Review*, vol. 32, no. 5, pp. 715–728, Oct. 2016, doi: 10.1016/J.CLSR.2016.07.002.

[10] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016, doi: 10.1109/ACCESS.2016.2566339.

[11] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008, Accessed: Sep. 13, 2024. [Online]. Available: www.bitcoin.org

[12] 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.

[13] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, pp. 173–190, Nov. 2018, doi: 10.1016/J.FUTURE.2018.05.046.

[14] A. Bahga, V. K. Madisetti, A. Bahga, and V. K. Madisetti, "Blockchain Platform for Industrial Internet of Things," *Journal of Software Engineering and Applications*, vol. 9, no. 10, pp. 533–546, Oct. 2016, doi: 10.4236/JSEA.2016.910036.

[15] 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.

[16] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, pp. 557–564, Sep. 2017, doi: 10.1109/BIGDATACONGRESS.2017.85.

[17] E. Androulaki *et al.*, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," *Proceedings of the 13th EuroSys Conference, EuroSys 2018*, vol. 2018-January, Jan. 2018, doi: 10.1145/3190508.3190538.

[18] A. de Vries, "Bitcoin's Growing Energy Problem," *Joule*, vol. 2, no. 5, pp. 801–805, May 2018, doi: 10.1016/J.JOULE.2018.04.016.

[19] 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.

[20] 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.

[21] 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.

[22] 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.

[23] 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.

[24] 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.
[29] 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.
[30] 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.
[31] 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.
[32] 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.

Conflict of Interest Notice
Authors declare that there is no conflict of interest regarding the publication of this paper.

Ethical Approval and Informed Consent
It is declared that during the preparation process of this study, scientific and ethical principles were followed, and all the studies benefited from are stated in the bibliography.

Plagiarism Statement
This article has been scanned by iThenticate ™.