Design and Development of an IoT-Blockchain Platform for Reliable Sensing Data Management

Abdul Nashar[1], Joko Tri Brata[1] and Arkan Adnan Imran[2]
[1]*Department of Government Science, Universitas Sulawesi Tenggara, 93126 Kendari, Indonesia*
[2]*Department of Computer Technique Engineering, Dijlah University College, 10021 Baghdad, Iraq*
abdulnashar@un-sultra.ac.id, djokotribrata@un-sultra.ac.id, engarkana@gmail.com

Keywords: IoT-Blockchain Platform, Data Integrity, Smart Contracts, Sensor Data Management, Decentralized Security.

Abstract: This paper presents an IoT-Blockchain platform to ensure reliable sensor data management in IoT systems. By integrating blockchain technology, the solution enhances data security, transparency, and decentralization, addressing vulnerabilities inherent in centralized architectures. Blockchain's immutability and decentralized nature enable secure data sharing, foster stakeholder trust, and automate processes via smart contracts. The study evaluates key performance metrics, such as device registration time, sensing data storage efficiency, and query execution speed, demonstrating the platform's superiority over existing blockchain systems. Results highlight its robustness in real-time data handling, scalability, and auditability. The proposed framework showcases the transformative potential of combining IoT and blockchain, offering a trustworthy infrastructure for applications like smart cities, supply chains, and industrial automation. Ultimately, this work underscores how decentralized architectures can revolutionize IoT data management, ensuring integrity while optimizing operational efficiency. The research underscores blockchain's role in overcoming IoT security challenges while enabling next-generation decentralized and auditable data ecosystems.

1 INTRODUCTION

As the Internet of Things (IoT) expands, many devices become connected, generating a vast amount of
data [1]. It is important to recognize, however, that this growth comes with significant challenges in terms of data integrity, security, and reliability. While this growth is significant, there are also significant challenges associated with it, including security, integrity, and reliability of data. Despite this growth, data integrity, security, and reliability continue to pose significant challenges. A decentralized, secure, and transparent environment can be provided by integrating blockchain technology with IoT to overcome these limitations [2]. This paper introduces a blockchain-based IoT platform designed to ensure reliable sensor data management. Since blockchain technology was initially recognized for its role in cryptocurrencies, some of its inherent security properties, such as immutability, decentralization, and transparency, have gained interest across a wide range of industries. As a data integrity enhancement in IoT, blockchain can ensure unaltered and reliable sensor data and transactions by creating a tamper-proof record. Integration of IoT and blockchain not only addresses security concerns, but also enables new functionalities, such as secure data sharing, improved trust among stakeholders, and automated processes through smart contracts [3].

Internet of Things (IoT) combined with blockchain technology is one promising solution for handling data integrity, security, and transparency challenges in the digital age. A wide range of sectors, including healthcare, smart cities, agriculture, and industrial automation, are increasingly deploying IoT systems that collect and exchange data. The Internet of Things allows for the monitoring of vast quantities of sensory data in real-time, but data management and trustworthiness remain significant challenges.

Cyberattacks and lack of transparency are common problems associated with IoT data

management. Also, it is imperative to ensure accuracy and reliability when it comes to data, especially when monitoring the environment and providing healthcare. In order for IoT to be widely adopted, data collected by IoT sensors must be accurate, secure, and accountable. Technology based on IoT can be used to create smart homes, smart transportation systems, or smart manufacturing systems, for example [4]. Technology innovations in embedded computing and networking have made it possible to create large-scale autonomous IoT systems [5]. Data produced and exchanged in the IoT system is widely regarded as being both safety-critical and privacy-sensitive. This makes the network more important than ever. Cyberattacks are particularly problematic due to the unattended nature of wireless sensor networks [6]. An IoT solution currently connecting to cloud servers is centralized. The elastic computation and data management capabilities of this solution are excellent, but there are still some security concerns. The Internet of Things infrastructure is susceptible to single points of failure. To ensure the security of IoT devices, a tamper-proof environment and a fault-tolerant network are required [7].

For the access control of IoT devices, researchers are investigating using blockchain technology as a decentralized technology, which could be more suitable [8]. Data from multiple sources is tracked, verified, executed, and stored using a distributed database, which is composed of numerous peers. A number of high-level use cases have already been developed to illustrate this idea, including intelligent transportation systems [9], medical record-keeping systems, decentralized web applications, and prediction systems. The benefits of blockchain technology include high transparency, high security, better traceability, low costs, and the absence of third parties [10].

Decentralized, immutable, and transparent ledger systems like blockchain have gained traction as robust solutions to these issues. Data integrity, traceability, and security can be ensured through blockchain technology, as well as data management and validation through IoT. In addition to improving the reliability of data, this combination of IoT and blockchain can also create a secure, automated, distributed, and distributed data management ecosystem. Using blockchain technology, the proposed platform ensures the authenticity and security of IoT data by leveraging its data immutability and decentralized consensus functions. Smart contracts are also implemented on the platform to automate processes, enabling real-time decision-making and enhanced data tracking. It is our goal to develop a method for managing data from the Internet of Things that is scalable, secure, and efficient, with applications across various industries dependent upon accurate and trustworthy data.

2 LITERATURE REVIEW

Because of its robust security features, blockchain has become increasingly popular as a platform for sharing IoT data. In [11], "Sensor-Chain" is described as a lightweight, scalable and secure blockchain framework designed to support Internet of Things applications. It is becoming increasingly difficult for IoT sensor devices to scale as blockchain chains grow in size. A potential solution is presented in this paper for improving mobile IoT device integration with blockchain technology. IoT devices have diverse capabilities, and even with efficiency gains, balancing the framework will be difficult.

A study showed that IoT devices and their interactions with services could be managed computationally trust through blockchain technology and reputation management systems [12]. The reward-penalty mechanism is used to establish trust architecture. It is possible that the proposed reward penalty system may be difficult to implement and maintain in spite of its promise. A user's security and costs need to be considered. Among the algorithms proposed in [13] include Proof of Authentication (PoA) and Proof of Work (PoW), which are suitable for edge computing and IoT setups with limited resources. Despite addressing efficiency concerns associated with PoW, PoA may have some limitations due to its specific authentication mechanisms [14]. Despite the reported latency of 3s, certain real-time applications might still be adversely affected. The importance of understanding how algorithms trade off performance and latency cannot be overstated.

According to the author, it implements a lightweight consensus protocol for Internet of Everything (IOE) environments. Power-intensive consensus algorithms are replaced by simple, easy-to-use algorithms that address the resource limitations of IoT devices. Due to the increasing number of IoT devices, 148.89 ms of latency can have a negative impact on performance and efficiency [15].

With the introduction of Wireless Sensor Networks (WSNs), a new authentication protocol was introduced. Data security in environments with resources and potentially distrustful actors is a primary objective of this project. Blockchain's security features are taken advantage of in this

protocol, but sensor nodes may feel overburdened as a result. In a similar report, WSN found that blockchain technology improved IoT data management and security. The architecture offers several advantages, including distributed storage of data, immutability, decentralization, and traceability. As a result of the architecture, data storage is distributed, mutable, decentralized, and traceable [16].

Data is collected and exchanged by physical devices through sensors, software, and networks in the Internet of Things [17]. Sensors, industrial machines, sensors, and controllers are all interconnected to automate, monitor, and make decisions across various domains using interconnected devices. Data generated by IoT devices creates a great deal of opportunity for innovation and efficiency because of the proliferation of these devices.

Transactions are recorded securely, transparently, and immutably using blockchain technology. Peer-to-peer ledgers ensure no single entity owns the ledger since each participant keeps a copy [18]. Cryptographic hash functions ensure data integrity along with consensus mechanisms on blockchains [19].

3 METHODOLOGY

Every block on a blockchain is time stamped, and every participant maintains it. Transactions are aggregated in blocks. Each block in a blockchain is cryptographically linked to the previous block by a hash value computed using the previous block's digital signature. Unlike traditional data storage systems, blockchain data is immutable: it can only be added at the end of a chain, so transactions cannot be modified once they are in place. A third-party authority does not need to be consulted to trust the occurrence of transactions. Historical transaction chains are immutable, providing non-reputability. Digital signatures and cryptography are used to protect the blockchain, verify identity, and control access. Originally, blockchains were used to record monetary transactions and were introduced by Bitcoin. Blockchains of the second generation provide a general, programmable infrastructure that stores computation results in a public ledger.

A smart contract [20] is an autonomous program that runs across a blockchain. It is possible to define entire business processes using smart contracts, including triggers, conditions, and conditions. Escrow services with smart contract capabilities can, for example, hold funds until smart contract obligations have been met. In Ethereum, smart contracts are considered to be first-class elements of a second-generation blockchain. Thus, the blockchain is an immutable, decentralized, auditable, and completely decentralized technology. Automated program execution could be implemented with blockchain smart contracts.

3.1 Peer-to-Peer File System

Globally distributed file systems have been the subject of extensive research. System success has been seen in some cases, while failure has been seen in others. A total of over 100 million simultaneous users are supported by Napster, KaZaA, and BitTorrent in the industry. There is currently a push towards developing decentralized, global, and low-latency file systems. There is no doubt that peer-to-peer (P2P) schemes were conceived to replace the client-server model, which was implemented to support small, distributed environments with more powerful servers. Synchronous communication is the primary characteristic of peer-to-peer networks. A peer can serve as a client as well as a client. Files can be shared between clients and servers using P2P systems. Peers are able to communicate directly through it. Rather than all requesting files from the server simultaneously, peers can share files in pieces. As a result, sharing files has become much more efficient and scalable.

3.2 Blockchain Architectural Design Considerations

An immutable, replicated, and synchronized distributed ledger (DLT) based on P2P architecture between untrusted parties can be defined as blockchain [21], [22]. As part of the consensus protocol, miners verify and validate data and identities for transactions. Traditionally, blockchain technology has been used for digital currencies; however, it is increasingly being integrated into IoT solutions [23], [24]. Integrated with IoT, blockchain provides efficient mechanisms for identifying nodes, safeguarding authentication and communication, securing distributed storage, and securing resources. Several industries can benefit from a combination of blockchain and IoT, including SC, agriculture, healthcare, smart grids, smart homes, and automotive.

3.3 Evaluate the Conceptual Model

After the conceptual model has been developed, it is evaluated by an expert focus group. This process could include presenting the model to a group of experts and getting their feedback, insights, and suggestions. To develop the simulation environment, the conceptual model can be refined and improved based on the feedback gained during this process. It is crucial to establish clear objectives for this evaluation. Our objectives were evaluated using SMART criteria in order to determine their feasibility and
effectiveness [25]. As a result, our objectives are specific, measurable, attainable, relevant, and time-bound. To validate our conceptual model, we conducted an expert survey and focus group with ten experts in the blockchain and IoT fields. Evaluation of the conceptual model was conducted using both approaches. The conceptual model took into account the needs of all relevant stakeholders by engaging experts and collecting their feedback.

3.4 The Proposed Blockchain-Connected Gateway

An illustration of the BC gateway architecture can be found in Figure 1 of this document. Using blockchain accounts, the BC gateway identifies users and preferences. Users do not have to register for every BC gateway individually. They can connect to multiple BC gateways simultaneously using the same account. The Android and IOS platforms now support the Bluetooth Low Energy specification, which has become the de facto standard for smartphones when it comes to communicating with IoT devices and wearable's. Researchers examine the case of a user accessing nearby BLE-enabled devices. BLE gateways provide REST-like interfaces for accessing BLE-based devices, according to current state-of-the-art:

- Devices can be locked/unlocked using Bluetooth Low Energy.
- Explore the gateways' connected devices and the services they offer.
- Invoke a BLE device's characteristic by sending read or write requests.
- A BLE device displays certain characteristics when notified.

IoT devices connected to BC gateways will remain connected. A gateway can act as an intermediary that forwards requests to specific devices and integrates their responses. BC gateways are also able to manage privacy preferences for IoT devices by providing interfaces for privacy preferences.

Device administrators can register devices with BC gateways by following the steps in Figure 2. The administrator creates a smart contract for an IoT device by creating a transaction to store information about the device and its privacy policies.

3.5 Device Binding

A Device Manager containing the addresses of the devices as well as privacy policies can then be created by the administrator. A device's Device Manager can provide information about the device and its privacy policies, as illustrated in Figure 2. Users can also listen to device update events.

Device Managers allow device administrators to obtain smart contract addresses. A device administrator can then provide a gateway administrator with the address of a device. Gateway administrators can request the binding of devices to BC Gateway Managers by providing the Device Manager's address.

3.6 Smart Contract Component

Decentralized data access control is a feature of Ethereum smart contracts since they are executed on the blockchain. Unlike smart contracts, which store data for free, blockchains store only hashes of data. Main data is stored and encrypted using SGX. In a smart contract, user and device registration are all included, as well as read/write access policies.

3.6.1 User Registration

User registration is facilitated by this module, which makes use of Ethereum user registration system. An Ethereum user generates a pair of public and private keys in order to identify themselves on the network. In smart contracts, devices can be registered, and data can be accessed using a private key.

3.6.2 Device Registration

The identifier for the IoT device can be provided by authenticated users when registering their devices. In smart contracts, user-owned devices are mapped to an owner's address on the blockchain (the owner's address = a list of the device's identifiers).

3.6.3 Access Policies for Writing Data

Data wished to be stored on the blockchain must be submitted by the device with the owner's address and

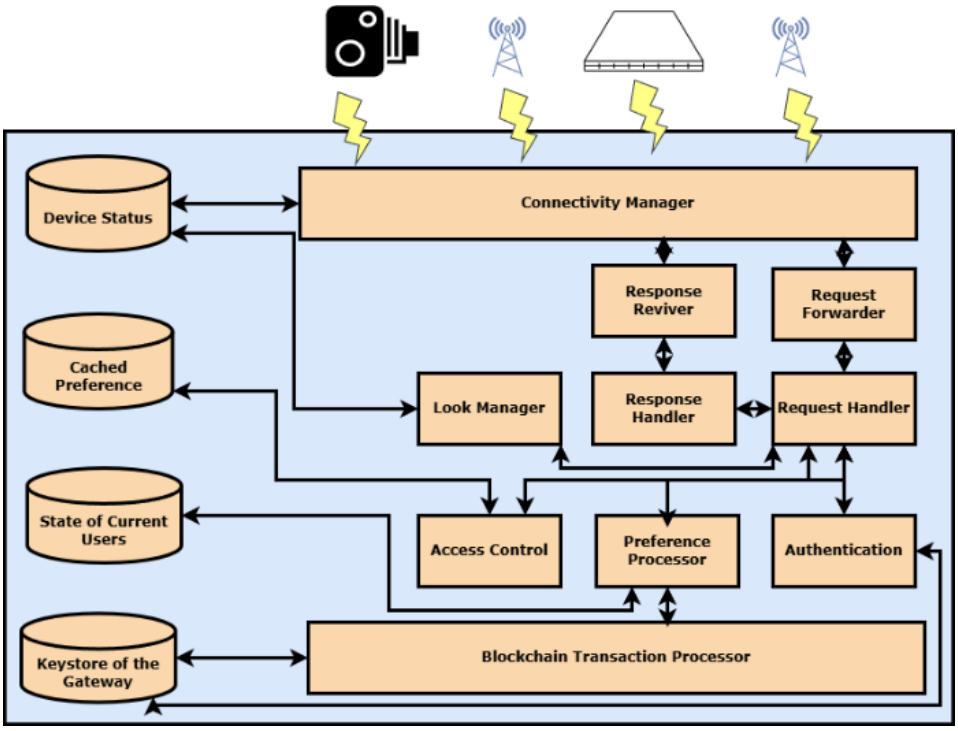

Figure 1: The architecture of a BC gateway.

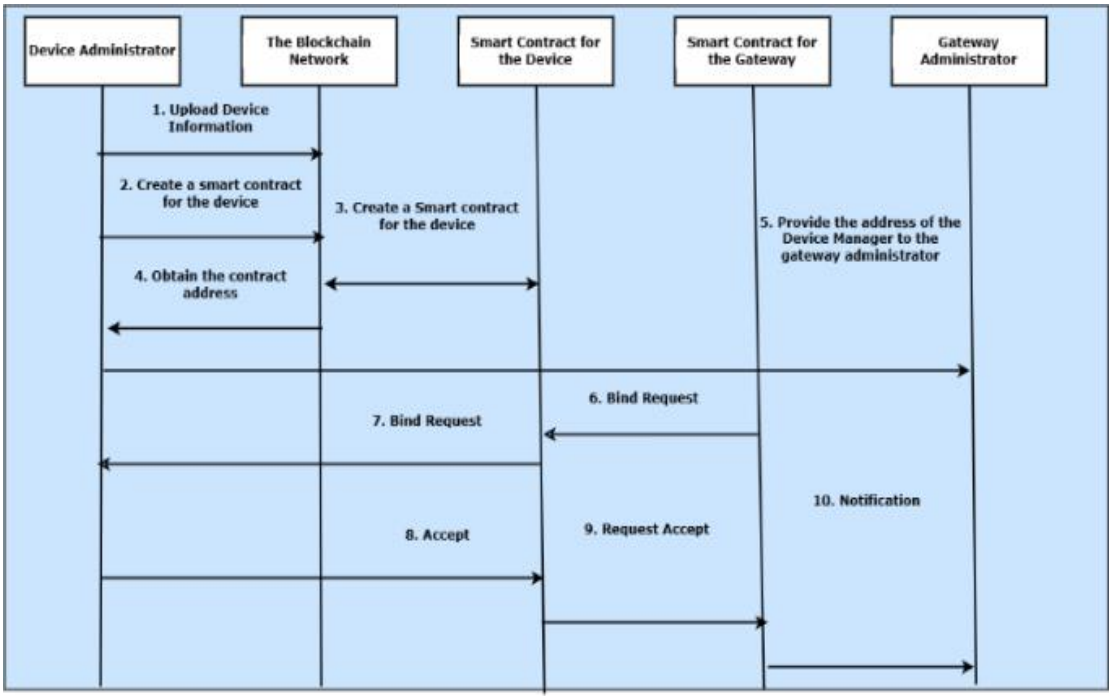

Figure 2: The device registration process.

the device's ID associated with it. A combination of owner address and device ID can allow us to uniquely store all data related to each device as shown in [(owner address, device ID) = list of device data]. A hash map consists of a list of hashes generated by devices. To allow data to be written to the contract, the smart contract verifies that the owner's address matches the ID of the device. The contract can only be written by the device owner.

3.6.4 Device Data Read Access Policy

It is the responsibility of the device owner to grant permission to unauthorized third parties wishing to access a device's data. As part of the request, we will need to know the user's address and device ID. Throughout smart contracts, keys and values are stored as a hash map consisting of the address of the device owner, the identifier of the device, and the list of users of the device. Using this formula, we have (owner, device id, third-party address) = bool access). Using hash maps, only registered third parties are granted access to data by checking if the requesting user is authorized to access it.

4 RESULTS AND DISCUSSION

Figure 3 shows the results of a study examining service execution time costs associated with device registration. This experiment registered 50, 150, 250, and 500 devices with the proposed platform. Using Hyperledger [26], the simulation recorded two minimums and a maximum for 50 devices: 2260 ms for the minimum, 2284 ms for the average, and 2373 ms for the maximum. The minimum and average times for 150 devices were 2255 ms, 2333 ms, and 2800 ms, respectively. The minimum time taken by the 250 devices was 2252 milliseconds, the average time was 2583 milliseconds, and the maximum time was 3002 milliseconds. Lastly, we found that the minimum time recorded was 2265 milliseconds, the average time was 2921 milliseconds, and the maximum time was 4011 milliseconds for the 500-device group.

The second study investigated the time required to process sensing data on a blockchain network. Using HTTP clients, each device could access the REST server to request sensor readings. REST servers retrieve execution results from blockchains and return them to devices after appending sensing data. According to Figure 4, sensor reading transactions take a long time to execute. A ten-fold repetition of each test was performed with multiple concurrent clients at different levels of resource utilization. Compared to well-known blockchain platforms, this proposed platform performs significantly better. The study was limited by the fact that it involved a relatively small network with only four peers.

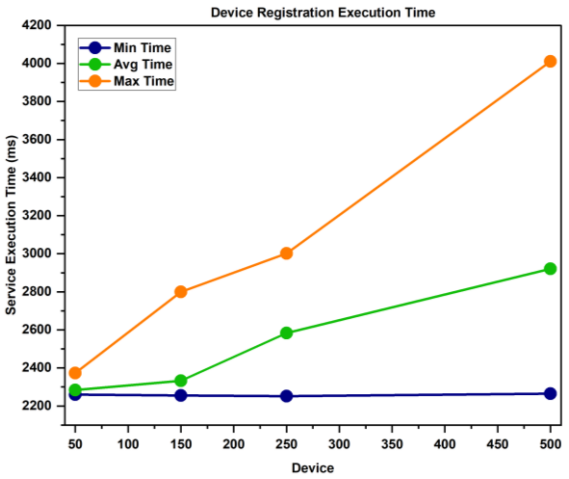

Figure 3: Analyze the performance of service execution (ms) versus no. of devices.

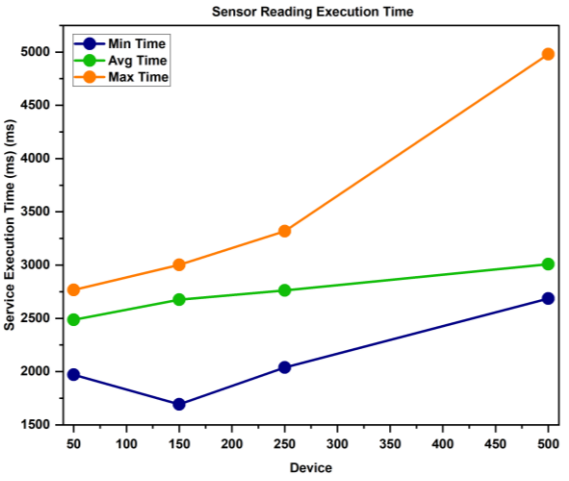

Figure 4: Sensor reading execution time (ms) versus no. of device.

A comparison of the execution time for querying data records on the blockchain is shown in Figure 5, which examines the execution time for 500 to 10,000 records of data. A random selection of 10 system resource utilization levels was used to determine the proposed platform's minimum, average, and maximum delay times for retrieving sensor records. Based on worst-case performance, the maximum delay would be 855 milliseconds with 10,000 records, the minimum delay would be 608 milliseconds, and the average delay would be 754 milliseconds.

According to the figure, the round-trip latency was greatly influenced by the size of the data records. As a result of the low increase, it was even possible to ignore the impact on the user's experience.

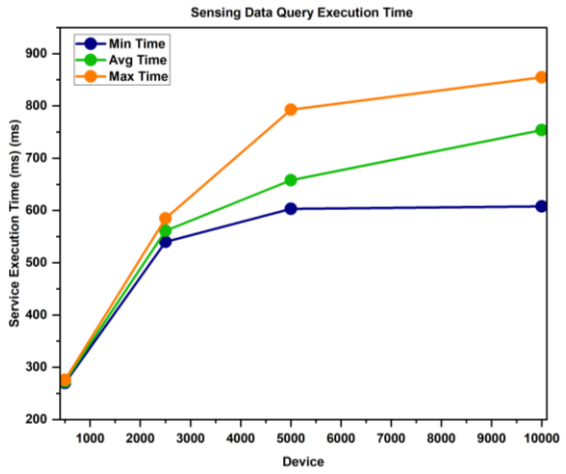

Figure 5: Sensing data execution time (ms) versus no. of device.

A comparison was made between this system and the proposed system. Simulating the environment from which the system operated [27]. It was simulated that 960 transactions would be executed in a network of 50 peers over 60 seconds. In the network, the processing time metric measures how long it takes to verify new blocks. According to Figure 6, the processing overhead was evaluated. We consistently achieved lower processing overhead than the selected method, with a number of blocks ranging from 10 to 60, as shown in the graph. A 23% reduction in processing time was achieved with the proposed approach.

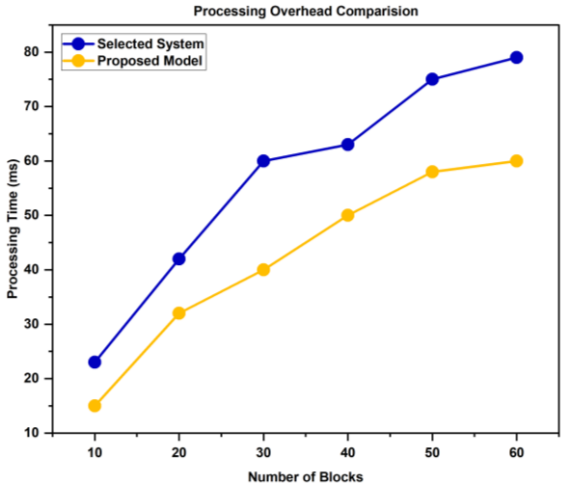

Figure 6: Processing time (ms) versus no. of blocks.

5 CONCLUSIONS

In this study, we developed an innovative IoT-Blockchain integrated platform designed to significantly enhance security, integrity, and transparency in IoT data management. Leveraging blockchain technology, the platform ensures robust data protection, providing tamper-proof mechanisms that maintain the authenticity and immutability of sensor-generated data. Performance evaluations revealed that our proposed solution registers IoT devices and transmits sensor data considerably faster and more reliably compared to traditional centralized systems. The incorporation of blockchain technology not only guarantees secure and reliable storage of data but also establishes a transparent audit trail, facilitating trustworthy data exchanges among various stakeholders. Despite these promising outcomes, the experiments conducted thus far have identified critical limitations, particularly regarding the small-scale network used in the initial testing scenarios. Consequently, there is a pressing need to optimize blockchain consensus algorithms tailored explicitly for resource-constrained IoT devices, which often have limited processing power and energy availability. As the platform matures and evolves, future work will focus extensively on scaling the network, refining consensus mechanisms for enhanced efficiency, and conducting rigorous evaluations with larger networks and diverse real-world applications. These enhancements will further validate the platform's capability to meet the increasing demands of complex IoT ecosystems and drive broader adoption in smart industries.

REFERENCES

[1] B. Bhola, E. S. B. Manjula, P. Rani, and M. H. Falaah, "Quality-enabled decentralized dynamic IoT platform with scalable resources integration," IET Commun., 2022.

[2] 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, [Online]. Available: https://doi.org/10.1109/ACCESS.2021.3129697.

[3] P. Shi, H. Wang, S. Yang, C. Chen, and W. Yang, "Blockchain-based trusted data sharing among trusted stakeholders in IoT," Softw. Pract. Exp., vol. 51, no. 10, pp. 2051–2064, Oct. 2021, [Online]. Available: https://doi.org/10.1002/spe.2739.

[4] P. Rani, S. P. Yadav, A. Singh, M. Almusawi, M. H. Falaah, and M. A. Farouni, "Federated Learning-Based Misbehavior Detection for the 5G-Enabled Internet of Vehicles," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4656–4664, May 2024,

[Online]. Available: https://doi.org/10.1109/TCE.2023.3328020.

[5] P. Rani and M. H. Falaah, "Real-Time Congestion Control and Load Optimization in Cloud-MANETs Using Predictive Algorithms," NJF Intell. Eng. J., vol. 1, no. 1, pp. 66–76, 2024.

[6] S. Sicari, A. Rizzardi, L. A. Grieco, and A. Coen-Porisini, "Security, privacy and trust in Internet of Things: The road ahead," Comput. Netw., vol. 76, pp. 146–164, Jan. 2015, [Online]. Available: https://doi.org/10.1016/j.comnet.2014.11.008.

[7] M. A. Khan and K. Salah, "IoT security: Review, blockchain solutions, and open challenges," Future Gener. Comput. Syst., vol. 82, pp. 395–411, 2018.

[8] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," IEEE Access, vol. 6, pp. 32979–33001, 2018.

[9] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in 2016 IEEE 19th International Conference on Intelligent Transportation Systems (ITSC), Rio de Janeiro, Brazil: IEEE, Nov. 2016, pp. 2663–2668, [Online]. Available: https://doi.org/10.1109/ITSC.2016.7795984.

[10] A. Singh, P. Rani, M. H. Falaah, and S. P. Yadav, "Blockchain-Based Lightweight Authentication Protocol for Next-Generation Trustworthy Internet of Vehicles Communication," IEEE Trans. Consum. Electron., vol. 70, no. 2, pp. 4898–4907, May 2024, [Online]. Available: https://doi.org/10.1109/TCE.2024.3351221.

[11] Y. Wang, M. Singgih, J. Wang, and M. Rit, "Making sense of blockchain technology: How will it transform supply chains?," Int. J. Prod. Econ., vol. 211, pp. 221–236, 2019.

[12] A. A. Battah, Y. Iraqi, and E. Damiani, "A trust and reputation system for IoT service interactions," IEEE Trans. Netw. Serv. Manag., vol. 19, no. 3, pp. 2987–3005, 2022.

[13] D. Puthal, S. P. Mohanty, P. Nanda, E. Kougianos, and G. Das, "Proof-of-Authentication for Scalable Blockchain in Resource-Constrained Distributed Systems," in 2019 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA: IEEE, Jan. 2019, pp. 1–5, [Online]. Available: https://doi.org/10.1109/ICCE.2019.8662009.

[14] P. Rani, P. N. Singh, S. Verma, N. Ali, P. K. Shukla, and M. Alhassan, "An implementation of modified blowfish technique with honey bee behavior optimization for load balancing in cloud system environment," Wirel. Commun. Mob. Comput., vol. 2022, pp. 1–14, 2022.

[15] X. Sun and N. Ansari, "Dynamic resource caching in the IoT application layer for smart cities," IEEE Internet Things J., vol. 5, no. 2, pp. 606–613, 2017.

[16] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. Challenges and opportunities," Future Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018, [Online]. Available: https://doi.org/10.1016/j.future.2018.05.046.

[17] J. Lockl, V. Schlatt, A. Schweizer, N. Urbach, and N. Harth, "Toward Trust in Internet of Things Ecosystems: Design Principles for Blockchain-Based IoT Applications," IEEE Trans. Eng. Manag., vol. 67, no. 4, pp. 1256–1270, Nov. 2020, [Online]. Available: https://doi.org/10.1109/TEM.2020.2978014.

[18] G. Pulkkis, J. Karlsson, and M. Westerlund, "Blockchain-Based Security Solutions for IoT Systems," in Internet of Things A to Z, 1st ed., Q. Hassan, Ed., Wiley, 2018, pp. 255–274, [Online]. Available: https://doi.org/10.1002/9781119456735.ch9.

[19] A. Singh, P. Rani, S. Verma, and S. P. Yadav, "Resilient wireless sensor networks in industrial contexts via energy-efficient optimization and trust-based secure routing," Peer–Peer Netw. Appl., vol. 18, no. 3, p. 132, Jun. 2025, [Online]. Available: https://doi.org/10.1007/s12083-025-01946-5.

[20] S. Omohundro, "Cryptocurrencies, smart contracts, and artificial intelligence," AI Matters, vol. 1, no. 2, pp. 19–21, Dec. 2014, [Online]. Available: https://doi.org/10.1145/2685328.2685334.

[21] L. Da Xu, Y. Lu, and L. Li, "Embedding blockchain technology into IoT for security: A survey," IEEE Internet Things J., vol. 8, no. 13, pp. 10452–10473, 2021.

[22] M. Maroufi, R. Abdolee, and B. M. Tazekand, "On the Convergence of Blockchain and Internet of Things (IoT) Technologies," J. Strateg. Innov. Sustain., vol. 14, no. 1, Mar. 2019, [Online]. Available: https://doi.org/10.33423/jsis.v14i1.990.

[23] P. Kumar, R. K. Singh, A. K. Sangaiah, M. Almusawi, P. Rani, and S. P. Yadav, "PPSF: A Privacy-Preserving and Secure Framework Using Blockchain-Based Machine-Learning for IoT-Driven Smart Cities," IEEE Trans. Netw. Sci. Eng., vol. 8, no. 3, pp. 2326–2341, Jul. 2021, [Online]. Available: https://doi.org/10.1109/TNSE.2021.3089435.

[24] J. Lindley, "Food regulation and policing: innovative technology to close the regulatory gap in Australia," J. Consum. Prot. Food Saf., vol. 17, no. 2, pp. 127–136, Jun. 2022, [Online]. Available: https://doi.org/10.1007/s00003-022-01372-2.

[25] M. R. Bataineh, W. Mardini, Y. M. Khamayseh, and M. M. B. Yassein, "Novel and Secure Blockchain Framework for Health Applications in IoT," IEEE Access, vol. 10, pp. 14914–14926, 2022, [Online]. Available: https://doi.org/10.1109/ACCESS.2022.3147795.

[26] H. Caliper, "Hyperledger Caliper," [Online]. Available: https://www.hyperledger.org/projects/caliper, [Accessed: 15 Jan 2019].

[27] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an Optimized BlockChain for IoT," in Proceedings of the Second International Conference on Internet-of-Things Design and Implementation, Pittsburgh, PA, USA: ACM, Apr. 2017, pp. 173–178, [Online]. Available: https://doi.org/10.1145/3054977.3055003.