International Journal of
INTELLIGENT SYSTEMS AND APPLICATIONS IN ENGINEERING
ISSN:2147-6799 www.ijisae.org Original Research Paper

# Leveraging Blockchain Technology for Robust Security and Privacy in Internet of Things (IoT) Systems: Challenges and Solutions

**Ghayth ALMahadin[1], Mohammad O. Hiari[2], Sumaya Alkhatib[3], Nidal Turab[4]**

**Submitted**: 06/05/2024 **Revised**: 19/06/2024 **Accepted**: 26/06/2024

**Abstract**- Supply chain management, healthcare, agriculture, smart cities, smart homes, and other industries have benefited from the real-time and sophisticated sensing capabilities that the Internet of Things (IoT) has brought to the field. This technology's intrinsic promise is highlighted by its exponential expansion across several application sectors. However, IoT has to be built on a flexible network architecture with strong support for security, privacy, and trust in order to reach its full potential. Concurrently, Blockchain (BC) technology has surfaced as a groundbreaking solution providing resilience, transparency, anonymity, decentralisation, and independent management. IoT applications raise serious security and privacy issues, and integrating IoT with BC technology is thought to be a potential way to overcome these issues. In order to improve security and privacy, this study aims to investigate the smooth integration of BC technology with IoT systems. This research suggests a revolutionary framework to guarantee safe and effective integration, which incorporates techniques like the gateway procedure and sensor devices. A range of security services within IoT systems would be enabled by the proposed architecture, which also seeks to solve current blockchain issues. This research evaluates the feasibility of many BC platforms in meeting the needs of diverse IoT applications and provides a thorough grasp of those requirements. Using the resources and data from current processes, an extra immutable ledger is produced by utilizing the benefits of blockchain technology. The findings show that blockchain considerably improves security and privacy on IoT systems, offering a reliable solution for a range of IoT applications. It is emphasized in the findings that combining BC technology with IoT not only solves current security issues but also opens up fresh and creative use-cases, eventually maximizing the potential of IoT systems.

***Keywords***- *Internet of Things (IoT), Blockchain Technology, Decentralization, Network Architecture, Data Integrity, Privacy*

## I. INTRODUCTION

The Internet of Things (IoT) has recently received widespread attention. It is not an exaggeration to say that this technology has become a part of modern society, with people, intentionally or unknowingly, using it in their daily routines. In the Internet of Things, tangible objects such as home appliances, vehicles, logistic items, infrastructure components, and so on may perceive their surroundings and interact with one another in real time [1]. Smart objects in IoT systems are typically diverse and operate under a unique administrative domain; as a result, establishing trust and maintaining security in the world of IoT is sometimes considered as a difficult task [2]. IoT devices rely on a variety of basic network infrastructure, which is vulnerable to cyber threats, as evidenced by recent cyber-attacks. Furthermore, the safety and privacy of data in IoT networks is a major concern [3]. Over the last few years, the use of blockchain has rapidly increased, spanning domains such as identity management, governance, IoT networks, financial services, and healthcare [4]. The combination of blockchain and IoT networks has immense promise in the areas of IoT device identification, authentication, sensor storage systems, and secure data transport. The promise of this convergence has fueled eagerness among researchers, academics, and industry professionals to disrupt various IoT applications as well as alleviate the previously identified shortcomings in IoT systems [5].

The main reason to develop this project is to minimize the effects of humans in technical conditions. By including blockchain in IoT the overall process becomes more efficient to use. Blockchain is a common type of technology that can enhance large sets of information in accessing order. Blockchain enables the service with the help of the crypto-currency of bitcoin. Blockchain produces a high range of bandwidth that is not suitable for all types of IoT devices. Blockchain produces some lightweight architecture that is sued to overcome the existing issues [6]. The original model of blockchain is used to process lots of information with suitable requirements by including IoT it will become more efficient. Like it is used to deliver some advanced exciting services into various sectors from social media, smart cities, etc. All the sectors used this type of approach to prevent the sensitive information of their client [7]. The blockchain

*Assistant Professor, Department of Networks and Cybersecurity, Faculty of Information Technology,*
*Al Ahliyya Amman University, Jordan[1].*
*Lecturer, Department of Networks and Cybersecurity, Faculty of Information Technology,*
*Al Ahliyya Amman University, Jordan[2].*
*Lecturer, Department of Computer Science, Faculty of Information Technology, Al Ahliyya Amman University, Jordan[3].*
*Professor, Department of Networks and Cybersecurity, Faculty of Information Technology,*
*Al Ahliyya Amman University, Jordan[4].*
*Email id: g.mahadin@ammanu.edu.jo[1], m.hyari@ammanu.edu.jo[2], sumayakh@ammanu.edu.jo[3], N.turab@ammanu.edu.jo[4]*

framework will be constant throughout the process flow model. The motivations for this paper are twofold: I to develop a comprehensive set of requirements for different categories of IoT applications, and ii) to establish an evaluation methodology to confirm the suitability of a provided blockchain platform for a specific type of application based on its identified requirements. With this in mind, the paper includes in-depth discussion of how to manage IoT devices and networks utilizing blockchain technology, with an emphasis on platforms and their appropriateness to fit into certain IoT applications, as well as the following additions. The background has been revised to include a more thorough explanation of blockchain, its features and advantages, and the blockchain-powered Internet of Things. Numerous IoT use cases have been found, and their functional and non-functional requirements have been thoroughly examined. Furthermore, some blockchain solutions have been explored to address the demands that an IoT-based system has identified. Fig 1 shows the Blockchain-based IoT system [8].

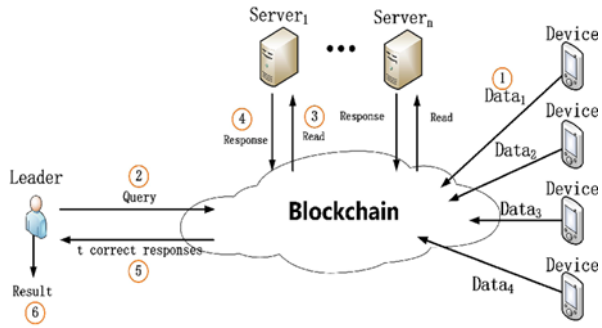


**Fig 1**. Blockchain-based IoT system

The key Contribution of this Study is as follows:

- Blockchain technology extends beyond cryptocurrency transactions, encompassing areas such as decentralized public ledgers, open-source platforms, and various industries like healthcare, supply chain management, smart assets, and the IoT.
- Utilizing cryptography, blockchain securely links blocks of data, forming an immutable chain. Anchored services ensure the integrity and security of transactions, enhancing trust in decentralized systems.
- Blockchain architecture addresses security vulnerabilities by replacing compromised sender and recipient addresses, ensuring the integrity of transactions. This enhances security in financial transactions and other exchanges.
- Blockchain maintains an immutable ledger of transactions, where each new block is added based on the consensus of the network, ensuring transparency and traceability of data.
- Blockchain technologies receive significant community support, aligning with democratic principles and global requirements for secure and transparent systems. This collaborative effort strengthens the development and adoption of blockchain solutions worldwide.

The rest of the paper are arranged as follows. Section 1 introduction is provided. Section 2 related works and Section 3 limitations of existing method. Section 4 overview for methodology. Section 5 findings and suggestions. Section 6 summary and further study.

## II. Related Works

The interest in things using the blockchain-based approach reaches its growth in the high stage. Blockchain approach of crypto-currency method like bitcoin is mingled with IoT that can enable high-security options. The connection of IoT gives some extra benefits from the process of a private immutable ledger. Bitcoin is another format that can maintain all types of network transactions. It is mainly used to solve cryptographic puzzles with the work consumption [9]. This paper list out the usage of existing blockchain protocols with the combination of IoT. Nowadays blockchain processes are used in all sectors to maintain the records safely. Quality of service plays a major role to access all types of stored data. According to bandwidth allocation memory of the total process will be carried out simply. Depending on the data management the blockchain application is divided into types private and public [10].

The smart contract is one type of program code that runs on blockchain to overcome the issues in business phase logic. It is used to delete all the unwanted types of agreements with the IoT platform. Cryptography plays a major role to access smart contracts with the help of blockchain networks to provide trustworthiness in the transaction process. Smart contracts become one of the trending technologies in the future to save sensitive information of the employees. It will save time and all processes become automated with internet connectivity. This advanced method will overcome the changes in all existing processes and provide stable requirements to allocate the contract first [11]. The overall concept of reliability in blockchain technology with IoT applications is described in this paper. The reliability concept of actions will be taken in each device. If some sector of the device because an issue means the overall process will be tested. Blockchain technology becomes more versatile because of the options like transparency, security, etc. The performance of system reliability improves as the order of factors increases. The reliability idea employs two types of logic: continuous-time Markov chain and continuous stochastic logic [12].

Identify applicable sponsor/s here. If no sponsors, delete this text box (*sponsors*).

The integrity options of the cloud are completely based on the Internet of Things because inherently is the major concept of IoT. Third-Party Auditors help to verify the public phase of audibility in framework format. In each type of framework, more forms of reliable data will be added and then accessed. This paper helps to provide all types of available protocols that are used to implement performance with the test results of existing protocols. IoT may enable lots of privacy options in the blockchain model that is used to manage the process execution of the tested results [13]. IoT technology options provide service in mobile-based applications that can manage large types of security threats in an easy manner. With the collaboration link of the network, it works efficiently. Some major changes are detailed in the IoT framework with blockchain technology. Network connectivity is applicable for all devices to transfer information to various device processes [14].

## III. Problem Statement

Every procedure in the current IoT system will be followed to safeguard user data. A few security services are included in the blockchain combo. With security providers, blockchain maintains a large amount of data, and at every stage, certain information is carried out to safeguard the users' stored data. [15]. The novel approaches would solve every problem with the current system. Consequently, it has certain extra benefits and is frequently employed in all areas. The objective of this research is to provide blockchain security for Internet of Things procedures. With the aid of various criteria and methodologies, all of the available data on this subject is being examined.

## IV. Enhancing IoT Security through Blockchain Integration

The methodology for ensuring security in IoT using blockchain technology encompasses several key steps aimed at safeguarding data, processes, and interactions within IoT systems. Initially, continuous security measures are established through the identification and monitoring of IoT zones, which are subdivided to monitor various trails and physical connections. Transition within these zones adheres to rules-based solutions, ensuring controlled access and mitigating potential security risks. The utilization of blockchain technology provides a robust foundation for enhancing security in IoT systems. Security measures such as encryption and cryptography are implemented to protect data integrity and privacy. The use of smart contracts within the blockchain framework enables the implementation of advanced security protocols and access controls for IoT applications. The methodology also involves addressing specific challenges such as securing NATted IoT devices through integration with the Ethereum blockchain [16], which facilitates secure communication and transaction processing. Dynamic access management for IoT devices is achieved through client-based modules, with future extensions planned for more sophisticated communication models using technologies like Markov models and neural networks. Moreover, the architecture-based design ensures that security considerations are integrated at each stage of the blockchain project, identifying suitable gateway options and optimizing device performance. Fig 2 depicts the proposed study framework.

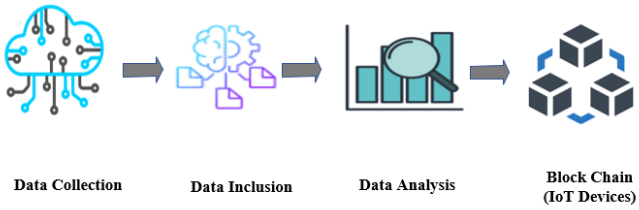


**Fig 2.** Proposed Framework

### *A. Data collection*

Data collection and types of each process encourage in each step of the blockchain and IoT process. All the processing steps follow some rules to provide an efficient process. Some important methods are carried out in detail to express the actions of the flow model. Data encryptions may alter the changes in stored data in the IoT process.

### *B. Data inclusion criteria*

The encryption type of process will be handled with suitable types of attribute methods to carry out each alteration and update of blockchain modules. Some criteria need to identify the data process. Table I shows the difference between attribute and data type.

**TABLE I.** The difference between attribute and data type

| Attribute Name | Data Type | Description |
|---|---|---|
| IoT zone | Storage | IoT zone helps to provide a large space of storage to access all the attributes that are stored in IoT. |
| Bitcoin process | Cryptography | All the internal processes of IoT are carried out with the help of a blockchain element called bitcoin which helps to process privacy options. |
| Security extraction | Security | All the security issues handle in this method and then produce exact result of the processed models. |

*C. Data Analysis*

Each process should execute some related output of the process that is extracted in each module of IoT technology with a detailed description face. In the data analysis process, all the external and internal memory allocations will be identified.

*D. Design Objectives*

For the advancement of blockchain technology extensive extension is followed in keeping with the studies to supply efficiencies, improve purchaser connections, and few imaginative objects supply comprehensively. Exchange, management, and kind of accurate approximately anchored trading give are used in the blockchain era. To distinct businesses, guidelines and information are greater inside the budgetary that is processed by using underlying innovation for buildup and bitcoin for blockchain utility of requirements. Blockchain and studies development is immensely assisted to recommend the evaluation of blockchain thoughts. Research hope, limitations, benefits, and operating precept concerning blockchain is special with stable superior safety features and characteristics concerning concurrencies, obligation, and incite contracts by way of blockchain offers. Cloud improvement and the internet of things are collaborated with quicker becoming a member of, closer client associations, and swifter element advancements regard chains to allow blockchain plan. Money scale is shaped digitally with essential management of blockchain a good way to allow for new popularity. All types of possibilities are explained in detail manner in the topic of blockchain technology usage in IoT platforms. User information or any other process if stored in IoT means it will be secure. Blockchain acts as the backbone of IoT technology in this project because all the internal types of processes are handled with efficient order because of the presence of blockchain. By involving some additional benefits, it will be used widely in all types of sectors that need to prevent the process with the security procedure.

*E. NATted IoT device by Ethereum blockchain*

In this paper, some important types of software methods are used in the platform of the distributed system like wallet types of functions that are processed in the network functions act as servers in this platform with the help of IoT device of blockchain storage. The smart contract is one type of advanced model to access all the IoT applications with the help of a blockchain process [17].

*F. Dynamic access for IoT device*

IoT client-based module allocates all types of IoT device configuration with a random blockchain process flow model of communication parties. This method future extends into the Markov model and neural network types. After the identification method, IoT tokens need to generate and validated. This method is mostly used in all types of wireless sensor types and smart contract types [18].

*G. Blockchain system with secure IoT process*

Architecture-based design exists in each step of the blockchain project. By using this method all the available architecture frameworks for the smart access process will be identified with possible gateway options. The legal sensor process helps blockchain to progress the device performance [19].

## V. RESULTS AND DISCUSSION

The blockchain model is a trending technology that helps to manage the changes and updating of the process and also protect the stored information. Some existing concepts of blockchain are used in various techniques to prevent stored data. Compare to other concept IoT use all forms of blockchain in a more efficient form. Both technologies used widely in today's world by the combination of the process will provide more security types of options compared to other technology. Figure 3 shows the Identification of Transaction Count.

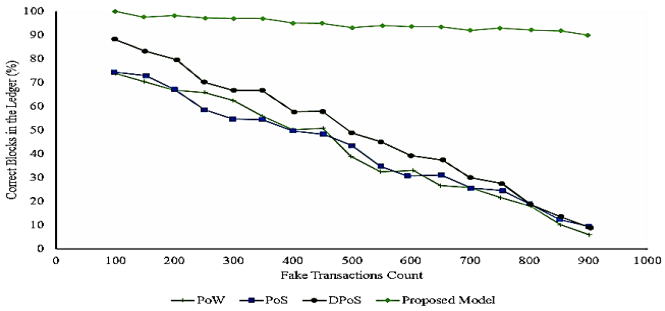


**Fig. 3**. Identification of Transaction Count.

Encryption details are focused on transparent services due to blockchain. To the general public, unreadable encryption offerings are made in blockchain to look at the context. WannaCry ransomware assault is encoded depending upon the encryption practice. A symmetric secret is generated as randomly that ought to be encrypted about the password. Different sorts of keys are generated that will be complicated to hack. The entire garage method is finishing the present-day blockchain. Depending upon the blockchain generation password retaining device is added because of passwords and internet bills difficulties appreciably. Figure 3 shows the Clustering Coefficient

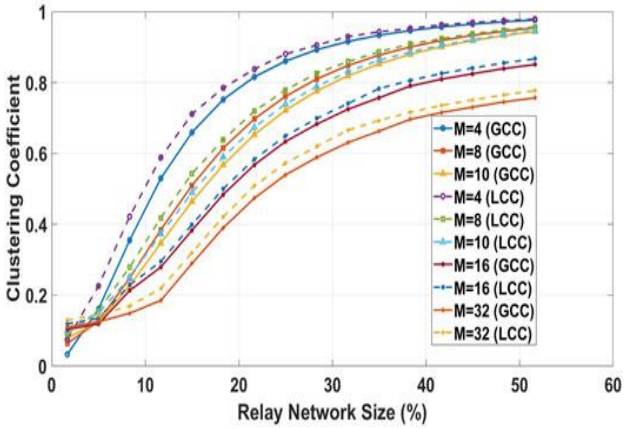


**Fig. 4.** Clustering Coefficient

Fig 4 depicts the clustering coefficient. IoT-based processes are commonly used in all sectors to minimize human effects and increase the automated process. Automatic update used in all trending technologies with sufficient usage process. With the mingling of blockchain processes, the whole process of IoT will be carried out in detailed order. Protection of the service will be doubled by combining both services to prevent the user's data information. All the data will be checked in auto format and updates will proceed as per the given information. Security will be carried out in each step of the process flow model.

### *A. Discussion*

The proposed work focuses on enhancing security in IoT systems through the integration of blockchain technology, offering several advantages over existing methods [20]. By employing blockchain's decentralized and tamper-resistant nature, the proposed approach ensures the integrity and confidentiality of IoT data and transactions. The use of smart contracts enables the implementation of automated and secure processes, enhancing trust and efficiency in IoT ecosystems. One significant advantage is the ability to secure NATted IoT devices using the Ethereum blockchain, thereby overcoming the limitations of traditional security measures in such environments. Dynamic access management and architecture-based design further enhance the security posture of IoT systems, ensuring resilience against evolving threats. Compared to existing methods, the proposed approach offers several advantages. Firstly, blockchain's immutable ledger provides a transparent and auditable record of IoT transactions, enabling real-time monitoring and forensic analysis. Secondly, the use of cryptography ensures data confidentiality and integrity, protecting sensitive information from unauthorized access and tampering. Smart contracts automate and enforce security policies, reducing the risk of human error and enhancing compliance with regulatory requirements. Furthermore, the architecture-based design ensures that security considerations are integrated from the outset, resulting in a robust and scalable solution. However, several challenges and areas for further study exist. One challenge is the scalability and performance of blockchain networks, especially in large-scale IoT deployments with high transaction volumes. Interoperability and standardization across different blockchain platforms and IoT devices need to be addressed to facilitate seamless integration. Future research should focus on addressing these challenges and exploring innovative solutions to enhance the security and usability of blockchain-based IoT systems.

## VI. CONCLUSION AND FUTURE SCOPE

The handling of private, public, and individual networks' sensitive and important data transfers is becoming more and more dependent on blockchain technology. With its encryption, decryption, and key generation techniques, it offers a strong data protection solution. Blockchain protects the security and integrity of records by using sophisticated algorithms for authentication and data access management, hence reducing cyber risks. This paper offers a thorough foundation for safe Internet of Things systems by drawing on earlier research on blockchain technology and cybersecurity. Through the creation of a complicated, impenetrable environment, the encryption techniques incorporated into blockchain architecture aid in the prevention of cybercrime. Comprehensive evaluations of the literature on cybersecurity and blockchain technology show that this conceptual framework provides an affordable answer to current data protection issues. The results show that blockchain encryption techniques significantly improve cyber security measures, which were assessed and improved using synthetic data. The tendency towards creative research in blockchain applications for cybersecurity is highlighted by this report. To handle the increasing number of IoT devices and transactions, blockchain networks' scalability and efficiency must be improved, necessitating optimized performance strategies. The creation of standardized interoperability standards would facilitate the smooth integration of blockchain technology into various IoT ecosystems, hence broadening its range of applications. The security and privacy of blockchain-based Internet of Things systems will continue to be strengthened by developments in cryptography and consensus processes. Resilience to cyberattacks may be increased by integrating AI and machine learning to enable proactive threat identification and predictive analytics. To reduce the impact on the environment, research on sustainable blockchain technology should also be prioritized. The potential and integration of blockchain with IoT may be further enhanced by investigating creative use-cases in a variety of industries, including supply chain management, smart cities, healthcare, and agriculture. Maximizing the potential of both technologies, addressing these areas will result in more secure, efficient, and scalable systems.

## REFERENCES

[1] R. Agrawal et al., “Continuous security in IoT using blockchain,” in 2018 IEEE international conference on

acoustics, speech and signal processing (ICASSP), IEEE, 2018, pp. 6423–6427.

[2] P. Ganesh et al., "Implementation of hidden node detection scheme for self-organization of data packet," Wireless Communications and Mobile Computing, vol. 2022, pp. 1–9, 2022.

[3] Ashok, M. Govindarasu, and J. Wang, "Cyber-physical attack-resilient wide-area monitoring, protection, and control for the power grid," Proceedings of the IEEE, vol. 105, no. 7, pp. 1389–1407, 2017.

[4] S. Manglekar and H. Dinesha, "Block Chain: An innovative research area," in 2018 Fourth International Conference on Computing Communication Control and Automation (ICCUBEA), IEEE, 2018, pp. 1–4.

[5] D. K. J. B. Saini, S. Kumar, A. Bhatt, R. Gupta, K. Joshi, and D. Siddharth, "Blockchain-Based IoT Applications, Platforms, Systems and Framework," in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), IEEE, 2023, pp. 1–6.

[6] K. Košťál, P. Helebrandt, M. Belluš, M. Ries, and I. Kotuliak, "Management and monitoring of IoT devices using blockchain," Sensors, vol. 19, no. 4, p. 856, 2019.

[7] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: Research issues and challenges," IEEE Internet of Things Journal, vol. 6, no. 2, pp. 2188–2204, 2018.

[8] L. Zhou, L. Wang, Y. Sun, and P. Lv, "BeeKeeper: A Blockchain-Based IoT System With Secure Storage and Homomorphic Computation," IEEE Access, vol. 6, pp. 43472–43488, 2018.

[9] 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.

[10] D. Tse, K. Huang, B. Cai, and K. Liang, "Robust password-keeping system using block-chain technology," in 2018 IEEE International Conference on Industrial Engineering and Engineering Management (IEEM), IEEE, 2018, pp. 1221–1225.

[11] Rashid and M. J. Siddique, "Smart contracts integration between blockchain and Internet of Things: Opportunities and challenges," in 2019 2nd International Conference on Advancements in Computational Sciences (ICACS), IEEE, 2019, pp. 1–9.

[12] D. Drozdov, S. Patil, V. Dubinin, and V. Vyatkin, "Formal verification of cyber-physical automation systems modelled with timed block diagrams," in 2016 IEEE 25th International Symposium on Industrial Electronics (ISIE), IEEE, 2016, pp. 316–321.

[13] P. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi, and N. Kumar, "Blockchain data-based cloud data integrity protection mechanism," Future Generation Computer Systems, vol. 102, pp. 902–911, 2020.

[14] 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, 2017, pp. 173–178.

[15] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, "A survey on the adoption of blockchain in iot: Challenges and solutions," Blockchain: Research and Applications, vol. 2, no. 2, p. 100006, 2021.

[16] S. Hossain, S. Waheed, Z. Rahman, S. Shezan, and M. M. Hossain, "Blockchain for the security of internet of things: A smart home use case using ethereum," Int. J. Recent Technol. Eng, vol. 8, no. 5, pp. 4601–4608, 2020.

[17] E. Kfoury and D. Khoury, "Securing natted iot devices using ethereum blockchain and distributed turn servers," in 2018 10th International Conference on Advanced Infocomm Technology (ICAIT), IEEE, 2018, pp. 115–121.

[18] D. Hwang, J. Choi, and K.-H. Kim, "Dynamic access control scheme for iot devices using blockchain," in 2018 international conference on information and communication technology convergence (ICTC), IEEE, 2018, pp. 713–715.

[19] Y. Liu, K. Zheng, P. Craig, Y. Li, Y. Luo, and X. Huang, "Evaluating the reliability of blockchain based internet of things applications," in 2018 1st IEEE International Conference on Hot Information-Centric Networking (HotICN), IEEE, 2018, pp. 230–231.

[20] S. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of IoT infrastructure with Ethereum transactions," Iran Journal of Computer Science, vol. 2, no. 3, pp. 189–195, 2019.