Research Output Journal of Engineering and Scientific Research 3(2): 26-29, 2024

ROJESR Publications Online ISSN: 1115-9790

https://rojournals.org/roj-engineering-and-scientific-research/ Print ISSN: 1115-6155

The Role of Blockchain in Securing IoT Devices

Mukantabana Phionah K

Faculty of Engineering Kampala International University Uganda

ABSTRACT

The proliferation of the Internet of Things (IoT) has led to increased concerns over security vulnerabilities due to the interconnected nature of these devices. This paper explores the application of blockchain technology as a solution to enhance the security of IoT devices. It examines the integration of blockchain's decentralized, immutable, and consensus-driven framework to secure data transmission, prevent unauthorized access, and ensure the integrity of IoT systems. Through case studies and theoretical analysis, the paper demonstrates the effectiveness of blockchain in addressing security challenges, including data breaches, device tampering, and cyberattacks, thus contributing to the overall resilience of IoT infrastructures.

Keywords: Blockchain, Internet of Things (IoT), IoT Security, Decentralized Networks, Data Integrity.

INTRODUCTION

The role of blockchain in securing IoT devices revolves around the fundamental process of adding a layer of security on top of the design to make it more secure and efficient. This essay presents the applications of blockchain that would strengthen the IoT, the security temperature's stability, and the use of a prototype blockchain to streamline these fields. The paper's range is mostly concerned with the use of blockchain technology to improve the IoT. Theoretically, the use of blockchain in the IoT can improve the protection of various IoT structures and technologies. The optimal output will be achieved using a key-value store blockchain prototype that implements the consensus mechanism. The initial implementation of the IoT prototype used the Raspberry Pi microcontroller and several IoT devices. This test showed a rise in the frequency of messages that passed through the entire network and affected all entities [1, 2]. The safety of cyberspace has several uses in the globe today, including the Internet of Things (IoT) technology. Numerous computers and end-user devices in the house, ranging from washing machines to refrigerators, are linked to the IoT. The majority of these tools have personal information presented or they integrate some part of the security mechanism to the network itself. "Industrial Internet of Things" (IIoT) refers to a network of systems and objects developed to collect and analyze data. The combination of technological innovation, hardware, and ideas behind IIoT improves the operational efficiency of various companies. One of the key constraints to the acceptance and use of the IoT, however, is protection. Every element of the IoT, including IoT endpoints, network coordination systems, and data repositories, is vulnerable to hackers [3].

UNDERSTANDING IOT DEVICES AND THEIR SECURITY CHALLENGES

The Internet of Things (IoT) is a network consisting of billions of smart devices connected over the internet. These connected devices communicate with each other, collect data, and may be controlled remotely through software and apps. IoT devices are used in various sectors, such as transport, healthcare, construction, and agriculture. They are classified in many terms like smart devices, smart gadgets, connected devices, intelligent devices, etc. IoT devices are classified based on different networks and sensors. From sensors such as motion, temperature, humidity, light, and contact, various network connectivity's are developed like BLE, Z-wave, Zigbee, Vera (Mi-Casaverde), Wi-Fi, Nest, Apple

Homekit, Amazon Alexa, and Google Home. IoT devices range from smart home security systems, automated appointment reminders, to the healthcare sector, where fitness trackers monitor calorie-burning, sleeping habits, and the user's heart rate [4, 5]. IoT devices face security challenges due to limited computational resources and lack of complex cryptographic algorithms. Security protocols are used to prevent unauthorized access to information. Low-security device manufacturers pose a potential cyberattack risk. Safety risks include data theft, device harm, and espionage. Main vulnerabilities include poor policy, network isolation approach, lack of security specialists, and staff education. IoT device weaknesses can lead to substantial disruptions. Misuse of a device can cause software system failure. Significant security risks are associated with IoT devices [6].

BLOCKCHAIN TECHNOLOGY OVERVIEW

Since its inception, blockchain has become a fundamental technology that is capable of transforming a variety of sectors ranging from finance to supply chain. The blockchain technology has a utility of veracity and confidentiality in as much as transactions are regarded. One of the key aspects of the blockchain technology is decentralization, which implies that the system is not under the control of a single entity or served by a central unit, but rather every participant in decentralized systems can have a copy of all the transaction history that happened in the systems [7, 8]. There are two more characteristics of blockchain technology: immutability and consensus mechanisms. The most popular consensus mechanisms are Proof of Work (PoW), Proof of Stake (PoS), BFT, and Raft, to name a few. Immutability is another key feature of blockchain, which means that the data once entered into a blockchain system cannot be tampered with by any unauthorized entity. The consensus mechanism is used to maintain agreement on the truth and accuracy of the blockchain data between the participants in the blockchain systems. While the blockchain technology is being used in various sectors, using blockchain for secure machine-to-machine communication in the Internet of Things (IoT) is still in its infancy. The current paper will discuss the role of blockchain technology in securing IoT devices [9]. Patents filed in the IoT field provide insights about companies and research trends in the applications related to IoT and blockchain. Publishing a paper on the role of blockchain in IoT patents is very enlightening. The authors stated, in their paper, that payments and clearing, supply chain management, privacy, security, compliance, IP protection, and trust systems are the major sectors in which blockchain has an influence for IoT. This can be seen from the distribution of patents [10].

INTEGRATION OF BLOCKCHAIN WITH IOT DEVICES

In addressing security challenges in IoT devices, the integration of smart devices with the blockchain network is observed. International organizations like Hyperledger have gained attention for advancing and deploying standardized metamorphosis. Blockchain is seen as a distributed ledger where members can share or transfer assets, while transactions are recorded in chained blocks. This tamper-proof database protects IoT devices and reduces liability. The potential for a secure co-constituted blockchain-IoT system has been proposed [11, 12]. While IoT initiatives present intrusion of a system when multiple verifications are implemented, the role of EOSD, the usage of initiation process of IoT network using blockchain to establish topology provides the importance of BIoT in the link of EOSD, to make possible initiation process of the blockchain. Therefore, making it easy for the role and the functionality of blockchain takes note of every new participant. It has created a starting of new presents in the blockchain approaches. Going by making it hard to make universal agreements on every step of IoT devices preventing the priming of individual IoT devices, every user can make query to the authenticated data of participants without turning to basic blockchain to query and record the primary listing of the devices [13].

BENEFITS OF USING BLOCKCHAIN IN SECURING IOT DEVICES

A. Enhanced Security: IoT devices usually transfer large volumes of data at a fast pace, thereby increasing the chances of vulnerabilities or security threats. Since blockchain secures the transactions and devices using decentralized, secure, and protected systems, it can guarantee improved security against threats.

B. Data Integrity: Blockchain ensures that once a transaction through IoT devices is recorded, it cannot be altered. This feasibility can be used to assure data integrity within the transmitted information through IoT devices.

C. Offers Immutable Audit Trails: Blockchain ledgers record all the transactions, and this has the potential to develop an immutable audit trail in the ledger for the transactions conducted through the IoT devices. Centralized systems can be easier to alter for traditional audit trails, but a distributed ledger customer variant is better at securing the audit trail.

D. Mitigating Various IoT Security Threats: IoT devices can be attacked by different types of threats like DDoS attacks, man-in-the-middle, IP Spoofing, and braking system authentication. Blockchain can mitigate these attacks as it can secure the system and load and data authentication.

Since blockchain uses smart contracts, it can also be used to enhance the level of security in IoT devices. While smart contracts have received limited success in their desired level of functionality till now, they need thorough investigation to be fully operational in IoT devices. One of the inherent functionalities of smart contracts is the need for automation, which is significant in zero-touch network programming and policy-making in IoT devices. The execution of smart contracts ultimately results in enforced logic that brings the mechanism towards policy-driven control in IoT applications. Every device will have its properties available on the smart contracts, same as with the devices attributes in IoT. Smart contracts will work as global-state validators due to their high-level responsibilities when it comes to governing operations. By having global-state validators, smart contract become a one-point single-transaction/multi-transaction global controller [14].

CASE STUDIES OF BLOCKCHAIN IMPLEMENTATION IN IOT SECURITY

Some examples of blockchain use in securing IoT devices were given earlier. Benefits include simplified access control, secure data management, transparent communication, data protection on the blockchain, and device identification. Blockchain can increase the security of IoT devices and systems. DUK PHONE uses blockchain to track devices in wireless networks and Ethereum, storing device properties, location, and owner for access control and location data queries [15, 16]. A successful integration of blockchain and an AIoT Edge Platform with several protocols (e.g., XACML) and a coherent IP-based security (e.g., DTLC) was presented in SPPW by the researchers from the Intel Research Collaboratory on Secure and Private Workstations. According to the presented study, during the World Forum on Internet of Things 2018, it was confirmed that blockchain may improve the missing part of security needed for IoT ecosystem's currency ecosystem. The solution designed by the research team referred to applying blockchain to the Keyless Smart Locking technology. This solution enables an add-on Nuki Bridge smart home device to manage the smart lock via remote access. A private and unforgeable blockchain is established for symmetric keys. The smart contract on the blockchain is executed only after the requester proves the ownership of the private key. This way, the advantage of blockchain, which is theoretically unforgeable, and the usability of symmetric keys are combined [17, 18].

CONCLUSION

Blockchain technology presents a robust solution to the security challenges faced by IoT devices. By leveraging its decentralized and immutable nature, blockchain can significantly enhance data integrity, prevent unauthorized access, and provide secure audit trails for IoT transactions. The integration of blockchain into IoT not only mitigates various security threats but also paves the way for more secure and trustworthy IoT ecosystems. As IoT continues to grow, the role of blockchain in ensuring its security will become increasingly critical, necessitating further research and development to optimize its application in this field.

REFERENCES

1. Khan AA, Laghari AA, Shaikh ZA, Dacko-Pikiewicz Z, Kot S. Internet of Things (IoT) security with blockchain technology: A state-of-the-art review. IEEE Access. 2022 Nov 18; 10:122679-95. ieee.org
2. Da Xu L, Lu Y, Li L. Embedding blockchain technology into IoT for security: A survey. IEEE Internet of Things Journal. 2021. e-tarjome.com
3. Pal D, Vanijja V, Zhang X, Thapliyal H. Exploring the antecedents of consumer electronics IoT devices purchase decision: A mixed methods study. IEEE Transactions on Consumer Electronics. 2021 Sep 27;67(4):305-18. researchgate.net
4. Tahaei H, Afifi F, Asemi A, Zaki F, Anuar NB. The rise of traffic classification in IoT networks: A survey. Journal of Network and Computer Applications. 2020 Mar 15; 154:102538. [HTML]
5. Krishnamurthi R, Kumar A, Gopinathan D, Nayyar A, Qureshi B. An overview of IoT sensor data processing, fusion, and analysis techniques. Sensors. 2020 Oct 26;20(21):6076. mdpi.com
6. Mousavi SK, Ghaffari A, Besharat S, Afshari H. Security of internet of things based on cryptographic algorithms: a survey. Wireless Networks. 2021. [HTML]
7. Moke KC, Low TJ, Khan D. IoT blockchain data veracity with data loss tolerance. Applied Sciences. 2021. mdpi.com
8. Singh S, Hosen ASMS, Yoon B. Blockchain security attacks, challenges, and solutions for the future distributed iot network. Ieee Access. 2021. ieee.org

9. Imteaj A, Amini MH, Pardalos PM, Imteaj… A. Introduction to Blockchain technology. … of Blockchain: Theory …. 2021. academia.edu
10. Shahzad A, Zhang K, Gherbi A. Intuitive development to examine collaborative iot supply chain system underlying privacy and security levels and perspective powering through proactive blockchain. Sensors. 2020. mdpi.com
11. Alam T, Benaida M. Blockchain, fog and iot integrated framework: review, architecture and evaluation. arXiv preprint arXiv:2006.03596. 2020. [PDF]
12. Zafar S, Bhatti KM, Shabbir M, Hashmat F, Akbar AH. Integration of blockchain and Internet of Things: Challenges and solutions. Annals of Telecommunications. 2022 Feb;77(1):13-32. academia.edu
13. Alrubei SM, Ball EA, Rigelsford JM, Willis CA. Latency and performance analyses of real-world wireless IoT-blockchain application. IEEE sensors journal. 2020 Mar 6;20(13):7372-83. whiterose.ac.uk
14. Wickström J, Westerlund M, Pulkkis G. Smart contract based distributed IoT security: A protocol for autonomous device management. In2021 IEEE/ACM 21st International Symposium on Cluster, Cloud and Internet Computing (CCGrid) 2021 May 10 (pp. 776-781). IEEE. researchgate.net
15. Šarac M, Pavlović N, Bacanin N, Al-Turjman F, Adamović S. Increasing privacy and security by integrating a blockchain secure interface into an IoT device security gateway architecture. Energy Reports. 2021 Nov 1; 7:8075-82. sciencedirect.com
16. Alfandi O, Khanji S, Ahmad L, Khattak A. A survey on boosting IoT security and privacy through blockchain: Exploration, requirements, and open issues. Cluster Computing. 2021. [HTML]
17. Lockl J, Schlatt V, Schweizer A, Urbach N, Harth N. Toward trust in Internet of Things ecosystems: Design principles for blockchain-based IoT applications. IEEE Transactions on Engineering Management. 2020 May 5;67(4):1256-70. researchgate.net
18. Rahman A, Islam J, Kundu D, Karim R, Rahman Z, Band SS, Sookhak M, Tiwari P, Kumar N. Impacts of blockchain in software-defined Internet of Things ecosystem with Network Function Virtualization for smart applications: Present perspectives and future directions. International Journal of Communication Systems. 2023 Feb 6:e5429. [HTML]

CITATION: Mukantabana Phionah K. The Role of Blockchain in Securing IoT Devices. Research Output Journal of Engineering and Scientific Research, 2024 3(2): 26-29