# Coevolution of Blockchain and Internet of things: Applications and Opportunities.

Faheem Ahmad reegu
*College of Computer Science & IT, Jazan University, Jazan, KSA*

[1]freegu@jazanu.edu.sa

***Abstract*— Due to a shortage of storage and poor processing speed, a network consisting of lightweight computers such as IoT has issues. Unfortunately, these problems make the implementation of solid protection solutions significantly more difficult, which decreases network security efficiency. A secure blockchain is ideal for IoT use cases that struggle with poor protection. An improvement in stability, lightness, and reliability of the IoT network is being pursued by blockchains use in IoT. Today's Internet of Things (IoT) applications are lacking in built-in protection technology, which puts out various security flaws and privacy issues. Blockchain is an effective technology, thus the open and autonomous technology behind it, blockchain, is a successful approach. This paper explores the ways in which blockchain technologies can be integrated into the Internet of Things**

***Keywords*— Internet of Things, Blockchain, Security**

## I. INTRODUCTION

IoT is a relatively lightweight network that consists of sensors connecting to the internet, which interact wirelessly. A set of lightweight sensors on a central node that handles administrative tasks is an IoT network. As for Internet of Things (IoT) applications, they have the following kinds of limitations: reduced battery life, low processing ability, and insufficient storage capacity, all of which increase the burden on application efficiency[1]. The fact that high-performance encryption algorithms cannot be used in resource-constrained environments like IoT causes a security issue in such environments. The blockchain, the essential infrastructure of Bitcoin, offers superior protection, and blockchain technology is showing considerable interest in areas that demand exceptionally high-efficiency authentication. Blockchain is seen as a viable solution for networks that are particularly vulnerable to security breaches like the Internet of Things[2][3][4].Security and safety is one of the IoT device's most important functions. Additional considerations that lead to the vulnerabilities of IoT systems include the restricted capacity of operating systems, vendor-specific device installations, and implementation in unregulated accessible environments [5]

It is important to reevaluate and redesign the IoT structures because of these obstacles [6][7]. At the moment, the most viable nominee technology for the IoT is blockchain [8][9].Haber et al. first identified blockchain technology in 1991 as a “cryptographically encrypted chain of blocks” [10][11].But, it was accepted worldwide when Satoshi Nakamoto used it as a public ledger to launch the digital currency Bitcoin (2018)[12].Blockchain can be defined as a chain of cryptographically connected, time-stamped blocks, where each block contains information that is simultaneously accessible to any member of the network. Thus, by using a distributed and stable environment, blockchain is capable of addressing the protection problems that conventional IoT networks are susceptible to. Several researchers are working to remove the need for a central trustworthy body, such as a government, and are instead using blockchain to allow decentralized IoT communications[13][14].

## II. APPLICATION OF BLOCKCHAIN IN INTERNET OF THINGS

In order to protect an IoT network from bugs, it is advised to use a blockchain-based IoT solution. Your most significant risk of lightweight computers is protection because of their low performance. The platform leverages distributed characteristics of blockchain to Internet of Things (IoT) networks to deal with established challenges that are created by the centralized infrastructure, including the removal of central nodes that experience limited battery issues. For this purpose, a number of studies have employed blockchain in the IoT[15]. Additional research is being conducted to improve security as well as to create a lighter weight blockchain suitable for usage in the Internet of Things (IoT) and for further extension of the spectrum of IoT devices[16][17][18]. In the field of IoT, certain implementations of blockchain enabling the integration of the Internet of Things (IoT) yields several advantages, among which are the enhancement of numerous facets of IoT and the several beneficial effects which include:

• **Enhanced security**: Blockchains may be used to store data that has been secured and cryptographically signed in the context of transactions so the data is saved in the form of encrypted and cryptographically signed transactions [19]. IoT devices driven through blockchain connectivity have safeguards toward vulnerable data breaches, and hence the whole infrastructure is strengthened [20][21][22]

• **Improved interoperability**: When used together, IoT-generated data will increase the networkability of IoT networks, as it can be stored and modified into blockchains. In addition to processing, transformation, mining, resizing, and recording, various IoT databases are transmitted, converted, stored, and reported via a decentralized distributed ledger[23][24].

• **Autonomous interactions**: IoT systems should be able to automatically communicate with each other. This can be done by the blockchain technologies. Wu et al. (2019) proposes the implementation of decentralized autonomous corporations (DACs) to handle transactions where hierarchical entities are unnecessary. In the context of digital currencies, DACs run on smart contracts and autonomously. This results in a substantial reduction in the overall expense. Decoupled and device-agnostic software may still use this feature[25].

• **Reliability**: The integrity of data in blockchain-based networks is protected by distributing knowledge across the network and maintaining the data's immutability over time. This means that users are able to confirm the integrity of the data and be certain that the data has not been tampered with. Sensor data accountability and traceability may also be provided by the blockchain[26].

• **Secure Code Deployment**: By using permanent storage protected by blockchain, you will ensure the code is efficiently and safely deployed. IoT devices may use this feature to upgrade the device's software without having to go through a potential crisis[27][28].

• **Service Market**: In other words, with the elimination of centralized authorities, blockchain allows peer-to-peer exchanges to happen more quickly and unobstructed, which speeds up the development of the Internet of Things (IoT) system of information and service markets, where micro services can be seamlessly installed and micro-payments can be completed in a fully secure environment.

• **Dependability and traceability**: Wherever and wherever the consumer wishes, they will verify and identify the data contained in the blockchain. Per transaction made on the blockchain is completely transparent. The product traceability network created by Wang et al. (2019) uses blockchain technology to ensure that supply chain retailers and manufacturers have access to product tracing services. Blockchain is also dependable because of its immutability function, which makes IoT data dependable[29].

## III. Conclusion

Due to the rapidly the adoption of IoT, a number of protection flaws have emerged, including data and system hacks. Due to its resource-constrained existence, immature requirements, weak interoperability, and absence of stable software and hardware design, distribution, and production, the existing IoT devices are unable to adequately protect themselves. As a result, a large amount of study focus has been paid to finding a comprehensive and solid global framework for IoT systems. Blockchain will provide solutions to stability, anonymity, traceability, reliability, and interoperability in such an environment. In contrast to conventional databases, blockchain technology establishes confidentiality, authentication, and non-repudiation by design, and thus automates and authorizes transactions by the use of smart contracts

### *References*

[1] F. Masoodi, S. Alam, and shams T. Siddiqui, “SECURITY\& PRIVACY THREATS, ATTACKS AND COUNTERMEASURES IN INTERNET OF THINGS,” *Int. J. Netw. Secur. \& Its Appl.*, vol. 11, no. 2, pp. 67–77, 2019.

[2] A. Boudguiga *et al.*, “Towards better availability and accountability for iot updates by means of a blockchain,” in *2017 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)*, 2017, pp. 50–58.

[3] I. Abrar, Z. Ayub, and F. Masoodi, “Current Trends and Future Scope for the Internet of Things,” *Internet Things Bus. Transform. Dev. an Eng. Bus. Strateg. Ind. 5.0*, pp. 185–209, 2021.

[4] I. Abrar, S. N. Pottoo, F. S. Masoodi, and A. Bamhdi, “On IoT and Its Integration With Cloud Computing: Challenges and Open Issues,” in *Integration and Implementation of the Internet of Things Through Cloud Computing*, IGI Global, 2021, pp. 37–64.

[5] A. Arora, A. Kaur, B. Bhushan, and H. Saini, “Security

concerns and future trends of Internet of Things," in *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)*, 2019, vol. 1, pp. 891–896.

[6] I. Butun, P. Österberg, and H. Song, "Security of the Internet of Things: Vulnerabilities, attacks, and countermeasures," *IEEE Commun. Surv. Tutorials*, vol. 22, no. 1, pp. 616–644, 2019.

[7] shadab alam faheem reegu, salwani daud, zaid hakami, Kaiser kareem reegu, "Towards Trustworthiness of Electronic Health Record system using Blockchain," *Ann. RSCB*, vol. 25, no. 6, 2021.

[8] B. Bhushan and G. Sahoo, "Recent advances in attacks, technical challenges, vulnerabilities and their countermeasures in wireless sensor networks," *Wirel. Pers. Commun.*, vol. 98, no. 2, pp. 2037–2077, 2018.

[9] S. A. Faheem Reegu, Salwani Mohd Daud, "Interoperability Challenges in Healthcare Blockchain System - A Systematic Review," *Ann. RSCB*, vol. 25, no. 4, 2021.

[10] A. Whitaker, "The eureka moment that made Bitcoin possible," *Wall Str. J.*, 2018.

[11] F. A. Reegu, M. O. Al-Khateeb, W. A. Zogaan, M. R. Al-Mousa, S. Alam, and I. Al-Shourbaji, "Blockchain-Based Framework for Interoperable Electronic Health Record," *Ann. Rom. Soc. Cell Biol.*, pp. 6486–6495, 2021.

[12] Satoshi Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," 2008. .

[13] F. A. Reegu, S. M. Daud, S. Alam, and M. Shuaib, "Blockchain-based Electronic Health Record System for efficient Covid-19 Pandemic Management," 2021, doi: 10.20944/preprints202104.0771.v1.

[14] F. Reegu, W. Khan, … S. D.-… C. on R., and undefined 2020, "A Reliable Public Safety Framework for Industrial Internet of Things (IIoT)," *ieeexplore.ieee.org*.

[15] O. Abdulkader, A. M. Bamhdi, V. Thayananthan, F. Elbouraey, and B. Al-Ghamdi, "A Lightweight Blockchain Based Cybersecurity for IoT environments," in *Proceedings - 6th IEEE International Conference on Cyber Security and Cloud Computing, CSCloud 2019 and 5th IEEE International Conference on Edge Computing and Scalable Cloud, EdgeCom 2019*, Jun. 2019, pp. 139–144, doi: 10.1109/CSCloud/EdgeCom.2019.000-5.

[16] F. S. Masoodi and M. U. Bokhari, "Symmetric Algorithms I," in *Emerging Security Algorithms and Techniques*, Chapman and Hall/CRC, 2019, pp. 79–95.

[17] F. Masoodi and others, "Machine Learning for Classification analysis of Intrusion Detection on NSL-KDD Dataset," *Turkish J. Comput. Math. Educ.*, vol. 12, no. 10, pp. 2286–2293, 2021.

[18] F. Masoodi, S. Alam, and M. U. Bokhari, "SOBER Family of Stream Ciphers: A Review," *Int. J. Comput. Appl.*, vol. 23, no. 1, pp. 1–5, 2011.

[19] P. J. Sun, "Security and privacy protection in cloud computing: Discussions and challenges," *J. Netw. Comput. Appl.*, vol. 160, p. 102642, 2020, doi: 10.1016/j.jnca.2020.102642.

[20] P. Zhang, M. A. Walker, J. White, D. C. Schmidt, and G. Lenz, "Metrics for assessing blockchain-based healthcare decentralized apps," *2017 IEEE 19th Int. Conf. e-Health Networking, Appl. Serv. Heal. 2017*, vol. 2017-Decem, pp. 1–4, 2017, doi: 10.1109/HealthCom.2017.8210842.

[21] M. U. Bokhari and F. Masoodi, "BOKHARI: A new software oriented stream cipher: A proposal," in *2012 World Congress on Information and Communication Technologies*, 2012, pp. 128–131.

[22] A. M. Bamhdi, I. Abrar, and F. Masoodi, "An ensemble based approach for effective intrusion detection using majority voting," *Telkomnika (Telecommunication Comput. Electron. Control.*, vol. 19, no. 2, pp. 664–671, 2021, doi: 10.12928/TELKOMNIKA.v19i2.18325.

[23] F. Ahmed Teli, T., & Masoodi, "Security Concerns and Privacy Preservation in Blockchain based IoT Systems: Opportunities and Challenges.," in *ICICNIS 2020*, 2021.

[24] F. Pandow, B. A., Bamhdi, A. M., & Masoodi, "Internet of Things: Financial Perspective and Associated Security Concerns.," *Int. J. Comput. Theory Eng.*, vol. 12, no. 5, 2020.

[25] Y. Yang, L. Wu, G. Yin, L. Li, and H. Zhao, "A Survey on Security and Privacy Issues in Internet-of-Things," *IEEE Internet Things J.*, vol. 4, no. 5, pp. 1250–1258, Oct. 2017, doi: 10.1109/JIOT.2017.2694844.

[26] F. Masoodi, S. Alam, and M. U. Bokhari, "An analysis of linear feedback shift registers in stream ciphers," *Int. J. Comput. Appl.*, vol. 46, no. 17, pp. 46–49, 2012.

[27] C. Lin and G. Wu, "Enhancing the attacking efficiency of the node capture attack in WSN: A matrix approach," *J. Supercomput.*, vol. 66, no. 2, pp. 989–1007, 2013, doi: 10.1007/s11227-013-0965-0.

[28] I. Abrar, Z. Ayub, F. Masoodi, and A. M. Bamhdi, "A Machine Learning Approach for Intrusion Detection System on NSL-KDD Dataset," in *2020 International Conference on Smart Electronics and Communication (ICOSEC)*, 2020, pp. 919–924.

[29] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in *2017 IEEE International Congress on Big Data (BigData Congress)*, Jun. 2017, pp. 557–564, doi: 10.1109/BigDataCongress.2017.85.