# Security Aspects & Challenges in Blockchain based IoT Systems

Shruti Jain[1], Aashvi Jain[2], Tushar Mehrotra[3], Manju Verma[4]

[1,2,3] *College of Computing Sciences & IT, Teerthanker Mahaveer University, Moradabad*

[4] *Research Scholar Galgotias University*

***Abstract- The advanced concept behind the IoT network is that smart devices such as sensors, actuators, and wearables collect data about their locations, connect wirelessly to the internet and other devices connected by routers and gateways, and share internal data. There are also unit remote devices (smartphones, tablets, PCs, and a variety of management panels) that operate IoT devices and transfer data to people. The acquired data in an IoT network flows between IoT devices and may be stored in the cloud, on a data area, on a remote device, or on the IoT devices themselves.***

***Index Terms- Blockchain, System scaling, Transfer guarantee.***

## I. INTRODUCTION

The Internet of Things (IoT) is a network of physical objects (or "things") that have embedded sensors, software, and various technologies with the goal of communicating and exchanging information with other devices and programmes on the internet. Blockchains are distributed digital ledgers that are tamper apparent and resistant to tampering (i.e., without a central repository) and often without a central authority (i.e., A bank, company or government)

*There are two types of Blockchain:*

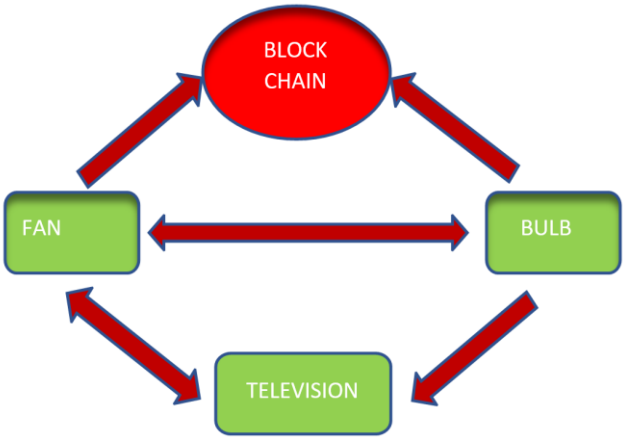
Permissionless Blockchain: -Anyone can join the network, which will search ledger knowledge and confirm transactions, replicating a high level of trust.

Permissioned Blockchain: -Formed by a group of well-known transacting parties, validation is overseen by a certain set of nodes, and ledgers mimic a high level of transparency and accountability.

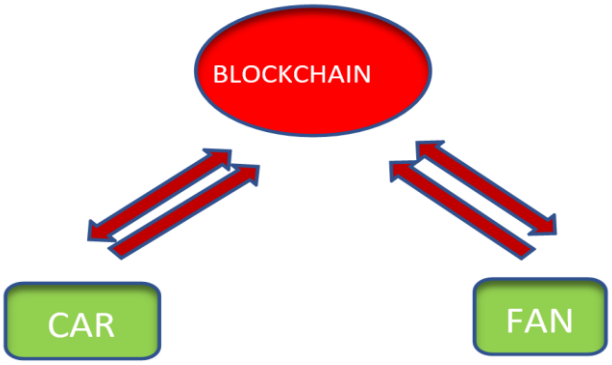
## II. IDENTIFY, RESEARCH AND COLLECT IDEA

*Blockchain IoT Interactions*

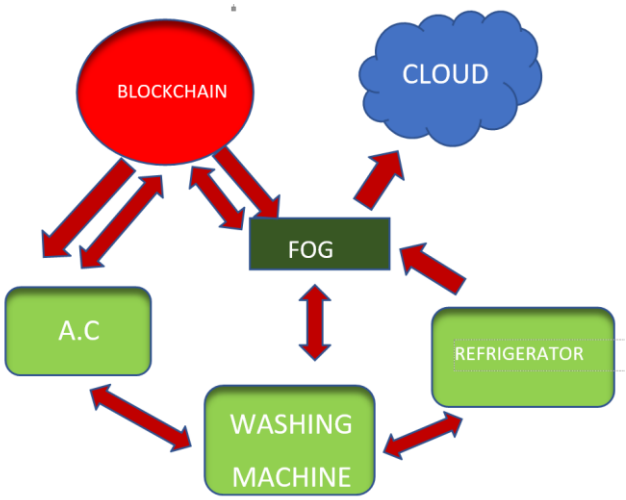
IoT-IoT This methodology uses blockchain to store solely a little of IoT knowledge. IoT devices communicate while not the utilization of blockchain, exploitation search strategies and routing strategies instead. Transactions move quicker thanks to shorter delays. This methodology is additionally thought-about safe because it permits devices to figure offline.




IOT-BLOCKCHAIN: - In this approach, all IoT device communications are routed through the blockchain, which takes the place of the cloud in traditional IoT networks. The records saved on the blockchain are unaltered, traceable, and protected from unauthorised access. This method promotes device autonomy while also ensuring communication safety and tracking. Recording and archiving all transactions on the blockchain, on the other hand, will increase information measures and knowledge.




HYBRID APPROACH: - This technique ensures that the majority information and connections square measure shared directly between IoT devices, whereas blockchain solely stores some information. Therefore, this style combines the advantages of blockchain communication with time period IoT. The hybrid technique permits fog and cloud computing to make blockchain and IOT devices.




## II. WRITE DOWN YOUR STUDIES AND FINDINGS

Lecturers and professionals are attracting considerable attention to IoT security nowadays. We tended to instruct thanks to addressing these challenges earlier. An explanation of the concept of victimization of the good home has been presented. Next, the good home layer and elements of varied activities are described. Then, all relevant analyses and their privacy and security are addressed. In the current study, a low IoT resource device was found to be manageable. These overlay devices do not seem to have equal value in terms of privacy and safety during vaginal birth. In our future analysis, we'll explore applications for the framework in alternative IoT domains. To the best of our knowledge, this study is the start geared toward increasing before Christ within the atmosphere of good homes. Despite the surge in IoT devices, they are insecure and are ill-equipped to defend themselves. This may be because resources are limited, the devices are still in their infancy, and the devices have insecure hardware and software. We tend to discuss key IoT security issues on each of these pages. The problems are classified into high, moderate, and low-level IoT layers. Procedures for exploiting IoT security individually square measure suggested within the literature.

The purpose of this paper is to provide a parameter analysis of IoT attacks and potential solutions. Many people believe that blockchain can solve certain IoT security problems. During this paper, we'll identify whether blockchain can properly protect IoT networks.

Blockchain will make IoT systems more secure and private by preventing transactions from being altered or deleted, providing a standardized event history record, and providing complete records to users.

Blockchain-based conceptual design facilitates access to IoT resources worldwide [1]. We will expand the program to include the fabric of a private blockchain platform, where nodes need permissions to participate in mining to expand blockchain coverage for IoT applications [2] This paper describes a prototype model which can be used in different cities, not just with energy management but with all the elements which smart citizens can use to improve their health. [3] IoT devices are being connected to the blockchain with the records of these connections being used as a separate location to ensure security and transparency to different users[4]IoT security is receiving considerable attention from both academics and industry these days. [5]

The adoption of blockchain in IoT environments can bring key benefits in several areas, for example, Health, Financial, Transportation, Welfare, and so on. Any solution using blockchain technology can benefit from these same benefits, such as transparency in the network, no-rejection of generated information from nodes, and high availability. [6] Modern IoT devices are unsafe and cannot protect themselves. This is due to restricted resources on IoT devices, immature levels, and a lack of secure hardware and software development, development, and deployment.[7] IoT and Blockchain present unique challenges due to the variety of factors concerned. Related challenges include a high resource utilization level, dispersal, and processing time. Blockchain offers smart contracts like a new communication method. Smart contracts allow us to use complex multi-step processes Devices on IoT are embedded in an ecosystem which allows physical contact with the earth [8]. We are facing the challenge of being unable to access human aging on billions of IoT restricted devices.

To deal with the increased load good [9] This paper dealt with various security and privacy issues on IoT. We identified this based on the IoT segment interactions. The blockchain technology developed to address challenges in IoT has been identified. An overview of how blockchain and IoT can be integrated can be found in the paper. Highlight the potential applications of IoT in blockchain technology. Moreover, blockchain technology offers the promise of IoT with the challenges it presents. This paper provides a basic understanding of the importance of a blockchain in IoT[10] Internet of Things (IoT) systems faces many challenges, such as inefficiency, resource constraints, privacy, and security[11] Blockchain technology is already having an impact on digital financial applications. Building blocks - distributed ladder, compact methods, and public key cryptography - blockchain technology allows for IoT and the monitoring of procurement systems [12] Blockchain and IoT are good technological innovations with a lot of potential to produce excellent results in every area. The ability to ensure efficiency and security in the sector for which it was hired. Briefly, this paper discusses the basics of technology, how they integrate, and what applications are available. Describe each of the technologies individually. In this chapter, a discussion is provided on the relationship between IoT and Blockchain [13] as well as the motive behind their integration. It is explained that there are many

opportunities and challenges. A peer-to-peer peer-to-peer network can connect all smart devices in real time to other devices using this approach. It could change the current internet system. As a result, costs and time can be slowed down, while relevant information is provided in real-time to the right device. As a result, it may prove useful in the future.[14] The main contribution of this paper is the development of a high-performance blockchain platform for smart devices. With the node-to-node mapping process, the platform is able to provide an effective intelligent device for connecting smart devices.[15]

| S.R. NO | YEAR | AUTHOR | WORK | ADVANTAGE |
|---|---|---|---|---|
| 1 | 2018 | Novo, O | The delays and throughput rates connected with the systems are shown in this research, as well as possible configurations of their solution to maximise its scalability. The goal of this study is to see if our approach can scale at the same rate as existing IoT management solutions. | When WSNs are connected to several Management Hubs, their solution is designed to favour horizontal scalability. The results of this study show that their approach is beneficial in a variety of IoT applications. |
| 2 | 2017 | Liang, Xueping, Juan Zhao, Sachin Shetty, and Danyi Li | The idea of protecting drone data gathering and communication using a public blockchain for data integrity and cloud auditing is presented in this study. The results reveal that their solution is a dependable and distributed system for drone data assurance and resilience, with reasonable overhead and scalability for a high number of drones. | They presented a blockchain-based general architecture for drone data collection and control, bringing us closer to a vision in which drone-based applications may collect sensor data and be managed in a trusted and dependable manner while lowering the risk of assaults and data loss. For real-time data collecting and drone control, this system can provide reliability and accountability, as well as data assurance. |
| 3 | 2019 | Rathee, Geetanjali, Ashutosh Sharma, Rajiv Kumar, and Razi Iqbal | They employed the blockchain method to extract data from IoT devices and then saved the collected records in the blockchain to preserve transparency among multiple users in various locations. | |
| 4 | 2017 | Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. | We demonstrate that our brilliance is built on Blockchain.<br>The home framework is secure because it has been thoroughly evaluated for basic confidential confidentiality, integrity, and availability. Finally, we provide the simulation results, highlighting the overheads (depending on traffic, processing, power, and time) presented by our method, which is minor in terms of security and privacy. | Both academia and industry are paying close attention to IoT security these days. Here are some security solutions that are not ideal for IoT due to their high energy consumption and subsequent processing. |
| 5 | 2019 | Huang, J., Kong, L., Chen, G., | We're presenting a credit-based blockchain system IIoT compatibility technique to address these issues. We | The proposed PoW-based debt consolidation strategy saves energy while increasing the computer |

| | | | | |
|---|---|---|---|---|
| | | Wu, M. Y., Liu, X., & Zeng, P | propose a credit-based method to the authentication procedure (PoW) for IoT devices.At the same time, system security and transactional performance are ensured. To safeguard the privacy of sensitive information,We establish a data management agency. | complexity of harmful sites, making DAG-built blockchain better suited for IoT systems. Also, the data authority management strategy, which operates in the IoT system, may secure data privacy without sacrificing system performance. Our system performs well in IoT, according to a variety of tests and outcomes.. |
| 6 | 2020 | Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L | This paper discusses research challenges in IoT-based agriculture in the green sector, including security and privacy concerns. We start by describing the four-line agricultural construction based on IoT and summarising existing agricultural intelligence surveys. | looked at privacy methods that inhibit privacy as well as green alignment techniques.<br>Agriculture based on the Internet of Things. There are still other research obstacles, such as machine learning algorithms and data sets.to detect intrusion detection, Analysis of blockchain-based solutions, how to select the best compatibility algorithm, and useable and compatible cryptographic design agreements are all things that should be looked into in the near future. |
| 7 | 2020 | Liu, H., Han, D., & Li, D. . | Based on the Hyperledger Fabric blockchain technology and Human-Based Access Control, this article proposes the IoT fabric-iot access control system. Device Agreement (DC), Policy Agreement (PC), and Access Contract are the three forms of smart contracts included in the strategy (AC). DC provides a URL for storing device data created by devices, as well as instructions on how to query it. For admin users, PC provides management functionality and ABAC policies. | We're thinking of employing a cluster or an edge computing provider to deploy and test this system's distributed performance. More physical devices could be employed in the future to verify the system's reliability and throughput. Fabric-scalability iot's could be improved in the future, and additional IoT application integration could be supported. |
| 8 | 2020 | Khan, M. A., & Salah, K. | We introduce and investigate significant IoT security challenges in this study. We examine and classify common security concerns in the context of IoT layer building, as well as the agreements utilised for communication, communication, and management. We go over the needs for IoT security, as well as actual attacks, threats, and technology solutions. | blockchain can be used to check again to solve some of the IoT security issues. It also indicates future and open research concerns, as well as challenges, that the research community must address in order to deliver dependable, efficient, and fantastic IoT security solutions. |
| 9 | | | | |

| | | | | |
|---|---|---|---|---|
| 10 | 2018 | Ye, Z., Yin, M., Tang, L., & Jiang, H. | In this study, a book review was used to introduce the description, characteristics, and applications of BIM, blockchain, and IoT in the AEC/FM business. Following that, there was an interaction between<br>These three technologies are compared to one another.<br>uses, advantages, and drawbacks The incorporation of<br>BIM and blockchain can also help with security<br>the effectiveness of the signing agreement, the project's metamorphosis<br>Asset management and procurement management are two of the most important aspects of asset management. However,<br>there is no apparent project data in the applications without the Internet of Things | Consolidation of BIM, IoT, and blockchain is a complicated and varied process. Once the integrated framework framework has been further developed, detailed techniques of integration must be devised. |
| 11 | 2020 | Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. | This paper covers a wide range of topics related to IoT integration systems and blockchain technology. Following an overview of the IoT system and blockchain technology, a comprehensive examination of blockchain integration with the IoT system is offered, emphasising the benefits of integration and how the blockchain may address IoT difficulties. | There have also been studies introducing IoT connection with the blockchain. The blockchain as an IoT service is then presented to demonstrate how various aspects of blockchain technology can be made available as a service for various IoT applications.<br>The implications of AI integration on both IoT and blockchain was then discussed. Future indicators of IoT research on blockchain have been discussed thus far. |
| 12 | 2019 | Dabbagh, M., Kakavand, M., & Tahir, M. | Blockchain has shown to be a cutting-edge technology that is transforming a variety of businesses. For starters, the Internet of Things (IoT) is one of the most prominent Blockchain app sectors. Many scientists' research interests in dealing with and resolving the integration of disruptive technologies, such as IoT and Blockchain, have waned as a result of Blockchain's ability to overcome the many issues of IoT services. | We looked at the articles that contradicted the four techniques, such as annual trends and quotation patterns, the most quoted papers, the most generally used keywords, and the most popular publishing venues. The findings provide crucial information to academics prior to the start of a study project on the integration of IoT and Blockchain. |

## III. PROPOSED IDEA

**Benefits of IoT and Blockchain Integration**

1. Information localization: - For IoT networks, information centralization could be a huge challenge. Information acquired by IoT devices is sometimes stored on a central server, allowing for the transfer of personal information to other parties. When one purpose fails, the entire network is frequently shut down. There is no central management in a distributed blockchain, which eliminates the risk of attack or failure, lowers infrastructure costs, improves integration and maintenance, and increases mistake tolerance. Unlike the cloud, all nodes in the blockchain are responsible for managing the distributed digital ledger and safeguarding new volumes.

2. Advanced System Scaling: - Idle time not only lowers IoT pits, but also helps to increased growth. Detergent networks transfer a lot more system power than medium networks since they spread greater hundreds on most PCs. They're extra storage, data measurement, and processing power. IoT networks that are incapable of supporting high-quality devices and transactions.

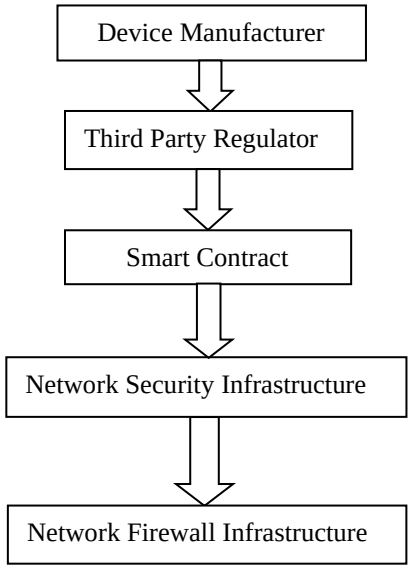
3. Information transfer guarantee: - Cryptography ensures the integrity of the data in the blockchain, allowing the distributed ledger to be reliable. Information transit and secure storage are frequently assured by including encryption into good devices. Blockchain will handle the synchronous history of excellent device communications via the IoT network in this method.

4. Sturdy recognition: - Everything is typically considered as one IoT with Blockchain. Furthermore, Blockchain will ensure the credibility of excellent devices, implying that everyone's data on the IoT network would be secure. Several blockchain systems employ a cryptologic authentication approach for public key infrastructure (PKI), which necessitates the employment of a key generator in the blockchain to generate personal and public keys.Standard PKI could be a melody, but it has flaws such as limits and the possibility of assaulting the average person. However, by reducing the PKI approach, blockchain technology is frequently enhanced. The user is the only one who has access to the personal key.

5. Improved privacy and security: - Blockchain will shield connections between IoT devices by storing sales information and making certain that transactions are unit geographical. It ensures observance and answerability of sensitive data. Blockchain additionally implements the present IoT rules by providing encryption. The utilization of cryptography on social media eliminates the danger of blockchain information breach. Each group action on the supplier's network is secure throughout travel because of the ultimate initial cryptography.

6. Automatic Communication: - Blockchain technology treats device messages as transactions and allows them to control through good contracts. These automatic pc programs enable IoT networks to use the foremost wide purchased everyday automation that improves information security. An IoT device will broadcast a sensible contract address to the network it joins. This good contract address is often freely accessed by network security tools to transfer this network manifest. The visual network itself should be signed and verified with a public key by the device manufacturer, or ideally a sector authority. This trilateral system is safer and supplies larger enhancements to IoT security, permitting the manufacturer to outline minimum network security rights.

A diagram giving an overview of such a process is below.




An IoT device will broadcast a wise contract address to the network it joins. This good contract address is freely accessed by network security tools to transfer this network manifest. The visual network itself should be signed and verified with a public key by the device manufacturer, or ideally a sector authority. This 3-party system is going to be safer and supply larger enhancements to IoT security, permitting the manufacturer to outline minimum network security rights.

1. Device manufacturer submit network manifest and information to 3rd party regulator or financial organisation
2. Third party regulator Create/update good contract on blockchain
3. Third party regulators transfer public keys and verify manifest signatures and good contract transfer device manifest from address.
4. Network security infrastructure apply network security policies

## IV. CONCLUSION

In this paper, foremost we've got explained in brief regarding IOT, Blockchain and their integration method and its implementation, challenges and edges. Since IoT devices and its technology is reaching each home and may connect lifestyle devices to the net and therefore the IoT technology is predicated on server/client model that has major drawbacks like quantifiability and security. Blockchain offers a North American country with a peer-to-peer commutation network wherever non-trusting nodes will interconnect with non-trusty median, during a verifiable manner. These 2 integrated technologies would be thus compelling that it's laborious to imagine the future while not it. Each rising technology has nice potential and is prepared to alter our society permanently. Blockchain is here to remain for long and over the previous couple of years it's been improved considerably. Last however not the smallest amount, there's no denying and there's still would like additional analysis and investigation required to implement IoT with Blockchain.

## REFERENCES

[1]. Novo, O. (2018). Scalable access management in IoT using blockchain: A performance evaluation. *IEEE Internet of Things Journal*, *6*(3), 4694-4701.

[2]. Liang, X., Zhao, J., Shetty, S., & Li, D. (2017, October). Towards data assurance and resilience in IoT using blockchain. In *MILCOM 2017-2017 IEEE Military Communications Conference (MILCOM)* (pp. 261-266). IEEE.

[3]. Lazaroiu, C., & Roscia, M. (2017, November). Smart district through IoT and blockchain. In *2017 IEEE 6th International Conference on Renewable Energy Research and Applications (ICRERA)* (pp. 454-461). IEEE.

[4]. Rathee, G., Sharma, A., Kumar, R., & Iqbal, R. (2019). A secure communicating things network framework for industrial IoT using blockchain technology. *Ad Hoc Networks*, *94*, 101933.

[5]. Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

[6]. Huang, J., Kong, L., Chen, G., Wu, M. Y., Liu, X., & Zeng, P. (2019). Towards secure industrial IoT: Blockchain system with credit-based consensus mechanism. *IEEE Transactions on Industrial Informatics*, *15*(6), 3680-3689.

[7]. Ferrag, M. A., Shu, L., Yang, X., Derhab, A., & Maglaras, L. (2020). Security and privacy for green IoT-based agriculture: Review, blockchain solutions, and challenges. *IEEE access*, *8*, 32031-32053.

[8]. Cha, J., Singh, S. K., Kim, T. W., & Park, J. H. (2021). Blockchain-empowered cloud architecture based on secret sharing for smart city. *Journal of Information Security and Applications*, *57*, 102686.

[9]. Liu, H., Han, D., & Li, D. (2020). Fabric-IoT: A blockchain-based access control system in IoT. *IEEE Access*, *8*, 18207-18218.

[10]. Khan, M. A., & Salah, K. (2018). IoT security: Review, blockchain solutions, and open challenges. *Future Generation Computer Systems*, *82*, 395-411.

[11]. Qiu, C., Wang, X., Yao, H., Du, J., Yu, F. R., & Guo, S. (2020). Networking Integrated Cloud-Edge-End in IoT: A Blockchain-Assisted Collective Q-Learning Approach. *IEEE Internet of Things Journal*.

[12]. Ye, Z., Yin, M., Tang, L., & Jiang, H. (2018). Cup-of-Water theory: A review on the interaction of BIM, IoT and blockchain during the whole building lifecycle. In *ISARC. Proceedings of the International Symposium on Automation and Robotics in Construction* (Vol. 35, pp. 1-9). IAARC Publications.

[13]. Atlam, H. F., Azad, M. A., Alzahrani, A. G., & Wills, G. (2020). A Review of Blockchain in Internet of Things and AI. *Big Data and Cognitive Computing*, *4*(4), 28.

[14]. IoT: a Dabbagh, M., Kakavand, M., & Tahir, M. (2019, June). Towards integration of blockchain and bibliometric analysis of state-of-the-Art. In *International Congress on Blockchain and Applications* (pp. 27-35). Springer, Cham.

[15]. IoT: a Dabbagh, M., Kakavand, M., & Tahir, M. (2019, June). Towards integration of blockchain and bibliometric analysis of state-of-the-Art. In *International Congress on Blockchain and Applications* (pp. 27-35). Springer, Cham.

## AUTHOR'S PROFILE

**First Author** – Shruti Jain, Student, College of Computing Sciences & IT, Teerthanker Mahaveer University, Moradabad shrutijain1215301@gmail.com

**Second Author** – Aashvi Jain, student, College of Computing Sciences & IT, Teerthanker Mahaveer University, Moradabad, jainaashvi21@gmail.com

**Third Author** – Tushar Mehrotra, Assistant Professor, College of Computing Sciences & IT, Teerthanker Mahaveer University, Moradabad, tusharmehrotra9@gmail.com

**Fourth Author-** Manju Verma, Research Scholar Galgotias University

**Correspondence Author** – Tushar Mehrotra, Assistant Professor, College of Computing Sciences & IT, Teerthanker Mahaveer University, Moradabad, tusharmehrotra9@gmail.com