ADDRESSING CHALLENGES AND SOLUTIONS OF IOT WITH BLOCKCHAIN

CANDIDATE NAME- PREETI GUPTA
DESIGNATION- RESEARCH SCHOLAR Glocal School of Computer science engineering,
THE GLOCAL UNIVERSITY, SAHARANPUR, UTTAR PRADESH
GUIDE NAME- DR. RAJEEV YADAV
DESIGNATION- PROFESSOR Glocal School of Computer science engineering,
THE GLOCAL UNIVERSITY, SAHARANPUR UTTAR PRADESH

PUBLICATION YEAR @ 2020

ABSTRACT

The next generation is showing a growing interest in blockchain technology because of its obvious use in today's digital world. The IoT is another area where blockchain technology may be put to use. There has been significant development in distributed systems thanks to the expansion of Internet of Things technology into new fields. The blockchain idea necessitates a distributed database management system for storing and propagating network data and transactions. We discussed the difficulties associated with Internet of Things (IoT) gadgets and how blockchain technology can help. Integration of blockchain with IoT was discussed in length, with the obstacles faced by IoT and the solutions offered by blockchain being highlighted. Finally, the difficulties caused by IoT gadgets can be mitigated thanks to blockchain technology.

Keywords: Internet of Things, Security, Blockchain, Integration, Network

I. INTRODUCTION

Blockchain is a distributed digital ledger that has lately taken the globe by storm because to its ability to be utilized to securely keep track of ever-expanding lists of data entries and transactions. Identity and access on a blockchain may be classified into three basic categories: public/less authorized, private/authorized, and consortium. The most groundbreaking and revolutionary aspect of the blockchain idea is the fact that all data is encrypted inside the transaction blocks themselves. Consistency, liveliness, and fault tolerance are the three hallmarks of its decentralized consensus approach.

There have been several successful implementations of blockchain technology. There are a few pertinent issues that are still being researched when blockchain technology is implemented in the IoT domain to exchange and share network data, records, validation, and security service, with a particular focus on the security of cyber-physical systems in the IoT domain. There are several official bodies striving to guarantee the IoT network's interoperability, integrity, and privacy. These groups are coordinating their efforts thanks to blockchain and cloud computing. This innovation improves the IoT data system's openness, dependability, and governance.

Governments have adopted blockchain for numerous Internet of Things applications, and the technology is rethinking data modeling. Its unparalleled adaptability and the ability to compartmentalize, secure, and exchange IoT data and services are the major selling points for these kinds of uses. Many recent innovations in the Internet of Things sector revolve around blockchain technology. This is because many IoT services may be easily disrupted or attacked. Many problems with cyber-physical systems in the Internet of Things domain can be resolved by employing blockchain technology. The benefits of the IoT industry's shift toward a network sensor paradigm should be taken into account while designing sustainable smart cities and its various constituent parts.

II. INTEGRATION OF IOT IN BLOCKCHAIN

As a result of the IoT, it is now feasible to handle massive volumes of data, transforming formerly manual operations into digitalized versions. Because of this massive amount, smart apps may be developed to do things like manage and enhance people's lives as they become increasingly digitized. As cloud computing has evolved over the past decade, it has provided the foundation for the Internet of Things by facilitating features like real-time data processing.

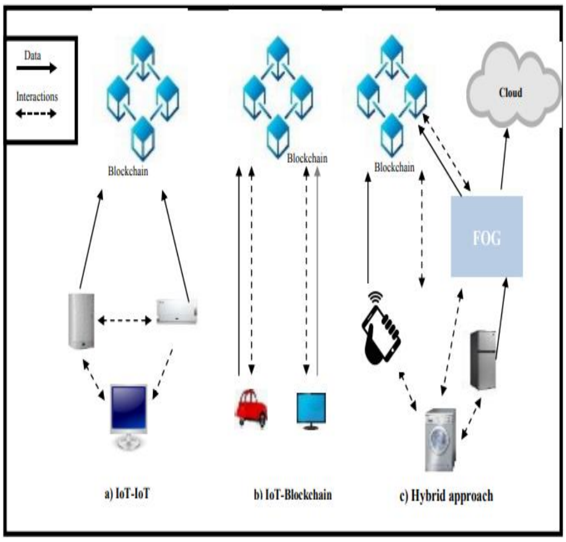

Figure 1: Types of integration of IoT and blockchains

Rapid expansion of the Internet of Things has unleashed unanticipated possibilities, such as novel ways to collect and distribute information. Since the public does not have a clear picture of where the data is going, they are skeptical about the topic. Many people see advantages in connecting IoT devices to cloud infrastructure. There are several ways in which blockchain technology might revolutionize the Internet of Things. The IoT may benefit from this since it provides a secure data-sharing platform where information can be confidently verified and quickly attributed. At any moment, the data's origin may be determined, which is a security bonus. This connection guarantees that data will be shared across the available users even in applications where security is the primary need. An organization stands to lose a lot of money and suffer a lot of damage if its data is compromised and used for fraudulent purposes or if its security measures are slowed down. As a result, it would be preferable to enhance the method of sharing the data amongst the designated users, hence shortening the time needed to locate the required information. Implementations like smart vehicles and smart cities can benefit from data sharing since it allows for better service and the ability to bring in more people to the ecosystem. As a result, the IoT may benefit from the use of the blockchain by providing more secure and trustworthy data. When it comes to the IoT paradigm, blockchain technology may be seen as a solution for addressing privacy, reliability, and scalability concerns. Blockchain's capabilities will be enhanced by IoT, and existing IoT technologies will see further advancement as a result. The use and integration of existing technology is complicated by a wide range of challenges and concerns that need investigation. Since this project is still in its early stages of development, there is a lot of room for investigation. Scalability, decentralization, dependability, autonomy, security, etc. will all see improvements as a result of this integration.

III. BLOCKCHAIN AND IOT ISSUES

Challenge	**Causes**
Security.	Information updates via off-site sources Employing corrupted hardware Lack of visibility into the network's endpoints Inadequate security patches for the Internet of Things Endpoint vulnerability grows in tandem with the number of connected devices.
Centralization	All equipment must be identified and authenticated. No matter how far apart they are, all connected devices always use the internet. Modeling interactions as interactions between clients and servers.
Transparency	Poorly maintained databases that are difficult to access Lack of a Data Privacy and Security Plan
Interoperability	Because of their integration with real-world software, IoT devices are notoriously difficult to standardize. There is currently no structure or accepted standard for IoT devices. Proprietary IoT devices are quite diverse in terms of fundamental communication protocols, data formats, and underlying technology.

Blockchain and IoT Security Issues

Sezer claims that security concerns are holding back the use of IoT technologies. The most common types of attacks against the Internet of Things include those that prevent prospective users from accessing network resources, that disrupt communication between systems, that spy on users and create intrusions that breach personal data, and that infect botnets with the goal of mining cryptocurrencies. Denial of service for the intended system's clients may be a problem when several computers simultaneously request large amounts of data or information from a single server. Without proper protections in place, the Internet of Things is wide open to hacking and DDoS assaults from hackers.

Due to the immutability of the blockchain ledger and the impossibility of eavesdropping on an individual communication thread, incorporating blockchain technology into the Internet of Things will increase the latter's security. Blockchain also offers direct payment services in crypto currencies like Bitcoin, which eliminate the need for a central administrator. As a result, the IoT solution is a flawless whole thanks to the sovereign security solution.

Blockchain's encryption is stronger than IoT's because no one can alter previously recorded transactions. Using blockchain to store data from IoT devices will offer an extra degree of security to prevent hacking. As a result of blockchain's encryption and decentralized storage, data recorded by Internet of Things (IoT) equipment may be kept permanently and without human intervention. All participants in the supply chain will have faith in the data now that it has been safeguarded. To guarantee that only the account owner is doing transactions, blockchain technology assigns a unique identifier to each user. Blockchain's encryption makes it harder to hack or otherwise disrupt the established chain's flow. The trustworthiness of the blockchain is ensured by having minors keep watch on all transactions. The security of the blockchain relies on the immutability of all transactions and blocks added to the ledger. To yet, hackers have been unable to breach the security of blockchain, demonstrating its reliability, immutability, and resilience against both technological failures and hostile attempts. Decentralization allows for this to happen.

Blockchain and IoT Centralization Issues

IoT systems' primary weakness is the reliance on a centralized client-server architecture, which may easily go down. Blockchain solves this problem by sending requests to every node simultaneously. One of the problems with the Internet of Things is that it may be difficult to centralize the vast volumes of data generated by the network of sensors because of very slow processing rates [32]. Congestion on the network is caused by the need for the central server to authenticate and approve many users. Alam [28] recommended a costly investment in a centralized server capable of handling the anticipated influx of data or information into the network as a means of solving this problem. Because an IoT network may process transactions involving devices from multiple companies, it might be difficult to determine the origin of data leaks if an attack happens. It's also not easy to tell who owns the data that's produced.

If a hacker gains access to the server where the data is stored, they may add, change, or remove whatever data they choose. In a blockchain, information is distributed to all participating nodes. A decentralized system will notify all connected nodes of any approved changes to the law. Distributed-ledger systems are more resilient to network strain than IoT networks, since queries are spread over the whole network rather than being concentrated on a single node. While in an Internet of Things (IoT) network a single failed server would bring down the whole network and create disruption for all parties involved, in a blockchain network, where many devices are interconnected, this may not happen.

Blockchain and IoT Transparency Issues

Blockchain's transparency makes it possible for authorized users to see transaction histories on the network. This makes it simple to spot cases of data loss and take corrective measures before it may be exploited by hackers. Blockchain records are transparent, so authorized parties may monitor and study traffic in real time. Massive data transactions are generated by organizations over many networks; an immutable ledger record acts as a safeguard by following information or products as they travel between each node. Blockchain improves the use of ledgers by securing data from Internet of Things devices. Since blockchain nodes are conceptually comparable to IoT system objects, the latter may be trusted more implicitly. IoT solutions built on the blockchain streamline company transactions, increasing transparency and ultimately improving the customer experience. Since blockchains are already used to record and verify financial transactions on the Bitcoin network, integrating them into an IoT network makes it possible for devices on the network to communicate securely yet distrustfully. Blockchain's capacity to provide smart contract-based networks (like Ethereum) ensures that all transactions between IoT devices will be handled in accordance with the established protocols. Blockchain transactions are immune to third-party interference because of the distributed ledger technology that underpins the system. Blockchain is capable of handling millions of linked devices and processing massive volumes of transactions far more quickly than an IoT system. Blockchain's inherent reliability helps businesses to cut down on spending on IoT gateways' associated processing overhead, which might include things like connectivity and hardware.

Blockchain and IoT Interoperability Issue

Interoperability is the capacity of different networked systems or devices to work together to achieve a shared goal. There is a dearth of standardized protocols, data formats, and technologies that would allow IoT systems and devices to communicate with one another and exchange data.Since this is the case, data cannot be transferred across linked gadgets. Unfortunately, the successful inclusion of new devices that may address other operational concerns is hampered by the fact that many IoT devices are still built to run on a preset hardware configuration. Problems arise with interoperability when IoT devices try to combine data or information from several sources or send service requests to the cloud. When one IoT device's services are used by another, it might compromise interoperability. Blockchain is able to facilitate cross-system, cross-device, cross-network data sharing thanks to cross-chain technology. Interoperability between private networks and public blockchains, or between private networks and public blockchains, is the primary emphasis of cross-chain technology. Tools like atomic swaps and multichain protocols are used by the blockchain to make interoperability a reality.

IV. BLOCKCHAIN TECHNOLOGY SOLUTION TO IOT

The issues that arise in IoT systems might be resolved more effectively with the help of blockchain technology. The potential for a larger number of interconnected items or devices to be present in future IoT systems is developing. The internet will serve as a conduit for the vastly expanded number of gadgets that will attempt to communicate with one another. Since most data in IoT devices resides on centralized servers, this would provide a number of problems. In order for the devices to access the data, they must communicate with one another via the centralized network, and all data must pass through the centralized server (as shown in Fig. 2). However, IoT was being portrayed as large-scale systems that integrated cutting-edge technology due to the expanding requirements of IoT and its applications. The centralized server model will not scale well in such massive IoT deployments. Currently deployed Internet of Things solutions rely heavily on the central server architecture.

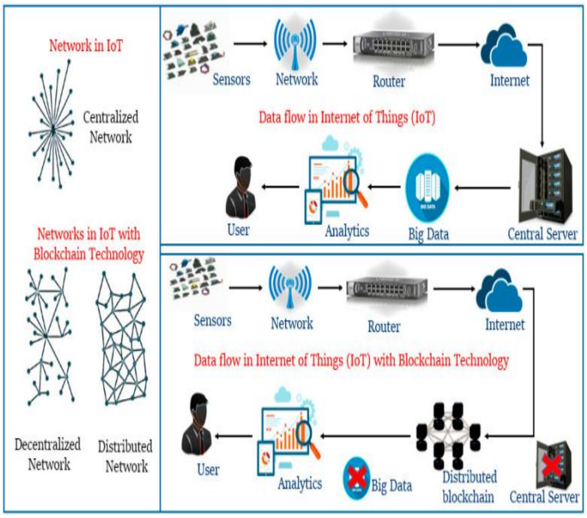

Figure 2: Types of IoT networks, and IoT data flow using blockchain technology

The internet of things relies on sensor devices to gather data from the targeted objects and relay that data to a centralized server through a wired or wireless network. Analytics were run from the central server at the request of individual users. In a similar vein, the processing capabilities of the current internet infrastructure may not adequately support the analysis that a large-scale IoT system desires to do. Expanding the capacity of the internet is essential in order to manage the massive amounts of data generated by large-scale IoT devices. Having "Peer-to-Peer Networking (PPN), Distributed File Sharing (DFS), and Autonomous Device Coordination (ADC)" functionalities available on decentralized or dispersed networks is one possible solution. Blockchain has the potential to do these three tasks, which will enable IoT systems to keep tabs on the countless interconnected gadgets. With the help of BC, IoT systems can conduct transactions between connected devices in tandem. BC will strengthen the security and privacy of IoT systems. As can be seen in Fig. 2, BC makes use of distributed ledger technology to provide instantaneous peer-to-peer communications. When compared to a purely IoT system, the data flow procedure in an IoT incorporating BC technology is distinct. The data pipeline in IoT with BC consists of the following nodes: sensors; network; router; internet; distributed blockchain; analytics; user. In this case, the immutability of the distributed ledger prevents any data from being misinterpreted or improperly authenticated. When applied to the Internet of Things, BC's elimination of STC complicates matters and makes the system less trustworthy. The introduction of BC in IoT will increase the security and dependability of the data flow.

V. CONCLUSION

In conclusion, both blockchain and the Internet of Things are cutting-edge technological phenomena with enormous promise, but widespread skepticism among businesses. Blockchain and IoT will continue to advance into a globally acknowledged standard, despite the fact that some are merging them to assess the potential of decreasing the security and other related business risks. Even if there might be hiccups, more and more companies are investing in IoT solutions that are underpinned by blockchain technology. Finally, blockchain will open up a lot of doors for the introduction of IoT infrastructure. Despite these limitations, blockchain technology offers a number of advantages, even if widespread adoption has yet to occur.

REFERENCES: -

1. Adanma Cecilia Eberendu, Titus Ifeanyi Chinebu. (2021). CAN BLOCKCHAIN BE A SOLUTION TO IOT TECHNICAL AND SECURITY ISSUES. International Journal of Network Security & Its Applications (IJNSA) Vol.13, No.6, November 2021 DOI: 10.5121/ijnsa.2021.13609.
2. Aditya Tandon. (2019). Challenges of Integrating Blockchain with Internet of Things. International Journal of Innovative Technology and Exploring Engineering (IJITEE) ISSN: 2278-3075, Volume-8, Issue-9S3, July 2019
3. P. Cui, U. Guin, A. Skjellum, and D. Umphress. "Blockchain in IoT: current trends, challenges, and future roadmap." Journal of Hardware and Systems Security vol.3, no. 4. Dec. 2019: pp. 338-364.
4. M. Alamri, N. Z. Jhanjhi, and M. Humayun. "Blockchain for Internet of Things (IoT) research issues challenges & future directions: A review." Int. J. Comput. Sci. Netw. Secur vol. 19 May, 2019: pp. 244-258.
5. Nallapaneni Manoj Kumara, Pradeep Kumar Mallickb . (2018) Blockchain technology for security issues and challenges in IoT. International Conference on Computational Intelligence and Data Science (ICCIDS 2018). Procedia Computer Science 132 (2018) 1815–1823.
6. H. F. Atlam, A.Alenezi, M. O. Alassafi, and G. Wills. "Blockchain with internet of things: Benefits, challenges, and future directions." International Journal of Intelligent Systems and Applications vol. 10, no. 6. 2018: pp. 40-48.
7. A. Dorri, S. S. Kanhere, R.Jurdak, and P.Gauravaram. "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), March. 2017. pp. 618-623. IEEE.
8. N. Kshetri, “Can Blockchain Strengthen the Internet of Things?,” IT Prof., vol. 19, no. 4, pp. 68–72, 2017.
9. S. Li, L D Xu, and S. Zhao. "The internet of things: a survey." Information Systems Frontiers vol.17, no. 2 April, 2015: pp. 243-259.