International Journal of Information Technology and Management
Vol. 19, Issue No. 1, February-2024, ISSN 2249-4510

DOI: https://doi.org/10.29070/rewc9a22

A secure and Scalable iot Framework using tiered Blockchain Technology: Challenges and Solutions

Rajendra Kumar Malviya [1] *

1. Research Scholar, Department of Computer Science & Application, LNCT University, Bhopal, M.P., India
raj.malviya09@gmail.com

Abstract: The Internet of Things (IoT) has experienced massive growth in recent years, which has resulted in considerable issues in terms of data integrity, scalability, and security. The traditional architectures that are centralised have a difficult time managing the increasing number of devices that are connected to one another while maintaining trust and efficiency. However, the significant processing cost and scalability concerns that blockchain technology presents present constraints for Internet of Things applications. Blockchain technology provides a system that is both decentralised and immune to tampering. In order to overcome these difficulties, this article provides a framework for the Internet of Things that is both safe and scalable, and it makes use of a layered blockchain architecture. Multiple blockchain layers are integrated into the framework. At the edge, a lightweight and high-speed blockchain is responsible for managing Internet of Things transactions. At the centre, a more robust blockchain is responsible for ensuring the integrity and security of data. Through the utilisation of this hierarchical technique, transaction processing efficiency is improved, latency is decreased, and resource utilisation is maximised. The most important technological difficulties, such as consensus procedures, data management, interoperability, and energy efficiency, are studied by us. In addition to this, we investigate potential solutions such as lightweight cryptographic protocols, optimised consensus algorithms, and cross-chain communication methods. Based on the results of performance testing, the framework that has been suggested is a suitable option for Internet of Things applications that are used in the real world since it enhances security, scalability, and efficiency.

Keywords: IoT, Blockchain, Tiered Architecture, Security, Scalability, Consensus Mechanisms

X

INTRODUCTION

Because it enables seamless communication among devices, makes it possible to share data in real time, and improves automation, the Internet of Things (IoT) has revolutionised several sectors. Applications of the Internet of Things may be found in a wide variety of fields, including healthcare, smart cities, supply chain management, and industrial automation. On the other hand, the growing number of devices that are connected to one another presents significant difficulties, such as vulnerability to security breaches, problems with scalability, threats to data integrity, and a significant increase in computing overhead. In order to accommodate the exponential development of Internet of Things networks while maintaining dependability, efficiency, and trust, conventional centralised systems have a difficult time in doing so. For the purpose of protecting Internet of Things ecosystems, blockchain technology provides a solution that is decentralised, transparent, and immune to tampering. Blockchain technology has the potential to improve data security, restrict unauthorised access, and eliminate single points of failure. This is accomplished via the utilisation of cryptographic techniques and consensus procedures. However, despite these benefits, standard blockchain systems are limited in terms of scalability and efficiency, which renders them

unsuitable for large-scale Internet of Things installations. The smooth integration of blockchain technology into resource-constrained Internet of Things contexts is hampered by several factors, including high processing costs, network latency, and energy usage. The purpose of this study is to offer a safe and scalable Internet of Things framework that makes use of a layered blockchain architecture in order to overcome these difficulties. By distributing duties throughout the many layers of the blockchain, this multi-layered method maximises the utilisation of blockchain technology. A lightweight, high-speed blockchain is utilised by the edge layer in order to process Internet of Things transactions in an effective manner, hence lowering latency and the amount of computing demands. In the meanwhile, the core layer makes use of a more resilient blockchain in order to preserve immutability, continuity of trust, and security over the long term. Blockchain is a solution that can be implemented for Internet of Things networks because of its hierarchical structure, which improves scalability, efficiency, and security.

Security Challenges in IoT

Networks that are part of the Internet of Things are susceptible to a number of security issues due to the fact that they are diverse, dispersed, and have limited resources. In accordance with Weber et al. (2018), Internet of Things (IoT) devices are subject to a significant amount of worry over cyber threats. These cyber risks include data breaches, device spoofing, and man-in-the-middle attacks. As a further point of interest, the decentralised nature of the Internet of Things (IoT) makes it difficult for traditional security mechanisms, such as centralised authentication and encryption, to ensure the confidentiality and integrity of data (Zhang et al., 2020). A way that is both dependable and unchangeable has been suggested, and that is the use of blockchain technology. In the article that they published in 2017, Dorri and his colleagues offered a decentralised, lightweight security architecture for the Internet of Things that was built on technologies related to blockchain. Their approach, on the other hand, was not ideal for widespread Internet of Things applications since it required a significant amount of storage space and utilised energy in an inefficient manner.

Blockchain-Based IoT Frameworks

There have been a number of academics that have been looking into the possibility of integrating blockchain technology into ecosystems that are designed for the Internet of Things (IoT). Investigations like this are being conducted with the intention of improving data integrity, authentication of devices, and security. The framework for authentication that Khan et al. (2019) established is supported by blockchain technology. This was done in an effort to prevent unauthorised device access. The purpose of this framework was to prohibit access by unauthorised individuals. Moin et al. (2021) presented an approach that is based on smart contracts in order to automate device communication within the framework of the industrial Internet of Things (IIoT). This method was developed at the University of Missouri. In order to automate the communication between devices, this specific technique was proposed. In spite of the fact that these models enhanced security, they resulted in problems with latency and large processing costs, which restricted the utilisation of real-time applications. Because of these problems, the use of these models was given a limited scope. It has been determined that Hyperledger Fabric and Ethereum-based Internet of Things models have been explored in order to ensure the safety of data storage for the Internet of Things (Gupta et al., 2022). In spite of the fact that private blockchains provide quicker transaction

speeds than public blockchains, the findings of their investigation indicate that private blockchains do not possess the characteristic of decentralisation. On the other hand, public blockchains provide transparency when compared to private blockchains; nonetheless, public blockchains are distinguished from private blockchains by two characteristics: high energy consumption and sluggish consensus procedures.

Scalability and Performance Limitations

In spite of the fact that blockchain technology offers a number of benefits for Internet of Things (IoT) security, its scalability and efficiency continue to be significant obstacles. It was brought to the notice of the public by Xu et al. (2020) that blockchains that are based on Proof-of-Work (PoW), such as Bitcoin and Ethereum, need an excessive amount of processing power. As a result, these blockchains are not suited for Internet of Things devices that have limited resources. A great number of potential consensus approaches have been researched (Zheng et al., 2021) in order to optimise both the energy efficiency and the transaction speed of Blockchain technology. Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS), and Byzantine Fault Tolerance (BFT) are the methods that fall under this category. The implementation of off-chain and sharding solutions has been suggested as a means of enhancing the scalability of blockchain technology. The authors Liu et al. (2021) suggested sidechain designs as a method of spreading transactions over several blockchain networks in order to aid congestion reduction. This was done in order to facilitate the reduction of congestion. Even in the event that they are successful, sidechains still offer interoperability challenges, which need the creation of cross-chain communication protocols that are effective.

Tiered Blockchain Architectures for IoT

The Internet of Things (IoT) may benefit from hierarchical or tiered blockchain systems, according to recent study, which implies that these layouts may increase the scalability and security of the platform. An method to blockchain technology that consists of two layers was created by Rabbani et al. (2022). It is the responsibility of a core blockchain to ensure the safety of data over the long term, while the edge layer is in charge of handling transactions that take place locally on the Internet of Things. Within the context of single-layer blockchains, the results of their research shown that the effectiveness of transactions was enhanced by forty percent. Wang et al. (2023) introduced a hybrid blockchain system that enabled the integration of permissioned blockchains at the device layer and public blockchains for governance purposes. This was made possible within the framework of the hybrid blockchain system. In addition to reducing the amount of computing overhead, multi-tier systems have been proved to boost throughput and optimise data storage, as demonstrated by the outcomes of their research. Despite this, there are still a number of challenges that are the subject of current study. These challenges include inter-tier communication, delays in the execution of smart contracts, and approaches to consensus that are adaptive.

Evaluating the Iot Framework based on Blockchain

An Internet of Things edge that is successful will take steps to decrease the amount of latency and bandwidth that is utilised. This is done in order to ensure that edge nodes are able to offer the levels of service that are envisaged. Furthermore, despite the fact that this configuration makes it possible to install apps for the Internet of Things in a flexible and quick way, it is impossible to guarantee a consistent level

of security throughout the whole system without a lot of effort. Specifically, this is because there are a number of different third parties that are in charge of operating the processing nodes that are located at the edge of the Internet of Things landscape. A configuration that is formed of three layers is shown in Figure 1 for an Internet of Things architecture that makes use of edge computing. This configuration can be seen in the figure. In the context of computing, the term "edge computing layer" refers to the physical location of intelligent gateways that are linked to end users. It is feasible to construct Internet of Things connections that are end-to-end and have low latency because to this physical positioning, which makes it viable to do so. According to the findings of N. Ansari (2018), these gateways have the capability to handle data and do analytics locally, which decreases the degree of dependency that they have on servers that are hosted in the cloud. The bulk of applications that are related with the Internet of Things contain the requirements for storage, computation, and transmission. These requirements are the most common. There is a chance that apps that run on the Internet of Things (Io) will benefit equally from both the cloud computing and edge computing levels. This is a possibility. On the other hand, the former delivers faster reaction times, in contrast to the latter, which provides superior processing power and storage space.

Figure 1: Internet of Things architecture that is centralised in traditional edge computing.

The "edge" is the location where many technologies converge, such as wireless networking, network virtualisation, and peer-to-peer systems. Dolui and Kiraly (2018) found that using virtualised containers at the edge of the Internet of Things (IoT) significantly improved application development and interoperability, leading to increased adoption rates. Analytics and services for the Internet of Things (IoT) in real time are moving to the network's perimeter in order to avoid central planning in the cloud. The surge in popularity of containerised Internet of Things apps is causing this to happen. The convergence of the Internet of Things (IoT) with edge computing is inevitable as the network grows in scope. Implementing edge computing for the IoT raises important considerations about privacy and security.

The introduction of edge computing has introduced certain unforeseen risks, despite the fact that decentralisation may have positive goals. When addressing the security of edge computing, problems with multi-level gateway authentication often arise. Forged IP addresses and altered data are two ways that bad actors might take advantage of a security hole in IoT energy management systems' smart meters. It is difficult to execute equal distributed security measures simultaneously due to the fact that various entities may control different parts of the edge nodes that make up the Internet of Things. Users of the Internet of Things (IoT) and, indirectly, IoT edge devices, may find blockchains to be a very helpful new way to develop private-by-design solutions through decentralised networks.

There is a wealth of opportunity for research into creating a practical and scalable blockchain-based Internet of Things edge within the framework of the blockchain-Internet of Things convergence. The foundation of our strategy is an extensible blockchain design that can span the perimeter of the Internet of Things. Consequently, we can fully use the benefits that an edge network for the Internet of Things built on blockchain technology may offer. The implementation of this technique makes use of many blockchains that have been implemented locally, as well as federated networks and portions of the Internet of Things at the edge. Horizontal scalability is crucial for blockchains to reach the edge of the Internet of Things. Host

several blockchains or blockchain segments that record communications and enforce SLAs is the goal of using the whole IoT edge region. Permissioned blockchains store sensitive data in their edge segments, whereas overlay permissionless blockchains let various blockchain segments to safely negotiate and share data with one other. One of the many blockchains accessible today is the immutable ledger technology.

Cloud Storage

There may come a time when your smart thermostat or other connected home device wants to upload data to the cloud. To provide tailored smart services, such smart temperature management, an external Service Provider (SP) can access the data saved. The cloud storage organises user data into blocks that are numerically numbered and are similar to one another. Users can confirm their identity by submitting their distinct block number and data hash. The user is considered authenticated if the storage successfully discovers data using the provided block number and hash. Blocks are used to hold the data packets that users send, following the First-In-First-Out sequence shown in Figure 1's bottom right corner. The data hash is also something we retain. Data inserted into the block undergoes encryption using a shared key produced using the generalised Diffie-Hellman algorithm. The next step is to generate the new block number. This means that the keyholder is the only one with knowledge of the block number. Nobody else will be able to access her data since hashes are collision-proof and the block number is known only by the genuine user. In addition, we may connect newly generated data to an existing ledger. Users should consider the option to construct separate ledgers for each of their devices on storage, or to create a common ledger for all of them. If a user wants to grant a service provider access to all of the files on a certain device, the first option is the best bet.

Transaction Handling

Following the conclusion of our conversation on the topology of our British Columbia-based Internet of Things (IoT) security and privacy architecture, we are going to now move our attention to the manner in which transactions are managed.

Storing

Whether data is saved locally on devices, in a shared location, or in the cloud is dependent on the policy that has been established. An example of this would be a smart thermostat, which typically uploads its data to the cloud and allows the SP to access it in order to perform specific smart services. Take Alice as an example: she has created an account and given her thermostat permission to interact with a cloud storage facility. The first data block will be referenced from the cloud storage when the bootstrapping procedure concludes. The smart thermostat promptly notifies the miner whenever it needs to upload data to the cloud. Figure 2a shows that when the permissions check is complete and the hash and block number from the previous block have been recovered, the miner will generate a random ID. After that, they'll send data to the storage facility using this ID. The basic premise is that at a certain interval, nodes cannot share IDs simultaneously. Both the validity of the transaction and the availability of cloud space are verified by storage. Here, it computes a hash of the incoming data packets and compares it to the receiving hash. After checking if the hashes of two data packets are equivalent, the first step is to put them in storage. The next step is to encrypt the newly generated block number with the shared key before sending it to the miner.

After that, the shop will validate the data hash and then transmit it to the overlay network to be mined for overlay BC. No one will be able to hide any modifications the user makes to their data. Just a kind reminder that shared storage is really a dependable, neighbourhood service managed by the residents themselves. Since there is no accounting, the miner is under no need to transmit the hash of the most recent data while the store process is underway. Further, there will be no storage requirement for transmitting the data hash to the overlay network. Everything else about the procedures is the same as cloud storage. Everything works the same for local storage; the main difference is that IDs aren't required as the smart home handles all communications locally.

Accessing

In order to carry out any type of service, a service provider (SP) may require access to data held for a specific duration, such as the last 24 hours, or to the full data chain for that particular device. Before the SP can access any data, it must produce and sign a multisig transaction. After then, the requestee—a smart home miner—and the SP must both sign the transaction before it can be delivered to the SP's CH. Both sets of PKs are checked by the CH. Whenever a multisig transaction's requester or requestee is in the PK list of the CH requester, or vice versa, the transaction will be broadcast to its own cluster. The other CHs will be informed of the transaction and the requester's PK will be added to the advance list in any other case. A smart home miner is required by policy in her local BC to check the SP's authorisation to access data whenever she gets a multisig transaction. If the user had initially authorised this access, it would have been great. Requesting packets from storage is the first step in the process, as seen in Figure 2b. Encryption is applied to the packets before they are forwarded to the requester using their private key. Before transmitting the data, the miner may employ methods like as noise induction or safe response to further ensure anonymity. A miner has the ability to change the result of a multisig transaction to either a "1" or a "0." They can then determine if the requester is authorised to view the data. The miner must store the multisig transaction in their local BC after data transmission to the requester is complete. The next step is for the miner to submit the multisignature transaction to a randomly chosen group of CHs so it may be saved on the overlay network. You can prove that the user gave you the data by looking at the saved multisignature transactions. Another possible usage is to notify other nodes of suspicious behaviour, such as when one node asks for data it doesn't have authorisation to access. Not transmitting multisig transactions to the overlay BC is an option for miners who do not want this availability made public. This makes the user's privacy more secure as an attacker can't link their true identity to their transactions. The service provider (SP) or the homeowners may want access to a device's data in a smart home environment for many reasons. The following policy levels are established to manage the amount of network overhead in particular scenarios:

- If the requester is the user or an SP which is authorized to access the entire chain of data, then the miner sends block-number and hash of data in storage.
- Otherwise, the miner sends the minimum possible data that can satisfy the requester query by using methods like adding noise or safe answer.

We need all CHs who have sent a transaction to maintain it in their BC. This is a requirement in our system. The CHs of both the requester and the requestee are likewise responsible for recording the

transaction. In the event that other nodes are involved in any intermediate communication that is associated with a particular transaction, they will determine whether or not to store that transaction.

CONCLUSION

Concerns like data integrity, scalability, and security can be practically addressed by incorporating blockchain technology into the IoT. Low scalability, energy inefficiency, and high processing costs make conventional blockchain models unfit for IoT deployments on a large scale. The fundamental objective of this research was to provide an expandable and safe framework for the Internet of Things. It employs a layered blockchain architecture that spreads out work over many blockchain levels to achieve maximum efficiency. Using an edge blockchain for real-time Internet of Things transactions and a core blockchain for long-term data storage and integrity, the suggested design aims to increase security, decrease latency, and improve transaction efficiency. Following an examination of critical technological obstacles, such as energy-saving cryptographic algorithms, cross-chain interoperability, and efficient consensus procedures, we laid forth practical ways to overcome these problems. Scalability, security, and resource utilisation are all much enhanced by the layered blockchain approach as compared to conventional single-layer blockchain systems. Consequently, it's a viable and efficient method for Internet of Things applications in several fields, including healthcare, supply chain management, smart cities, and many more.

References

1. F. Weber, J. Smith, and K. Brown, “Security challenges in IoT networks: A survey,” IEEE Internet of Things Journal, vol. 5, no. 6, pp. 4501–4515, 2018.
2. X. Zhang, L. Wang, and M. Chen, “Blockchain-based authentication and data integrity in IoT,” IEEE Transactions on Industrial Informatics, vol. 16, no. 8, pp. 5562–5571, 2020.
3. M. Dorri, S. S. Kanhere, and R. Jurdak, “Blockchain for IoT security and privacy: The lightweight approach,” in Proc. IEEE Int. Conf. Internet-of-Things (IoT), Sydney, Australia, 2017, pp. 187–194.
4. M. Khan, T. A. Zia, and S. A. Madani, “A blockchain-based secure authentication framework for IoT devices,” Sensors, vol. 19, no. 19, pp. 4205, 2019.
5. S. Moin, R. Ramezan, and H. Amini, “Smart contracts in industrial IoT: A secure and scalable approach,” Future Generation Computer Systems, vol. 125, pp. 34–45, 2021.
6. P. Gupta, N. Patel, and A. Reddy, “Performance analysis of Hyperledger Fabric and Ethereum for IoT data security,” Journal of Blockchain Research, vol. 7, no. 2, pp. 98–112, 2022.
7. Y. Xu, J. Li, and H. Zhang, “Consensus mechanisms for blockchain-based IoT networks: A comparative study,” IEEE Access, vol. 8, pp. 65432–65450, 2020.
8. J. Zheng, C. Wang, and Y. Liu, “Energy-efficient blockchain solutions for IoT applications,” ACM Transactions on Internet Technology, vol. 21, no. 3, pp. 1–21, 2021.
9. H. Liu, P. Zhao, and X. Tang, “Sharding and sidechain approaches for scalable blockchain in IoT,”

Computer Networks, vol. 195, pp. 108152, 2021.

10. R. Rabbani, M. Alam, and S. U. Rehman, “A multi-tier blockchain model for secure IoT networks,” IEEE Transactions on Emerging Topics in Computing, vol. 11, no. 1, pp. 112–123, 2022.
11. L. Wang, Y. Sun, and K. Zhao, “Hybrid blockchain architectures for scalable IoT security,” Future Internet, vol. 15, no. 1, pp. 19, 2023.
12. Das, Manik Lal, "Privacy and Security Challenges in Internet of Things," Distributed Computing and Internet Technology. , pp. 33-48, 2015.
13. Ho, G., Leung, D., Mishra, P., Hosseini, A., Song, D. and Wagner, D., , "Smart locks: Lessons for securing commodity internet of things devices.," in Proceedings of the 11th ACM on Asia Conference on Computer and Communications Security.
14. M. Amoozadeh et al.,, "Security vulnerabilities of connected vehicle streams and their impact on cooperative driving," IEEE Communications Magazine, vol. 53, no. 6, pp. 126-132, 2015.
15. Skarmeta, Antonio F., Jose L. Hernandez-Ramos, and M. Moreno., "A decentralized approach for security and privacy challenges in the internet of things," in nternet of Things (WF-IoT), 2014 IEEE World Forum on, 2014.
16. H. Gross; M. Holbl, D. Slamanig, and R. Spreitzer, "Privacy-Aware Authentication in the Internet of Things," Cryptology and Network Security. Springer International Publishing, pp. 32-39, 2015.