International Journal of Computer Applications (0975 - 8887)
Volume 186 - No.47, November 2024

Hierarchical Blockchain-based Security Solutions for IoT Infrastructure: A Technical Review

Rakshitha K. Manru
Department of Computer Science Engineering,
R V College of Engineering, Bangalore,
560059, Karnataka, India.

Sowmyarani C.N., PhD
Associate Professor
Department of Computer Science Engineering,
R V College Of Engineering, Bangalore,
560059, Karnataka, India.

ABSTRACT

The use of Internet of Things (IoT) devices has increased dramatically in this era. An serious lack of storage resources may someday result from the exponential increase in the amount of data produced by these devices. The lack of standardisation in IoT device data format is another issue. This necessitates the requirement for a highly adaptable and scalable system that can securely store the data from these devices while also offering the required protection against several cyberattacks. To address these problems, blockchain offers a practical answer. In addition to offering immutability qualities, its decentralised architecture avoids a single point of failure. It allows for easier coordination between different IoT devices and is more reliable than the conventional centralised solution. However, when employed in Internet of Things applications, the present blockchain systems have constraints regarding security and scalability. It is feasible to build a more effective, safe, and scalable system that can manage the massive amount of data produced by IoT devices by creating a hierarchical blockchain. This study examines the difficulties that current blockchain-based systems encounter and the several hierarchical blockchain-based solutions that scholars have suggested to address these problems.

Keywords

Internet of Things, Hierarchical Blockchain, Data security, Scalability

1. INTRODUCTION

The exponential expansion of the Internet of Things (IoT) has ushered in a multitude of advantages and possibilities.[1][2], but it has also introduced challenges in managing and securing a large number of interconnected devices. According to forecasts made by the International Data Corporation (IDC), there will be an astounding 41.6 billion IoT devices by 2025, producing 79.4 zettabytes (ZB) of data. However, there are serious problems with the conventional approaches of controlling IoT devices via centralised servers, which compromises their security and efficacy.

A single point of failure arising from centralised systems is one of the main worries. When every Internet of Things device is reliant on a single server, any malfunction or hacking of that server has the potential to bring down the entire system, creating disruptions and security holes. Centralised servers are appealing to malicious actors because they provide a profitable target for assaults[3]. Exploiting a central point of failure could result in widespread disruption or unauthorized access to sensitive data[4].

The over-reliance on centralised servers, where customers give a third party complete access and control over their IoT devices and data, is another problem. Because the central server might misuse its power by taking complete control over IoT devices or by taking advantage of the personal data contained within them, this concentration of power creates privacy issues. Moreover, physical separation between the Internet of Things (IoT) devices and the central server, which is frequently cloud-based, can cause latency and responsiveness delays, impeding timely operations and real-time interactions.

The use of blockchain technology has emerged as a viable way to address these issues. Blockchain, which was first created as the core technology behind cryptocurrencies, provides a decentralised, unchangeable record that doesn't depend on a reliable middleman[5]. This makes it suitable for securing IoT data in a transparent and tamper- resistant manner.IoT devices may securely record and validate their interactions and transactions without requiring a centralised authority by utilising blockchain. Because every device has a copy of the blockchain on it, there is never a single point of failure. The decentralised structure of blockchain improves system resilience and keeps devices from being manipulated or controlled by unauthorised par- ties. Furthermore, it is simpler to identify and track any unauthorised alterations or tampering efforts because to the openness and immutability of blockchain technology.

A Private blockchain on the Hyperledger Fabric platform that uses a consensus mechanism based on Byzantine Fault Tolerance (BFT). This method offers potential efficiency advantages and shows notable improvements over conventional linear blockchain configurations. One significant drawback, though, is that the results were obtained using synthetic data rather than real IoT devices, which might have an impact on how successful it is in practical IoT applications[6].

A Public blockchain built on the Bitcoin platform that uses the Proof of Work (PoW) consensus method. Although PoW is known for its security and resilience, its high computing require-

ments make it unsuitable for large-scale IoT networks where efficiency and scalability are crucial[7]. Another method makes use of a public blockchain and a simple, Bitcoin-based bespoke consensus mechanism. Despite being intended to be more scalable, this approach has trouble managing a high volume of IoT devices, which restricts its use in big IoT networks where scalability and flexibility are required[8].

Hyperledger Fabric is a private blockchain that uses swarm-based communication consensus. This strategy seeks to improve communication efficiency, but because there is a dearth of experimental data, it is challenging to assess its practical relevance, which raises concerns about its dependability and efficacy in real-world situations.Another method makes use of a virtual computer and local servers to construct a lightweight Proof of Random consensus mechanism on a private blockchain. For academics looking for alternatives in IoT applications, this approach provides a comparative study of different consensus processes. The potential of various consensus models for certain use cases may be assessed with the use of such comparisons[9]. A public blockchain built on Ethereum using a leader-based bespoke consensus method. For tiny networks, when large-scale scalability is not required, this solution is especially made. Although it works well in small contexts, its inability to scale restricts its use in bigger or more intricate network configurations[10].

In conclusion, these techniques demonstrate a variety of blockchain implementation strategies, each with unique frameworks and consensus processes. While private blockchains based on Hyperledger and virtual machines provide interesting but experimentally restricted choices, public blockchains based on Bitcoin and Ethereum confront scalability issues, especially for massive IoT applications[11]. The criteria for scalability, computing efficiency, and real-world applicability—particularly in the context of the Internet of Things and other specialised domains play a major role in determining whether a methodology is appropriate[12].

2. CHALLENGES FACED FOR CURRENT BLOCKCHAIN-BASED SYSTEM

The security and dependability of Internet of Things (IoT) data have significantly improved with the combination of blockchain technology and IoT. To fully realise the promise of this integration, other obstacles must be addressed as well. It is likely that the make up will change after file submission. For this reason, we ask you to ignore details such as slightly long lines, page stretching, or figures falling out of synchronization, as these details can be dealt with at a later stage.

2.1 High Computational power requirement

The high processing power needed for blockchain operations, especially for carrying out consensus procedures, is one of the main obstacles to integrating blockchain technology with IoT. In blockchain networks, consensus techniques are crucial for reaching consensus across dispersed nodes, guaranteeing the validity of transactions and the security and immutability of the ledger. Despite being built with security and resilience in mind, many mechanisms—like Proof of Work (PoW), Proof of Stake (PoS), and other computationally demanding algorithms—require a lot of computing power to operate efficiently[14]. However, the majority of IoT devices are made to be small and energy-efficient. Because they are frequently used in settings where resource efficiency and power conservation are crucial, these devices usually have restricted processing power, memory, and battery life. For example, a wearable health monitor or a smart sensor in an industrial environment may be built with low power consumption in mind, intended to carry out basic computing or data collection rather than intricate cryptographic computations. Using a consensus mechanism that requires a lot of resources on such devices might quickly deplete their batteries, shorten their operating life, and perhaps cause hardware failure or overheating. For IoT devices, this disparity in processing power poses a significant obstacle to full participation in conventional blockchain networks. To validate transactions and produce new blocks, for instance, nodes in a PoW-based blockchain compete to solve challenging cryptographic problems. Although this method protects against assaults and guarantees security, it necessitates high-performance processors that are normally found in data centres or specialist mining rigs, which are considerably more than the majority of IoT devices can provide. As a result, many IoT devices are unable to handle these computing demands, which restricts their capacity to actively engage in consensus procedures and, thus, reduces their potential for integration into blockchain networks.

Furthermore, many IoT devices lack the processing capacity necessary for even alternative consensus processes like PoS, despite the fact that they are often less resource-intensive than PoW. A move towards lightweight consensus algorithms that can function within the limitations of IoT hardware is necessary if IoT networks are to take use of blockchain's security and data integrity characteristics. The high processing demands of conventional blockchain consensus algorithms continue to be a major barrier to the smooth integration of blockchain with IoT in the absence of such modifications.[15]

2.2 Very high memory requirement

The growing memory need brought on by blockchain's evolving data structure is another major obstacle to integrating blockchain with IoT. For a blockchain network to remain transparent, secure, and immutable, every node has to have a copy of the complete ledger, including all previous transactions. For strong servers and PCs with large storage capacities, this need is doable, but it becomes an issue for Internet of Things devices. The majority of Internet of Things devices, including wearables, sensors, and smart appliances, are made to be small, light, and have little memory or storage. Each node must keep more data as the blockchain expands over time, possibly exceeding the storage capacity of many IoT devices.This mismatch limits the ability of IoT devices to function as full nodes, creating a fundamental barrier to their integration with blockchain technology. The memory limit has an impact on network performance in addition to limiting storage. Every transaction that is added to the chain in a blockchain has to be synchronised with every node, including Internet of Things devices if they are connected to the network. Handling and processing massive volumes of blockchain data can have a substantial influence on the fundamental functionality of devices with limited memory, either slowing them down or causing them to malfunction. Off-chain storage, in which IoT devices store just transaction references while the whole ledger is kept elsewhere, and lightweight or pruned blockchains, in which only current or crucial transaction data is saved on IoT nodes, are two options being investigated to solve these issues.Though these methods aid in lowering memory needs, they may also add additional complications, especially in the areas of data security and accessibility, which need to be worked

out further before IoT devices can completely fulfill blockchain's requirements.

2.3 Does not support parallel Transaction

The inability of blockchain's inherent architecture to provide parallel transaction processing is a major obstacle for handling the massive volumes of data produced by Internet of Things devices. To guarantee that only legitimate, validated blocks are appended to the chain, transactions in a blockchain are handled precisely sequentially. Because each transaction must be validated in connection to the ones that came before it, in a precise order, this sequential processing is crucial to preserving the network's security and integrity. But when it comes to managing real-time data from IoT devices—which frequently generate massive amounts of data quickly—this architecture has drawbacks. The sequential structure of blockchain transactions makes it challenging to interpret and analyse IoT data since it cannot keep up with the fast data stream.Timely insights from IoT data are delayed due to blockchain processing's lack of parallelism. Since many IoT devices are constantly producing data, the blockchain's sequential processing method creates a bottleneck that hinders effective analysis and reaction. These delays reduce the usefulness of utilising blockchain to administer IoT networks in situations where real-time data analysis is essential, including tracking assets in logistics, monitoring environmental conditions, or controlling smart city infrastructure. Therefore, it becomes difficult to extract rapid, meaningful insights from the massive amounts of data generated by IoT devices unless blockchain is modified to support parallel processing or other solutions are used.[15]

2.4 Blockchain Consensus Tradeoff

The effectiveness of the consensus process and the number of nodes in the network are fundamentally traded off in blockchain technology. Reducing the number of nodes participating in the consensus process is frequently necessary to achieve high transaction throughput, typically expressed in transactions per second. Limiting node involvement speeds up processing by cutting down on the amount of time required to obtain agreement. However, this strategy sacrifices two of blockchain's primary advantages: scalability and decentralization. This trade-off limits the capacity to grow successfully while keeping a decentralized structure, which can compromise the resilience and security usually associated with blockchain networks in the context of the Internet of Things, where large networks of devices may need to participate.[16]

The idea of a hierarchical blockchain has surfaced as a viable way to overcome these obstacles and increase scalability and dependability. Groups of nodes are arranged hierarchically in hierarchical blockchain architectures, which improve scalability by establishing a tiered approach to consensus and enabling more effective processing without sacrificing security. While supporting bigger and more complicated networks, hierarchical blockchain can lessen the consensus load on individual nodes by dividing the network into smaller, more manageable portions, each of which is in charge of a distinct subset of transactions. For blockchain-based IoT applications, this approach provides a more stable platform, making it possible to manage the particular requirements of IoT systems in sectors like smart cities, logistics, and healthcare.[17]

3. HIERARCHICAL BLOCKCHAIN-BASED APPROACHES IN IOT

A blockchain variation known as a hierarchical blockchain adds a hierarchical structure to improve efficiency and scalability. This method arranges several linked blockchains in a hierarchical fashion, where each level corresponds to a distinct network layer. While the highest levels combine these blocks and produce a summary of transactions, the lower levels handle individual transactions and record them in their separate blocks. This hierarchical structure is appropriate for large-scale applications such as the Internet of Things (IoT) because it enables quicker transaction processing and lowers computational needs. The fundamental ideas of security and decentralisation are upheld by the hierarchical blockchain, which also provides increased scalability and performance. This section covers current IoT blockchain research that has used a hierarchical architecture to overcome the problems outlined above. It investigates how well the technique used works and how it affects getting over these obstacles.[18]

Adam Ibrahim Abdi's [1] proposed solution is a hierarchical, multi-layered access control system that uses chaincodes to ensure secure communication between different entities without relying on third parties. Because of its scalability and lightweight construction, the system may be used in a variety of sectors and industries. The The authors suggest a novel architecture that gives IoT devices and data fine-grained access control using blockchain technology. The system facilitates safe communication between many entities by having numerous levels, each with its own set of chaincodes. The Edge Blockchain Manager (EBCM), which is in charge of device authorisation and authentication, is the initial layer (IoT devices).The Aggregated Edge Blockchain Manager (AEBCM), which consists of several AEBCM nodes and allows devices to communicate and administer ABAC (Attribute-Based Access Control) rules, is the second layer. The Cloud Consortium Blockchain Manager (CCBCM), which is The last layer is made up of CCBCM nodes that ensure that only those with permission may access the resources. The authors also do a security analysis and prototype implementation to assess the suggested solution.The Hyperledger Calliper tool is utilised to evaluate the system's performance using many metrics, including transaction latency and throughput. The possible uses of this system in a number of sectors, such as smart cities, transit, and healthcare, are covered in the study. By using blockchain technology to address data privacy and security concerns, the proposed solution has the potential to revolutionize these industries.

Mohammad Saidur Rahman. [12] proposes an innovative and interoperable blockchain platform that ensures IoT data integrity in smart cities. The paper highlights the challenges of existing cloud-based centralized IIoT data management processes for smart cities, which are untrusted and can be compromised by attackers to generate false data and disrupt administrative tasks. In order to overcome these obstacles, the suggested platform introduces a hierarchical blockchain architecture that makes sure that hierarchical organisations in smart city applications may communicate easily with one another. In order to ensure the integrity of heterogeneous IoT data in the smart city system, the suggested platform employs a blockchain tree topology. The authors make the assumption that a legislative body, such the city council, is in charge of overseeing a smart city and that it offers a number of smart services, such as electricity, water, and environmental management.Through the introduction of multi-level blockchain interaction, the suggested platform also tackles the problem of blockchain interoperability.

Interoperability is a problem that has to be resolved since various blockchains may have distinct transaction formats. The proposed platform overcomes this challenge by introducing an innovative and interoperable blockchain platform that ensures IoT data integrity in smart cities.The authors conducted experiments on a testbed to evaluate the performance of the proposed platform. The testbed consisted of a hierarchical blockchain system that ensured smooth communication among hierarchical organizations in smart city applications. The outcomes of the trial demonstrated how well the suggested platform worked to protect the integrity of IoT data in smart cities. By identifying and stopping assaults on IoT devices and data, the platform made sure that only reliable data was utilized for administrative activities. The platform worked well in several circumstances according to the authors' evaluation of its throughput and latency performance.

Zhiguo Wan et al.[14] proposed a novel blockchain system that addressed scalability and security issues associated with traditional blockchain systems in large-scale IoT applications. The system uses a Hierarchical Identity-Based Encryption(HIBE) approach to create distinct and verifiable identities for each IoT device which function as the respective public keys. HIBE Chain is a blockchain tree structure. It consists of IoT devices at the bottom of the hierarchy and validators above (as per the required levels of hierarchy). This system has been designed with a PBFT consensus algorithm to enable effective transaction validation under the assumption of a Byzantine threat model. From leaf blockchain to root blockchain, HIBEChain constructs consensus layer by layer. Parallel processing and effective storage management are made possible by the hierarchical structure that HIBEChain developed. Large-scale IoT networks with high throughput, low latency, and safe data exchange may be supported by HIBEChain, according to the testing results. Large-scale Internet of Things applications now have an effective and safe option thanks to the technology, which also offered a potential way around the drawbacks of conventional blockchain systems.

Toka et al. [13] proposed a novel approach that uses the Hyperledger Fabric blockchain network to address the security issues with IoT-based devices. The design comprises of an IoT device, three Hyperledger Fabric organisations (publisher, broker, and subscriber), a simple Hyperledger Fabric blockchain network, and the MQTT protocol for IoT data transport via Docker Swarm Network. It uses the smart contract functionality, access control policy, and consensus mechanism of the Hyperledger Fabric blockchain network to offer a safe and scalable solution for Internet of Things (IoT) based devices. The method is shown using simulated Internet of Things devices and a basic Hyperledger Fabric blockchain network. It is demonstrated that the shortcomings in IoT security (identity, authenticity, authorisation, accountability, and integrity) have mostly been addressed.

Mahmoud Tayseer Al [2] Ahmed proposed a hierarchical blockchain architecture based on a simplified version of the POA consensus algorithm. Here nodes are verified by a group of adjacent nodes by verifying a transaction containing digitally signed information. The proposed architecture mainly consists of two main stages namely clustering process and blockchain-based authentication process. The primary task of the clustering process is to create the architecture's hierarchical structure. The arrangement of nodes is determined by the average energy and processing power. The cluster head at the top level will be the node with the largest computing power. Based on their average energy, the nearby nodes will then be designated as the cluster head. The cluster head of every blockchain will be a node that is present in the level above it for node authentication. The cluster head stores all of the node information in an authentication table. Omnet++, an event simulator built on the C++ programming language, and the NED environment configuration language are used to mimic clustering. Docker containers and the network are used to imitate the network for Blockchain authentication. The simulation results have shown the framework is lightweight and resources requirement for computation and storage is lower to existing protocols.

Dongjun Na [12] proposed a hierarchical blockchain architecture consisting of two levels. IOT chain level manages the storage of data from IoT Devices and Monitoring Chain controls the access control of the data and metadata present in the IoT chain and also manages size of Iot Chain. The author has used the Schnorr signature method to export the blockchain from IoT chain to Monitoring Chain to guarantee that the network communication is not lost. In IoT Chain, the authors have considered mainly 3 kinds of nodes: Nodeleader , Nodeic and Nodeexport . leader node is elected via VRF (Variable Random Function). Export Node is the node containing the export module which is responsible for sending the block for access control to Monitoring chain. Node.js is used to implement the IoT chain, and three Raspberry Pi 4 computers are used for the implementation.Hyperledger Fabric is used in the Monitor chain's deployment. GoLang is used in the monitoring chain smart contract implementation. The findings of the experiment demonstrated that a blockchain of a particular size may beat the state-of-the-art system and cut time by 96 percent[5].

4. CONCLUSION

Using blockchain technology has shown to be an effective solution for addressing a variety of IoT data security problems. The Hierarchical Blockchain is a prominent use of this technology that has significantly advanced the Internet of Things. We are able to address a greater num- ber of practical issues and improve the use of IoT devices by employing effective designs. The mainstream adoption of these devices has been significantly hampered by security concerns around IoT data. The adoption of Blockchain Technology has successfully reduced these difficulties. IoT device data integrity and secrecy are guaranteed by the decentralised and unchangeable nature of blockchain technology. Blockchain increases trust and transparency by offering a tamper-proof system for data storage in a distributed ledger. Many IoT applications have been developed with the help of the Hierarchical Blockchain architecture. It makes hierarchical control and organisation of IoT devices and the data they are connected with possible. Better scalability, efficiency, and coordination between devices and IoT ecosystem players are made possible by this technique.[11] IoT devices' full potential may be realised through effective designs based on the foundation of hierarchical blockchain technology. They facilitate the creation of creative solutions for pressing issues by enabling smooth device integration and communication. This can include a wide range of industries, including energy management, transportation, and healthcare. We can fully utilise IoT devices and so enable the resolution of a wider range of real-life difficulties by addressing security concerns and offering effective frameworks.

5. REFERENCES

[1] Adam Ibrahim Abdi, Fathy Elbouraey Eassa, Kamal Jambi, Khalid Almarhabi, Maher Khemakhem, Abdullah Basuhail, and Mohammad Yamin. Hierarchical blockchain-based

multi-chaincode access control for securing iot systems. *Electronics*, 11(5):711, 2022.

[2] Mahmoud Tayseer Al Ahmed, Fazirulhisyam Hashim, Shaiful Jahari Hashim, and Azizol Abdullah. Hierarchical blockchain structure for node authentication in iot networks. *Egyptian Informatics Journal*, 23(2):345–361, 2022.

[3] Sînică Alboaie, Lenuta Alboaie, Zeev Pritzker, and Adrian Iftene. Secret smart contracts in hierarchical blockchains. 2019.

[4] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen 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)*, pages 618–623. IEEE, 2017.

[5] Ali Dorri, Salil S Kanhere, Raja Jurdak, and Praveen Gauravaram. Lsb: A lightweight scalable blockchain for iot security and anonymity. *Journal of Parallel and Distributed Computing*, 134:180–197, 2019.

[6] Akshay Gapchup, Ankit Wani, Durvesh Gapchup, and Shashank Jadhav. Health care systems using internet of things. *IJIRCCE*, 4(12), 2016.

[7] Seyoung Huh, Sangrae Cho, and Soohyung Kim. Managing iot devices using blockchain platform. In *2017 19th international conference on advanced communication technology (ICACT)*, pages 464–467. IEEE, 2017.

[8] Yiming Jiang, Chenxu Wang, Yawei Wang, and Lang Gao. A cross-chain solution to integrating multiple blockchains for iot data management. *Sensors*, 19(9):2042, 2019.

[9] Aditya Kulkarni and Sonal Sathe. Healthcare applications of the internet of things : A review. 2014.

[10] Ahmed Afif Monrat, Olov Schelén, and Karl Andersson. A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, 7:117134–117151, 2019.

[11] Dongjun Na and Sejin Park. Iot-chain and monitoring-chain using multilevel blockchain for iot security. *Sensors*, 22(21):8271, 2022.

[12] Mohammad Saidur Rahman, MAP Chamikara, Ibrahim Khalil, and Abdelaziz Bouras. Blockchain-of-blockchains: An interoperable blockchain platform for ensuring iot data integrity in smart city. *Journal of Industrial Information Integration*, 30:100408, 2022.

[13] Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. A survey on the adoption of blockchain in iot: Challenges and solutions. *Blockchain: Research and Applications*, 2(2):100006, 2021.

[14] Zhiguo Wan, Wei Liu, and Hui Cui. Hibechain: A hierarchical identity-based blockchain system for large-scale iot. *IEEE Transactions on Dependable and Secure Computing*, 2022.

[15] Gang Wang, Zhijie Shi, Mark Nixon, and Song Han. Chainsplitter: Towards blockchain-based industrial iot architecture for supporting hierarchical storage. In *2019 IEEE International Conference on Blockchain (Blockchain)*, pages 166–175. IEEE, 2019.

[16] Qingqing Xie, Fan Dong, Xia Feng, et al. Hlochain: A hierarchical blockchain framework with lightweight consensus and optimized storage for iot. *Security and Communication Networks*, 2023, 2023.

[17] Yuchen Yang, Longfei Wu, Guisheng Yin, Lijie Li, and Hongbin Zhao. A survey on security and privacy issues in internet-of-things. *IEEE Internet of things Journal*, 4(5):1250–1258, 2017.

[18] Zibin Zheng, Shaoan Xie, Hongning Dai, Xiangping Chen, and Huaimin Wang. An overview of blockchain technology: Architecture, consensus, and future trends. In *2017 IEEE international congress on big data (BigData congress)*, pages 557–564. Ieee, 2017.