Blockchain Applications in IoT: A Literature Review

ZhengYuan Zhang (A paper written under the guidance of Prof. Raj Jain) Download

Abstract

This paper reviews the applications of Blockchain on the Internet of Things (IoT). Firstly, the basic concepts of IoT and Blockchain are introduced. Then, the main challenges faced by IoT infrastructure are discussed, such as security and privacy issues, scalability, and observability issues. Next, how Blockchain can enhance IoT system management through immutability, decentralization, and traceability is analyzed. In addition, the challenges and limitations of applying blockchain technology in IoT are discussed, such as the limited computational capabilities of edge devices and the overhead of consensus protocols. Finally, the main application scenarios of Blockchain in IoT are summarized, such as Intellectual property protection access control systems.This paper has used IoT-related concepts from Module 11.

Keywords: *Blockchain, Internet of Things, IoT, Scalability, Observability, Immutability, Decentralization, Traceability, Intellectual property protection, Access control system*

Table of Contents

1. Introduction

In recent years, the integration of Blockchain (BC) and the Internet of Things (IoT) has garnered increasing attention across various industries, attracting interest due to its potential to enhance security, transparency, and efficiency. The motivation behind this literature review is to investigate how these two technologies can work together to facilitate secure and transparent data sharing, as well as to improve the efficiency and reliability of IoT devices. The objective is to analyze the current state of research on the integration of Blockchain and IoT, identify the challenges and opportunities present, and provide an abstract and fundamental introduction to the future study of combining Blockchain with IoT.

2. Fundamentals of IoT and BlockChain

The Internet of Things (IoT) has undeniably revolutionized the way we interact with devices and data, creating a network of interconnected objects that brings convenience and efficiency to various sectors, including healthcare, telecommunications, and industry[Qureshi22]. These devices have the capability to collect and exchange data with each other, utilizing unique identifiers within the network [Qureshi22]. While IoT devices like smartwatches and smartphones are commonly known, they are also being utilized across various industries to enhance efficiency and improve quality of life. In sectors such as agriculture, healthcare, and transportation, IoT sensors and connectivity play a crucial role in monitoring and optimizing processes. On the other hand, Blockchain technology, with its distributed ledger and transparency, has transformed transaction processes[Hu20]. It is being implemented in various industries, including the food industry, where it enhances traceability and creates a sustainable competitive advantage [Qureshi22]. Blockchain technology is also being utilized in supply chain management, enhancing traceability and creating innovative business models.

2.1 Internet of Things

Overall, IoT means the interconnection of heterogeneous devices, which can be sensors, actuators, or any other devices that can be connected to the Internet except traditional computers. Those devices are usually small, low power, and low cost. They are usually connected to the Internet through a Local Area Network (LAN) or a Wide Area Network (WAN). IoT devices often use various layer-2 wireless and wired protocols to communicate with each other, like Wi-Fi, Zig Bee Smart [Jain16]. Less noticeable, power line communication is also being used. HomePlug GP has provided a smart management plane solution for IoT management at home[Jain16]. IoT devices often use message-passing protocols like MQTT, CoAP, etc., to communicate with each other.

IoT Layer 2

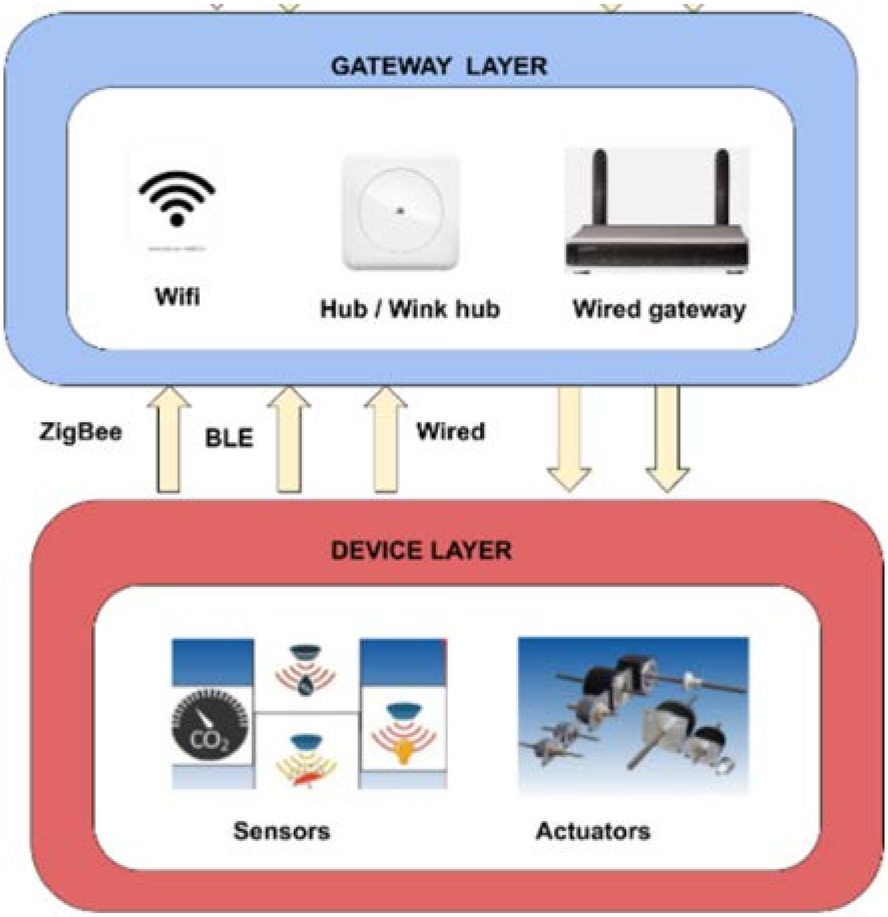


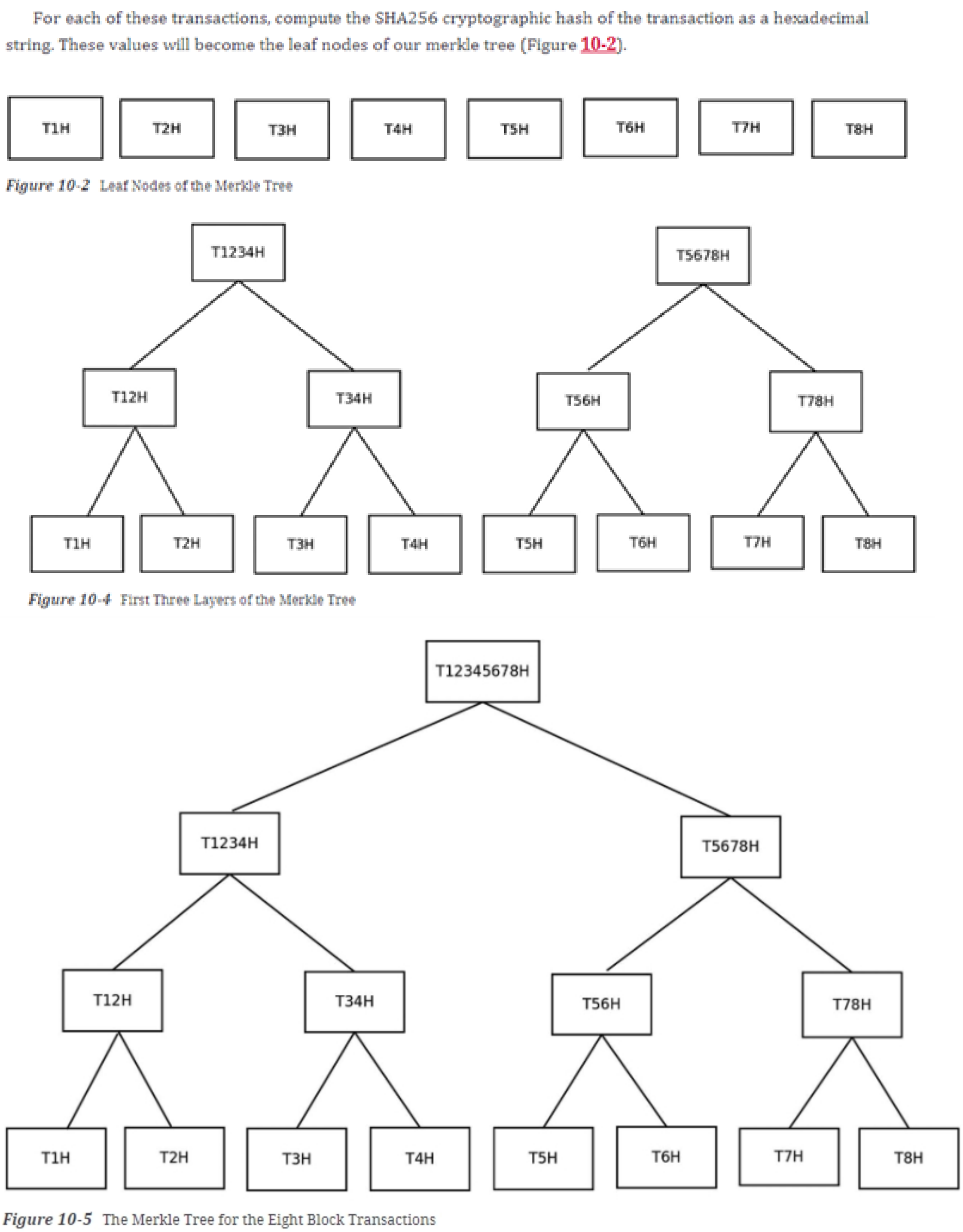
Fig.1

J. N. Qureshi, M. S *Blockchain applications for the Internet of Things: Systematic review and challenges.* URL: https://doi.org/10.1016/j.micpro.2022.104632

2.2 Blockchain

A distributed ledger technology (DLT) like Blockchain typically consists of three main components: a data model representing the current state of the system, a CRUD (Create, Read, Update, Delete) mechanism to modify that model, and a synchronization protocol[Qureshi22]. The ledger in a DLT is distributed among all participants, and each copy of the ledger needs to be synchronized to maintain a uniform view of the system state[Sunyaev22]. To represent the data model in a blockchain, a common approach is to use a linked-list data structure made up of blocks[Garewal20]. Each block in the Blockchain has two main sections: the header and the body. The body contains the hash codes of transactions using the SHA256 algorithm [Garewal20]. The header contains important fields such as the identifier of the previous block [Qureshi22]. The identifier for each block is generated using the SHA256 hash algorithm on the entire block's content, forming a Merkle tree, creating a transparent and immutable record of all transactions within the Blockchain [Garewal20]. The root of the Merkle tree becomes the unique identifier of the block [Garewal20]; any change to a block would result in a mismatch with the previously generated identifier, which is stored in the headers of subsequent blocks, preserving the integrity of the system [Garewal20]. An abstract view of the process is below

Merkle Tree Construction



For each of these transactions, compute the SHA256 cryptographic hash of the transaction as a hexadecimal string. These values will become the leaf nodes of our merkle tree (Figure 10-2).

Figure 10-2 Leaf Nodes of the Merkle Tree

Figure 10-4 First Three Layers of the Merkle Tree

Figure 10-5 The Merkle Tree for the Eight Block Transactions

Fig.2

K. S. Garewal, *Practical Blockchains and Cryptocurrencies: Speed Up Your Application Development Process and Develop Distributed Applications with Confidence*
URL:https://learning.oreilly.com/library/view/practical-blockchains-and/9781484258934/

3. Key Challenges in IoT Infrastructure

IoT is not without its challenges. The main challenges IoT faces are inherent in its heterogeneous, highly distributed, limited computational resources. Three aspects are discussed in this review: Security and Privacy, Scalability, and Observability.

3.1 Scalability

Scalability is another issue. If the IoT network were implemented as having a centralized management plane over distributed data nodes spread over different geolocations, Single point failure occurring at the management plane could severely impair the availability of the system, as every edge node requires that central management plane to properly distribute necessary configuration files, and to authorize and authentication a transaction.[Waheed,2019] . If every operation of IoT devices is required to be secured and observability is desired, then the control and management plane would be the upper bound of the IoT network since every operation happens after the necessary control and management operations are blocked.

3.2 Obvervability

Observability refers to the ability to infer the internal state of a system from its external outputs. By implementing effective observability mechanisms, organizations can gain real-time visibility into the functioning of their IoT systems. This includes monitoring the connectivity and communication between devices, tracking data flows, detecting anomalies or failures, and identifying potential bottlenecks. In the context of IoT, The sheer volume of data generated by numerous devices and the heterogeneity of data formats and protocols pose significant obstacles. Additionally, the distributed nature of IoT networks makes it essential to have mechanisms in place for centralized monitoring and analysis of data from multiple edge devices.

When a user taps on a button on a smartphone, the entire IoT system has to send back a response to the user, which requires heavy synchronization among all the edge nodes and the central management plane. Meanwhile, due to its distributed nature and real-time data production model, IoT requires a real-time message-passing model. Therefore, a reliable and scalable message-passing model is required. Such a message-passing model should be able to handle the message passing between the management plane and the edge nodes, as well as the message passing between the edge nodes. However, the traditional message-passing model such as MQTT, while used widely in IoT, is not able to provide such a reliable and scalable message-passing model. The gaps in tracking caused by the inability of MQTT brokers to continuously and reliably gather metadata on requests/messages directly impact service level objectives[Qureshi19]. Without the reliability to track the state of the system, it is difficult to identify and resolve issues in a timely manner.

4. Blockchain for Enhanced IoT Systems Management

To address the challenges of scalability and security in IoT systems, researchers have proposed various approaches. One approach is the integration of blockchain technology to provide secure access control in IoT systems. Overall, the immutability, decentralization, and audibility features of Blockchain [Qureshi22] have offered a natural approach to tackle the issues discussed in the previous section.

4.1 Blockchain records are immutable

The immutability of records in the Blockchain renders them tamper-proof, as any attempt to modify previously saved data would require an attacker to breach a block, and any modification on that code would result in any nodes holding a reference to the original block noticing the difference because the identifiers would mismatch with each other[Novo19]. A similar concept can be found in a well-known version control system, Git. Indeed, some implementation of the data structure used by the Blockchain is like Git. Both Git and Blockchain utilize a distributed storage architecture and a data structure composed of blocks[Rahmani22]. In the case of Blockchain, the data structure is called a "block" and is connected in the form of a hash chain, ensuring that the data cannot be arbitrarily modified. Similarly, Git uses a data structure called a "commit" to store changes to files, and these commits are connected in a chain-like structure[Rahmani22]. However, in Git, the consensus of a version of the software, any merge conflict must be agreed upon by all programmers in the project. In the Blockchain, devices use automated consensus protocols to synchronize with the state of the Blockchain.

Blockchain Structure

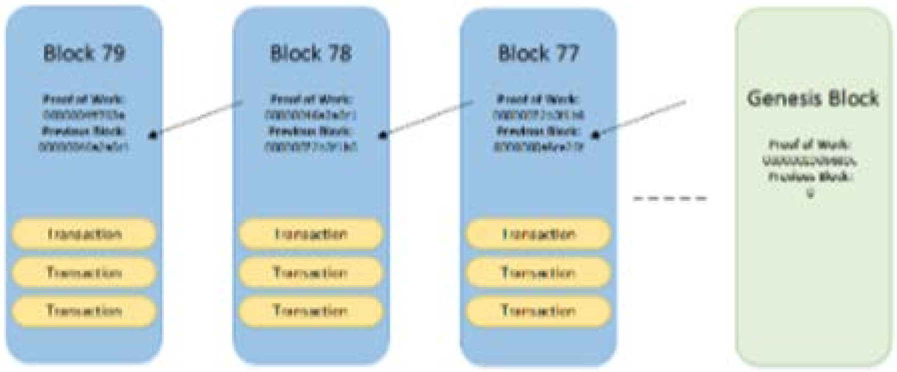


Fig.3

Novo, *Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT* URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8306880&isnumber=8334665

4.2 Decentralized

In traditional Web 2.0 technology, Data transactions are securely authenticated and endorsed within incorporated system frameworks by trusted central third-party entities. This process involves costs associated with server maintenance and potential bottlenecks that may impact execution quality. As authentication and authorization are an inevitable blocking operation, and any software-level asynchronous I/O techniques would not apply the authentication and authorization part are also the bottleneck of the entire IoT infrastructure[Qureshi]. However, in the context of Blockchain (BC), the implementation mechanism differs significantly. BC relies on a decentralized architecture that facilitates block-to-block transactions, eliminating the need for third-party involvement in authentication and verification. Instead of waiting for the control plane to respond to the result, BC allows individual IoT devices to do the authentication and authorization just in time and distributes the work over the entire BC.

4.3 Combining MQTT and Blockchain in IoT

The convergence of MQTT and blockchain technologies presents a revolutionary approach for enhancing security, reliability, and efficiency in IoT systems. MQTT, known for its lightweight and efficient messaging protocol, complements the robust, tamper-proof features of Blockchain, offering a comprehensive solution for IoT communications.

Firstly, the immutable nature of Blockchain ensures data integrity and security for the vast amounts of data transmitted by IoT devices via MQTT. This integration guarantees that data remains unaltered during transmission, maintaining its authenticity and reliability. Furthermore, the decentralized structure of Blockchain eliminates single points of failure, thereby augmenting the overall system's resilience and stability. This aspect synergizes with MQTT's distributed messaging capabilities, enhancing the network's robustness against disruptions.

Additionally, Blockchain's transparency and permanent record-keeping complement MQTT's data-sharing features. This combination fosters trust and transparency in data exchanges, making it particularly valuable for tracking the history of IoT device interactions and transactions.

5. Challenges and limitations

The decentralized nature of blockchain technology allows for the creation of a shared and immutable ledger, which grants authorized participants access to a comprehensive record of all transactions. This transparency not only fosters trust among stakeholders but also enables greater accountability and traceability. However, when it comes to enhancing IoT infrastructure using Blockchain, certain challenges arise due to the inherent characteristics of IoT devices.

5.1 Overhead of verification and digital signature

One specific challenge is that IoT devices often have limited computational capabilities, making them ill-equipped to handle CPU-intensive tasks effectively. In the context of blockchain-enabled IoT devices, this poses a significant issue as signing digital signatures for each block, and the verification process are CPU-intensive tasks. If the IoT devices are not able to handle the CPU-intensive tasks, the entire IoT network will be slowed down. More problematic, since Blockchain is distributed and decentralized, IoT devices might wait for each other for workload not initiated by themselves, which does not happen in the traditional centralized approach.

5.2 Overhead of consensus protocol

Also, the overhead of consensus protocols is another challenge. Consensus protocols play a crucial role in achieving decentralization in blockchain networks. These protocols enable nodes in the network to coordinate and reach a common consensus or single truth without the need for a central authority. They ensure the integrity and security of distributed computing systems. The decentralized nature of blockchain technology presents challenges for edge devices in terms of their limited computational capabilities and the encryption and decryption overhead involved in each transaction[Conoscenti16]. Also, IoT devices may not possess the computational capabilities required by consensus protocols on blockchains[Conoscenti16]. Furthermore, it is not realistic to have a public BC network deployed on IoT devices, as it is unknown if the computational capabilities of IoT devices are able to handle the workload of a public BC network. Due to the limited capabilities of IoT devices, it is likely the Proof of Work (PoW) consensus protocol would not be able to produce a block in a reasonable amount of time, and the node owning more than 50% of the computational power would be able to control the entire network. Therefore, a private BC network is more likely to be deployed on IoT devices. However, the private BC network would not be able to provide the same level of security as a public BC network, as the nodes responsible for the verification now are limited to a set of limited "manager" nodes.

To address the issue just discussed above, Blockchain-optimized protocols often shard the communication domain into sub-domains [Li18]. Consensus protocols play a crucial role in achieving decentralization in blockchain networks. These protocols enable nodes in the network to coordinate and reach a common consensus or single truth without the need for a central authority. They ensure the integrity and security of distributed computing systems. Sharding is a technique used to improve the scalability and efficiency of blockchain networks [Li18]. It involves dividing the network into smaller sub-networks called shards, each of which processes transactions separately. Sharding can help address the computational limitations of edge devices by distributing the workload across multiple shards. This allows for parallel processing and can improve the overall performance of the network. In addition to addressing computational limitations, sharding can also enhance the security of blockchain networks. Sharded blockchains can provide better resistance against attacks and reduce the impact of a compromised shard on the entire network [Li18]. Sharding protocols can assign nodes to shards in a way that ensures a higher level of security[Li18].

5.3 Alternative centralized approach

It is important to note that Blockchain is not the sole solution to scalability, security, and observability challenges faced by IoT devices. In fact, within the traditional perspective of Web 2.0, there still exist centralized, scalable, and observable IoT solutions. For example, In the realm of real-time data analysis on the web, it is common to deploy distributed messaging systems such as Apache Kafka to store messages over a certain period. Apache Kafka itself maintains at least three replicas of each partition, and the entire system consists of multiple nodes. In the event of a node failure, a leader election algorithm is executed to improve availability. As the number of nodes increases, the system's throughput increases linearly. Additionally, cloud service providers have long offered their users the ability to dynamically deploy multiple authorization servers with just a few clicks to meet large-scale demands. With the help of the cloud and Big Data, tools like Apache Kafka, those servers for the control and management plane can be deployed in a distributed manner, and thus, the system can scale proportionally to the number of edge nodes.

Centralized vs. Decentralized

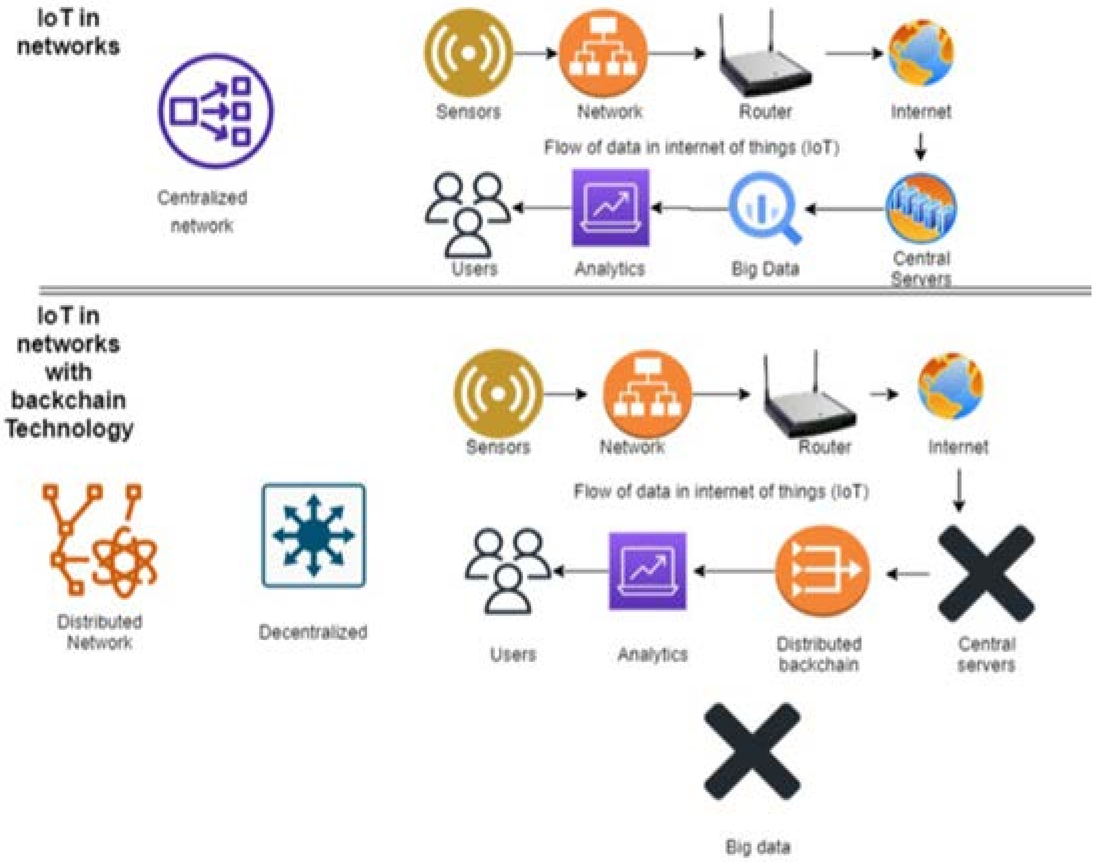


Fig.4

J. N. Qureshi, M. S *Blockchain applications for the Internet of Things: Systematic review and challenges*
URL: https://doi.org/10.1016/j.micpro.2022.104632

6. Use Cases

Blockchain technology has been applied in various industries, including healthcare, supply chain management, and finance. In the context of IoT, Blockchain can be used to enhance the security and efficiency of IoT devices. The following section discusses some of the main use cases of Blockchain in IoT.

6.1 Intellectual property protection

[Lin19] has proposed a method to combine Blockchain and IoT technologies together that can enhance intellectual property protection. Blockchain technology ensures the security and immutability of transaction records, making it difficult for unauthorized people to forge intellectual property rights. The use of IoT devices enables automated processes and real-time data collection, reducing the risk of human error and increasing the accuracy of IP verification. This combined approach provides a more powerful and efficient system for IP protection.

The blockchain system demonstrates the full process of transaction data processing, including hashing, digital signing, sending to the blockchain network through IoT gateways, and validation and storage. Users can retrieve and verify all relevant transaction data using computers or mobile applications, all without human intervention. The system also adheres to popular and standard blockchain header data structures and provides detailed transaction information. All transaction data, after hashing and digital signing, is sent to the blockchain network through IoT gateways with edge computing capabilities. The data is then validated, added to the transaction pool, and stored in the Blockchain. Intellectual property transaction clients can retrieve and verify all relevant transaction data using their computers or mobile apps. For example, a person who purchases a handicraft in an online market can use the app to retrieve information about the author, production process, raw materials, logistics data, etc. All this information can be verified through the blockchain system without human intervention.

Blockchain system architecture

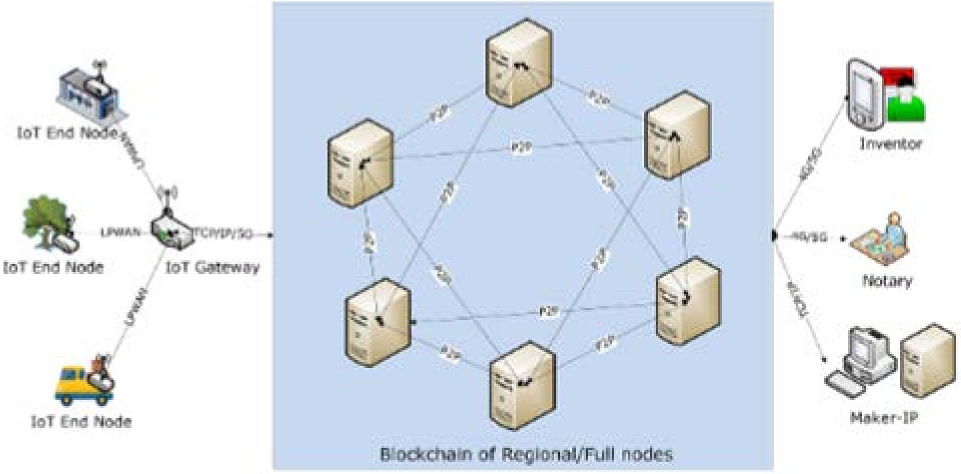


Fig.5

J. Lin et al., *Using Blockchain and IoT Technologies to Enhance Intellectual*
URL:https://doi.org/10.1145/3371238.337124

6.2 Access control system

[Novo19] discusses how Blockchain can be utilized to secure access control to IoT devices and proposes a new architecture of a fully distributed access control system based on blockchain technology for access control. The architecture includes six components: wireless sensor network, manager, agent node, smart contract, blockchain network, and management center. Among them, the manager is responsible for managing the access control permissions of a set of IoT devices. An agent node is a specific blockchain node responsible for deploying the only smart contract in the system. The Smart contract is the core of the management system, and the access control is realized by blockchain technology. The management center is responsible for providing uniform access control policies to managers. The advantages of the proposed architecture include scalability, mobility, accessibility, and concurrency.

Architecture

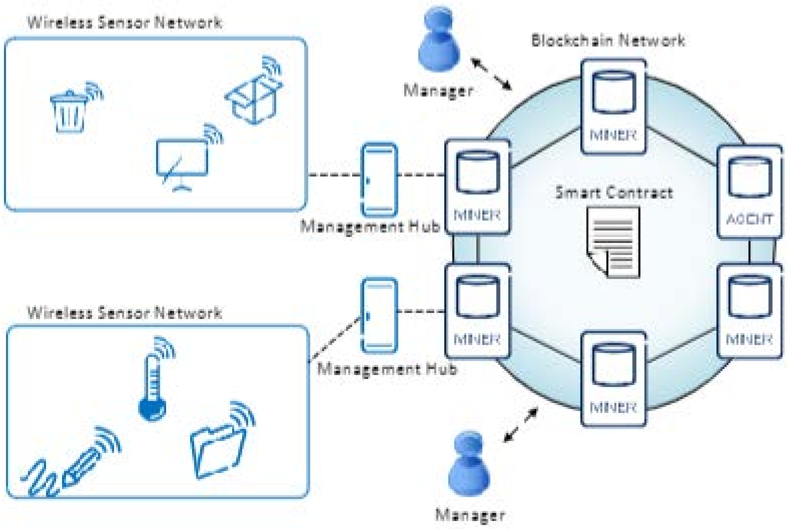


Fig.6

Novo, *Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT* URL:https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8306880&isnumber=8334665

Summary

Blockchain technology has the potential to enhance the security and efficiency of IoT devices. It can be used to improve the security of IoT devices by providing a tamper-proof record of all transactions. It can also be used to enhance the efficiency of IoT devices by reducing the computational overhead involved in each transaction. However, there are certain challenges associated with the integration of Blockchain and IoT, such as the limited computational capabilities of edge devices and the overhead of consensus protocols. These challenges need to be addressed before Blockchain can be widely adopted in IoT applications.

List of Acronyms

- BC: Blockchain
- IoT: Internet of Things
- DLT: Distributed Ledger Technology
- CRUD: Create, Read, Update, Delete
- LAN: Local Area Network
- HTTP: HyperText Transfer Protocol
- MQTT: Message Queuing Telemetry Transport
- WAN: Wide Area Network

References

- J. N. Qureshi, M. S., "Blockchain applications for the Internet of Things: Systematic review and challenges," Microprocessors and Microsystems, vol. 94, 2022. [Online]. Available: https://doi.org/10.1016/j.micpro.2022.104632.
- X. Hu, Y. Su, and R. Guo, "IoT adaptive dynamic blockchain networking method based on discrete heartbeat signals," Sensors, vol. 20, no. 22, art. 6503, 2020. [Online]. Available: https://doi.org/10.3390/s20226503.
- K. S. Garewal, Practical Blockchains and Cryptocurrencies: Speed Up Your Application Development Process and Develop Distributed Applications with Confidence, Apress, 2020. [Online]. Available: https://learning.oreilly.com/library/view/practical-blockchains-and/9781484258934/.
- R. Jain, "Data-Link Layer and Management Protocols for IoT," CSE570S, Fall 2023. [Online]. Available: https://www.cse.wustl.edu/~jain/cse570-23/ftp/m_11dpiz.pdf.
- U. Waheed et al., "Decentralized approach to secure IoT-based networks using blockchain technology," 3C Tecnologia_Glosas De Innovacion Aplicadas a La Pyme, pp. 182-205, 2019. [Online]. Available: https://doi.org/10.17993/3ctecno.2019.specialissue2.182-205.
- Qureshi, "IoT Observability: What is it and how does it help?" Hivemq, 2019. [Online]. Available: https://www.hivemq.com/article/iot-observability/.
- M. K. I. Rahmani et al., "Blockchain-based trust management framework for cloud computing-based internet of medical things (IoT): a systematic review," Computational Intelligence and Neuroscience, 2022. [Online]. Available: https://doi.org/10.1155/2022/9766844.
- J. Lin et al., "Using Blockchain and IoT Technologies to Enhance Intellectual Property Protection," in Proc. of the 4th International Conference on Crowd Science and Engineering (ICCSE'19), New York, NY, USA, 2019, pp. 44-49. [Online]. Available: https://doi.org/10.1145/3371238.337124.
- Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, Apr. 2018. [Online]. Available: https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8306880&isnumber=8334665.

- M. Conoscenti, A. Vetro, and J. C. De Martin, "Blockchain for the Internet of Things: a systematic literature review," in 2016 IEEE/ACS 13th International Conference of Computer Systems and Applications (AICCSA). [Online]. Available: https://doi.org/10.1109/aiccsa.2016.7945805.
- S. Li et al., "Polyshard: coded sharding achieves linearly scaling efficiency and security simultaneously," 2018. [Online]. Available: https://doi.org/10.48550/arxiv.1809.10361.

Last modified on November 20, 2023
This and other papers on recent advances in networking are available online at
http://www.cse.wustl.edu/~jain/cse570-23/index.html
Back to Raj Jain's Home Page