Application of Blockchain in IoT Data Trust and Information Available Technology

Shuo Liu
School of Data Science and Computer
Sun Yat-sen University
Guangzhou, China
Email:liush97@mail2.sysu.edu.cn

***Abstract*—Due to the lack of flexible and effective processing mechanism in the process of data interaction and information transmission in Internet of Things(IoT), this has seriously hindered the process of realizing "interconnection of all things, sharing of all information " in IoT. In order to optimize the above problems, this paper introduces Blockchain technology, and focuses on the analysis of the mapping relationship of Blockchain technology for the hierarchical architecture of IoT. At the perception level of IoT, Merkle tree technology is used to realize the encryption and security of data; at the network level of IoT, the consensus mechanism for the correct use of the information is compared and analyzed. Based on the preliminary discussion of the application of the above Blockchain technology in IoT, the development trend of " IoT + Blockchain" technology in the future is conceived.**

Keywords—IoT; Blockchain; Merkle tree; consensus mechanism

I. INTRODUCTION

In recent years, IoT technology innovation and application practice activities are being widely carried out. In the field of information and communication, IoT is a highly technology-intensive professional comprehensive subject. IoT is a knowledge-intensive network that can obtain on-site information with the help of a variety of sensing devices and interact with the Internet [1].

How to solve the problem of IoT data credibility and information availability has become a bottleneck in the development of IoT technology and applications. In order to make data safe, reliable and interaction information convenient, Blockchain technology is introduced [2].

Blockchain is also a knowledge-intensive compound subject, which combines mathematics, economics, cryptography, network science and other technologies in a certain way to form a decentralized distributed database. Blockchain can provide transparency, distributed storage, trust and other technical support for the entire IoT, so as to build a more credible, secure and efficient IoT network [3,4].

II. ANALYSIS OF CHARACTERISTICS OF IOT AND ADVANTAGES OF BLOCKCHAIN

A. Research on characteristics of IoT

At present, the development of IoT presents an iterative innovation trend of “edge intelligence, connectivity ubiquity, service platformization and data extension”. The operating system and hardware of various terminals are continuously decoupled. The rise of edge computing strengthens the cooperation between terminal devices and accelerates the development of real-time services that meet the requirements of agile connection and data optimization. The ubiquitous connectivity provided by Low Power Wide Area Network (LPWA) has broadened the coverage of the new generation of information infrastructure and helped the digital economy take off. IOT platform is constantly penetrating into various vertical industries. With the cross-innovation of new frontier technologies such as Blockchain and artificial intelligence, the level of intelligent service based on the platform has been continuously improved, and the application breadth and depth of smart cities have been expanded. Multiple types of application data are continuously integrated. In the whole life cycle, cross-industry and cross-link, the penetrating management of data has continuously improved production efficiency, promoted the optimization of business model and the emergence of new business model. And the application of new business has constantly emerged.

With the continuous research and promotion of IoT technology, IoT is faced with the problems of huge and complex types of redundant data and the explosion of data volume, the aggravation of heterogeneous network load, and the difficulty of centralized management risk control. The above problems are categorized as follows.

a. Secure access to equipment and data collection

Due to the variety of devices in IoT and the large amount of on-site data acquired through the devices, the security issues of the IoT devices and the inherent security issues of data have become increasingly prominent.

b. Information privacy management specification

Due to the centralized data management model, privacy data leakage occurs from time to time. At present, the whole network information privacy management standard under IoT mode needs to be formulated.

c. Centralized disposal mechanism

The current data of IoT is managed in a centralized mode, which is bound to lead to the continuous additional work of construction and expansion . When dealing with large-scale data volume and complex scenario applications, this model seriously hinders data application and information matching in IoT.

d. Communication compatibility

Due to the numerous types and quantities of devices involved in IoT, it is difficult to complete the compatibility work of interconnection and interoperability between devices in a short time, which leads to the research work of robust communication protocols. Otherwise, with the deep

application of IoT in a certain industry, it seriously hinders the work of improving the quality and efficiency of IoT communications.

e. Collaboration system

Because the collaboration system, trust system and value system among users, objects, perceptual control equipment, service platform, supervision platform and third-party resource system in the industry are not perfect, it is difficult for IoT to integrate into the industry.

B. Analysis of Blockchain advantages

Combining with the characteristics of IoT and the ways of optimization and improvement, the advantages of Blockchain are summarized as follows [6].

a. Decentralization

In the ecological environment of Blockchain, data is stored in a distributed way, and associated with each other in a cooperative mechanism. Such data is both lightweight and safe.

b. No tampering

Blockchain adopts encryption method to track and control the data in the whole life cycle. Data can be independent of each other and can reach a consensus with each other.

c. Openness, transparency and traceability

According to different business requirements, blockchain will fully record each operation of data on the chain, and associate the operation record with the information before and after data operation. At the same time, the blockchain provides a public interface for data query, and the demander carries out relevant data interaction work according to the consensus reached before.

d. Collective maintenance

In view of the characteristics of the blockchain data distributed architecture, the instructions driving the data interactive operation come from different business requirements. Therefore, the maintenance of data on the chain is transferred to each party who interacts with the data on the chain. This makes the blockchain data maintenance more targeted and more solidified the intrinsic safety of the data on the chain.

C. Blockchain technology mapping association for IoT hierarchical architecture

In order to ensure the security and credibility of IoT data and the correct use of information, Blockchain technology is one of the supporting methods of IoT technology, and the mapping work of Blockchain technology is carried out for the IoT hierarchical architecture [7].

1）. The hierarchical structure of IoT

The hierarchical structure of IoT is roughly divided into three layers: perception layer, network layer, and application layer [8].

Perception layer: IoT data perception mainly relies on wireless sensor system, multimedia information system, UAV carrying system, electronic tag and artificial intelligence technology to complete the information extraction and editing of the objective environment, so as to achieve the purpose of restoring the real attributes of the objective environment to the greatest extent.

Network Layer: IoT network communication mainly relies on wireless sensor network(WSN), mobile communication network and Internet to achieve the purpose of data level transmission and information level interaction.

Application layer: IoT application service mainly includes two aspects: application protocol formulation and industry scenario design. Among them, the application protocol is mainly used to support the technical architecture of the whole IoT to provide external applications; and the industry scenario mainly provides customized service solutions for various industry demanders.

2）. The hierarchical structure of Blockchain

The hierarchical structure of Blockchain technology includes six layers: data layer, network layer, consensus layer, incentive layer, contract layer and application layer [9].

Data layer: the data layer mainly describes Blockchain physical form o, which is the chain structure starting from the creation block on the block chain, including block data of the Blockchain, chain structure, random number, timestamp, public and private key data on the block, etc., and is the bottom data structure in the whole Blockchain technology.

Network layer: the distributed network mechanism is realized mainly through P2P technology. The network layer includes P2P networking mechanism, data transmission mechanism and data verification mechanism. Therefore, the block chain is essentially a P2P network with automatic networking mechanism.

Consensus layer: it mainly includes consensus algorithm and consensus mechanism, which enables highly dispersed nodes to reach consensus on the validity of block data in a decentralized Blockchain network efficiently. It is one of the core technologies of Blockchain and also the governance mechanism of Blockchain community.

Incentive layer: it mainly includes the issuance system and distribution system of economic incentives, whose function is to provide certain incentive measures to encourage nodes to participate in the security verification in the block chain, and to incorporate economic factors into the Blockchain technical system, to encourage nodes that abide by rules to participate in accounting, and to punish nodes that do not abide by rules.

Contract layer: mainly includes various scripts, code, algorithm mechanism and smart contract, which is the basis of Blockchain programmable. By embedding code into a Blockchain or token, implement a smart contract can be customized; and if a certain constraint is reached, it can be executed automatically without a third party, and is the basis for Blockchain trust.

Application layer: it mainly encapsulates various application scenarios and cases, which are similar to applications on computer operating system, web portals on Internet browsers. The future of programmable finance and programmable society will also be built on the application layer.

3）. The mapping relationship of Blockchain technology oriented to the hierarchical structure of IoT

Based on the analysis of the hierarchical structure of IoT and Blockchain, the mapping relationship of Blockchain technology oriented to the hierarchical structure of IoT is described in detail below, as shown in Fig.1.

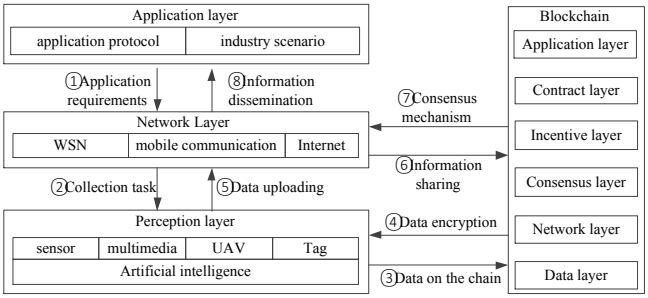

Fig.1 Mapping Relevance Design of Blockchain Technology for IoT Hierarchical Architecture

From Fig.1, it can be seen that the hierarchical relationship logic of IoT with Blockchain: the mapping relevance design of Blockchain technology oriented to the hierarchical architecture of IoT is mainly embodied in data encryption at perception layer and information sharing at network layer. In order to take advantage of Blockchain, the data obtained in perception layer of IoT is chained, and the data is encrypted with a distributed chain structure; information authentication is carried out in network layer of IoT, and information in IoT is de-trusted through the consensus mechanism algorithm of Blockchain.

III. Preliminary Study on Merkle Tree Technology Applied to Data Security of IoT

The blockchain is composed of blocks with certain logical relationship, and the information set of each block itself is shown in Table 1. The Merkle tree contained in the block information set serves as a data security function [10].

Table.1 Block information set

Block head	Version record
	preBlock Hash
	Merkle root
	Timestamp
	Random number
	Difficulty coefficient
Block content	Interaction counter
	Interaction content

The architecture mode of Blockchain is formed by following the working mechanism of Blockchain, and its display effect is shown in Fig.2. The main working mechanism of Blockchain: store the interaction information of the current block itself into the block body; generate a Merkle tree based on the interaction information, and store the data of the Merkle tree root in the block header; the block header data is obtained by the SHA256 algorithm, and the value is used as the preBlock Hash of the current block; the current time information is recorded, and the time data is used as the content of the current block header timestamp field; the difficulty coefficient is used as the measurement area; the block generates statistical indicators corresponding to the workload, which is used to balance the link work of the preBlock, the current block and the subsequent block; finally, the independent blocks are formed into blockchains according to the interaction requirements.

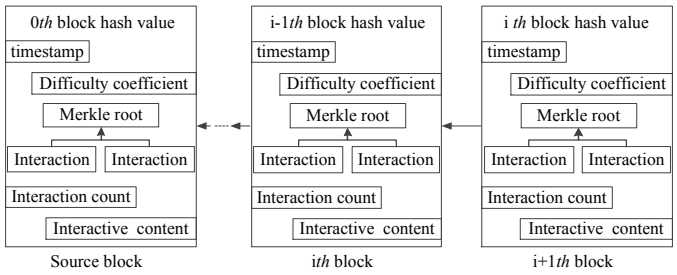

Fig.2 Blockchain structure

A. Merkle tree structure model establishment

Through the above block overview analysis, Merkle tree plays a vital role in the data on the block chain; At the same time, it is also the premise of blockchain opening.

Specifically, Merkle Tree is a binary Tree that stores hash values. Leaf nodes store hash values of data blocks, while non-leaf nodes store hash values of leaf nodes. Any modification to the data will affect its corresponding Hash value and propagate up to the Root node, which means that the Root node is a digital summary of all the data at the bottom. The above data correlation operation logic is highly consistent with the idea that blockchain is independent and associated.

Each block has a Merkle tree, and the Merkle root in the block header is generated by the hash value of all information interaction work in the block body. If a block has n information interactions, its Merkle tree structure is shown in Figure 3.

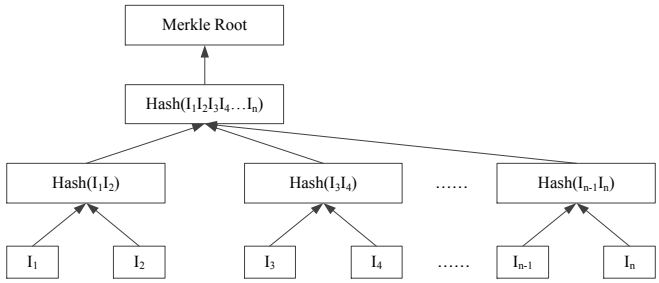

Fig.3 The structural expression of the Merkle tree

According to the composition rule of the binary tree node, the value of the root node of a tree is related to the value of all leaf nodes. The value of any intermediate node is related to the value of all leaf nodes under this node sub-tree. This feature allows any leaf node to quickly be authenticated. Due to the characteristics of the Merkle tree, it is very suitable for the security field. In the IoT perception layer, the Merkle tree is used to record the collected information of the interaction. When verifying the existence of the collected information, the verification path is obtained by only performing $\log_2 N$ calculations. It is possible to prove the existence of some action in a large amount of information interaction of IoT. N is the number of leaf nodes under the Merkle tree.

B. Introduction of Merkle Tree Traversal Algorithms

The traversal algorithm of Merkle tree refers to the algorithm that calculates and outputs the authentication path of each leaf node in order.

The traversal algorithm of Merkle tree is usually divided into three stages: key generation stage, path output stage and authentication stage. The specific tasks of the three stages are described as follows.

Key generation stage: calculate the root value of the tree, initial authentication path and node value to be verified.

Path output stage: output the value of each leaf node and its authentication path in turn, update the structure of the tree, change the storage value of the structure, and prepare for the output of the value of the next leaf node and authentication path.

Authentication stage: for a given leaf node value, let N be the number of leaf nodes. According to the stored authentication path, after $\log_2 N$ hash calculation, the root node value is obtained and compared with the given root value. If the same, the node value is considered to exist in the Merkle tree. Otherwise, the given node is a forgery number. According to the data, it does not exist in this tree.

IV. Analysis and Comparison of Consensus Mechanisms Applied to Information Availability in IoT

The information availability in IoT is mainly guaranteed by the consensus mechanism of block chains. Through the point-to-point communication mode, a decentralized distributed network environment is constructed. All nodes in the network have equal status. Each node can act as a server and undertake the work of block data transmission, verification and storage.

In the existing Blockchain system, there are four main consensus mechanisms: PBFT (Practical Byzantine Fault Tolerance), PoW (Proof of work), PoS (Proof of Stake) and DPoS (Delegated Proof of Stake). Other consensus mechanisms include PoET (Proof of Elapsed Time), PoA (Proof of Authority), and so on.

According to different accounting node selection strategies, Blockchain consensus algorithm can be divided into five types: election, proof, random, alliance and hybrid. Election-type consensus means that in each round of consensus process, the nodes elect the accounting nodes by means of "elections". Proof-type consensus means that in each round of consensus process, the node proves that it has powerful computing power or enough currency age through established methods to obtain billing rights, such as PoW and PoS consensus algorithms. Alliance-type consensus means that in each round of consensus process, the representative node is selected first, and then the representative node obtains the accounting rights in a rotating or competitive manner, such as the DPoS consensus algorithm. Random-type consensus refers to adding different random algorithms in the process of selecting the voters, depending on the random number to select the accounting nodes, and increasing randomness. Hybrid-type consensus refers to the adoption of a variety of consensus algorithms to select accounting nodes, such as DPoS+BFT consensus algorithm.

For the above five types of consensus, the characteristics of the commonly used consensus mechanism algorithms are compared in Table 2.

Table.2 Comparison of algorithm features of consensus mechanism

consensus mechanism	Election-type	Proof-type		Alliance-type	Random-type		Hybrid-type	
	PBFT	PoW	PoS	DPoS	Algorand	Ouroboros	DPoA+PBFT	DPoS+BFT
Performance efficiency	High	Low	Higher	High	High	High	High	High
Degree of decentralizati	Low	High	High	Low	High	High	High	Low
Fault-tolerant node ratio	1/3	1/2	1/2	1/2	1/3	1/2	1/3	1/3
Resource consumption	Low	High	Low	Low	Low	Low	Low	Low
security	High	High	Low	Higher	High	High	Higher	Higher

V. Technology Development Trend under "IoT + Blockchain" Model

The technology development trend under the “IoT + Blockchain” model will present a highly integrated and sustainable development trend in the future. Its main performance is reflected in the following aspects.

a. The IoT provides more application scenarios and the support of the physical world for the Blockchain. The integration of the two can innovatively return to solving the real problems of the physical world.

b. The Blockchain solves the problem of information security and privacy in the IoT, and innovatively establishes the mechanism and capability of decentralization, trustworthiness and privacy protection of the IoT.

c. Combined with industry applications, with the intelligent contract of Blockchain as the technical support, the IoT cross-industry application ecosystem has been innovatively established.

d. Combining the consensus mechanism and incentive mechanism of Blockchain, it will bring innovative business models to the application of the IoT industry.

[1] Gubbi J , Buyya R , Marusic S , et al. Internet of Things (IoT): A vision, architectural elements, and future directions[J]. Future Generation Computer Systems, 2013, 29(7):1645-1660.

[2] Strawn G. BLOCKCHAIN[J]. IT Professional, 2019, 21(1):91-92.

[3] Ali M S , Vecchio M , Pincheira M , et al. Applications of Blockchains in the Internet of Things: A Comprehensive Survey[J]. IEEE Communications Surveys & Tutorials, 2018:1-1.

[4] Reyna A , Martín, Cristian, Chen J , et al. On blockchain and its integration with IoT. Challenges and opportunities[J]. Future Generation Computer Systems, 2018:S0167739X17329205.

[5] Siris V A , Fotiou N , Mertzianis A , et al. Smart application-aware IoT data collection[J]. Journal of Reliable Intelligent Environments, 2019, 5(1):17-28.

[6] Sultan K , Ruhi U , Lakhani R . Conceptualizing Blockchains: Characteristics & Applications[C]// 11th IADIS International Conference on Information Systems. 2018.

[7] Boudguiga A, Bouzerna N, Granboulan L, et al. Towards Better Availability and Accountability for IoT Updates by Means of a Blockchain[C]// IEEE European Symposium on Security & Privacy Workshops. 2017.

[8] Chatterjee A . Internet of Things (IoT)[M]// Building Apps for the Universal Windows Platform. Apress, 2017.

[9] Homoliak I, Venugopalan S, Hum Q, et al. A Security Reference Architecture for Blockchains[J]. 2019.

[10] Garg N, Bawa S. RITS-MHT: Relative indexed and time stamped Merkle hash tree based data auditing protocol for cloud computing[J]. Journal of Network & Computer Applications, 2017, 84:1-13.

[11] Huang J, Kong L, Chen G, et al. Towards Secure Industrial IoT: Blockchain System With Credit-Based Consensus Mechanism[J]. IEEE Transactions on Industrial Informatics, 2019, 15(6):3680-3689.