Hindawi
Mobile Information Systems
Volume 2022, Article ID 1038526, 11 pages
https://doi.org/10.1155/2022/1038526

*Research Article*

# Discussion and Application of Blockchain Technology in Information Management of Internet of Things in Smart Lab

**Jian Zhong,[1] Hang Chen ,[2] Qianyun Zhang,[3] and Weiying He[3]**

[1]*Information and Network Center and School of Computer Science and Engineering, Guangzhou Institute of Science and Technology, Guangzhou 510540, Guangdong, China*
[2]*School of Information Engineering, Guangzhou Vocational College of Technology & Business, Guangzhou 511442, Guangdong, China*
[3]*School of Computer Science and Engineering, Guangzhou Institute of Science and Technology, Guangzhou 510540, Guangdong, China*

Correspondence should be addressed to Hang Chen; chenhang@gzkmu.edu.cn

Received 11 May 2022; Revised 16 July 2022; Accepted 29 July 2022; Published 28 August 2022

Academic Editor: Imran Shafique Ansari



In today's rapid development of higher education, the reform of higher applied undergraduate institutions and higher education has become an effective way to improve the quality of higher education personnel training and improved the quality of teaching. With the continuous expansion of the scale of university laboratories, the number of managers is also increasing, but the management of laboratories is still in the exploratory stage. The current laboratory information management system of Internet of Things has high degree of data heterogeneity, poor data interoperability, and difficult guarantee of data privacy, all of which lead to the difficulty in mining the data value of Internet of Things. The decentralized and zero-trust architecture of blockchain subverted the traditional centralized system architecture and has been applied in many aspects. Blockchain technology was a good addition to IOT to improve the privacy security, versatility, and reliability of the network. This thesis developed an IOT information management system for smart labs based on blockchain technology and the Internet of Things. The data processing efficiency, accuracy, and system throughput are compared with the original IOT laboratory information management system. The results showed that compared with the current laboratory IOT information management system, this system had higher speed, higher efficiency, and better performance in processing the information and data.

## 1. Introduction

Along with the gallop of national higher education and the rapid development of computer technology, experimental teaching is increasingly valued by the majority of applied undergraduate, vocational universities, and institutes of higher education. Guided by the national demonstration standards and based on the requirements of talent cultivation and innovation, universities have made rapid development in specialty construction, curriculum reform, improvement of teaching methods, and infrastructure construction, especially in the construction of experimental training bases, which not only invested in funds and equipment, but also in personnel management and software management, and the laboratory infrastructure is relatively complete. Currently, universities generally adopt network technology for laboratory information management and gradually adopt a variety of intelligent IOT devices, and various intelligent Internet of Things devices are gradually being applied to the laboratory management. While the Internet of Things management is developing vigorously, it also encounters some problems, such as big differences among different systems, complex whole heterogeneous systems, big data differences among heterogeneous systems, backward data management mode, complex network communication modes, low hardware performance of nodes, and weak information privacy security.

The emergence of blockchain technology brought hope to overcome the shortcomings of the IOT, improved its management efficiency, and ensured users' personal privacy. Blockchain is essentially a distributed ledger on a P2P (Peer to Peer) network, and all devices on the Internet of Things can be regarded as nodes in a distributed system. Blockchain was a great addition to IOT, which was effective in improving the privacy, interoperability, and reliability of the Internet of Things system, effectively improving the data processing capacity of the system. Through in-depth investigation of information management, this paper has carried out the research of information management of IOT of intelligent laboratory, and combined with blockchain technology, constructed an information management system of intelligent laboratory based on blockchain technology, and proposed a new idea of establishing an intelligent IOT laboratory. This paper firstly analyzed the current domestic and international research status from the informationization of Internet of Things and the development and application of blockchain technology. Secondly, the IOT technology and blockchain technology involved in the system were elaborated, and the definition, structure, and query process of blockchain were elaborated, and the three levels of perception, transmission, and application of IOT were elaborated. Then, the overall planning and design of the whole system was described in detail, including the specific design of data layer, blockchain consensus layer, and application layer. The designed system was tested in terms of data and information processing to check the feasibility and effectiveness of the system. This article focused on the application of blockchain technology in laboratory information management to achieve intelligent, secured, and visualized management of laboratories, which made laboratory information management more systematic and formed a more efficient whole, and had certain reference significance for future research and construction of smart campus and smart city. This paper analyzes the research of various IoT blockchain technologies through related work, focuses on the introduction of blockchain technology in the method part, and uses the IOT intelligent laboratory information management system and the original information management system for comparative analysis in the experimental part.

## 2. Related Work

The Internet of Things (IOT) is the center of today's industrial revolution of information and intelligence, and is a current area of research and application. IOT has been widely used in people's production and life, and a large amount of information has emerged to provide a basis for achieving intelligence. The weak collaboration among systems, complex network, high degree of data heterogeneity, and poor interoperability makes the information management and value mining of IOT a major problem. At present, many scholars in China and internationally have conducted in-depth discussions on the information management of IOT. Din et al. aimed to explore the challenges faced by information systems management, particularly the accuracy and integrity of information. To identify and analyze these issues, he reviewed the relevant literature. The research in this paper identifies five major challenges of information system governance, integrity, interoperability, personalization, and self-organization in the IOT supply chain [1]. In view of the serious network security loopholes in the traditional centralized energy management scheme, Zhiyi et al. proposed a distributed energy management framework for network security, which applied distributed decision intelligence to the interconnected microgrid, while ensuring their respective tasks to achieve the best operation [2], and concluded that the framework could play an important role in improving the efficiency, reliability, resiliency, and sustainability of ADN's electricity services. Almomani et al. have created an information management system of the Internet of Things, which is used for the security protection of smart homes and farm systems, such as protecting the security of farms and houses, improving rain, irrigation and watering systems, food supplement systems, and other issues.

And to protect the privacy of users and the processing of data from these systems, he has created a network of networking [3].

Research on the application of blockchain technology was widely carried out, and the prospect of the integration of IOT and blockchain was also very broad. The decentralized and zero-trust characteristics of blockchain perfectly compensated for the problems of relying on third-party trust institutions and the existence of malicious nodes in centralized data management. Blockchain-based IOT information management research has received widespread attention. Rane and Narvel has developed an integrated blockchain IOT architecture for the many problems faced by the resource-intensive EPC industry, which can provide various functions such as real-time data collection and autonomous resource coordination for the EPC industry, thus enhancing the flexibility of the PRM system of the EPC industry. He combined the advantages of IOT technology with the development direction of other asset-intensive industries and proposed a new idea of blockchain application [4]. Since the concept of IOT was introduced, disruptive technologies such as big data and cloud computing have been applied to the Internet of Things to overcome its limitations. Reyna et al. believed that the blockchain would be one of the next- generation technologies. She studied blockchain and its integration with IOT, investigated the most meaningful work on its application in the field of IOT to analyze how blockchain can better improve the Internet of Things [5]. Based on blockchain technology, Si et al. proposed a lightweight information sharing security system based on the Internet of Things. In this paper, a dual-chain architecture based on data blockchain and transaction blockchain was proposed, and the attack capability, dual-chain processing capability, and latency were verified in simulation experiments. The experiments demonstrated that the proposed approach can effectively verify the location information of the secure storage device [6]. On this basis, Ray et al. proposed a novel secrecy mechanism based on blockchain and group exchange technology to achieve

seamless transmission of user information (EHR) using secure peer-to-peer communication group nodes. The research results showed that the method had good performance in the fields of blockchain IOT, group exchange, and EHR transmission [7]. This paper mainly compares and analyzes the blockchain technology in improving the information processing efficiency, accuracy, and throughput of the Internet of Things system through the IOT intelligent laboratory information management system and the original information management system.

## 3. Blockchain and Internet of Things Technology

*3.1. Blockchain Technology.* Blockchain is essentially a distributed database, which first appeared in the public's field of vision as the underlying technology of Bitcoin. Blocks include all transactions in P2P network for a period of time. Blockchain is a chain structure formed by connecting blocks according to cryptography, which integrates P2P networking technology, consensus mechanism, cryptography, and other technologies [8].

Blockchain is based on P2P and it includes the various nodes in a P2P network. Take Bitcoin as an example, it is constructed similar to Figure 1, in which each transaction is listed as a set of hash scattered data in a block, and the Merkle tree is stored in a block with a hash pointer, which then encapsulates all the transactions in that block, calculate the hash value that satisfies the current difficulty value, generate a block and record the hash value of the previous block, with each block pointing to the previous block [9]. Within the block, the main components include the transaction information stored in the current block, a field describing the current block size, and a field for the total number of transactions within the block. The two most important components of the block are the block headers and the block data.

Many important information fields in this block are saved in the block header, and the main data items contained in the block header are shown in Table 1.

In a P2P network, nodes are equal, communicate with each other, and function in the same way. All the shared resources can be shared by other nodes. Such as computing resources, storage space resources, and network resources. As the number of nodes increases, more resources are available, thus improving the overall performance of the system. The non-central nature of P2P makes it highly scalable and robust, laying a solid foundation for its development [10]. Therefore, blockchain has many advantages:

(1) Decentralization: the blockchain is built on a decentralized P2P network, so the blockchain itself has the characteristics of decentralization.

(2) Nontampering: blockchain uses cryptography to ensure data security and facilitate verification. Every node in the blockchain has to save the data on the chain, and the data is subject to most nodes. It is very difficult to change the data of most nodes.

(3) Openness and transparency: the data on the blockchain is open to all nodes, so it is best not to put the data in plain text on the blockchain.

(4) Traceability: once the data are written into the blockchain, it cannot be changed or deleted, and the data will be permanently stored in the blockchain, so the blockchain can realize traceability.

(5) Collective maintainability: blockchain consists of nodes, exists in the network composed of nodes, and is jointly maintained by nodes.

(6) Consistency: all the nodes participating in the blockchain will abide by the consensus agreement, so their stored data are consistent.

Agreement is the core charter of blockchain operation and the cornerstone of building trust in blockchain. It contains the consensus algorithm of all nodes and the incentive mechanism to ensure the continuous and stable operation of blockchain [11]. The consensus protocol uses mathematical methods to construct a fair and just algorithm, so that all nodes in the blockchain get completely equal rights and obligations, and reach a unified consensus. The existing consensus agreements are mainly divided into probabilistic consensus agreements and deterministic consensus agreements.

Block query requires two steps. The first step is to construct a Bloom filter about all query indexes in each block, which is used to query whether there are spatial location attribute related data in the block; Part 2: Establish a double-layer combined Bloom filter of all query indexes in each block, which is used to query the exact location of the query index corresponding to the spatial location attribute [12]. Both query structures use hash function to construct encrypted query index, which can quickly query data during query operation.

The criterion of the best performance Bloom filter is that the false normal probability is the lowest, and the memory is the least. If a block $B_i$ is a block in the whole blockchain $B = \{B_1, B_2, \ldots, B_i, \ldots, B_s\}$, in which there is $n_i$ certain index data, and the length of Bloom filter $BF_i$ constructed for this block is $m_i$, and the false normal probability can be calculated according to the existing situation, which is represented by $P_{fi}$ as follows:

$$P_{fi} = \left(1 - \left(1 - \frac{1}{m_i}\right)^{n_i \times k_i}\right)^{k_i} \approx \left(1 - e^{-\left(n_i \times k_i / m_i\right)}\right)^{k_i}. \quad (1)$$

When the probability of false normality is the lowest,

$$k_i = \frac{m_i}{n_i} \times \ln 2,$$
$$m_i = -\frac{n_i \ln P_{fi}}{(\ln 2)^2}. \quad (2)$$

Assuming that the $R$ th spatial location attribute is to be written into Bloom filter $BF_i$, that is, $k_i$ hash functions are used to map elements to $BF_i$, and the position of each hash function mapping data to Bloom filter is set to 1. Inserting a

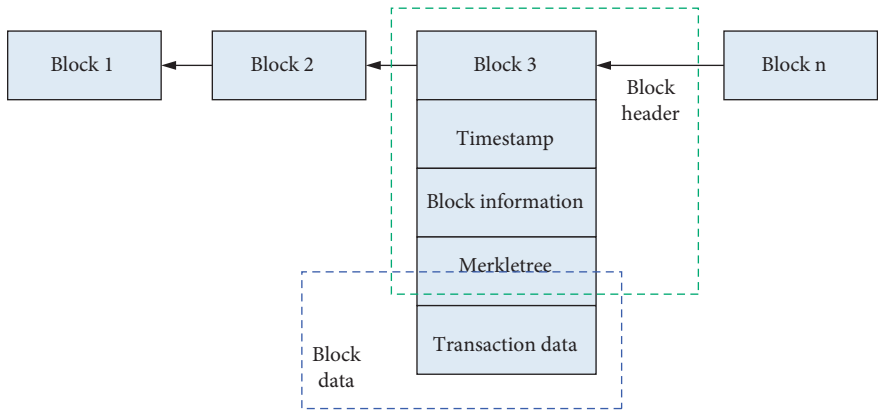


Figure 1: Block chain structure diagram.

Table 1: Block header field description.

| Data fields | Description | Byte |
|---|---|---|
| Version | Current version of the system | 4 |
| Previous block hash | 256 Bit hash from previous block | 32 |
| Random number | Random number satisfying the target hash value | 4 |
| Timestamp | Current time in UTC format | 4 |
| Merkle tree root node hash | Hash value of all transactions in the block | 32 |
| Target hash | Recording rights for obtaining blocks | 4 |

spatial location attribute into Bloom filter with all hash functions can be expressed as follows:

$$BF_i\left[h_j(e_r)\right] = BF_i[l] = 1, \quad 0 \le j \le k_i. \tag{3}$$

Insert all spatial location attributes in the block into the corresponding Bloom filter $BF_i$, which can be expressed as

$$BF_i\left[h_j(e_r)\right] = BF_i[l] = 1, \quad 0 \le j \le k_i - 1,\ 0 \le r \le n_i - 1. \tag{4}$$

The total number of hash calculations required to insert the spatial location attributes of all blocks into the Bloom filter of the corresponding block is

$$\text{Insert}_{\text{num}} = \sum_{B}\sum_{n} k_i. \tag{5}$$

According to the characteristics that the time attribute of Internet of Things data corresponds to the block timestamp, querying the data in a certain time range only needs to query the data in the corresponding time block [13]. To query the spatial location attribute $y$, it is necessary to first determine the query time range, that is, to determine the range of the search block, and then check whether each block within the range has the spatial location attribute $y$. Check Bloom filter $k_i$ corresponding to block $BF_i$, and calculate the mapping position result of spatial position attribute $Y$ by using all $BF_i$ hash functions in, which can be expressed as

$$BF_i[y] = h_j[y], \quad 0 \le j \le k - 1. \tag{6}$$

Suppose to query an index, the block range to be queried is $B$, the corresponding Bloom filter set is BF, $BF_i \in BF$, $BF_i$ has $k_i$ hash functions, then the number of hash calculations required to query this index is

$$\text{Query}_{\text{Num}} = \sum_{BF} k_i. \tag{7}$$

Each block and its corresponding Bloom filter are independent, and each Bloom filter $BF_i$ also has its own false normal probability $P_{fi}$, so the error probability of each query is

$$P_f(BF) = \sum_{BF} P_{fi}. \tag{8}$$

After the first-level query screens out all the blocks with data, the second-level accurate query is carried out by using the double-layer combined Bloom filter.

It is assumed that the spatial location attribute $Y$ corresponding to an index in a block needs to be written into the first-level combined Bloom filter. The binary vector of space attribute $Y$ corresponding to public key coding has $f+1$ bits (0⟶f), and all the combined bits $U$ represent $U = \{u_0, u_1, \ldots, u_{f-a+1}\}$. Each combination bit corresponds to a combination bit Bloom filter, and the probability that the combination bit $U$ to be written occupies the combination bit set $U$ is $\theta$, so the number of hash calculations required to write the spatial location attribute $Y$ is

$$\text{Insert}(y)_{\text{num}} = (f - a + 1) \times \theta_y \times \frac{h}{a}. \tag{9}$$

Then, all the space position attributes in the write block need to be written with the following operands:

$$\text{Insert}(\text{all})_{\text{num}} = \sum_{i\in n}(f-a+1)\times\theta_i\times\frac{h}{a}. \tag{10}$$

Check whether the spatial location attribute $Y$ exists by using all the combined bit Bloom filters corresponding to block $k_i$. The number of hash calculations required to query the spatial location attribute $Y$ is

$$\text{Query}(y)_{\text{num}} = (f-a+1)\times\frac{h}{a}. \tag{11}$$

Then, the number of hash calculations required to query all spatial location attributes in block $B_i$ is

$$\text{Query}(all)_{\text{num}} = \sum_{n}(f-a+1)\times\frac{h}{a}. \tag{12}$$

Then, the number of hash calculations required to query all spatial location attributes in block $B_i$ is

$$P_f(B_i) = P_f(UBF0) + P_f(UBF1) + \ldots + P_f(UBFf-a+1). \tag{13}$$

Actually, although there are $n$ indexes in Block $B_i$, the public key codes of each index are distributed independently and evenly, so each combined bit Bloom filter does not necessarily write the spatial location attributes corresponding to all $n$ indexes, that is, the number of indexes $n$ will be greater than or equal to the actual situation [14]. Therefore, the sum of the false normal probabilities of all combined bit Bloom filters in the actual block $B_i$ is smaller than the theoretical case, i.e.,

$$\text{actual}P_f(B_i) \le (f-a+2)\times\left(1-e^{-(n\times(h/a)/m)}\right)^{h/a}. \tag{14}$$

Since 2 is equal to 1, this probability is still small.

Assume that a spatial location attribute $Y$ in block $B_i$ needs to be written into the Bloom filter corresponding to the block. The public key code, that is, the binary vector shares $f+1$. Only the single bit Bloom filter corresponding to the bit with coded bit 1 needs to be written into the spatial position attribute $Y$. Assuming that the proportion of bits to be written to all coded bits is $\eta$, then the proportion of public key coded bits corresponding to the spatial position attribute $Y$ with coded bit 1 is $\eta_y$. Therefore, the number of hash calculations required to write the spatial location attribute $y$ is

$$\text{Insert}(y)_{\text{num}} = h\times\eta_y\times(f+1). \tag{15}$$

Then, the number of hash calculations required to write all elements is

$$\text{Insert}(\text{all})_{\text{num}} = \sum_{i\in n}h\times\eta_i\times(f+1). \tag{16}$$

The second layer of combined Bloom filter is different from the traditional combined Bloom filter. It only needs to query the coded bits filtered by the first layer of combined Bloom filter, without checking all the coded bits [15]. It is assumed that after the first layer check, the ratio of nonzero coded bits to all codes is $\lambda$. Then, the number of hash calculations required to check the spatial location attribute $y$ is

$$\text{Query}(y)_{\text{num}} = (f+1)\times\lambda_y\times h. \tag{17}$$

Then, the number of hash calculations required to query all spatial location attributes is

$$\text{Query}(\text{all})_{\text{num}} = \sum_{i\in n}(f+1)\times\lambda_i\times h. \tag{18}$$

The actual situation is the same as that of the first layer combined Bloom filter. Although there are $n$ indexes in block $B_i$, each single bit Bloom filter does not necessarily write the spatial location attributes corresponding to all $n$ indexes, that is, the number of indexes $n$ will be greater than or equal to the actual situation.

*3.2. Internet of Things Technology.* The Internet of Things was proposed in 1999 by the MIT Center for Automation Accreditation. The ITU Internet Report 2005: Internet of Things was published in 2005, which expanded the meaning of IOT and regarded it as an extension of the Internet. Since then, with the development of IOT technologies, including RFID technology, sensing network technology, wireless network technology, and cloud computing technology [16, 17]. The Internet of Things refers to the interconnection of things and things, things and people according to the drafted protocol, and the interaction of data and information, which realizes the extension and expansion of the network, so as to achieve intelligent identification, positioning, monitoring, and management. The essence of the Internet of Things is a network that can form a mutual perception between objects and objects, and is used to solve the interconnection problem between objects and objects and people to people. Figure 2 shows the schematic diagram of an IOT layering.

The sensing layer is an information resource based on the Internet of Things. Digital signals from the target are acquired by sensors and also contain data obtained from certain electronic devices, which are finally transmitted to the application layer via the transport layer, which also has a controller for responding to signals from the transport layer [18]. The transport layer is the connection between the sensing layer and the application layer, which includes various private networks, the Internet, wired and wireless communication networks, and these application layers are the interface between the IOT and the users, including people, organizations, and other systems [19]. The application layer is based on data-aware technologies for data storage, query, analysis, mining, understanding, and decision making. IoT applications can be divided into four kinds: monitoring type (logistics monitoring, environmental monitoring), query type (smart retrieval, remote meter reading), control type (intelligent transportation, smart home), and scanning type (mobile wallet, expressway nonstop tolling) . It includes public goods, industrial applications, and individual applications, and has different requirements in different application environments.

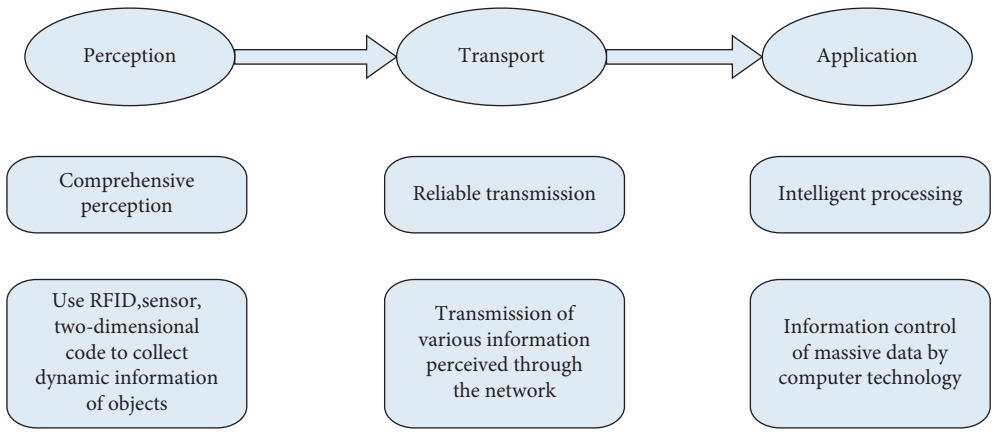


Figure 2: Internet of things hierarchy diagram.

The basic characteristics of the Internet of Things include three aspects: first, perception, which can dynamically detect the object with identification function through the identification device, read the attributes of the object, and transform the information of the object into a form that can be carried out online, so as to identify the object. The second is the transmission characteristic, which transmits the target information collected in the sensing process through the network, and transmits the target information in real time. The third is intelligence, that is, using computer technology such as cloud computing to mine and apply a large amount of data and information to realize the intelligent control of objects [20].

## 4. Construction of Internet of Things Information Management System for Smart Laboratory Based on Blockchain Technology

*4.1. Discussion of System Design Requirements.* In the stage of system requirements design, the performance and functional requirements of the system are summarized.

*4.1.1. The Need for Decentralization.* The laboratory information management system uses blockchain technology to ensure the decentralization of the system, and carries out transaction processing and data storage in each node. Each node operates independently, and every time the data changes, the data is synchronously updated to each node for storage, forming a decentralized structural model of nodes [21].

*4.1.2. Data Privacy Security Requirements.* The data security requirements of laboratory information management system include not only the security of data storage, but also the privacy of user data. In the data storage module, the relevant fields of block data need to be designed to facilitate the storage and verification. In terms of user data protection, it is necessary to protect the user's account information, and use cryptography-related technology to achieve anonymous effect on user information, while ensuring the security of data information recording.

*4.1.3. Functional Requirements.* The information management system has several functions, such as user information storage, data storage, and data verification. First of all, users register their identities in the system, publish data information, and relevant users sign the data, then publish it, and store it in the system. In the data verification stage, the user node requests relevant data information from the system. The system retrieves and compares the data with the data stored in the blockchain to verify the authenticity of the data. The coupling degree of stored data used by the application layer and the blockchain consensus layer is reduced as much as possible, and data storage and verification operations are relatively independent in the blockchain system.

*4.2. Overall System Structure Design.* The whole system mainly consists of data layer, blockchain consensus layer, and application layer. Among them, the data layer combined with the application layer completes all the basic functions of the contract deposition system, while the blockchain protocol is based on the data layer to complete the distributed storage. In Figure 3, the main model of the system is shown.

The blocks and the user's data are stored in the data layer. The block data contains the content of the data and the data of the area block. The production time stamp of the block is stored in the block header and is sequenced to it. The block stores the hash value of the current block in the block header along with the hash value of the previous block, so that each block points to the previous block in turn, thus logically constituting a chained data structure.

In which the table dltdb_user is used to store the relevant data information of users. The application layer involves the user's registration and login function modules, so the user's username and password fields are first created. The data in the password field is generated by md5 algorithm. In addition, in the process of signing the data, the user is required to sign the data with a private key, and in the data verification process, the public key signature verification process needs to be performed on the previously signed data. The user's rsa public-private key pair field is added to the table. Finally, in order to fine-grained control the permissions of data management operations, a user permission field is

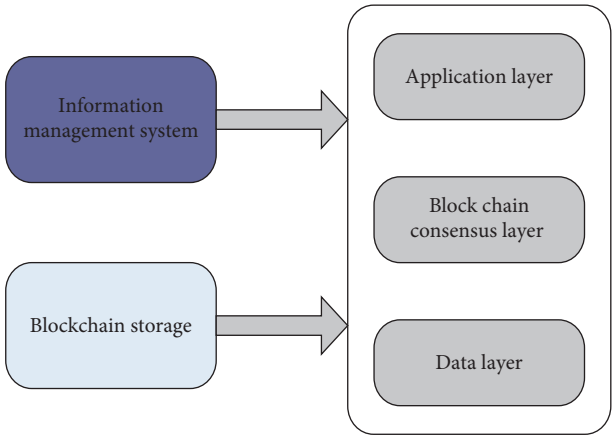


Figure 3: System overall structure model diagram.

added. The specific contents of the data table dltdb_user are shown in Table 2:

The table dltdb block mainly stores the current block data information. The id field is used to mark the height of the current blockchain, the data field is set to store the data information in the block, the prev_hash field is set to store the hash value in the previous block, and the cur_hash field is set to store the current block the hash value in. Set the date_time field to store the timestamp data of the current block data. The specific contents in the table are shown in Table 3:

In the consensus layer, the focus is on the synchronous transfer of information between nodes. At the system startup, each node first selects a proxy node. After the proxy nodes are selected, each proxy node communicates with each other and identifies each proxy node, and this phase prepares the system for startup. When the system is running, the user sends a request to the host and then transmits this information to the host, and then the agent performs the corresponding service. After the transaction is completed, a node generates a block to synchronize the data on the agent node and distributes the data to each node and stores it in the database of each node, thus achieving data consistency.

In the block consensus stage, the main agent nodes in the network need to complete the generation of block data in the service cycle of each node in sequence. In the process of implementation, in order to make each node work according to the sequence in the group, a node work scheduler needs to be designed to control the running sequence of the current node and manage the switching between the following state and the leading state of the node. The master agent node running in the service cycle will acquire the changed data in the application layer, check the current blockchain height stored locally, and send the block information to other nodes in the network if the block data needs to be updated, and write the new block data locally. After the current operation is completed, the completion information is sent to the scheduler. After receiving the information, the scheduler designates the subsequent node to update the blockchain. The scheduler and node model diagram is shown in Figure 4.

The application layer is mainly composed of the interaction between the front and back terminals to realize the

Table 2: dltdb_user table.

| Field name | Field type | Description |
|---|---|---|
| Id | Int | The current number of users |
| name | Varchar | User name |
| md5_password | Varchar | User password |
| rsa_pubk | Varchar | User rsa public key |
| rsa_prik | Varchar | User rsa private key |
| user_priority | Int | User permissions |

Table 3: dltdb_block table.

| Field name | Field type | Description |
|---|---|---|
| Id | Int | Store current blockchain height |
| Data | Varchar | Store current block data |
| prev_hash | Varchar | Store the previous block hash value |
| cur_hash | Varchar | Store the current block hash value |
| date_time | Datetime | Store current timestamp data |

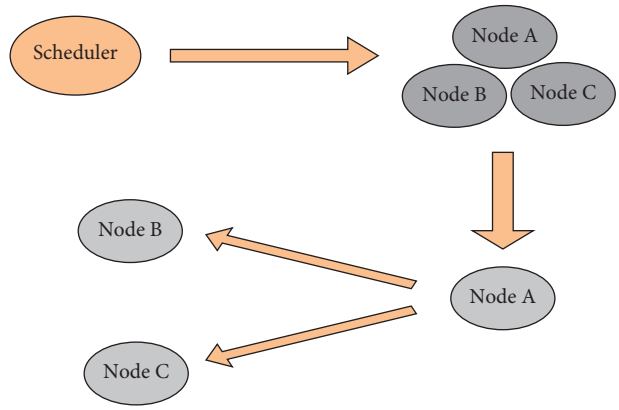


Figure 4: Schematic diagram of the scheduler control node.

corresponding requests from users. It mainly contains registration of user information, login, display of current user information, creation of contract data, signing of current data by the user, query and confirmation of specified data, and so on. The entire functionality is shown in Table 4.

The user registration function mainly includes submitting a request to the server, which verifies the user's registered name. If there is no registered user name in the system, the RSA public-private key pair is generated for the user, and the md5 algorithm is used to generate the set password for the user. At the user login stage, after the user inputs the user name and password, the front-end password is converted by md5 algorithm and compared with the corresponding password field value in dltdb user table in the back-end database, and the successful login is verified to enter the user page.

This section firstly introduces the designed information management system and analyzes its application in the IOT information management system. Based on this, the requirements of the system are analyzed in conjunction with the proposed agent consensus mechanism, and the data layer. Blockchain consensus layer and application layer are designed on this basis. On this basis, the functional modules

Table 4: List of main functions of the application layer.

| Main function name | Description |
|---|---|
| User registration login | Register user data and log in to the system for new users |
| User information | Display the current user main information |
| Data creation | Create new contract data and set up related users |
| Data signing | User signs current data with RSA private key |
| Data query | Query the specific content of the specified data |
| Data verification | Verify the specified contract data with the RSA public key |

to be implemented in each model layer are given, and the specific design steps and methods are given. Next, we will test each of the main functional modules designed and test their throughput.

## 5. The Experimental Design of IOT Information Management System for Smart Laboratory Based on Blockchain Technology

In order to verify the feasibility and effectiveness of this system, this paper has carried out an experiment of IOT information management in intelligent laboratory based on blockchain technology to explore the feasibility and effectiveness of this system in practical application.

This section compares the data classification and data query performance between the existing intelligent laboratory information management system and the designed intelligent laboratory information management system through experiments. The experimental platform is intel i3 3.3GhzCPU, 8 GB RAM, 120G SSD; the software environment is Windows10 64 bit system, Intelli JIDEA2019, and Java1.8.0_20. About 104,000 pieces of data are simulated in the experiment, including four groups of experiments (comparison of time spent writing information, comparison of time spent reading information randomly, comparison of time spent in data classification, comparison of time spent in data query, comparison of the number of classification errors, comparison of query errors, and comparison of throughput). The experimental results are shown in the following figures.

As shown in Figure 5, through independent sample $T$ test, it is found that the difference probability value of information writing time between the two groups of systems is $0.03 < 0.05$, and the difference probability value of information random reading time between the two groups of systems is $0.02 < 0.05$, indicating that there are significant differences between the two groups of systems in information writing and random reading time. In the intelligent laboratory IOT information management system based on blockchain technology, the average time spent writing information is 872 ms, and the average time spent reading information randomly is 76.275 $\mu$s. In the existing intelligent laboratory information management system, the average time spent writing information is 1385.5 ms, and the average time spent reading information randomly is 131.75 $\mu$s. The application of blockchain technology in the intelligent laboratory information management system of Internet of Things can improve the rate of writing information and random reading information.

As shown in Figure 6, through the independent sample $T$ test, the difference probability value of data classification time between the two groups of systems is $0.01 < 0.05$, and the difference probability value of data query time between the two groups of systems is $0.02 < 0.05$, indicating that there are significant differences in data classification and data query time between the two groups of systems. In the Internet of Things information management system of smart laboratory based on blockchain technology, the average time for data classification is 1301 ms, and the average time for random information reading is 111 $\mu$s. In the existing intelligent laboratory information management system, the average time spent writing information is 3666.75 ms, and the average time spent reading information randomly is 571 $\mu$s. The information management system designed in this paper integrates the blockchain technology and Internet of Things technology, which can improve the data classification rate and data query rate.

As shown in Figure 7, through independent sample $T$ test, it is found that the difference probability value of data classification errors between the two groups of systems is $0.03 < 0.05$, and the difference probability value of data query errors between the two groups of systems is $0.03 < 0.05$, indicating that there are significant differences in data classification errors and data query errors between the two groups of systems. In the Internet of Things information management system of smart laboratory based on blockchain technology, the average error of data classification is 6, and the average error of data query is 2.25. In the existing intelligent laboratory information management system, the average error of data classification is 10, and the average error of data query is 4.5. The Internet of Things information management system of smart laboratory based on blockchain technology is not only faster in data classification and data query, but also higher in accuracy.

As can be seen from Figure 8, the throughput performance of the system is tested. The average throughput of the designed system is 810.1 tx/s, and that of the original information management system is 80 tx/s. This is because the

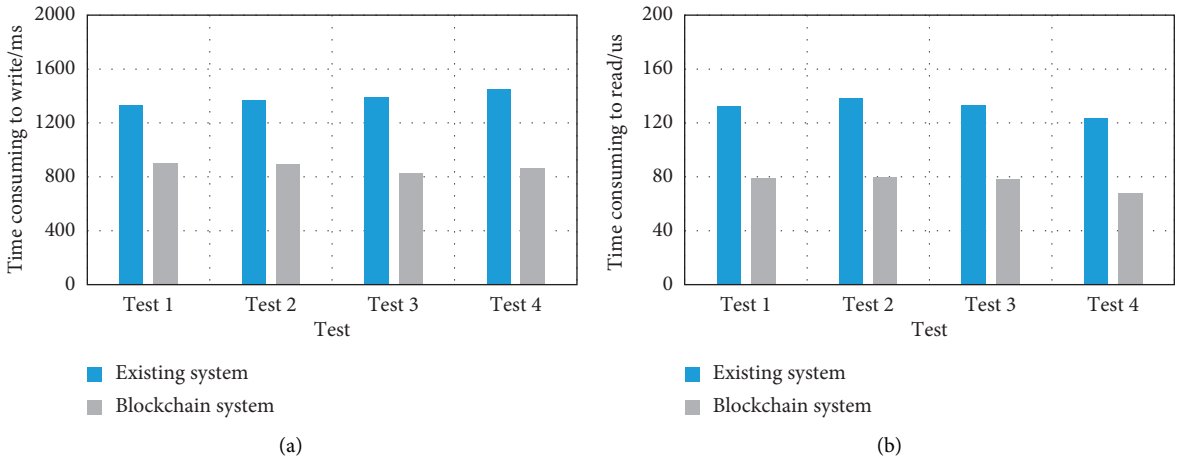


Figure 5: Comparison of information processing time between two groups of systems. (a) is a comparison diagram of the time spent writing information in two groups of systems. (b) is a time-consuming comparison diagram of two groups of systems randomly reading information.

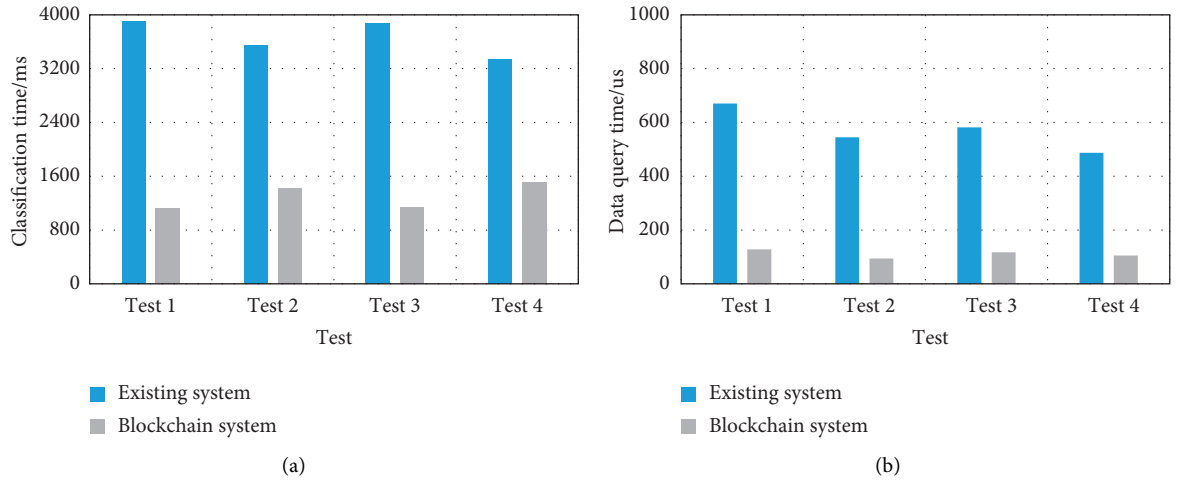


Figure 6: Comparison of data processing time between the two groups of systems. (a) is a time-consuming comparison diagram of two groups of system data classification. (b) is a comparison diagram of time consumption of two groups of system data query.

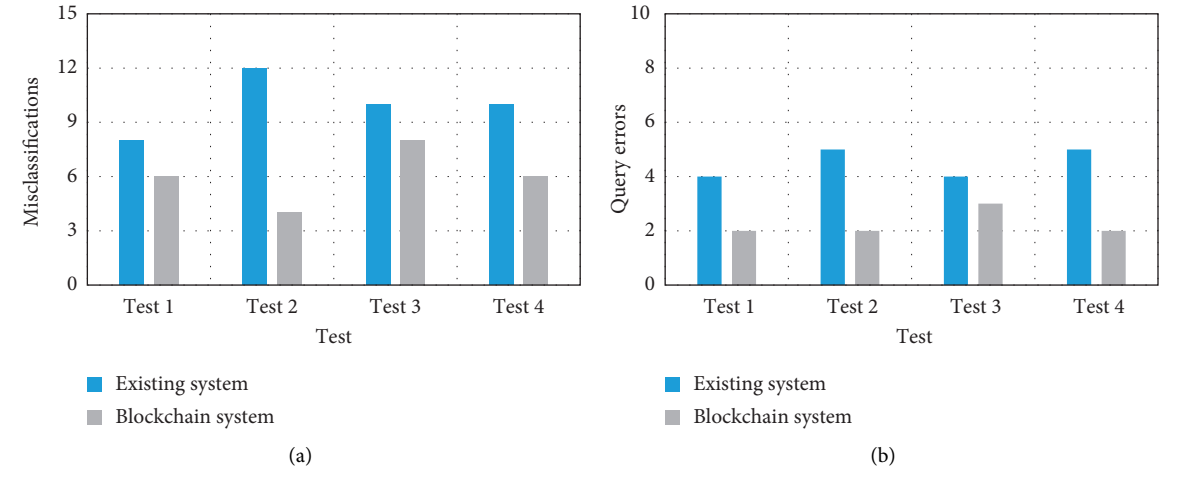


Figure 7: Comparison of data processing errors between two groups of systems. (a) shows the number of errors in data classification of two groups of systems. (b) shows the number of errors in two groups of system data queries.

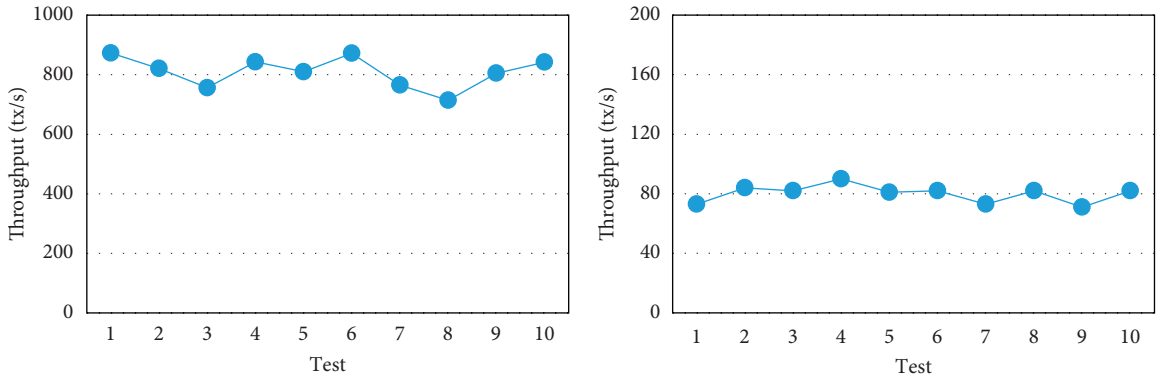


Figure 8: Throughput of two sets of information management systems. (a) shows the throughput of the designed information management system. (b) shows the throughput of the original information management system.

designed system uses blockchain technology, and the PBFT consensus mechanism in blockchain technology does not need to consume CPU computing resources, so the throughput of the system is larger.

## 6. Conclusions

Based on blockchain technology, this paper constructed a smart laboratory information management system of Internet of Things, and designed each model layer in the system. Through experiments, the system environment of the information management system designed in this paper was deployed, and the information processing module, data processing module, and system throughput are tested in turn. In addition to this paper, there were still many problems that need to be explored and solved. In the consensus mechanism proposed, the process of node grouping can effectively guarantee the fairness of proxy node generation in blockchain and the degree of decentralization of blockchain. However, when the number of nodes in the blockchain network was small, it was impossible to effectively group the nodes to elect proxy nodes. Therefore, the following work need to optimize the design of scenarios with different numbers and scales of nodes in the blockchain network to improve the flexibility and applicability of the blockchain technology consensus mechanism.

## Data Availability

Data sharing is not applicable to this article as no new data were created or analyzed in this study.

## Conflicts of Interest

The authors declare that there are no conflicts of interest.

## Acknowledgments

This work was supported by Feature Innovation Project of Colleges and Universities in Guangdong Province (2021KTSCX158) and Guangzhou Science and Technology Planning Project (202102100011).

## References

[1] Z. Din, D. I. Jambari, and M. M. Yusof, "Challenges in IOT technology adoption into information system security management of smart cities: a review[J]," *Advances in Science, Technology and Engineering Systems Journal*, vol. 6, no. 2, pp. 99–112, 2021.

[2] L. I. Zhiyi, M. Shahidehpour, and X. Liu, "Cyber-secure decentralized energy management for IOT-enabled active distribution networks[J]," *Journal of Modern Power Systems & Clean Energy*, vol. 6, no. 05, pp. 60–77, 2018.

[3] A. Almomani, A. Al-Nawasrah, W. Alomoush, M. Al-Abweh, A. Alrosan, and B. B. Gupta, "Gupta. Information management and IOT technology for safety and security of smart home and farm systems[J]," *Journal of Global Information Management*, vol. 29, no. 6, pp. 1–23, 2021.

[4] S. B. Rane and Y. A. M. Narvel, "Data-driven decision making with Blockchain-IoT integrated architecture: a project resource management agility perspective of industry 4.0," *International Journal of System Assurance Engineering and Management*, vol. 13, no. 2, pp. 1005–1023, 2021.

[5] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Diaz, "On blockchain and its integration with IoT. Challenges and opportunities," *Future Generation Computer Systems*, vol. 88, no. NOV, pp. 173–190, 2018.

[6] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "IoT information sharing security mechanism based on blockchain technology," *Future Generation Computer Systems*, vol. 101, pp. 1028–1040, 2019.

[7] P. P. Ray, B. Chowhan, N. Kumar, and A. Almogren, "BIoTHR: electronic health record servicing scheme in IoT-blockchain ecosystem," *IEEE Internet of Things Journal*, vol. 8, no. 13, pp. 10857–10872, 2021.

[8] L. Yong, H. J. Kim, and G. Y. Lee, "Design of GDPR compliant personal information management procedure in the IOT devices," *Journal of the Institute of Electronics and Information Engineers*, vol. 57, no. 10, pp. 3–14, 2020.

[9] T. B. Kksal, "Architecture design approach for IOT-based farm management information systems," *Precision Agriculture*, vol. 20, no. 5, pp. 926–958, 2018.

[10] K. LepenIOTi, A. Bousdekis, D. Apostolou, and G Mentzas, "Prescriptive analytics: l," *International Journal of Information Management*, vol. 50, pp. 57–70, 2020.

[11] J. A. Kaw, N. A. Loan, S. A. Parah, K. Muhammad, J. A. Sheikh, and G. Bhat, "A reversible and secure patient

information hiding system for IoT driven e-health," *International Journal of Information Management*, vol. 45, no. APR, pp. 262–275, 2019.

[12] Y. Cheng, X. Zhao, J. Wu et al., "Research on the smart medical system based on NB-IoT technology," *Mobile Information Systems*, vol. 2021, no. 4, pp. 1–10, 2021.

[13] P. Brous, M. Janssen, and P. Herder, "The dual effects of the Internet of Things (IOT): a systematic review of the benefits and risks of IOT adoption by organizations," *International Journal of Information Management*, vol. 51, no. Apr, Article ID 101952, 2020.

[14] X. Wang, X. Zha, W. Ni et al., "Survey on blockchain for Internet of things," *Computer Communications*, vol. 136, no. FEB, pp. 10–29, 2019.

[15] I. Mistry, S. Tanwar, and S. Tyagi, "Blockchain for 5G-enabled IOT for industrial automation: a systematic review, solutions, and challenges," *Mechanical Systems and Signal Processing*, vol. 135, Article ID 106382, 2020.

[16] I. Makhdoom, M. Abolhasan, H. Abbas, and W. Ni, "Blockchain's adoption in IoT: the challenges, and a way forward," *Journal of Network and Computer Applications*, vol. 125, no. JAN, pp. 251–279, 2019.

[17] P. Cui, U. Guin, A. Skjellum, and D. Umphress, "Blockchain in IoT: current trends, challenges, and future roadmap," *Journal of Hardware and Systems Security*, vol. 3, no. 4, pp. 338–364, 2019.

[18] Y. P. Tsang, K. L. Choy, C. H. Wu, G. T. S. Ho, and H. Y Lam, "Blockchain-Driven IoT for food traceability with an integrated consensus mechanism," *IEEE Access*, vol. 7, no. 1, Article ID 129000, 2019.

[19] M. Alaslani, F. Nawab, and B. Shihada, "Blockchain in IoT systems: end-to-end delay evaluation," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8332–8344, 2019.

[20] M. S. Ali, M. Vecchio, and F. Antonelli, *IEEE Internet of Things Magazine*, vol. 1, no. 2, pp. 24–29, 2018.

[21] M. Tanriverdi, "A systematic review of privacy preserving healthcare data sharing on blockchain," *Journal of Cybersecurity and Information Management*, vol. 4, no. No. 2, pp. 31–37, 2020.