Research on the Financial Supply Mode of Agricultural Products Based on the Integration of the Internet of Things and Blockchain

Hongbin Lin, Peichang Zhang(✉), Jihong Zhang, and Gongbin Qian

Electronic and Information Engineering, Shenzhen University, Nanshan, Shenzhen, China
{pzhang,zhangjh,qiangb}@szu.edu.cn

Abstract. As a big agricultural country, "agriculture, rural areas, and farmers" is one of the critical areas of national economic development. Among them, rural finance is related to the development of the agricultural economy and the poverty alleviation of thousands of farmers. The existing agricultural finance has exposed many problems in the supply mode: poor information, inaccurate information, information insecurity, and so on, which have seriously hindered the development of agriculture. With the rapid growth of big data, the Internet of Things, blockchain, and other financial technologies, how to rely on new technologies to build a new agricultural financial supply model to achieve accurate and secure information transmission is the focus of this research. This paper mainly discusses the system architecture of integrating the Internet of Things and blockchain and its data collection, processing, and storage. In order to solve the accurate and safe information of the agricultural financial supply chain, an intelligent security system combining the Internet of Things and blockchain was designed based on the requirements of a security management system.

Keywords: Agricultural finance · Data security · Blockchain · System architecture

1 Introduction

The structure of the intelligent factory system is very complex, and all modules are inextricably linked. Recently, the scale of intelligent factory system construction has become bigger and bigger, and the number of functional modules and equipment is rapidly expanding. The frequency of internal module commands and data interaction in the system is increasing [1]. Generally speaking, there are four most critical functional modules in the system. Besides data storage and safety, it also includes command control and authority management modules.

All systems related to industrial manufacturing have personalized commands and protocols. Each system uses different formats when storing data. Multiple systems cannot communicate instantly [10]. In addition, IoT devices do not have enormous storage

Z. Zeng et al. (Eds.): ECIT 2022, AHE 11, pp. 617–626, 2023.
https://doi.org/10.2991/978-94-6463-005-3_63

and computing capabilities. It is pretty limited, so it is more troublesome to process the data, and the data has to be uploaded to the center of the cloud, disrupting real-time performance on the field. From this, it can be seen that the Internet method under the traditional model is mainly centered on the cloud. With the continuous increase in the demand for intelligent equipment, it is gradually shifting to the fields of distributed computing and regional centralization. In addition, according to statistics from authoritative departments, every device in a manufacturing plant generates an incalculable amount of data every day. However, more than 95% of it is temporary data. If these data are stored and processed, it will likely lead to resources. Excessive waste, so the essential requirement of the Industrial Internet of Things lies in the safe storage of critical data [6]. Recently, Scientific development has continued to accelerate, communication technology has become more advanced, and the demand for network security has increased. The Internet of Things equipment is likely to be illegally operated by illegal personnel in the actual operation process. You can successfully log in directly through the password and IP address, often bringing incalculable losses. At present, the research emphases of scientists are mainly on improving the security of the Industrial Internet of Things. To improve the safety of the IIoT, this article mainly studies the design of system functional module architecture, data storage-double chain storage structure, edge computing, and other aspects. The data collected and processed by the IoT are stored on the blockchain [9], which plays the role of data correctness and tamper-proofing.

2 Industrial Internet of Things

The IoT means the real-time collection of anything or process that needs to be monitored, connected, and interactive through various information sensors and the collection of all kinds of the required information. Through various possible network access, the close connection between things and things and between things and humans are realized, and the intelligent perception, recognition, and management of things and processes are realized. Through the IoT, the Internet and things can be quickly connected, and on this basis, seamless docking can be achieved. In the specific application process, short-range mobile transceivers can be embedded in everyday items and small accessories, which only the IoT operation can be realized. This is also a new way for the IoT, things, and people to communicate, making the communication more smooth, Real-time sharing [2]. Many devices, including sensors, mobile phones, and tags, are linked together to form a powerful perception system through the IoT. It can be seen that through the Internet, some things can be linked to terminal equipment anytime and anywhere, intelligent identification can be performed in a short time, and personalized services can be provided by following per customer needs.

Newly, the global manufacturing industry is in a period of transformation, and its development direction is concentrated in the fields of ecological green and intelligence, and with the characteristics of networking, personalization, and service [6]. The Industrial Internet of Things is a brand-new network system that connects systems with people in a short time and provides various services for the manufacturing industry. Based on the Internet, personalized solutions and related standards can be provided in the light of the specific situation, and the gap in equipment data can be bridged. Therefore, operators

inside and outside the shopping mall can obtain valuable communication data. Besides the immediate processing of the intelligent connection of multiple physical objects, the Industrial IoT can also apply IT tools for processing in various scenarios in the digital shopping mall. It uses cloud data to realize online Internet applications, mainly through the production and logistics system, to collect resources and processes. Dynamically, the ability matching is completed on this basis. This article mainly discusses the framework model, data storage, and RFID things in-depth and puts forward a new management framework based on product communication as a reference. The framework mainly runs in the IoT manufacturing environment to achieve intelligent manufacturing.

3 System Function Module Architecture Design

An In-depth discussion on the personalized needs of the intelligent factory system, while focusing on the research of Ethereum smart contracts and blockchain technology, and specifically developed a matching safety management system. Taking specific functions and attributes as a reference basis, the intelligent factory system can be divided into four different layers [7], the top layer is the user layer, the second layer is the application layer, the third layer is the container layer, and the last layer is the device layer. Two significant modules play a vital role in the system infrastructure. The first is a business interaction module, and the other is an intelligent contract module.

3.1 Device Layer

The device layer includes all the edge devices required for enterprise Internet operations, including computing and perception devices. Among them, the sensing device is composed of various controllers, which mainly provide a sensing method for the manufacturing process, quickly perceive the internal and external environment information of the object, and fully support the management and operation of the equipment at the physical level. The sensing device itself does not have any computing power. Therefore, to reduce the computing capacity of the server and comprehensively improve the data analysis and processing capabilities, BEIIoT, which is an edge computing IIOT architecture based on blockchain, specifically adds powerful computing devices at the end close to the user, which is mainly composed of IoT gateways and access points. In addition, it also includes a micro data center that can achieve fast calculations, which is also an effective remedy for the lack of its computing power, but it is lightweight in terms of computing power. There is also an IoT gateway at the device layer, an industrial Internet data transmission terminal, which can perform fast calculations or cache required data based on the actual situation and quickly connect the Internet with edge devices. On this basis, comprehensive management and control of IoT terminals and Gateway.

3.2 Container Layer

The number of servers in the manufacturing factory is vast. In terms of structure, they are distributed P2P structures. They have a consensus mechanism combined into a robust blockchain through data storage. All servers are in the same local area network and are

owned by the same enterprise. The authentication process is mainly completed with the firewall IP, maintaining a high degree of trust, and other enterprise servers usually cannot access it, so the blockchain belongs to a private chain. In the container layer, one IoT gateway can manage more than two edge devices at one time, and one server can manage more than two IoT gateways. BEIIoT can directly encapsulate all servers and devices in the container, virtualize their resources and publish them in the middle layer. When users manage edge devices, they can directly access the blockchain platform. Expand the combination to have powerful functions and make full use of resources. After rapid processing through multiple containers, the original data becomes more streamlined and more valuable data is obtained, and the amount of data dissemination will be significantly reduced. On this basis, the stable and safe operation of the BEIIoT architecture can be ensured. All servers belong to the P2P network so that P2P communication will come true through BEIIoT, and relevant data can also be shared in real-time.

3.3 Application Layer

The role of the application layer is to sort out and analyze all the data and services provided by the middle layer, combine diversified analysis needs, manufacturing process accuracy, and user personalized needs to refine advanced application services and implement multi-level applications on this basis.

3.4 User Layer

The user-level platform can be divided into two or more roles by combining the differences in specific types. There are certain differences in the permissions of each role. The management and operation of the BEIIoT platform are mainly completed through the application-level service interface, and the user types can be deleted or added at any time according to personal needs. The BEIIoT system mainly includes four different users, with differences in specific permissions: (a) Administrator, who has all operating permissions and comprehensively manages equipment, servers, and users; (b) Operator, who only has operating permissions for the system, such as reading data, operating equipment and accessing server terminals; (c) analysts can read data at any time and carry out in-depth analysis, for example, analyze whether the equipment fails and conduct an in-depth analysis of the product life cycle; (d) security Supervisors, once any abnormal situation occurs in the manufacturing environment, the system will automatically send out an alarm signal.

4 Primary Technology

4.1 Distributed Structure-P2P

At present, most manufacturing systems are single-point systems. Problems such as failure of a single node and excessive pressure make efficient use and share manufacturing resources. To effectively avoid equipment safety, integrity, and scalability issues caused by extended processing time, reduced reliability, and inconsistent interface protocols

in the communication process of the system, distributed storage is specially introduced based on the actual situation. The BEIIoT server node belongs to the P2P structure, which can carry out network communication at any time and can complete distributed coordination during decentralized processing. The system operation will also become more accessible, with greater scalability, and it can also solve traditional server terminals.

4.2 Data Storage: Double-Chain Storage Structure

4.2.1 Double-Chain Storage Structure

The BEIIoT architecture stores relevant data based on time. As one of the nodes, all servers compete with their computing and storage capabilities. If the storage rights are successfully obtained, the server integrates the data blocks and quickly stores them in the blockchain. The administrator can trace the data source at any time, fully guarantee the security of data operation, and prevent the single-node server from being maliciously controlled by illegal personnel to cause information theft [8]. A typical block-chain is mainly connected by sequence when storing data blocks, and the reference basis is the timestamp, and the data blocks are stored on the corresponding nodes. Node storage rights mainly depend on the consensus mechanism, including proof of rights POS and proof of POW. The battery life of industrial IoT edge devices is short, and the networking and computing capabilities are generally low. Therefore, it is necessary to deploy a consensus mechanism inside the server. If the edge device data block is successfully generated, it needs to be completed by the server when participating in the correct storage competition, and then the data block is written internally; the device data can be quickly generated at any time during application, and it has the characteristics of delay sensitivity [4]. If the Industrial Internet of Things is directly combined with the regional block, all devices will generate data blocks and write them into the corresponding data chain for the first time. Because the consensus algorithm calculation process is more complicated, data storage cannot be completed quickly, resulting in a gradual decrease in platform sensitivity, which is very likely. This leads to confusion in block data. Therefore, manufacturing companies generally add more than two production lines in the actual application process. If only valuable data is stored without distinguishing the production lines, it is likely to confuse the internal production data of the blockchain.

4.2.2 Edge Computing

Edge computing (EC) is often used in the IoT. It is one of the common distributed structures. It is also a popular Internet evolution method in recent years. Through edge computing, various intelligent communication devices, including smartphones, cameras, displays, and sensors, are integrated with the data center and then processed in a virtual environment [3]. On this basis, the end-to-end life cycle will complete informatization. In specific practice, edge computing nodes can be used as a distributed network component to provide Internet services, storage, and computing to terminal devices. In other words, edge computing refers to adding analytical data and computing capabilities to network edge devices, and most of the previous servers are migrated in. Network bandwidth pressure will gradually decrease, and server computing tasks will also be reduced [3]. The processing speed of the data will go on increasing, as will the computational speed.

4.3 Data Security Strategy Design

Analyze and study the criticality of the internal data of the intelligent factory system, which can be classified into two types, the first is non-critical data, and the other is critical data. Combining the design characteristics of the data itself, the system will give differentiated protection [5]. There are significant differences between these two data storage methods within the system. The former is usually stored in off-chain devices, such as common AGV motion path data; the latter is stored in the blockchain, such as user permissions and personal identity information.

4.3.1 On-Chain Data Security Strategy Design

The data stored in the blockchain is also called data on the chain. Because the blockchain itself has consensus mechanisms, tampering with this data is extremely difficult and is usually used to preserve critical data within the blockchain.

4.3.2 Design of Off-Chain Data Security Strategy

The amount of data stored on the internal blockchain of the system is not much. From the relevant data, it can be seen that the block-chain cannot help to store a vast amount of data. Therefore, other data in the system can be stored off-chain, such as non-critical ecological information in the production process of an intelligent factory.

5 Reliable Traceability Data Collection

5.1 Construction of Application System Environment

To enable users to track the source of information more quickly, ensure the security and authenticity of the information, and comprehensively reduce the instability of the acquisition equipment itself and the vulnerability of being vulnerable to external attacks, this paper designs a new data collection mechanism in combination with the actual situation. The basic structure includes different modules; besides communication and equipment acquisition modules, it also includes IOT gateway and data storage modules.

5.2 Construction and Implementation of Test Environment

Create a user interface, smart contract, and blockchain system through the existing device data to jointly build a robust security management system. Environment tests and data collection of this system mainly come from the intelligent factory system of the beef. The system includes critical equipment, such as industrial PCs, data collectors, and substantial production lines. Based on the part of the control data in the production line, a comprehensive test is carried out in combination with system operation and AGV control commands.

The data collection mechanism mainly includes three items; in addition to data collection and processing, it also includes data storage. Data storage is mainly done with the help of the database BigchainDB. The database includes two items, the first item

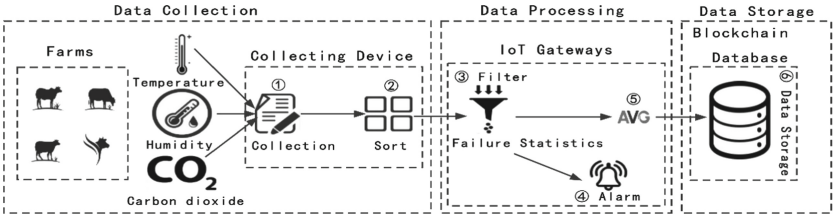

Fig. 1. The flow chart of the data collection mechanism.

is additional data, and the other item is asset data. The former is attribute information, which can be adjusted or deleted using transfer and asset creation; the latter generally refers to the traceability object information; for example, the input number has a relative and unique asset ID. It cannot be changed; the specific operation can be seen in Fig. 1. The process of the data collection mechanism is mainly as follows: collecting the environmental temperature of animals for classification, comparison, filtering, calculating the average value, etc. If the number of failed statistical data is too much, the system will give a false alarm. Finally, the critical information of the processed data is stored in the blockchain, and the non-critical information is stored outside the chain.

5.3 System Security Test

The Internet of Things environment usually refers to storage systems, IoT gateways, and acquisition devices. This article mainly verifies them through experiments. The environment is an indoor simulation environment. (1) Acquisition equipment: a board composed of a microcontroller module, a power supply module, a sensor module, a LoRa radio frequency module, etc. (2) IoT gateway: The gateway carrier mainly chooses Raspberry Pi 3B+, the memory capacity is 1 GB, the operating system is a Linux system, with Wi-Fi function support; (3) Storage system: After data collection is completed, it can be saved through BigchainDB, because the Internet of Things devices is easily affected by the external environment during use. Fluctuations may occur in the process, resulting in distortion or failure of data collection. According to the actual situation, the data collected in this article mainly uses 3 NodeMcus, and the environment chooses breeding or transportation and contains every 5 s for a total of 500 collections. Assuming that the temperature is between 21 °C and 29 °C, if it is lower or higher than this temperature, it is a failure (Fail).

The experimental results show that device 1 collected the environmental temperature value at the third, the 43rd, and the 65th failure times, a total of 16 times, device 2 failed a total of 10 times, and device 3 failed a total of 8 times. It is not difficult to see that all IoT devices fail during data collection, so the device is unstable during operation. This article uses 3 NodeMcu collection devices to minimize the risk of data loss and transfer it to the raspberry after collection. Send gateway.

After receiving the data, the Raspberry Pi gateway filters it, sorts and counts useless information, counts and warns abnormal devices, and calculates the storage temperature value. This way can reduce the data redundancy, errors, and deviations caused by the unstable operation of the device. And other issues.

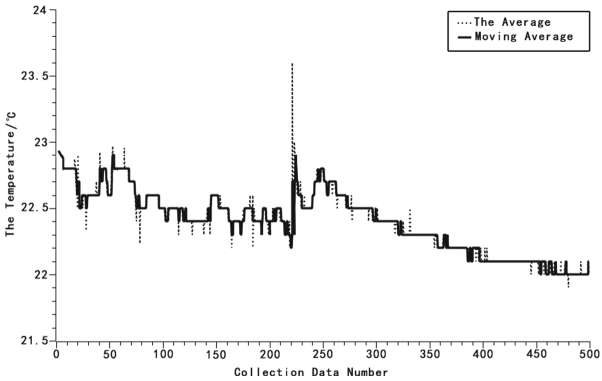

Fig. 2. Comparison of error temperature data of Internet of Things gateway

Two methods are mainly used to reduce data errors. The first is a moving average, and the other is the average. The Fail data is directly processed with 0. The black dotted line belongs to the average temperature, and the unstable operation of the device may cause deviations in the results. For example, when collecting data, the 21st, 41st, 185th, and 222nd times all experienced sharp fluctuations, and the value of the 222nd time directly soared to 23.6 °C. Using the moving average calculation method helps the temperature value smooth, as shown in Fig. 2.

From the experimental results, it can be seen that collecting temperature and humidity data through multiple devices can help reduce the deviation caused by data missing, and then analyze and process with the help of the Raspberry Pi gateway to reduce the data redundancy caused by the instability of the device itself, Errors and deviations, etc. It makes the data more authe and reliable.

The security of the data stored on the blockchain in the system is mainly responsible for the blockchain. The system usually only stores digital information such as digest and does not have security protection. However, the digital digest is usually stored inside the blockchain. Therefore, to quickly identify whether the data has been tampered with when selecting the used data, the digest needs to be removed and then contrasted with the digital digest saved in the blockchain to confirm whether the data has been tampered with [10]. When testing, you first need to encrypt the information, get the digital digest, and store it inside the blockchain. After comparison, you can get an entirely consistent digital digest, and the system will not release a warning signal; but if the data is tampered with in contrast, the system is likely to release a warning message.

6 Conclusions

At present, the penetration rate of the manufacturing industry and blockchain technology is getting higher and higher, and the probability of the manufacturing industry applying blockchain technology will continue to improve. Brilliant factory for all-round development in recent years, the system operation scale continues to expand, and network topology is not enough to focus. However, the rate of interactions between system data

and devices is higher. The traditional control system will cause a considerable impact on the Internet of things and development as the foundation block chain combination technology mature and stable intelligent factory system is a trend for future development. This article mainly discusses IoT data collection and data processing in depth. The integration of the IoT and blockchain saves the critical information of the data processed by the IoT on the blockchain and designs an intelligent safety system integrating the IoT and blockchain with the requirements of the safety management system as a reference.

Acknowledgment. This work is supported in part by the Foundation of Guangdong Key Areas of "Service for Rural Revitalization Plan" under Grant 2019KZDZX-2014, 2020ZDZX1037, in part by the Natural Science Foundation of China under Grants 61601304, U1713217, U1501253, 61801297, and 61801302, in part by the Foundation of Shenzhen under Grant 20200823154213001, JCYJ20170302142545828, and in part by Guangdong Laboratory of Artificial-Intelligence and Cyber-Economics (SZ), Shenzhen University, Shenzhen, China.

References

1. Abolhasan M, Makhdoom I, Abbas H, Ni W (2019) Blockchain's adoption in IoT: the challenges, and a way forward. J Netw Comput Appl 125(JAN.):251–279
2. Cao J, Shi WS, Sun H, Zhang Q, Sun W (2017) Edge computing: a new computing model in the era of Internet of Everything. Comput Res Dev 54(5):907–924
3. Liu F, Zhao ZM, Cai ZP, Xiao N (2018) Edge computing: platforms, applications, and challenges. Comput Res Dev 55(2):327–337
4. Quan L (2018) Blockchain: open the era of finance 2.0. Sci News 2:21-15
5. Reyna A, Martín C, Chen J, Soler E, Díaz M (2018) On blockchain and integration with IoT. Challenges and opportunities. Future Gener Comput Syst 88:173–190
6. Sun BY (2018) Current status and prospects of blockchain technology development. Digit Commun World 167(11):59
7. Wang SC, Gao LS (1998) Information support system of modern manufacturing. Comput Integr Manuf Syst 02:3–6
8. Yan JW, Li N, Liu M (2011) Framework for the industrial internet of things oriented to steel continuous casting plant MRO. Comput Integr Manuf Syst
9. Yuan Y, Wang FY (2019) Parallel blockchain security issues: research status and prospect Tian. Acta Automatica Sinica 45(1):206–225
10. Zuo Y, Tao F, Xu LD, Zhang L (2014) loT aced intelligent perception and access of manufacturing resource toward cloud manufacturing. IEEE Trans Ind Inf 10(2):1547–557