Research on Agricultural Internet of Things Data Sharing System Based on Blockchain

Shujing Lu
School of Automation
Southeast University
Nanjing, China
220181513@seu.edu.cn

Xiaojun Wang
School of Automation
Southeast University
Nanjing, China
101011042@seu.edu.cn

Jiaqiang Zheng
School of Automation
Southeast University
Nanjing, China
220181597@seu.edu.cn

Abstract—**The rapid development of technology in the field of Internet of Things has ushered in new changes in traditional agriculture. Blockchain has attracted the attention of various industries due to its unique characteristics of decentralized trust and distribution. The emergence of blockchain provides new possibilities for breaking down the barriers to data sharing and realizing the trusted interconnection of data. This article introduces the data quantification and isomerization problems presented by the progress in the agricultural IoT industry and the solutions provided by the blockchain technology. Designed a blockchain-based agricultural data sharing model and system architecture. The key mechanisms of system process design and data sharing were studied.**

Keywords—agricultural; Internet of Things; blockchain; data storage; data sharing

I. INTRODUCTION

The Internet of Things technology has become the focus of national industrial development and technological innovation, and it is also facing huge challenges. How to deal with challenges and solve development problems is a very critical topic in the current IoT industry. Blockchain provides solutions to many core issues faced by the Internet of Things, such as trust issues, big data management issues, and privacy protection issues.

In this article, through a lot of literature review and discussion of relevant blockchain technology and Internet of Things technology literature, the following aspects are studied: (1) the problems faced by the progress of the agricultural Internet of Things and the characteristics of the data (2) the core concepts, characteristics, core technologies of the blockchain and the problem-solving ideas obtained after the integration of the Internet of Things and the blockchain (3) carrying out the design of the blockchain-based agricultural Internet of Things data sharing system and research on the key mechanisms of data sharing.

II. PROBLEMS FACING THE PROCESS OF DEVELOPING OF THE INTERNET OF THINGS IN THE AGRICULTURAL FIELD

A. Problems Facing the process of developing of the Internet of Things industry

At present, the Internet of Things industry has initially developed. The conditions for large-scale application are rapidly forming, and industry development will enter a critical period [1]. However, at this stage, there are still many problems in the Internet of Things industry, which limits its development. Due to the complexity of the integration of the Internet of Things with different industries, the cost of applying the Internet of Things is very high, and privacy and security issues need to be resolved urgently. At the same time, the current Internet of Things industry is dominated by infrastructure construction and local application innovation. The great value of integration with various industry fields has not yet been deeply explored.

At this stage, the technical research on the Internet of Things mostly focuses on the business application layer[2], network layer and the perception extension layer. The storage and query processing of massive sensor data is one of the core issues facing the future development, its technical research is still relatively limited for the future development of the Internet of Things.

B. Analysis of Agricultural IoT Data Characteristics

The Agricultural Internet of Things maps agricultural objects in the real world to a computer storage system to facilitate decision support for agricultural applications [3-6]. It uses sensors to collect various information of agricultural objects, and passes the data information to the data layer storage center through the computer network. With the in-depth application of information technology in the agricultural Internet of Things[7], the data layer of the agricultural Internet of Things increasingly showing two key issues: one is that the amount of data is showing a trend of quantification; the other is the heterogeneity of data categories.

1) Massive quantification of agricultural IoT data: In order to make reasonable use of various effective information, so a provide more accurate decision-making judgments for agricultural objects, the underlying sensors of the Internet of

Things need to collect richer dynamic data information for data analysis and decision support or real-time control. This will inevitably lead to the need for sensors to collect more information and dynamic data at a certain frequency, and directly increase the amount of data stored, which places higher requirements on the storage capacity of the data center.

2) Data heterogeneity in the agricultural IoT: Various sensors are included in the Internet of Things system. The Internet of Things system contains a variety of sensors, which are not only different in structure and function, but the collected data is also heterogeneous. This heterogeneity greatly increases the difficulty of software development and data processing.

III. The solution provided by the integration of blockchain and Internet of Things

A. Technical Characteristics of Blockchain

Melanie Swan proposed in the book "Blockchain: A Blueprint for a New Economy and a Guide" [8] to divide the structure of the blockchain from different perspectives of development stages. Blockchain 3.0 mainly refers to other applications beyond financial transactions, especially in fields such as scientific research, industry and agriculture, and the Internet of Things. Generally speaking, such blockchains exist in the form of enterprise alliance chains or private chains. At present, there is still no mature blockchain 3.0 platform in the industry.

Blockchain is a method of implementing and implementing transaction processing by using transparent and reliable rules to build traceable data structures in a peer to peer environment (also known as a distributed network or peer to peer). It has the typical characteristics of decentralized peer to peer, chain data block, anti-counterfeiting and tampering protection, transparency, credibility and high reliability. Blockchain can provide three aspects of application capabilities [9,10]: The first aspect is to supply base installation resources such as network, storage, computing, and platform via a peer to peer network. The second aspect is managing, querying and analyzing data in peer to peer networks. The third aspect is to use peer to peer networks to provide application services such as digital asset transactions, finance, payment and settlement.

Blockchain has unique technical characteristics, it may play a good role in solving the problems of trust, big data management, privacy and security that may be faced in the development of the Internet of Things[11]. It can promote the further development of the IoT industry to a distributed and intelligent advanced form.

B. Application of Blockchain Technology in Modern Agriculture

The Agricultural Internet of Things generally adopts a centralized management method. With increasingly more smart devices connected to the Internet of Things, data center hardware and software infrastructure, maintenance costs and energy consumption are facing unprecedented challenges. The decentralized management method of blockchain technology can effectively reduce the input and maintenance the cost of agricultural IoT [12-14]. By realizing the combination of agricultural Internet of Things and blockchain technology, the monitoring equipment connected to the network can realize self-management and maintenance. It can save high infrastructure construction and maintenance and energy consumption costs centered on cloud control, reduce the later maintenance cost of Internet equipment, and help to improve the level of intelligence and scale of the agricultural Internet of Things [15].

IV. Design of Agricultural Internet of Things System Based on Blockchain

A. Design of Agricultural Data Sharing Model Based on Blockchain

The blockchain-based agricultural data sharing model is composed of four parts including data demand side, decentralized data sharing platform, data owner and data source, as shown in Fig.1. Data demand side refers to researchers, research institutions, companies, or project teams who have access to data, and they can be divided into commercial applications, scientific research, and public services according to different application fields [16-18]. The data owner is an individual or institution that has all management authority over the data, such as agricultural scientific research institutions, enterprises, laboratories, and individuals [19]. A data source represents a computer, central server, or cloud server that has basic functions of a database management system and can provide remote data access.

In this model, each model subject has a clear role definition. The roles can depend on each other and switch. Among them, the data owner releases data through a decentralized data sharing platform as the starting point of the information flow. Later, both parties can retrieve data, view data quality evaluation, and publish data subscription requirements. Eventually, the two parties can share the data with credibility, transparency and equality on the platform.
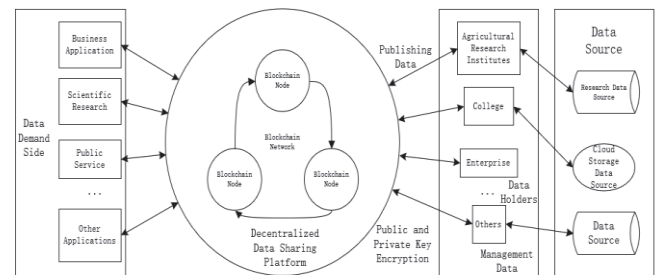

Fig. 1.   Blockchain-based data sharing model

As a fusion of multiple technologies, blockchain has the advantages that traditional distributed databases and centralized databases cannot match. The current requirements of big data for system security, data trust, and trustworthy scalability coincide with it [20]. Blockchain technology consists of P2P network transmission protocols, consensus algorithms, encryption algorithms and other technologies. Essentially a distributed ledger database under a peer to peer network, providing decentralized trust under data sharing. Including the following aspects:

1) Trustworthy system security: Each node in the blockchain network permanently embeds transaction information in the data block, any node damage will not affect the normal operation of the entire database, so it can effectively avoid malicious attacks in the centralized architecture and single point of failure and other issues.

2) Trustworthy data rights management: The data on the blockchain is transparent and time-stamped, which adds a time dimension to all data authority interaction data, making the process easier to trace, so that the interaction process is not stolen or tampered with.

3) Trustworthy data privacy protection: The blockchain is based on the IP communication protocol and distributed network. All nodes have the same status, and there is no need to host the data with a third-party organization, so the data owner has data ownership.

B. System Architecture Design

A layered architecture for agricultural data sharing based on blockchain, including management plane, control plane and data plane. It is composed of user layer, service layer, platform layer and facility layer, as shown in Fig.2.

The data plane is responsible for the information interaction between the sensor node and the data storage module. The control plane uses the programmable features of smart contracts to encapsulate all business logic related to data sharing and store core information and processes on the blockchain network. The management plane is responsible for packaging the functional interfaces provided by the control plane into different data management services, and adopts multiple visualization methods to present the management functions of agricultural data sharing to users in a diversified form.
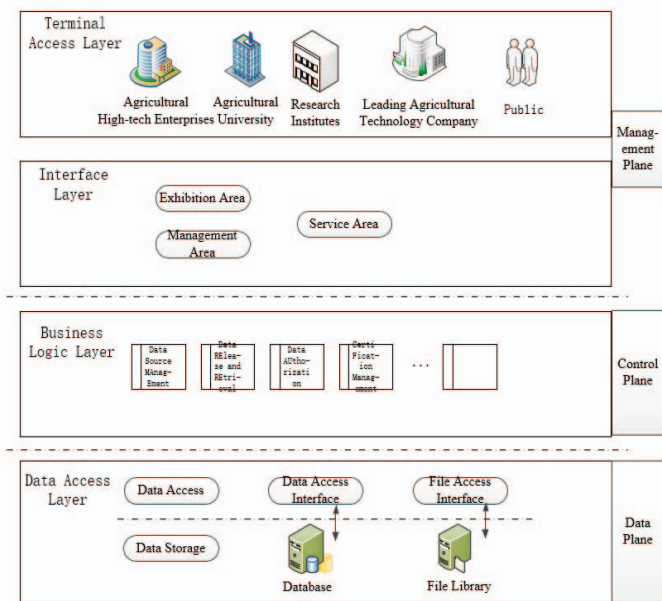

Fig. 2.   Layered architecture

The facility layer includes multiple sensor nodes for collecting crop data information and a base station for gathering crop information. The base station is in communication with the data storage module and is used to realize the information interaction between the sensor node and the data storage module.

As the core part of the architecture, the platform layer is mainly used to store data and interact with key business logic based on smart contracts to achieve authentication management and data sharing. Blockchain technology is composed of P2P network transmission protocol, encryption algorithm, consensus algorithm and other technologies. It is essentially a distributed ledger database under a peer-to-peer network, providing decentralized trust under data sharing.

C. System Flow Design

This system has designed a data collection and sharing system for agricultural Internet of Things based on blockchain. It includes multiple data monitoring and acquisition modules, transmission modules, data storage modules, authentication management modules, data processing modules, and blockchain sharing modules.

Each data monitoring and collection module collects crop data information and sends it to the data storage module through the transmission module. The data processing module includes a preprocessing unit, a clustering unit, an anomaly detection unit, and a database. The pre-processing unit pre-processes the crop data information with a value of 0 or negative, and replaces the value of 0 or negative with a preset replacement value. The clustering unit is used for clustering the pre-processed crop data information. The anomaly detection unit is used to perform anomaly detection processing on the clustered crop data information, mark the abnormal crop data information, and send the crop original owner identity information and the processed crop data information to the database for storage. The authentication management system is used for key issuance and identity authentication for each node in the system. When the authentication between nodes is allowed to access, the data processing module is used to process the data into a unified format. The blockchain sharing module is used to display and share crop data information.

Among them, the data monitoring and collecting module includes a plurality of sensor nodes for collecting data information and a base station for gathering crop data information. The base station is in communication with the data storage module and is used to realize the information interaction between the sensor node and the data storage module.

V.   Research on Key Mechanisms of Agricultural Heterogeneous Internet of Things Data Sharing Based on Blockchain

A. Information Connection Mechanism of Agricultural Data Sharing Based on Blockchain

The core of the blockchain-based data sharing model is to connect the shared information. Due to the wide distribution of agricultural data, different connection methods, lack of unified standards, large volume, and the limited storage space of the blockchain itself, excessive redundant data can easily affect the

performance of the blockchain. This model separates data sources and data management. There is no longer a third-party data management organization, and each enterprise and individual perform distributed storage and control of data. The data source is composed of data centers of various institutions, enterprise databases and even personal IoT sensing devices. Due to the development of cloud storage technology and various database management system tools that provide visual support, database construction has become more convenient to use.

The participating parties interact with the public and private keys generated by the blockchain asymmetric encryption technology. The role of the public key is a public address, and the private key is kept by all parties. When a user needs to broadcast data, the private key is used to encrypt the information to determine its authenticity. For example, the private key is used to encrypt the data description and access method during the data distribution process, and to guarantee the data copyright in the form of transaction. When mutual authorization is required for both parties, the private information can be encrypted with public and private keys. Take A to B as an example. The specific method is: A first encrypts the authorization information with B's public key to get $\{message\}_B$. B can decrypt and view it, and then use his private key to encrypt it as a digital signature to obtain $\{\{message\}_B\}_A$ to ensure the credibility of the source of the information. When B obtains the message, it is first decrypted with A's public key to get $\{message\}_B$, ensuring that the source is trusted. Then use its own private key to decrypt to obtain the original data authorization message $\{message\}$.

All information processes involving data interaction and copyright are recorded in the blockchain network in a transparent and complete manner. The blockchain consensus algorithm performs verification records to ensure that it cannot be tampered with. The user's original data and non-desensitization data do not need to be hosted in a third-party organization, nor will they be cached by anyone. In the event of a copyright dispute, the authority can be traced from the records on the chain to ensure data protection.

Since all the data of the blockchain is backed up by each node, the excessive amount of redundant data on the chain will reduce the consensus efficiency and increase the storage and calculation costs of each node. Therefore, a distributed file system is introduced to record non-critical information such as data descriptions and data access methods after authorization verification.

In the above model, various big data sources are managed and maintained by various data providers. It is only necessary to put detailed descriptions and sharing protocols in the form of files into the distributed file system network, and publish data summary on the blockchain Set data ownership. When the rest of the users need data, they retrieve the data from the chain according to the type or summary keyword, locate the data description through the distributed file system, and implement data interaction on the chain.

B. Blockchain-based Authentication Management Mechanism

The specific process of authentication by the authentication management module is displayed in Fig.3:
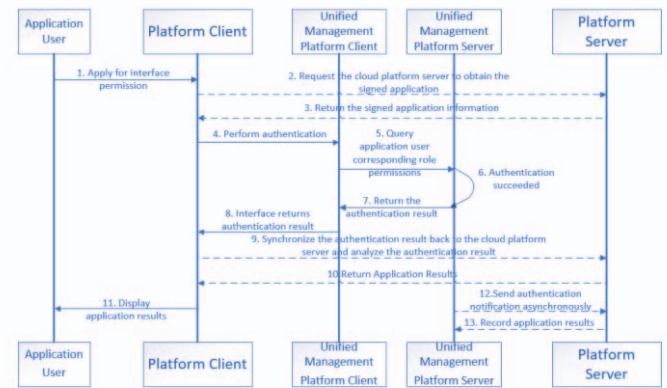

Fig. 3. Blockchain-based authentication management flowchart

1) The authentication management module issues a pair of security keys to each data owner and the blockchain sharing module, which are divided into public keys and private keys. The block chain sharing module stores the public key passwords of various research institutes, and at the same time, the data owner saves the public key passwords of the sharing modules.

2) Each subject in the authentication system has clear role boundaries. Roles can depend on each other and transform, different roles correspond to different data source permissions. The unified management platform performs role authority authentication.

3) Data demand-side users apply for interface access rights on the platform client. The client will request the platform server through the interface. After receiving the request, the server will use the user's private key to encrypt the request information, then generate a digital signature, and splice the digital signature after the plaintext request.

4) The platform server returns the encrypted request to the platform client. The client of the unified management platform verifies the request, and queries the role of the corresponding user on the server of the unified management platform to obtain an authentication result (authentication success, authentication failure, etc.) The server of the unified management platform will also use the private key of the shared module to encrypt the authentication result.

5) The server of the unified management platform will synchronously return the signed authentication result to the platform client. The platform client needs to return the authentication result to the platform server for verification. After the server end verification, the real authentication result is returned to the client. The client makes corresponding interface processing according to the authentication result.

6) After the authentication of the server of the unified management platform is completed, the signing result will be returned to the platform server asynchronously. The server uses the public key of the shared module to verify the authentication result. After the verification, the corresponding request is processed according to the payment result. The server will return the processing result to the server of the unified management platform after processing.

224

VI. CONCLUSIONS

This article analyzes the methods and applications of agricultural Internet of Things data sharing technology under the blockchain. Blockchain is not a new technology, but a multi-dimensional cross-application model. It is a technology produced by the integration of distributed data storage, P2P transmission, databases, encryption algorithms, time stamps, and other mature IT technologies. In order to ensure the smooth operation of the system, the blockchain not only has decentralization, but also protects user information security to a certain extent. This paper combines the trend of data quantification and data category isomerization presented by the Agricultural Internet of Things, and combines the technical characteristics of blockchain decentralization, and proposes a blockchain-based agricultural data sharing model to carry out the overall system architecture and process design. Research on key mechanisms such as the agricultural data sharing information connection mechanism based on blockchain in the research process. The next step will be optimized for the efficiency of data sharing. The application of blockchain technology in agricultural data sharing also needs to be verified and improved through continuous practice.

REFERENCES

[1] M. Marjani et al., "Big IoT Data Analytics: Architecture, Opportunities, and Open Research Challenges," in IEEE Access, vol. 5, pp. 5247-5261, 2017, doi: 10. 1109/ACCESS. 2017. 2689040.

[2] K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," in IEEE Access, vol. 4, pp. 2292-2303, 2016, doi: 10. 1109/ACCESS. 2016. 2566339.

[3] S. B. Baker, W. Xiang and I. Atkinson, "Internet of Things for Smart Healthcare: Technologies, Challenges, and Opportunities," in IEEE Access, vol. 5, pp. 26521-26544, 2017, doi: 10. 1109/ACCESS. 2017. 2775180.

[4] M. Chiang and T. Zhang, "Fog and IoT: An Overview of Research Opportunities," in IEEE Internet of Things Journal, vol. 3, no. 6, pp. 854-864, Dec. 2016, doi: 10.1109/JIOT.2016.2584538.

[5] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," in IEEE Access, vol. 6, pp. 32979-33001, 2018, doi: 10.1109/ACCESS.2018.2842685.

[6] P. K. Sharma, M. Chen and J. H. Park, "A Software Defined Fog Node Based Distributed Blockchain Cloud Architecture for IoT," in IEEE Access, vol. 6, pp. 115-124, 2018, doi: 10.1109/ACCESS.2017.2757955.

[7] Z. Zheng, S. Xie, H. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," 2017 IEEE International Congress on Big Data (BigData Congress), Honolulu, HI, 2017, pp. 557-564, doi: 10.1109/BigDataCongress.2017.85.

[8] K. Haseeb, N. Islam, A. Almogren and I. Ud Din, "Intrusion Prevention Framework for Secure Routing in WSN-Based Mobile Internet of Things," in IEEE Access, vol. 7, pp. 185496-185505, 2019, doi: 10.1109/ACCESS.2019.2960633.

[9] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," in IEEE Access, vol. 7, pp. 10127-10149, 2019, doi: 10. 1109/ACCESS. 2018. 2890507.

[10] O. Novo, "Blockchain Meets IoT: An Architecture for Scalable Access Management in IoT," in IEEE Internet of Things Journal, vol. 5, no. 2, pp. 1184-1195, April 2018, doi: 10.1109/JIOT.2018.2812239.

[11] D. Miller, "Blockchain and the Internet of Things in the Industrial Sector," in IT Professional, vol. 20, no. 3, pp. 15-18, May./Jun. 2018, doi: 10.1109/MITP.2018.032501742.

[12] F. Tschorsch and B. Scheuermann, "Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies," in IEEE Communications Surveys & Tutorials, vol. 18, no. 3, pp. 2084-2123, thirdquarter 2016, doi: 10.1109/COMST.2016.2535718.

[13] K. Salah, M. H. U. Rehman, N. Nizamuddin and A. Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," in IEEE Access, vol. 7, pp. 10127-10149, 2019, doi: 10. 1109/ACCESS. 2018. 2890507.

[14] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[15] S. Yaji, K. Bangera and B. Neelima, "Privacy Preserving in Blockchain Based on Partial Homomorphic Encryption System for Ai Applications," 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW), Bengaluru, India, 2018, pp. 81-85, doi: 10.1109/HiPCW.2018.8634280.

[16] S. Malik, V. Dedeoglu, S. S. Kanhere and R. Jurdak, "TrustChain: Trust Management in Blockchain and IoT Supported Supply Chains," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 184-193, doi: 10.1109/Blockchain.2019.00032.

[17] S. Yaji, K. Bangera and B. Neelima, "Privacy Preserving in Blockchain Based on Partial Homomorphic Encryption System for Ai Applications," 2018 IEEE 25th International Conference on High Performance Computing Workshops (HiPCW), Bengaluru, India, 2018, pp. 81-85, doi: 10.1109/HiPCW.2018.8634280.

[18] A. Nawaz, T. N. Gia, J. P. Queralta and T. Westerlund, "Edge AI and Blockchain for Privacy-Critical and Data-Sensitive Applications," 2019 Twelfth International Conference on Mobile Computing and Ubiquitous Network (ICMU), Kathmandu, Nepal, 2019, pp. 1-2, doi: 10.23919/ICMU48249.2019.9006635.

[19] W. Wang et al., "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," in IEEE Access, vol. 7, pp. 22328-22370, 2019, doi: 10.1109/ACCESS.2019.2896108.

[20] K. Sarpatwar, V. S. Ganapavarapu, K. Shanmugam, A. Rahman and R. Vaculin, "Blockchain Enabled AI Marketplace: The Price You Pay for Trust," 2019 IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW), Long Beach, CA, USA, 2019, pp. 2857-2866, doi: 10.1109/CVPRW.2019.00345.