2024 4th Asia-Pacific Conference on Communications Technology and Computer Science (ACCTCS) | 979-8-3503-5998-5/24/$31.00 ©2024 IEEE | DOI: 10.1109/ACCTCS61748.2024.00121

The Application of Blockchain Technology in Network Information Security

Yan Li
Tianjin University of Technology, Tianjin, China
L18831388824@163.com

***Abstract*—With the rapid development of the Internet, the problem of network information security has become increasingly prominent. The traditional network security solutions have the weaknesses of centralization and vulnerability to attack, and cannot effectively deal with the risk of attack and data tampering. As a decentralized and tamper-resistant distributed ledger technology, blockchain technology has a good potential to be applied to network information security protection. This paper aims to summarize the basic principle and security characteristics of blockchain technology, discuss the network information security protection method based on blockchain, and analyze the application of blockchain technology in identity protection, food supply chain, O2O catering and other aspects for reference.**

Keywords—Blockchain technology, Network information security, Decentralization

I. Introduction

With the rapid development of the Internet, the problem of network information security has become increasingly prominent, and the traditional centralized security mechanism has gradually revealed its limitations in the face of increasingly complex network attacks. As an emerging distributed ledger technology, blockchain technology has the characteristics of decentralization, non-tampering and encryption protection, which is widely considered to be an effective means to solve the problem of network information security. This paper aims to discuss the protection and application of network information security based on blockchain technology. Through the comprehensive analysis of existing research and practice, some specific application cases and development directions are proposed to provide reference for the research and practice in the field of network information security.

II. Overview of Blockchain Technology

A. Blockchain Concept

There are narrow and broad definitions of blockchain. In a narrow sense, blockchain is an unforgeable distributed ledger, which is cryptographically secure and tamper-resistant. At the same time, each block forms a chain structure in chronological order. Broadly speaking, blockchain is a new distributed architecture computing method, which uses chained data structure, uses distributed algorithms, uses cryptography to ensure data transmission and security, and uses smart contracts to operate data. It can be seen that both broad and narrow definitions of blockchain concepts emphasize distributed data storage, distributed ledgers, cryptographic encryption algorithms, smart contracts and consensus mechanisms. Its essence is a decentralized distributed storage database, and each data block stores transaction information to verify the validity and generate the next block. The blockchain contains an ever-expanding log of transactions and their temporal order. In other words, a data structure is a ledger that may contain digital transactions, data records, and executable files. Transactions are aggregated into larger groups, called blocks, which are linked to previous blocks using timestamps and passwords, forming a chain of records that determines the order of events or "blockchain". In addition to describing the data structure itself, the term is also widely used in the literature to refer to digital consensus architectures, algorithms, or application domains built on top of such structures.

B. The basic principle of blockchain

The basic principle of blockchain can be summarized as follows: First, the distributed ledger, the data in the blockchain is maintained by multiple nodes, and each node has a complete copy of the data. This distributed feature makes the blockchain highly reliable and anti-attack ability. The second is the consensus mechanism. The nodes in the blockchain reach consensus through the consensus algorithm to ensure the consistency and correctness of data. The common consensus mechanisms include Proof of Work and Proof of Stake [1]. The third is the encryption algorithm, which is used by the blockchain to ensure the security and integrity of data. Each block contains the hash value of the previous block. Once the data in the blockchain is tampered with, its hash value will change, so that it can be identified by other participants in Figure 1.

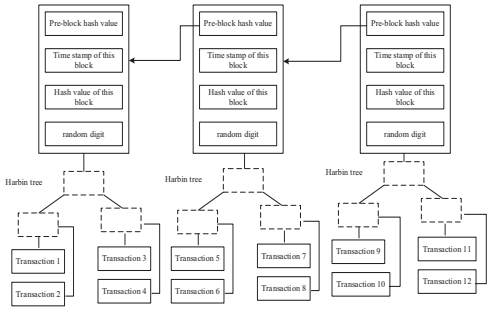

Figure 1 The basic principle of blockchain

Biometric technology protects the security of users and improves the accuracy of user identity authentication. The drawback is that the centralized storage method will lead to malicious tampering of user information. Combining blockchain technology with biometrics technology and storing the collected user biological information on the block can solve this problem, greatly improve the accuracy of identity authentication, and achieve the purpose of protecting user information security. The architecture of biometric identification system based on blockchain mainly includes four layers, namely, application layer, network layer,

979-8-3503-5998-5/24/$31.00 ©2024 IEEE
DOI 10.1109/ACCTCS61748.2024.00121

transaction layer and physical layer.

1) Application layer

The application layer allows users to communicate with the system through a web application or a mobile application. By connecting to the blockchain-based network, user requirements are sent to the system through a mobile application or a web application[2].The application layer provides a direct service to the end user when the user communicates directly with the system.

2) Network Layer

The network layer is responsible for the interaction between the system and the user and consists of communication technologies that help users, service providers, and iot devices such as sensors and security cameras to connect to each other. This layer provides the guarantee of physical layer security.

3) Transaction layer

Responsible for all consensus mechanisms of the entire blockchain network and also for operations between nodes in the system. Users use smart contracts and consensus mechanisms to exchange data in a secure way, the transaction layer interacts with the blockchain network and verifies new transactions, and the block link is subject to user information interaction as a transaction and authenticated through the smart contract. The biometric information public ledger is also updated through this layer.

4) Physical layer

This layer is mainly composed of different types of actuators and sensors, WirelessSensorNetworks (WSN) devices. It uses a cryptographic device driver to authenticate and then updates the information in Figure 2.

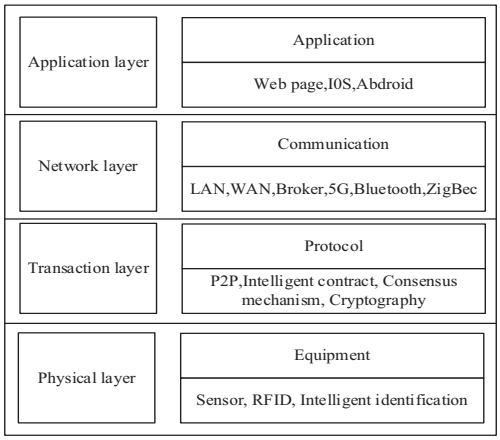

Figure 2 Biometric system architecture for blockchain

III. Blockchain Protection Methods

The traditional network user security protection matrix is mostly one-way, although it can achieve the expected protection goal, but the efficiency is low, the quality of protection is not high, and it has a negative impact on the user's network application. Therefore, this time, combined with blockchain technology, a multi-level cross information security protection matrix is established. Firstly, it is necessary to design an anti-attack abnormal signal capture program in the matrix. Secondly, combined with the blockchain program, a complete information security protection structure was formed. At this point, the abnormal intrusion signal capture time is calculated, as shown in Formula (1).

$$P = \bar{\omega}^2 + \sum_{y=1} \xi y - \rho a \tag{1}$$

In Equation (1), P represents the abnormal intrusion signal capture time, ω represents the protection coverage, ξ represents the protection unit value, y represents the response frequency, ρ represents the directional information conversion ratio, and a represents the difference in attack identification. Based on this, the captured signal was analyzed and studied, and multiple safety protection goals and cross protection standards were set. It was imported into the matrix to strengthen the safety protection ability of the matrix. At the same time, the trajectory of the abnormal signal could be calibrated, which laid the foundation for the subsequent upgrading of the protection structure.

IV. Application of Blockchain Technology

A. KSI replaces PKI

Each public key cryptosystem is an independent identity that is not under the control of any third party or individual. Any private key can be used on different platforms, and each platform has a unique authentication number for it. Public key cryptosystems can also be copied and decrypted to ensure access to digital resources (including files, email addresses, etc.)[3]. Keyless Signature Infrastructure (KSI) also allows access to secret information in asymmetric cryptography such as RSA. KSI will not allow any unauthorized user to obtain or view the private key, nor will it allow any unauthorized user to change the secret information in the public key encryption such as RSA. All public-key cryptosystems have their own set of keys, and private keys can be used on different platforms, such as file systems, browsers, email addresses, and so on. KSI can provide asymmetric cryptographic services for different platforms. Figure 3 shows the blockchain user data management system.

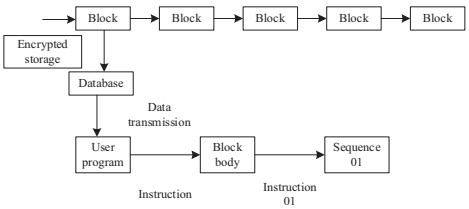

Figure 3 User data management system based on blockchain

B. Application of blockchain technology in O2O catering delivery supply chain

In order to understand the reality of O2O catering takeaway supply chain security, the author investigated three main participants: takeaway merchants, takeaway delivery workers and consumers. The survey was carried out in the urban area of Changsha City, Hunan Province, using the method of questionnaire survey, mainly offline survey, supplemented by online survey. A total of 90 food and beverage outlets providing delivery services were surveyed,

After data cleaning, the effective rates of the questionnaire were 97%, 97% and 91%, respectively. Most of the food delivery merchants were able to do the procurement, storage and food preparation of raw materials,

but the food delivery workers and consumers still had low confidence in the safety of food for sale. More than 60% of delivery staff think that takeaway food is not safe, about 90% of consumers have heard or experienced the safety problem of takeaway food, and most consumers think that it is difficult to protect their rights once the safety problem of takeaway food occurs. On the one hand, food safety needs to be interlinked, and no problem can be allowed in any link. On the other hand, the non-contact of takeaway service is strong, and the opacity of information between each subject is easy to cause distrust. Distribution security mainly refers to whether there are cheating and information leakage in the process of food delivery from the business to the consumers. About the customer's personal information, most takeout platforms for customers Privacy protection is relatively strict, it is difficult for merchants and delivery staff to see sensitive information, but in the process of delivery service, consumers 'contact information often needs to be disclosed, which is easy to cause confusion to consumers. Most takeout delivery workers do not contact customers when delivering food, and there are hidden dangers[4].

Consumers may encounter problems such as packaging contamination, delivery overtime, food error or substandard, and takeaway loss in receiving takeaway, among which delivery not on time is the most serious problem. In general, due to the limited or even no contact between consumers and takeout merchants and delivery workers, it is difficult to supervise the safety of food delivery, food safety and their own rights and interests cannot be fully protected, and it also leads to the lack of confidence of consumers in catering takeout. In order to promote the healthy development of the catering takeaway industry, it is necessary to enhance the transparency of information between the subjects and strengthen the safety management of the whole chain.

To ensure the security of the entire supply chain, blockchain technology needs to penetrate into all key links of the O2O catering takeaway supply chain, as shown in Figure 4. By hashing the data uploaded by each node of the takeaway supply chain, taking a summary of the data, and then using the asymmetric encryption technology in the blockchain system, the private key is used to encrypt the data, and the encrypted and digitally signed data is uploaded to the database, and then the public key is used to decrypt the data, so that the data can be compared to verify the authenticity and non-tampering of the data. So as to ensure that the relevant data in the system can be trusted by all subjects in the takeaway supply chain.

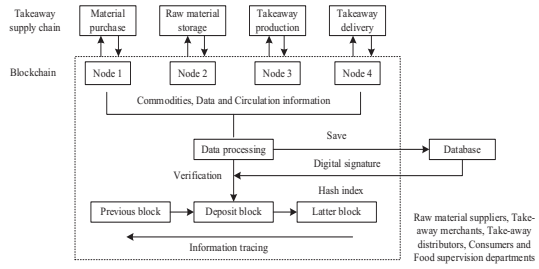

Figure 4 Security management framework of catering delivery supply chain based on blockchain technology

The information collection of the raw material procurement link is jointly completed by the takeaway merchant and the raw material supplier. The delivery merchant shall draw up a purchase list according to its own needs of food materials, tableware, packaging and other materials. The corresponding supplier shall input the production date, purchase time, freshness and transportation information of raw materials into the blockchain system, and the delivery merchant shall supervise and confirm. In the raw material storage link, take-out merchants need to take photos of the kitchen environment, the location of raw material storage, ventilation and moisture-proof conditions every day, and upload the real raw material storage environment to the blockchain system to facilitate the supervision of the storage link. The information of takeaway food production is mainly collected by the takeaway merchants in real time. In the process of food production, cameras, environmental detectors, information collectors and other equipment can be used for real-time monitoring and data archiving to facilitate subsequent information calls[5]. In the food packaging link, a QR code containing blockchain information should be attached to the receipt of the merchant, and the information of the entire food production link should be input into the system, which is supervised by consumers.

If problems are found, feedback can be given in time to protect their own rights and interests. In the takeaway delivery link, when the delivery clerk receives the takeaway food, the Internet of things technology can be used to detect the temperature, humidity and other information in the takeaway box that may affect the food safety status, record the time of delivery and the information of takeaway delivery in real time, and input it into the blockchain system. At the same time, the positioning system can also be used to upload the distribution route to the blockchain system, and consumers can obtain distribution related information in the system. Raw material suppliers, takeout merchants, takeout delivery workers, consumers and food regulators are the main users of the blockchain system. Each subject can complete the information traceability of the entire takeaway supply chain through the system, consult the relevant information generated in the whole process of takeaway food supply according to the need, so as to facilitate the supervision of food safety and distribution safety, and make accurate responsibility division when safety problems occur.

Takeaway merchants can query the source and information of food ingredients through the blockchain system, and also adjust the procurement and production of food ingredients according to the information feedback from consumers. Through information disclosure, raw material suppliers and takeaway merchants with higher service quality can obtain more benefits, while subjects with integrity problems will be punished, so as to improve the safety credit system of takeaway food and the level of supply chain management. The delivery staff can automatically upload the status, delivery route and delivery time of food delivery through sensors and systems, which can better communicate with merchants and consumers and improve the quality of delivery service. At the same time, when the distribution problem occurs, it is beneficial to distinguish the responsibility and protect their legitimate rights and interests.

By scanning the QR code link blockchain system on the takeaway receipt, consumers can clearly view the qualification information of takeaway food raw materials, storage environment, production conditions and other information directly related to the safety of takeaway food, enhance the supervision of takeaway food, and maintain their own "safety on the tip of the mouth". The food supervision

department can view the relevant information of each link of the takeaway supply chain through the blockchain system at any time to realize the quality supervision of the whole process. When there is a food safety problem or accident, it can be traced through the system, accurately locate the problem point, and improve the efficiency of food safety management[6].

C. Application of blockchain technology in food supply chain

Blockchain technology has advantages in improving the management level of food quality and safety and improving the efficiency of supervision and early warning. The data information recorded in each link of the supply chain is recorded to the blockchain, which improves the level of food quality monitoring. Consumers can have an intuitive understanding of the production process, obtain real and reliable food information, avoid buying fake and shoddieable food, and enhance consumers 'trust in food safety. Whether for enterprises or regulatory authorities, compared with the traditional food product traceability, it is easier to obtain food information and improve information.

At the same time, it can integrate the national food safety supervision data resources, share the food safety monitoring information of the whole industry chain, and exchange information in real time, so that the evaluation and early warning of food safety are more timely, and the risk monitoring and early warning capabilities of regulatory departments are improved. The process management of the supply chain from production to sales is optimized, such as providing shelf life management to retailers to reduce the waste and the probability of safety accidents caused by food expiration. The seed of crops is the basis of agricultural production, and the quality of the seed directly affects the quality and output of grain.

In the seed market, there are many kinds of seeds and the market quality supervision and management mechanism is not perfect, resulting in inferior seeds and even fake seeds flooding the market, seriously harming the interests of farmers, endangering food security and affecting economic development. Blockchain technology can solve market chaos and regulatory pain points, write the information from breeding to seed production into the blockchain, provide a credible channel for breeders to query germplasm resources, make full use of germplasm resources, promote the selection of seed varieties needed by the market, and reduce the repeatability of breeding. The information of all links from breeding to seed production can be inquireable, so that fake and inferior seeds have no place to hide, and the source can be trusted to promote the healthy and stable development of the seed industry.

Our country attaches great importance to food safety. Food traceability has been written into the food safety law, and it is an obligation that enterprises must fulfill. In the massive data information of each link of the supply chain, consumers only care about the data that can prove the source and quality of food, and the regulatory authorities need to query the detailed traceability data to facilitate the definition of responsibility. When cooperating with the construction of the food safety traceability system, enterprises do not want to disclose the private information such as the flow of sales goods, enterprise procurement channels, processing technology and formula.

The network user privacy information protection model is constructed by integrating the blockchain technology. According to the privacy protection requirements of network users, multiple protective processing modules can be designed, which are privacy information collection module, privacy information storage module, privacy information encryption module, privacy information sharing module, privacy information multi-dimensional protection module and privacy information management module. The specific protection execution structure is shown in Figure.5.

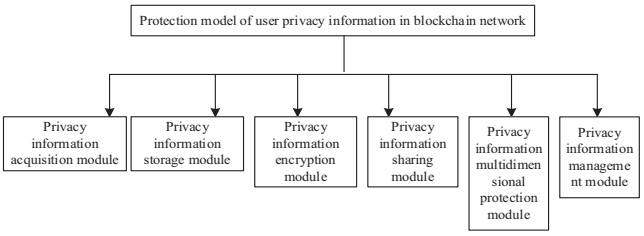

Figure 5 Module structure of block chain network user privacy information protection model

Without the complete record of all links of the whole industry chain, consumers or regulatory authorities can query the origin, variety grade, quality change, storage time, processing, whether there is mixing and other indicators and data with reference value when tracing the source of the food, so that they can determine that the food they buy is healthy, safe and in line with national standards. Basically, the real goal of food quality traceability is achieved[7].

The sensors in the Internet of things system are responsible for information collection, and the storage of data is completed by the blockchain, using EPC code, RFID(radio frequency identification), WSN(wireless sensor Network), BDS(Beidou satellite navigation System),

GIS(Geographic information System) and other information data are identified by "one thing, one code". Consumers or regulatory authorities scan the code to obtain electronic documents related to the product that are recorded in the blockchain, query the detailed information of each link, and realize traceability. The combination of blockchain and Internet of things makes it possible to remote control and real-time monitoring of agricultural production, reduce the cost of agricultural production and improve production efficiency. Yang Jun et al built a new model of "smart food inspection" based on the Internet of Things, and created a quality monitoring and traceability mechanism for grain harvest, inventory, processing and sales on enterprise platforms such as Zhejiang Grain Information Management Platform.

They used specific identifiers such as geographical location and commodity bar code to monitor and analyze data, and combined with blockchain to realize on-site control of sampling and monitoring. It lays a solid foundation for the

quality of stored grain and the source pollution control of harvested grain in the province. In the granula management, the Internet of things technology is used to upload the granula environment, trading conditions and in-out and in-out information to the blockchain in real time, avoiding human factors, eliminating false information from the root chain, and enhancing information security and reliability helps regulatory authorities to improve the storage, supervision and scheduling of regional grain data.

"Shanliangflavor" applies Internet of things sensors to the monitoring system of farmland, which automatically captures the growth environment, climate temperature, pests and diseases and other information of seeds around the clock, and accurately monitors and manages the rice growth process.Through the perfect combination of blockchain and Internet of things technology, "Grain Through Chain" in Guangdong Province realizes food traceability, supply chain management, supply chain finance and other functions, shares information and data, and improves food security.

V. Conclusion

To sum up, the essence of blockchain technology is to establish a platform that shares trust and everyone can trust. It is a technology that must be used in the future information society, and it can also be used for safer and more efficient transactions and cooperation, which is a new technology that is more pleasant and effective for cooperation.

References

[1] Zhiping Z .The Application of Blockchain Technology in Enterprise Value Chain Cost Management[J].Pacific International Journal, 2024,7(1).

[2] Kunwar S ,Karthik B ,Aaditya J , et al. Assessment of barriers impeding the incorporation of blockchain technology in the service sector: a case of hotel and health care[J].Journal of Modelling in Management, 2024, 19(2):407-440.

[3] International R B. Retracted: Design and Application of Electronic Rehabilitation Medical Record (ERMR) Sharing Scheme Based on Blockchain Technology[J]. BioMed research international,2024.

[4] Ling C, Zeng T .Exploration and Practice of Blockchain Technology Application in the Field of Digital Commerce[J].Academic Journal of Business Management,2023,5(24).

[5] Khuram S , Qingyu Z , Muhammad A , et al. Pre- to post-adoption of blockchain technology in supply chain management: Influencing factors and the role of firm size[J].Technological Forecasting Social Change,2024,198

[6] Shenghao X, Yu G, Martin K, et al. The application of blockchain technology in the recycling chain: a state-of-the-art literature review and conceptual framework[J]. International Journal of Production Research, 2023, 61(24): 8692-8718.

[7] Ma Y. Research on the Progress of Blockchain Technology Application in Supply Chain Finance[J]. Financial Engineering and Risk Management, 2023,6(10)