A Study of Financial Engineering Security Issues Based on Block Cryptography

Lin Zhang[1,2(✉)] and Hongmei Wen[1,2]

[1] School of Finance, Harbin University of Commerce, Party School of Boli County Party Committee, Heilongjiang 150010, China
13845097740@163.com

[2] School of Finance, Harbin University of Commerce, Heilongjiang 150010, China

Abstract. With the gradual maturity of big data and cloud computing technology, blockchain, as an innovative part in the evolution of information technology, has brought new opportunities for the development of various fields. Blockchain technology encryption algorithm can provide feasible solutions to the complex problems in financial transaction data. This study attempts to analyse the problems faced in financial transactions through blockchain technology, and attempts to build a process framework for financial data security management, thus forming a blockchain financial data security management system model, and exploring the elements of financial data security management in terms of multiple dimensions such as the subject, object and media field involved in the data model. As an innovative financial tool in the field of financial engineering, blockchain technology can play a positive role in the massive amount of transaction data, facilitating the formation of a secure and irreversible financial data system on the one hand, and minimising the risk of loss of control in financial institutions on the other. The application of block cryptography algorithms to financial engineering data security management systems is only a preliminary idea and does not incorporate the degree of openness of the data. The research will further incorporate the confidential management authority of financial institutions to provide a reference for the formation of blockchain financial data management.

Keywords: blockchain · financial institutions · data security

1 Introduction

With the advent of the fourth industrial revolution, China's economic and social environment has undergone radical changes, and information processing technologies such as the Internet and cloud computing have continuously penetrated into people's lives, gradually changing their production and life style, payment and transaction means, etc. In the process of the evolution of the digital economy, the data information generated by financial institutions is also undergoing severe tests. In the process of development and evolution of digital economy, the data and information generated by financial institutions are also experiencing severe tests, such as leakage of confidential information, frequent

N. Akhtar et al. (Eds.): PMIS 2023, AHIS 8, pp. 707–717, 2023.
https://doi.org/10.2991/978-94-6463-200-2_73

transactions of personal information in the market, and the appropriateness of safety supervision of financial data, which directly affects the stable development of financial market.

Blockchain technology, as an emerging information technology processing model in recent years, can develop a higher level of information traceability protection in response to possible malicious acts in a complex data environment. For example, in recent years, there have been many incidents of courier information leakage, big data pushing malicious pop-ups, telecommunication fraud, etc., which can largely affect people's lives and even cause serious consequences. The use of block cryptography algorithms as a medium for financial data monitoring can control the spread of false information in the financial transaction market to a certain extent. Therefore, this study will build a basic theoretical framework based on the combination of blockchain technology and the financial market, from the supply, demand, regulation and data connection hub of financial data, and propose a financial data security management model under the conditions of block cryptography technology, so as to extend and optimise the blockchain technology in the field of financial technology security.

2 Review of Domestic and International Research

Blockchain technology was first proposed by Satoshi Nakamoto, and then scholars have researched and practiced it and applied it widely in many fields. The characteristics of blockchain technology, such as decentralization, immutability, security and trustworthiness, have greatly changed the understanding of the traditional process of centralized management mode, and provided a more secure solution to the problems of data silos and easy tampering of information. Blockchain technology is arguably the most secure information processing technology from the current point of view, with elements covering verifiable queries, smart contracts, hashing algorithms, asymmetric encryption, etc. It has significant advantages that are difficult to replace by other technologies in dealing with privacy leakage. In recent years, China's leadership group has actively released the signal of innovative application of blockchain technology. In 2017, Premier Li Keqiang mentioned blockchain technology for the first time in public, and in the same year, General Secretary Xi Jinping proposed to build a digital economy with data as the key element, and to use blockchain technology to explore the innovative mode of digital economy, and actively promote the wide application of blockchain technology in various fields, so as to provide the people with more secure and convenient quality services.

From the current research of experts and scholars at home and abroad on the application of blockchain technology in the financial field, it can be broadly divided into two aspects, on the one hand, mainly from the perspective of digital currency, as Satoshi Nakamoto proposed blockchain technology in the article "Bitcoin: A Peer-to-Peer Electronic Cash System", positioning it as a peer-to-peer electronic Porru S (2017) first discusses the revolutionary role of blockchain in finance, economy, and currency, and since bitcoin is the first application of blockchain technology, its superiority in performance is rapidly emerging along with the gradual expansion of the field of blockchain technology applications [4]. Cheng, Navy (2022) and other scholars argue about the risks of cryptographic digital currencies, assets and their governance methods, and explore the

theoretical and practical issues of China's Internet financial market access and regulatory legal system [1]. Scholars such as Lan Hong (2021) take third-party payments and private digital currencies, which have penetrated more deeply into people's lives, as research objects to analyze the impact of digital currencies on China's overall macroeconomic and monetary policies [2]. On the other hand, it is analyzed from the perspective of supply chain finance, and scholars such as Wang Haiquan (2022) propose that in solving the problem of enterprise financing, by building an encrypted blockchain supply chain finance system, it can compensate to a certain extent for the vulnerability problems such as data nodes being cracked and the difficulty of artificial suspension of capital loss [3]. Junyi Guo (2018), on the construction of supply chain information sharing platform, proposes that should start from the perspective of supply chain information sharing, and believes that the blockchain scenario application in the field of supply chain should be reconstructed [5].Ghazouani (2019) and other scholars form a cloud data security de-weighting scheme under the condition of blockchain and multi-agent system, that is, the data information uploaded to the cloud by users can be safely de-weighted through multi-agent system, and at the same time [6], based on blockchain technology to ensure that the file information is difficult to be tampered with, thus Wei (2020) and other scholars mainly design cloud applications by combining the advantages of cloud computing and blockchain to achieve the security and completeness of data in the cloud [7].

In fact, from the current point of view, the research on the application of blockchain technology to financial data security is still tentative, while the application of blockchain technology in the field of financial services still faces many difficulties. ①Due to the relatively mature development of the Internet economy, different trading platforms have accumulated a huge amount of user data. On the premise of ensuring the safety of user data, the research and exploration of data value cannot be maximised due to the different standards of data integration [11]. ②The scale of the platform is relatively lacking. At present, the financial service platform that integrates information and data has been operating in the financial market, but the scale of the data security system is relatively lacking, and there is also a lack of relevant technical support in the financial data security [12]. ③Single measures of supervision, as China's financial market has developed later than that of western countries, the CBRC's policies on financial supervision are also being gradually improved, and at present the main supervisory instruments are still macro-prudential and micro-prudential supervision, with intangible and tangible supervisory systems not yet formed. For example, at present, this kind of social regulation, mainly based on network public opinion, using digital technology in the field of financial engineering is relatively little practice [13]. Therefore, there is an urgent need to integrate the elements of data security management and establish a perfect model of financial data security management system using blockchain technology. With the advent of the fourth industrial revolution, whether China's financial market development can seize the opportunity of this technological revolution, at present, many innovative technologies have not been able to be used comfortably in the field of financial science and technology innovation, blockchain technology first came into contact with financial services from the insurance business, and in the tide of the information revolution, how can the value of data be developed safely and efficiently, for the development of financial modernization In the information revolution, how to exploit the value of data in a safe and efficient

manner is of profound significance to the development of financial modernization [14]. Based on the characteristics of blockchain technology in data processing and the important role of financial data to social organisations and individuals, this paper attempts to use blockchain technology to build a model of financial data security management system so as to improve the efficiency of financial services to the real economy and reduce credit costs.

3 Analysis of the Basic Framework of Blockchain Technology Applied to Financial Data Security Management System

3.1 General Idea

China's development of blockchain technology in various fields is still at the primary trial stage, and the development of digital information intelligence has a lot of room for development. Thus, it is urgent to deeply integrate and analyze the data information in the financial capital market and blockchain technology, and build a data security management model in the financial field. The elements of financial data security management should be fully understood in the early stage of establishing the model, which can be seen in detail in Fig. 1, and explored in multiple dimensions such as the subject, object and media field involved in data.

Considering that there are many subjects generating financial data, including financial institutions, non-governmental organizations, as well as government-related departments and the public, it is obvious that the traditional centralized technology processing method cannot meet the complex needs of multiple subjects. The use of blockchain technology can help solve the problem of complex groups of data sources in the financial market, and at the same time, it can bring into play the characteristic advantages of blockchain technology to highly control and trace the safety of data. Thus, firstly, we analyze the superiority of blockchain technology applied to financial data security management compared with traditional technology; secondly, we sort out the subjects,

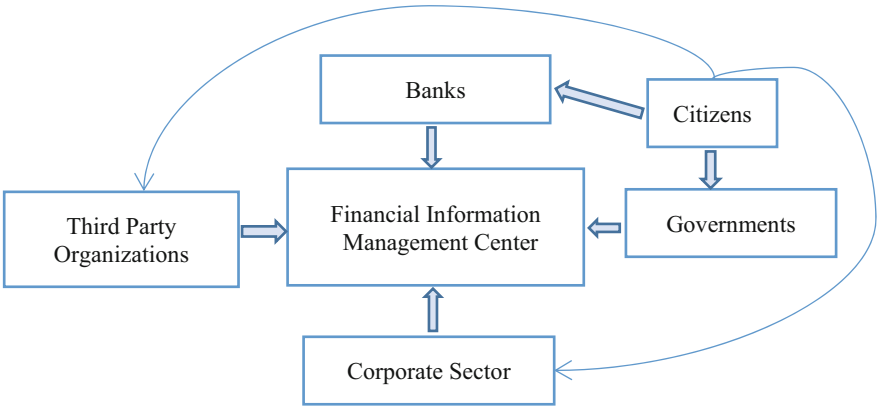

Fig. 1. Analysis of subjects related to financial data management

objects and media involved in generating financial data; finally, we explore the process of applying blockchain technology to financial data and integrate and analyze the whole framework.

3.2 Model Design of the Financial Engineering Security Management System

The initial purpose of building a data security management system in the financial sector is to solve the security problem of transaction information. In the process of building its basic framework by combining blockchain technology, the large, material, intelligent and cloudy data elements should be further considered, and the relationship between the subject and the object as well as the interests and demands that may arise in the scenario should be coordinated, and the basic framework of the management system should be integrated and designed. This paper will combine the basic model of blockchain technology and its corresponding characteristics to design a financial data security management model in layers, which can be seen in Fig. 2.

The security management model for the financial sector built using block technology simplifies the original block model structure by reducing the initial six-layer block model to a data collection layer, a business logic processing and a block data layer. The perceived first-hand data is processed through a hashing algorithm, identified and then processed through business logic for high performance, decentralisation and security, with the following formula, $P = \frac{\alpha}{S*D}$, making the three variables a specific constant and ultimately achieving the purpose of data.

3.3 The Operation Mechanism of Financial Data Security Management System

(1) Analysis of financial data security management model basic data generation subjects.

As an important asset and core competitive resource of the financial industry, the construction of financial data management model using blockchain technology is a project with a wide coverage, and its coverage includes the data storage of financial institutions, including banks, trusts, securities, insurance and other financial institutions. At the same time, in order to construct the effectiveness of the model should also include the citizens, enterprises and institutions and third-party institutions, in order to solve the relevant financial events, such as financial transactions, changes in equity, financial disputes, etc. In the process of handling financial events among multiple subjects, the decentralized data processing mode using blockchain technology can make the information sharing among subjects more convenient and effective compared with the traditional centralized data processing mode (Figs. 3 and 4).

In the process of data processing, the data collected in the early stage is relatively complicated due to the structured and semi-structured reasons, so the original data needs to be processed in a unified and standardized way, and the data of different subjects are cleaned, screened and unified with the help of data processing tools, so as to provide efficient data information for the later business processing. The primary link of data processing is the standardized conversion of different data, and another link that cannot be ignored is the encryption privacy protection in the process of data processing. In the process of data processing, blockchain data related technologies such as asymmetric encryption and timestamp are used to recreate the block hash value for the upstream

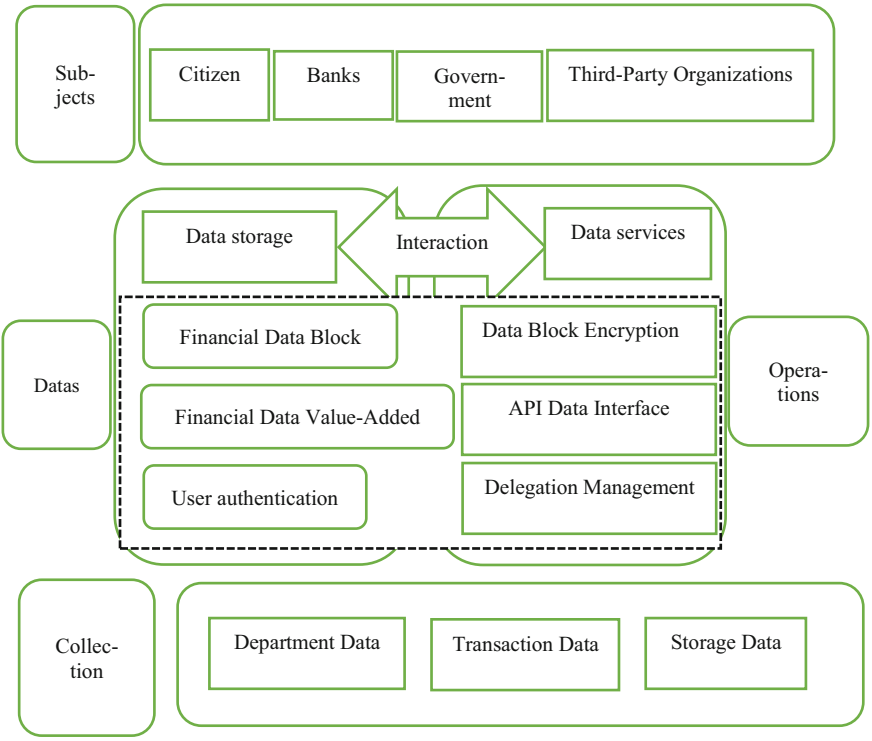

Fig. 2. General framework of financial data security management model

Fig. 3. With centered mode.

and downstream of data, and block storage processing for the privacy information of users, and at the same time, the sharing and reversibility of financial data generated in the process of transaction. The financial data sharing as well as reversible issues are analyzed to prevent the tampering of data, and the upstream of the generated data can be operated in a tamper-evident manner, so as to ensure the authenticity and trustworthiness of the data. The use of blockchain technology to integrate the huge amount of financial data can solve the phenomenon of data silos in financial institutions to a certain extent and also maximize the value of data.

(2) Financial data security management model block data algorithm analysis.

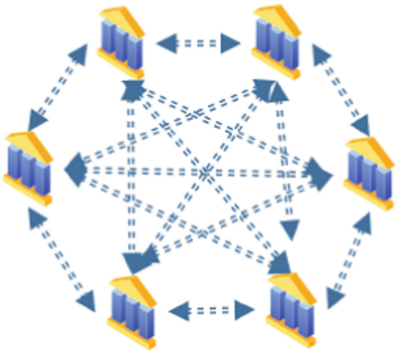

Fig. 4. Decentralized mode

Blockchain uses time as an important basis for the order of distribution, and is able to form a checkable bookkeeping list using time series. Each block is connected with a hash value, which is what we call a block transaction. Merkle tree is a relatively common and efficient data structure, through the hash value between the blocks to verify the specific hash value in the tree, Merkle tree any change in the transaction data will generate a different hash value. Taking arbitrary data x as an example, randomly selected parameters r, using the hash algorithm, the data can be key-generated HG, hash-generated CH, hash-verified HV and hash-collision HC [8–10].

$HG(1^n) = (hk, tk)$ This algorithm is a key generation algorithm, hk representing the hash public key, rk representing the hash private key, then n indicates the security factor.

$CH(hk, x; r) = (h, \xi)$ This algorithm is hash generation algorithm, by hashing the public key hk, any given data x and random values r, resulting in hash values h and random numbers ξ.

$HV(hk, x, (h, \xi))$ This algorithm is hash verification algorithm, through the hash public key hk, any given data x, hash value h and random number ξ, to verify (h, ξ), if the correct hash value, the result output 1, otherwise 0.

$HC(tk, (h, x, \xi), x\prime)$ This algorithm is a hash collision algorithm, with trapdoor rk, triplet (h, x, ξ) and data x' to calculate and derive a new random number $\xi\prime$ to derive $HV = (hk, x, (h, \xi)) = HV(hk, x\prime, (h, \xi\prime)) = 1$.

Addressing the authentication of users and the private data generated by their use, the user's data is processed through the encryption of hashes in the block structure. This feature can thus be fully utilised to input the user's private information, and as long as most of the nodes are authentic, changes by means of malicious blocking, for example, will be rejected, thus ensuring the security of the data. Secondly, in addressing the data generated by the large number of transaction agreements in the financial market, smart contracts in blockchain technology can be used, a special code protocol that allows for one-way secure and traceable transactions without the involvement of a third party. After a financial uplink subject sends a transaction request, it borrows the smart contract code from the Ethernet application, and developers on the trading platform use the smart contract in the blockchain network to send data fields and transmission addresses to

other contracting parties, resulting in a special transaction protocol with relatively low risk and high accuracy.

(3) Financial data security management model business logic implementation.

The system framework through block data processing mainly contains three levels, firstly, three levels of perceptual data collection, block data integration and business logic processing, among which business logic processing belongs to the intermediate level, which includes both logical examination of perceptual data and also gives medium-term verification for later data integration and storage. The business logic processing is mainly realized through smart contracts, and the data privacy is processed with privacy computing service and federal learning technology to make the data available invisible, forming a deep integration of blockchain and computer technology, storing data, traceability data and shared data in financial data for staging and integration, forming a user-visible Internet and App platform, so as to provide conditions for value-added services of financial data It also provides space for the efficient operation of data between blocks.

4 Blockchain Technology-Based Financial Data Security Management Model - Exploration of Housing Property Transactions

4.1 Application of Blockchain Financial Data Management System in Housing Property Rights Transaction

Taking housing property rights transaction as an example to discuss the applicability of the data model, housing property rights transaction is accompanied by the overheating in the previous years, and the means of national macro-control, including the second set of property tax for purchasing houses and the policy of household registration restriction and so on, have curbed the rise of housing price to a certain extent. And along with the aggravation of China's aging degree of newborn rate is low and so on, many experts and scholars put forward to housing pension, delayed retirement and other policy views. Throughout China, the housing prices in the cities preferred by the retired elderly are relatively high, so many elderly people become "migratory birds" after retirement, which has inspired some scholars to put forward the idea of retirement with housing. Whether it is the mortgage of property rights or the replacement of property rights, these data have a certain degree of security risks in the trading platform. Blockchain technology can provide financial data completeness, authenticity and tamper-evident guarantee for the process of home ownership transaction (Fig. 5).

4.2 Realization of Value of Blockchain Financial Data Management System in Housing Property Rights Transaction

(1) Break the business barriers and realize data linkage. Starting from the real estate transaction market in the financial market, with government notary departments, bank lending institutions, individual citizens and third-party credit assessment organizations, etc., more network nodes are involved, while each party has different supply and demand.

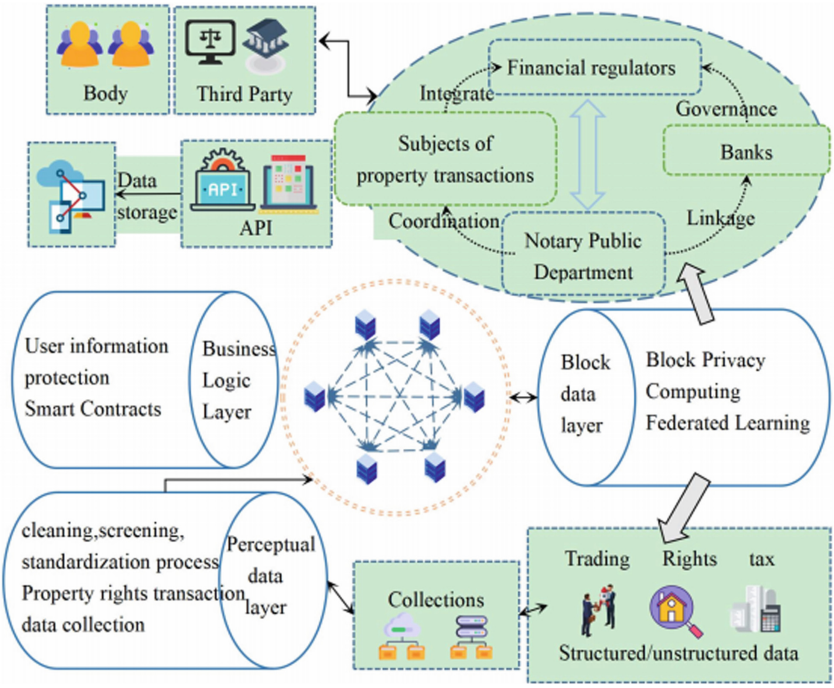

Fig. 5. Analysis of the application of financial data management model in housing property transactions with blockchain technology

The decentralized and peer-to-peer network structure built by using blockchain technology breaks the original data communication structure, enhances the will of each participating subject, realizes the linkage effect of information and data among various business sectors, and solves the problems of inefficient information transmission and information asymmetry in the troubled market.

(2) Mining data value, multi-party collaborative governance.

The use of open API interface to realize the decentralized sharing of data in the financial transaction market can add value to the shared value of data, and comprehensive analysis, mining and tracking of data, so as to realize value-added services of data. With the safeguards of smart contracts, the results of data mining can be protected. On the one hand, the value of data can be maximized, and on the other hand, several data subjects of the open API port can get the maximum benefit and make full use of the value of data.

(3) Improve the credit system and guarantee data security.

The establishment of a perfect credit system is mainly realized through the technology of smart contract and time stamp in blockchain, and the data is encrypted and preserved. It is very important to form a perfect credit system to facilitate both parties of the transaction to authenticate the user information through the digital certificate created by blockchain, and also to ensure the authenticity and trustworthiness of the data to the greatest extent.

5 Conclusion

From the current development of data technology and its combination with various fields, blockchain technology has been widely used in many fields, bringing new opportunities for the development of many industries with its unique decentralized and non-tamperable characteristics. The financial market generates complicated data, and the promotion of the use of block cryptography algorithms can protect customer privacy rights to a certain extent. The innovative development and practical application of technology is more to be able to meet people's needs and improve the quality of life. Thus, this paper combines the algorithm of block encryption with financial data to pursue maximum data security by applying the data leakage problem faced by people in real life. Thus, this study attempts to build a financial data security management model by analyzing data generating subjects to analyze data sources, sensing and collecting business data, and processing related data with hash encryption algorithms. And combined with the housing property transaction as the analysis, the overall process is drawn from data generation, perception, acquisition and encryption processing, in order to provide reference for other financial transactions.

References

1. Cheng Xuejun, Li Xinhe. On the legal risk and governance path of cryptographic digital currencies: a perspective from bitcoin [J/OL]. E-Government:1–15[2022–09–29].
2. Lan Hong, Yang Wen, Wei Dongyun. The impact of legal digital currency on China's structural monetary policy [J]. Southwest Finance,2021(11):89-100.
3. Wang Haiquan, Yang Yang, Yi Qingling. Research on the application of blockchain technology in supply chain finance--based on chain code implementation and privacy protection [J]. Financial Development Research,2022(03):77-82.
4. Porru S, Pinna A, Marchesi M, et al. Blockchain-oriented Software Engineering: Challenges and New Directions[J].2017, 57(4):124–138.
5. Guo J, Lu Z. A Supply Chain Information System of the Supply-Hub Based on Blockchain [J]. Proceedings of the 2018 2nd International Conference on Economic Development and Education Management, 2018.
6. Ghazouani M E, Kiram M a E, Errajy L. Blockchain & Multi-Agent System: a New Promising Approach for Cloud Data Integrity Auditing with Deduplication [J]. International Journal of Computer Network and Information Security, 2019, 11 (1): 175–184.
7. Wei P C, Wang D, Zhao Y, et al. Blockchain Data-Based Cloud Data Integrity Protection Mechanism [J].Future Generation Computer Systems,2020, 102: 902–911.
8. Garay J, Kiayias A, Leonardos N. The Bitcoin backbone protocol: analysis and applications. In: Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Sofia, Bulgaria: Springer, 2015. 281–310.
9. Ateniese G, Magri B, Venturi D, Andrade E. Redactable blockchain-or--rewriting history in Bitcoin and friends. In: Proceedings of the 2017 IEEE European Symposium on Security and Privacy. Paris, France: IEEE, 2017. 111−126.
10. Qin R, Yuan Y, Wang F Y. A novel hybrid share reporting strategy for blockchain miners in PPLNS pools. Decision Support Systems, 2019, (118): 91−101.
11. Jiao Yuanyuan, Yan Xin, Du Jun et al. Research on the evolutionary game of three parties in factoring financing from the perspective of blockchain empowerment [J/OL]. Journal of Management:1–12[2023–03–06].

12. Liu Yi, Dong Min. Path optimization of insurance fraud regulation under blockchain empowerment[J]. Jianghuai Forum, 2022, No.314(04):69–74+182.
13. Lin YM, Zhang ZS, Duan ZK. Trustworthy data flow: a study on the path of blockchain-enabled financial product innovation[J]. Credit, 2022,40(12):25-33.
14. Wu Jinghui. Research on the co-regulation rules of credit risk of bills - a perspective of blockchain application[J]. Legal Business Research, 2023,40(01):104-116.