Eng Int Syst (2024) 5: 435–443

Engineering
Intelligent Systems

Blockchain Data Privacy Protection Mechanism for Enterprise Finance and Data Mining Algorithms

Xuejun Ma[1,a] **and Yongshan Zhang**[2,b,*]

[1] *School of Economics and Management, Weifang University, Weifang 261061, Shandong, China*
[2] *School of Economics and Management, Weifang University of Science and Technology, Shouguang 262700, Shandong, China*

The establishment of a data privacy protection scheme that integrates information and public query is of great benefit to promoting the development of the financial aspects of a supply chain. Based on data encryption technology, this study adopted appropriate encryption methods for transaction information without changing the original consensus algorithm and verification mechanism of the blockchain, thus ensuring that attackers could not obtain transaction information in clear text form. This paper constructed a blockchain model for the financial data of enterprises, and achieved data sharing and visualization of enterprise asset management, asset securitization, and cross-border trade, thus ensuring that financial data was protected in a timely manner. Data mining algorithms were used to select the optimal financial data privacy protection scheme from multiple potential suppliers of financial data. This study established 60 accounts for retailers, and the Bitcoin model established a total of 25 accounts for sales parties. This model is able establish new accounts for active retailers and block adjacent retailers, thereby better protecting the privacy of the financial data of retailers.

Keywords: Corporate finance, data mining algorithms, blockchain data, privacy protection

1. INTRODUCTION

Data storage on a blockchain needs to be done through consensus mechanisms. That is to say, only nodes with permissions on the blockchain are allowed to store data on the chain and synchronize updates to other blockchain nodes after verification. This mechanism ensures mutual trust among multiple parties, and data must undergo consensus verification at multiple nodes in order to be effectively recorded. However, it is difficult to effectively verify the transaction background of small and medium-sized enterprises in blockchain financing.

Blockchain is based on a digital technology that can solve the problems in supply chain finance. Previous research on blockchain has examined only its advantages through theoretical stacking, or analyzed its application modes and potential risks. There are few related case studies. Moreover, blockchain technology has many technical characteristics that are unlike those of other technologies. However, the traditional model of supply chain finance still has many problems, and blockchain technology can be utilized to solve these problems. To a certain extent, early warning and effective control can be provided in regard to the numerous risks associated with the operation of supply chain finance.

To address the above issues, this study developed a blockchain-based data exchange optimization mechanism to address security and privacy protection issues during the data exchange process. As people began to attach greater importance to Bitcoin, blockchain, as its underlying technology, gradually became the focus of industry and academia. Blockchain is a relatively new data encryption

*[a] Email: wfmxj@163.com, [b] Email: zhangyongshan2023@163.com

technology based on distributed consistency, which can provide data integrity, security, and correctness. In addition, the data structure of blockchain makes it more stable and traceable, which can effectively address the problems of single node failures and data tampering.

2. RELATED WORK

In the financial field, blockchain technology has the advantages of offering traceable transactions, immutability, and simplified business processes. By utilizing blockchain technology, the underlying architecture of the financial industry can be reconstructed. Storm believed that blockchain did not comply with European Union privacy laws. However, this did not mean that blockchain would be applicable to all usage and deployment scenarios [1–2]. Chen believed that the previous schemes had single point of failure and lacked privacy protection and access Sharma defined blockchain technology as a decentralized ledger that was secure, distributed, and privacy protected. In blockchain, transactions are flexible, secure, verifiable, and permanent [3]. Kang et al. believed that blockchain technology ensured the transparency and objectivity of cryptocurrencies [4]. An proposed a decentralized privacy protection model based on blockchain double validation and consensus [5]. However, their research did not take into account the privacy protection methods of blockchain technology.

The application scenarios of blockchain technology in the financial industry mainly include asset management, securities, clearing and settlement, payment, and so on. Luo proposed a trust-based location privacy protection scheme and a data structure that enabled blockchain to record the credibility of vehicles on publicly available blocks in a timely manner [6]. Fan proposed a blockchain based solution to address privacy issues in mobile networks. In addition, the openness and tamper resistance of blockchain ledgers ensured provider access control and privacy [7]. Nie proposed a controllable data transmission mechanism based on federated blockchain to meet the needs of IoT scenarios [8]. Wu believed that the blockchain achieved decentralization, and reduced the communication cost between the cloud and the edge. It addressed the problem of data forgery, and also provided an incentive mechanism to alleviate the problem of data islands in edge computing [9–10]. Onik et al. saw blockchain technology as an "immutable" distributed ledger that could be used to establish a transparent data audit platform [11]. However, their research did not take into account the cost of using blockchain.

3. EXPLORATION METHODS FOR BLOCKCHAIN DATA PRIVACY PROTECTION

3.1 Mechanism of Blockchain Technology to Solve Enterprise Financial Problems

Blockchain can generally be divided into two categories: public chain, and alliance chain [12–13]. In a public blockchain, all nodes can access the link and enjoy the same usage rights; in the alliance chain, all node members need to obtain approval from specific departments and corresponding authorizations, and their usage rights vary due to the different entities. This is because the participants in supply chain finance can be roughly divided into three categories: core enterprises, financial institutions, and small and medium-sized enterprises. The work content and operational requirements of the three participating entities in the supply chain business execution process are different, and the required usage permissions are also different. Typically, the alliance blockchain is more suitable for supply chain finance [14]. By utilizing the distributed ledger principles of blockchain, key technology, consensus mechanisms, smart contracts, and other technologies, the problems faced by supply chain finance can be effectively solved.

(1) Distributed ledgers reduce information asymmetry

The blockchain finance business involves many enterprises on the industrial supply chain, with various transaction information, logistics information, and fund flow information dispersed among their own financial data trading systems. This dispersion of information increases the difficulty and cost of verifying information, thus making it easy to encounter problems such as information monopoly and fraud. This restricts the support and participation of financial institutions in supply chain finance [15]. Blockchain is a distributed storage method that is different from centralized data storage mode. For example, Tencent saves all WeChat user data in its own database, and each WeChat user can see only their own chat records, thus making it difficult to tamper with. Only by modifying both the user and the central database can data be tampered with. Blockchain, on the other hand, is a decentralized storage mode where new data is saved to other data simultaneously. In the supply chain finance business, the participants include core enterprises, financial institutions and small and medium-sized enterprises in the upstream and downstream of the supply chain [16–17]. They upload trade order information, accounts receivable information, invoices and other information to the blockchain to enable other entities to view information, thus breaking the information silo phenomenon and reducing information asymmetry.

(2) Cryptographic mechanisms ensure data privacy

In supply chain finance, most of the data uploaded by enterprises are associated with trade secrets. If all users can access it easily it would lead to the leakage of commercial data, which would have a negative impact on the operation of the enterprise. Blockchain adopts asymmetric encryption to ensure privacy security. Asymmetric encryption algorithms have a public key and a private key, and each password pair comprises both keys. Usually, the private key is kept by the company itself, while the public key is open to all companies on the blockchain node. If the company's information needs to be decrypted and queried, the company's private key is required. This cryptographic mechanism strengthens the privacy of company data, while the encryption mechanism enhances the functionality of blockchain, thus achieving both information sharing and confidentiality.

(3) Consensus mechanism ensures the authenticity of information

Generally speaking, in ERP (Enterprise Resource Planning) systems, only transactions with the first supplier are recorded, while the second supplier does not engage in direct transactions with the third supplier. Therefore, it is very difficult to verify the information provided in an ERP system. Hence, some companies privately use methods such as whitewashing data and fabricating transaction orders to defraud financial institutions of funds. However, due to risks, financial institutions may not provide credit to multi-level suppliers. The consensus mechanism of blockchain restricts this, and the information submitted by small and medium-sized enterprises must be verified by affiliated enterprises, accounting firms, or other relevant nodes in order to successfully save it on the chain, thus ensuring the authenticity of trade information. At the same time, it can also strengthen the trust between core enterprises, small and medium-sized enterprises, and financial institutions, and reduce transaction costs between participating entities so as to improve collaboration efficiency.

(4) Smart contracts improve operational efficiency

Smart contracts are generally established for automated transactions between blockchain members. They are based on the principle of mutual recognition among participating entities, and the triggering conditions and execution process are written into code. When the triggering conditions are met, the smart contract automatically performs pre-set operations, thereby automating the execution process. The smart contract mechanism enables blockchain nodes to follow the principle of fair notarization during the transaction process, and it does not involve manual operations, thereby improving operational efficiency. In supply chain finance businesses, when certain conditions are met, smart contracts can be used to perform operations such as automatically connecting to the China Securities Depository Platform to query the disposal status of assets, updating the status of assets to this Platform, automatically transferring the repayment of core enterprises to various accounts receivable, sending goods transportation instructions, and so on. Automated operations can effectively prevent issues such as tampering and intentionally delayed payments caused by manual operations.

3.2 Enterprise Financial Data Blockchain Model

In third-party fintech companies, blockchain technology is applied in supply chain finance. The process is based on blockchain technology and is combined with artificial intelligence, data mining algorithms, and other technologies to construct a comprehensive enterprise financial data blockchain model of "data mining+blockchain finance". It provides convenient and fast supply chain finance solutions for core enterprises, financial institutions, and small and medium-sized enterprises, and has rich experience in implementing supply chain finance solutions.

The enterprise financial data blockchain model is divided into three layers, described below.

The first layer is the blockchain application layer. The smart application platform is used to achieve network visualization configuration and quickly construct blockchain distributed applications, so as to build an enterprise level supply chain finance application market and ecosystem. Specific application scenarios include asset management, asset securitization, cross-border trade, data sharing, etc.

The second layer is the blockchain platform layer. Based on real business scenarios and the visualization and convenience requirements for the underlying infrastructure, the service-oriented and componentized capabilities of blockchain have been implemented, thus providing better platform support for upper-level applications. This layer is based on the actual application scenario requirements of the first layer and has developed multiple functional platforms using blockchain technology. Its main function is to provide a good platform support for the first layer of applications, while also visualizing the underlying blockchain infrastructure. The main research content includes platform technologies such as blockchain trust service gateway, blockchain privacy computing platform, and blockchain key assistant.

The third layer is the blockchain infrastructure layer. This layer is the core part of building the entire blockchain technology product. It is mainly combined with technologies such as blockchain and cloud computing to quickly build blockchain networks and support services, and build a native, scalable, and easy-to-maintain underlying blockchain infrastructure. The blockchain model of enterprise financial data is shown in Figure 1.

The enterprise financial data blockchain model integrates various financial technologies such as privacy computing, artificial intelligence, data mining, and cloud computing. Based on this, this study conducted in-depth research on this model. Cloud computing technology can provide a full range of services for each important link of supply chain asset management, including supplier registration, asset digital verification, supply chain management, electronic contract signing, etc., and can also automatically register asset transfers handled by banks on their WeChat official account. In general, companies that want to use the reputation of their core enterprises to solve financial problems choose to register on this platform, and upload their information to this platform so as to record all company transactions on this platform.

Financial data providers have the optimal benefit value of z_x:

$$z_x = \frac{\partial u}{\partial y} - p - \frac{c}{x}(ay - b) \tag{1}$$

To solve the optimal trading strategy of financial data provider c, it is assumed that the benefit function x_y is as follows:

$$x_y = p + c(by + b) \tag{2}$$

The optimal strategy x_i of financial data provider c is calculated as follows:

$$x_i = \frac{px}{2ax} - \frac{b}{x} \tag{3}$$

The selected data provider must meet the following privacy preference requirements:

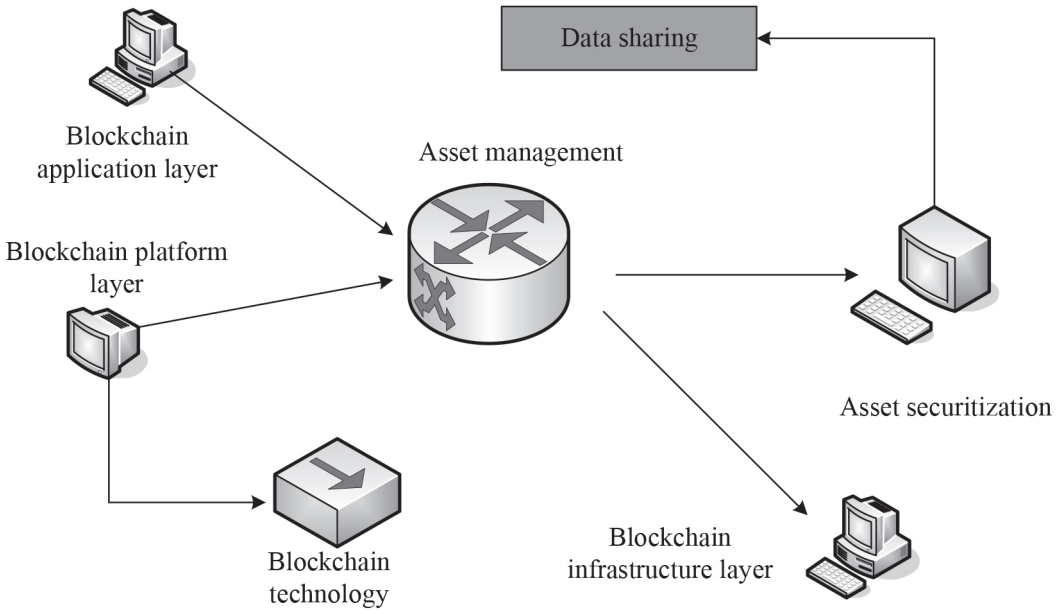

Figure 1 Enterprise financial data blockchain model.

$$p_i = \theta - \frac{pz}{mc} \tag{4}$$

For data trading, data buyers can retrieve the description information of financial data p_i through smart contracts, such as the size of financial data volume and collection time. The transaction volume of financial sellers is a computable value. v_i is used to represent the sum of the seller's first i financial transactions. The formula is as follows:

$$v_i = \sum v - v_j \tag{5}$$

The traceability enabled by blockchain technology can effectively strengthen regulation, which plays a very important role in the future development of information technology and improves the service efficiency of the financial industry, thereby promoting the latter's high-quality development. The optimal order quantity z_d under blockchain technology is as follows:

$$z_d = \sum (b - a) - \frac{a}{2} \tag{6}$$

In the blockchain environment, all transaction data needs to be fully open to distributed nodes to ensure consistency of block data on peer-to-peer networks. Clear text trading is the use of specific network analysis techniques by attackers to discover transaction rules and infer information such as the user's identity and geographical location.

In regard to financial payments, attackers analyze transaction data and behavior trajectories of different accounts to predict various macro trends, thereby threatening user privacy and information security of countries and businesses. To make a mature blockchain application recognized by the public, it must be effectively processed.

There are significant differences in consistency and networking technology between blockchain technology and traditional computer network structures. The existing security protection methods in traditional computer network structures are not suitable for blockchain-based network structures. In traditional computing architectures, privacy protection mainly involves the adoption of multiple protection measures to ensure that data from the central server is not leaked. For example, managers can use conventional measures such as configuring intrusion detection devices and installing specialized data-leakage prevention software to enhance the security of the central node.

Each distributed node in a block has a different ability to resist attacks, so nodes with poor defense capabilities are easily attacked. Therefore, hiding transaction data by technical means to prevent attackers from obtaining plaintext transaction data is an important direction for blockchain privacy protection. To achieve this goal, targeted privacy protection strategies must be adopted based on the specific needs and characteristics of the application.

4. EXPLORATION RESULTS OF BLOCKCHAIN FINANCIAL DATA PRIVACY PROTECTION

Solving the financing problem of small and medium-sized enterprises is an important goal for companies and financial institutions involved in supplying financial services to the supply chain. Regarding the current development status of various supply chain financial products and service platforms, small and medium-sized enterprises are undoubtedly the groups that benefit the most, and the enterprise financial data blockchain model examined in this study is representative of such platforms. The assets that financial institutions come into contact with are all recorded and documented on the blockchain, which ensures the authenticity of the transaction background of the assets and the credibility of the data, thereby reducing the credit risk to financial institutions; financial institutions can utilize the big data and privacy computing technologies provided by the platform to repeatedly evaluate and analyze assets, thereby reducing fraud risks and improving financial institutions' returns.

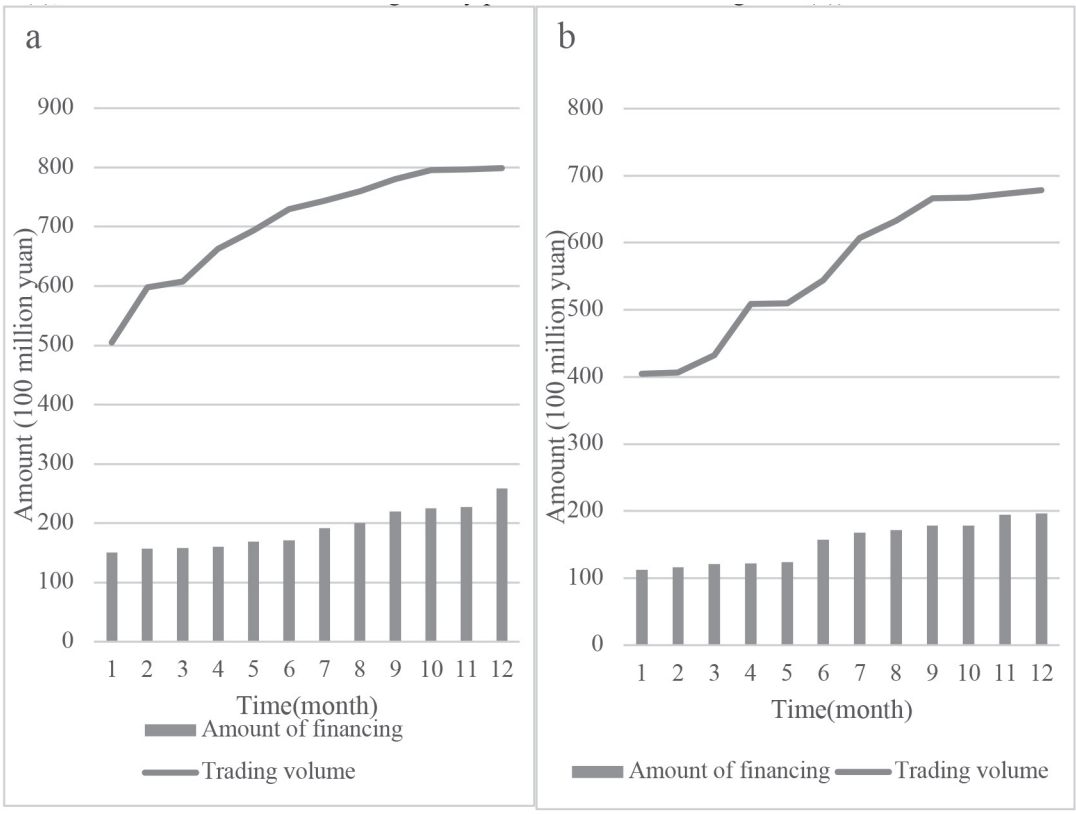

Figure 2a: Financial data blockchain model Figure 2b: Traditional financial supervision platform

Figure 2 Comparison of transaction volume and financing amount between enterprise financial data blockchain model and traditional financial regulatory platforms.

Specifically, the enterprise financial data blockchain model utilizes blockchain technology to digitize the rights and interests of accounts receivable, and achieves financing for supply chain end enterprises by splitting and circulating electronic detail lists. Electronic detail sheets can be freely transmitted on the platform, which is very convenient. Therefore, suppliers at or below the second level in the supply chain can also obtain credit splitting for core enterprises. This is not only conducive to helping small and micro enterprises at the end of the supply chain to achieve their financing goals smoothly, but also helps to reduce the financing costs incurred by many small and micro enterprises. The enterprise financial data blockchain model in this proposal completed a transaction volume of 79.9 billion yuan and a financing amount of 25.9 billion yuan in December, which reduced the financing difficulties of a large number of small and medium-sized enterprises in the supply chain. The comparison of transaction volume and financing amount between the enterprise financial data blockchain model and traditional financial regulatory platforms is shown in Figure 2 (The enterprise financial data blockchain model is shown in Figure 2 (a), and the traditional financial regulatory platform is shown in Figure 2 (b)).

The characteristics of the blockchain model for enterprise financial data are light assets and high returns. Firstly, P Bank provides supply chain financial services, and the fees it charges are one of its main sources of income. Secondly, the model enables P Bank to expand the business scope and customer base of small and medium-sized enterprises. P Bank can obtain more financing information for small and medium-sized enterprises from this platform and use these enterprises as its new customer acquisition channels. At the same time, P Bank makes use of blockchain technology, further strengthening, the company's credit structure and effectively controlling the quality of its assets.

In the past few years, the asset quality and solvency of Bank P has significantly improved. From 2018 to 2021, P Bank's non-performing loan ratio decreased from 2.1% in 2018 to 1.2% in 2021, showing an overall downward trend. In 2019, the loan provision coverage rate of banks reached 172%. During the same three-year period, there was also a significant increase in the reserve ratio for overdue loans of 90 days or more. The comparison of non-performing loan ratio, provision coverage ratio, and provision coverage ratio for loans over 90 days overdue is shown in Figure 3 (Non-performing loan ratio is shown in Figure 3 (a), and provision coverage ratio and provision coverage ratio for loans over 90 days overdue are shown in Figure 3 (b)).

Blockchain, is a disruptive technology contributing to a technological and industrial revolution in the future. Currently, the widespread application of blockchain in supply chain traceability and management, energy trading, financial asset management, intellectual property certification, and other aspects inevitably brings new technological and industrial developments.

Different enterprises provide different supply chain financial services based on their own business models and resource strength. Basically, as the risk posed to the platform increases,

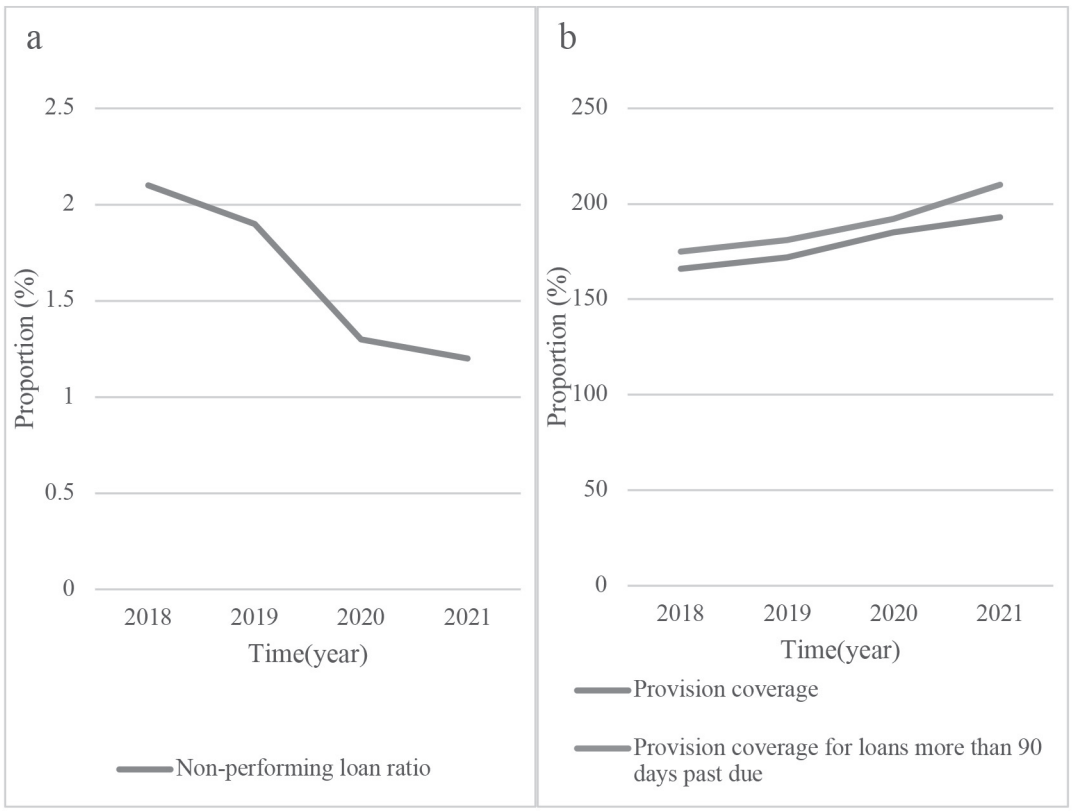

Figure 3 Comparison of non-performing loan ratio, provision coverage ratio, and provision coverage ratio for loans overdue for more than 90 days Figure 3a: Non performing loan ratio Figure 3b: Provision coverage and provision coverage for loans over 90 days overdue.

Table 1 Loan financial services for different enterprises.

Enterprise	Loan interest rate (%)	Term of loan (month)
1	5.5	6
2	6.1	12
3	10.5	8
4	11.3	9

the borrowing costs increase. Among them, the financing channels of the supply chain financing platform are mainly bank credit or self-owned funds; the product model also involves accounts receivable, prepayments, and goods. Credit loans incur high costs, and most of the repayments come from the platform's own funds. For Company 4, the loan interest rate was 11.3% and the loan period was 9 months. The loan financial services of different enterprises are shown in Table 1.

The credit financing solution for small and medium-sized enterprises mainly utilizes technologies such as blockchain and data mining to improve the digital risk management capabilities of financial institutions such as commercial banks, factoring companies, and small loan companies, so as to provide more effective financing for small and medium-sized enterprises. The enterprise financial data blockchain model also provides credit financing for small and medium-sized enterprises through its own funds. Its purpose is to accumulate relevant financing data and optimize risk assessment models. The blockchain model of enterprise financial data adheres to the essence of financial technology service companies. With the increasing number of financial institutions on the credit technology solution platform for small and medium-sized enterprises, the financing scale of their own funds is increasing year by year.

The development and increasing use of blockchain technology has had a profound impact on global commerce, organizations, economy, and society. A blockchain has an extensible chain structure, and each transaction data is encrypted into blocks in chronological order. It creates a brand new commercial environment in which all forms of transactions are embedded in digital codes and protected from arbitrary deletion or tampering.

In this study, data mining technology is used to select the most likely financial data privacy protection scheme from multiple possible suppliers of financial data. If financial information is purchased at a higher cost, the purchaser would obtain greater benefits. When the pricing strategy of data buyers is higher, the financial data that providers are willing to sell would also be more, so the value that data buyers can obtain from the data would also be higher. When data suppliers have different privacy rights, data purchasers have an optimal purchase price (that is, the optimal transaction

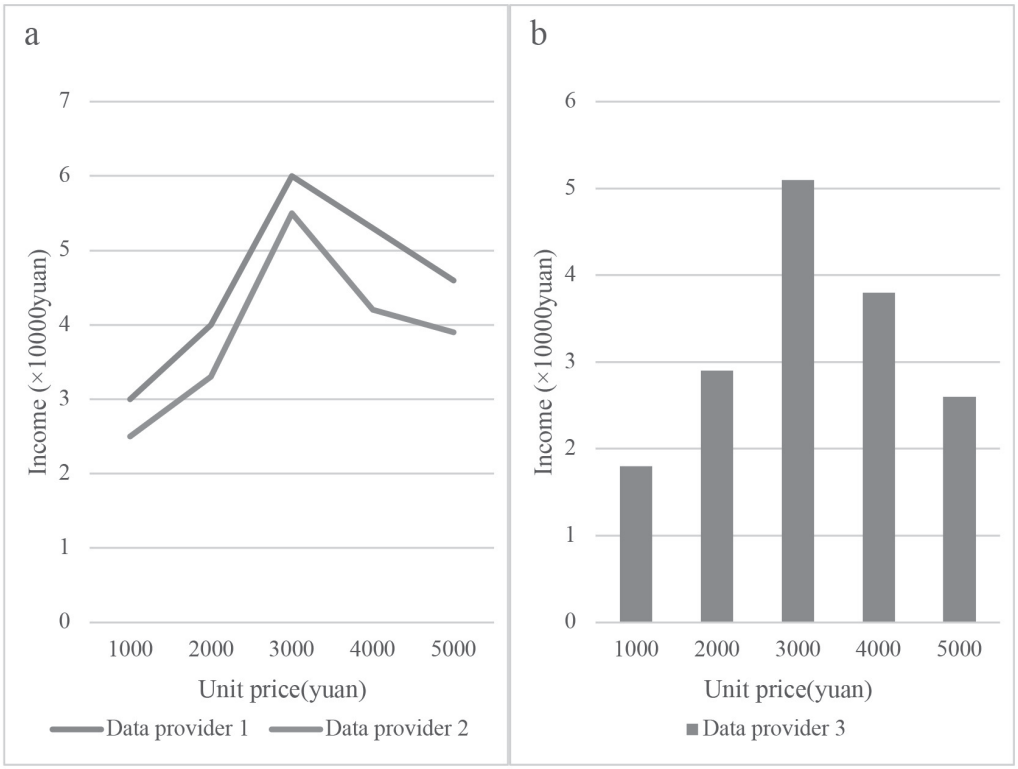

Figure 4a: Data Provider 1 and Data Provider 2 Figure 4b: Data Provider 3

Figure 4 Data benefits of data providers with different privacy preferences.

strategy). Under the same pricing conditions, the amount of data sold by data providers who are less concerned with privacy protection would be greater, and their revenue value would be higher. Data Provider 1 earned a profit of 30000 yuan at a unit price of 1000 yuan. The data benefits of data providers with different privacy preferences are shown in Figure 4 (Data Provider 1 and Data Provider 2 are shown in Figure 4 (a), and Data Provider 3 is shown in Figure 4 (b)).

In order to package supply chain assets into qualified asset securitization products, this model used advanced artificial intelligence technology and big data analysis technology to assist financial institutions in automatically verifying supply chain assets and related transaction documents. At the same time, it can also disclose regulatory information related to assets. For example, the seller's and buyer's concentration ratio, related transaction volume, legal disputes and other information are sorted out and a visual analysis report is created. After reviewing these assets, they would be packaged as asset securitization products available for investors to purchase.

Compared to the Bitcoin model, the method proposed in this paper requires a shorter transaction confirmation time for financial transactions. All transactions are carried out by local aggregators, so effective consensus can be obtained in a relatively short period of time. Also, the time required for energy nodes to exchange energy is relatively short, and the number of energy exchanges that energy nodes can complete is significantly higher than that of Bitcoin. Finally, the effectiveness and practicality of the proposed method were verified through numerical analysis.

This study established 60 accounts for sales enterprises, including 50 new accounts and 10 virtual accounts. The Bitcoin model established a total of 25 accounts for sellers, including 20 new accounts and 5 virtual accounts. This model was able to not only establish new accounts for active sellers; it also blocked adjacent sellers, thus better protecting the privacy of sellers. In addition, this study proposed the establishment of a virtual account for inactive sellers, which is an account with a sales volume of 0. The proposed method can effectively conceal the energy allocation of sellers and improve the personal privacy of users. The verification time and the ability to create an account are shown in Figure 5, The verification time is shown in Figure 5 (a), and the ability to create an account is shown in Figure 5 (b).

5. CONCLUSIONS

This study took the security application of big data as the background and used blockchain technology to examine the issues of transaction fairness and privacy protection associated with the open sharing of financial data. It focused on solving the difficulties and bottlenecks in privacy protection, data sharing, and transaction fairness in blockchain, and conducted in-depth research based on current international and Chinese theories and latest research results on data open sharing and privacy protection. The main focuses of this study were: the establishment of a traceable and verifiable blockchain protocol; the establishment of a big data exchange and sharing mechanism based on blockchain; and privacy protection and fair trading mechanisms in data mining based on smart contracts. Using blockchain as the foundation and combining cutting-edge technologies such as big data and artificial intelligence, the proposed enterprise

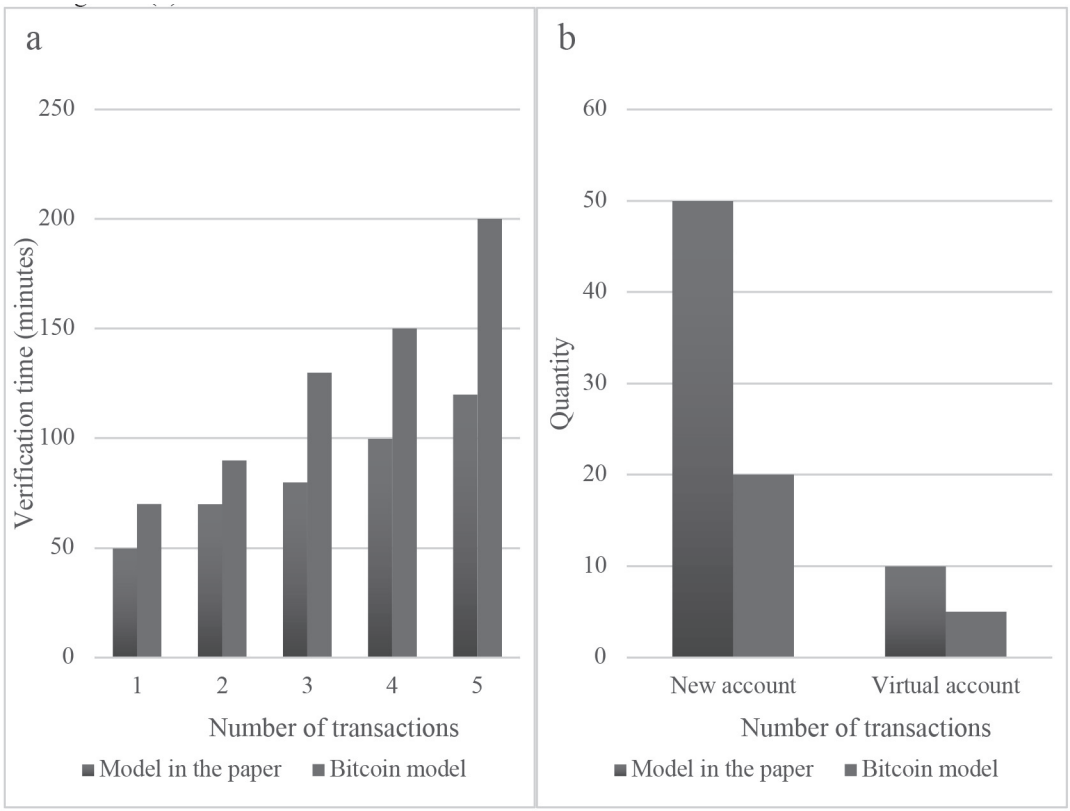

Figure 5a: Verification time

Figure 5b: Ability to create accounts

Figure 5 Verification time and ability to create accounts.

financial data blockchain model offer a solution based on supply chain finance technology, which could optimize supply chain assets and facilitate credit flow for core enterprises, thus alleviating financing difficulties for small and medium-sized enterprises. The "privacy computing" technology of the proposed model facilitates information sharing on the supply chain, and the "automation" technology improves the efficiency of enterprise operations. At the same time, the proposed model also had important application value in solving the financing difficulties of small and medium-sized enterprises, enhancing the competitiveness of core enterprises, and improving the returns of financial institutions. In future practical applications, it is hoped that this model can achieve good results and be adopted by an increasing number of core enterprises and financial institutions.

FUNDING

Study on social adaptability and life satisfaction of Chinese employees in the Philippines (2024BS51, 2024.01-2026.12), Research on high-quality development of financial development serving real economy in Shandong Province (2023-XWKZ-043)

REFERENCES

1. Storm, M., and L. Moerel. "Blockchain can both enhance and undermine compliance but is not inherently at odds with EU privacy laws." Journal of Investment Compliance, 22.2(2021):122–132.
2. Rai, H.M., Atik-Ur-Rehman, Pal, A. et al. Use of Internet of Things in the context of execution of smart city applications: a review. Discov Internet Things 3, 8 (2023).
3. Sharma, Eask. "A Framework of Big Data as Service Platform for Access Control & Privacy Protection Using Blockchain Network." Turkish Journal of Computer and Mathematics Education (TURCOMAT), 12.11(2021):476–485.
4. Kang, J. M., B. Kim, and S. J. Kim. "A study on privacy protection method applying blockchain technology for big data utilization (focus on the blockchain technology for monero, dash and Z-cash to ensure anonymity)." Journal of Engineering and Applied Sciences, 13.3(2018):691–695.
5. An, J. "TCNS: Node Selection with Privacy Protection in Crowdsensing Based on Twice Consensuses of Blockchain." Network and Service Management, IEEE Transactions,16.3(2019):1255–1267.
6. Luo, B. "Blockchain Enabled Trust-Based Location Privacy Protection Scheme in VANET." IEEE Transactions on Vehicular Technology, 69.2(2020):2034–2048.
7. Fan, K. "Blockchain-based efficient privacy preserving and data sharing scheme of content-centric network in 5G." IET Communications, 12.5(2018):527–532.
8. Nie, Z. X. "A controllable privacy data transmission mechanism for Internet of things system based on blockchain." International Journal of Distributed Sensor Networks, 18.3(2022):303–315.
9. Wu, G. "Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System." IEEE Journal of Biomedical and Health Informatics, 26.5(2022):1917–1927.
10. Sankaranarayanan, M., Mala, C., & Jain, S. (2024). Traffic Density Estimation for Traffic Management Applications Using Neural Networks. International Journal of Intelligent Information Technologies (IJIIT), 20(1), 1–19.

11. Onik, Mmh. "Privacy-aware blockchain for personal data sharing and tracking." Open Computer Science 9.1(2019): 80–91.
12. Qi, Y. "Privacy-preserving blockchain-based federated learning for traffic flow prediction." Future Generation Computer Systems, 117.2946(2021):328–337.
13. Yan, Zabc, and B. Hla. "Distributed privacy protection strategy for MEC enhanced wireless body area networks - Science Direct." Digital Communications and Networks 6. 2(2020):229–237.
14. Shen, M. "Privacy-Preserving Image Retrieval for Medical IoT Systems: A Blockchain-Based Approach." IEEE Network, 33.5(2019):27–33.
15. Lee, D., and N. Park. "CCTV Video Privacy Protection Scheme Based on Edge Blockchain." The Journal of Korean Institute of Information Technology, 17.10(2019):101–113.
16. Zhu, Qixiang. Design of a PLC DC Motor Speed Regulation System Based on Fuzzy Control Algorithm. Engineering Intelligent Systems, v 32, n 2, p 127–137, March 2024
17. Hongjie, Chen, Chuan, Xiao. Longitudinal Deformation Analysis of High-Resolution Integrated Images Based on Multi-Sensors. Engineering Intelligent Systems, v 31, n 1, p 33–42, January 2023

Xuejun Ma: Associate professor, Weifang University/School of Economics and Management, Weifang, Shandong Province, 261061, China, DBA. Master tutor, Pan Pacific University. Research interests: business enterprise management, human resource management, logistics management.
Email: wfmxj@163.com

Yongshan Zhang: Associate professor, Weifang University of Science and Technology/School of Economics and Management, Shouguang, 262700, Shandong Province, China.Master Tutor at Linyi University. Research interests: business management, trade and investment.
Email: zhangyongshan2023@163.com