

Research Article

Research on Accounting Information Security Management Based on Blockchain

Huaqing Shao ¹, Zongli Zhang ¹ and Bin Wang ²

¹College of Economics and Management, Jiamusi University, Jiamusi, China

²College of Information Science and Electronic Technology, Jiamusi University, Jiamusi, China

Correspondence should be addressed to Zongli Zhang; jeanneettee@163.com

Received 6 March 2021; Revised 10 May 2021; Accepted 25 July 2021; Published 18 August 2021

Academic Editor: Zengpeng Li

Copyright © 2021 Huaqing Shao et al. This is an open access article distributed under the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original work is properly cited.

At present, accounting information presents various and complex characteristics, which leads to the decline in the comprehensive scheduling level of accounting information security management system. For this problem, a blockchain-based accounting information security management information model is designed. This paper constructs the blockchain accounting information security association blockchain Big Data analysis model and processes the sample data, uses the semantic rough feature matching method to decompose the characteristics of blockchain accounting information, realizes the feature information fusion and autocorrelation feature matching and finally reorganizes and manages the blockchain accounting information security. The simulation results show that this method has better comprehensive scheduling ability, information fusion scheduling ability is greater than 92%, convergence is greater than 91.8%, feature recognition rate is greater than 90.1%, and management accuracy is greater than 95.6%. The design method can effectively improve the security and stability of accounting information storage and management.

1. Introduction

With the development of Big Data information processing and cloud computing technology, it makes the current accounting information security data present diverse, complex, and massive characteristics. In this background, methods concerning the improvement of accounting information security management capabilities have received much attention, while the study of accounting information security management methods is also of great significance in promoting the secure integration and scheduling of accounting information [1].

Privacy and security issues are involved in accounting information databases, and data anonymity can protect the security of accounting information data. In this area, many techniques on data security and privacy protection have been proposed by researchers, such as homomorphic encryption and attribute-based encryption schemes [2, 3]. In recent years, with the development of cloud storage technology, researchers have proposed a cloud technology-based

storage service, which achieves the purpose of sharing accounting information data through the control of access rights. Esposito et al. proposed a data sharing model using cloud storage technology in the context of accounting information and enumerated the possible challenges of using blockchain technology in accounting data sharing. However, these accounting information networks rely on a role that is trusted by both parties to the transaction, that is, the use of a trusted third party (TTP) to guarantee the proper conduct of the transaction. This requires the third party to be absolutely trusted and not subject to cyber-attack. However, such an ideal network environment is almost impossible to achieve, so traditional healthcare information solutions are not a good solution.

The research on accounting information security management methods by Zhao and Cheng [4] is based on the Big Data fusion and characterization of blockchain accounting information. The method uses similarity information feature decomposition and quantitative parameter regression analysis methods for internal control and quantitative

parameter analysis for accounting information security management and uses local parameter search control for accounting information security management. Among the traditional methods, there are mainly accounting information security management methods of fuzzy information feature detection, accounting information security management methods based on similarity feature analysis, and accounting information security management methods based on elastic template feature matching. These methods construct the elastic Big Data feature analysis model for accounting information security management and perform accounting information security management through fuzzy similarity feature decomposition [5]. Massicotte and Henri [6] discuss how management accounting information is used to monitor strategy implementation in the context of corporate governance. By establishing theoretical attributes and proposing a measurement model, the model captures the board's use of budget, financial, and nonfinancial performance indicators to monitor strategic plans.

However, the adaptability of this method to accounting information security management is not strong, and the level of feature recognition is not high. Pérez-González et al. [7] verified the information security management performance model by collecting data through questionnaire surveys. The results show that information security knowledge sharing, information security education, information security visibility, and security organization practice have a positive impact on information security management performance. But this method for accounting information security management, feature recognition level is low, information clustering is poor. Chen et al. [8] construct an application-oriented quantitative evaluation method of urban security. A new evaluation concept of "comprehensive screening, key analysis, and comprehensive evaluation" is put forward. However, this method has great variability and poor convergence in accounting information management. Mehedi et al. [9] proposed the security management of Ethereum transaction Internet-of-things infrastructure based on blockchain. This method points out that blockchain technology is a luxury technology, which will bring high bandwidth, extended time, and memory cost incompatible with IOT devices. Using terminal equipment as network technology and Ethereum as the blockchain platform, it can produce a back-end system to ensure high availability, improved security and privacy, and replace the traditional back-end system. Xu et al. [10] proposed the integrated application of blockchain in power information management system. The method points out that blockchain technology has been applied in many fields to improve the management and data security of information systems. This paper introduces the application of blockchain technology in power management information system.

First, the composition and structure of blockchain framework are introduced. Then, the blockchain-based authentication application is studied to realize the integration with the existing IT infrastructure. Finally, the advantages and limitations of the integration framework are analyzed. Based on this analysis, it can be seen that the application of blockchain technology in accounting

information security management has certain effectiveness. Datta et al. [11] solved the problems in the process of dealing with network attacks based on pin security system and proposed a module to help the secure transmission of sensitive data by encrypting images and other files. However, this method has not been implemented in specific enterprises to verify its effectiveness. Patel et al. [12] proposed a hybrid anomaly detection method in order to solve the problem of consumer network attack under the condition of limited resources. This method only uses basic network information, such as packet size, source port, and target port, time between subsequent packets, transmission control protocol (TCP) flag, and so on. However, this method is difficult to distinguish sensitive data and easy to cause processing error.

In order to solve the problems of poor adaptability and low-level feature identification in the existing accounting information management, this paper proposes a blockchain-based accounting information security management model. Through the feature decomposition of accounting information in blockchain, the features of accounting information are matched by autocorrelation features to realize the security reorganization and management of accounting information in blockchain. The simulation test shows the superiority of the proposed method.

2. Statistical Analysis and Feature Extraction for Accounting Information Security Management

Before designing the accounting information security management model based on blockchain technology in this paper, we first need to statistically analyze the accounting information security management information, extract features, and perform feature fusion processing on this basis. During the risk identification phase of accounting information security management, the focus should be consciously expanded to focus on learning activities in an effort to find gaps between the system and the environment. These gaps can bring reverse effects and threats to the security of accounting information systems. Accounting information security risk identification is the need of accounting information security risk strategy. Risk identification identifies, classifies, and prioritizes the accounting information and accounting-related information in an enterprise to understand which accounting information in an enterprise is the target of various threats and threat tactics, with the goal of protecting this accounting information from threats. The details are shown below.

2.1. Statistical Analysis of Accounting Information Security Management. Due to the large amount of accounting information security management data, which leads to the problem of large errors when building accounting information security management models, the method of fuzzy information feature detection and correlation fusion is used to realize the sample clustering processing of blockchain accounting information. The block-link regression analysis

method is used to obtain the random neighbor characteristic parameter analysis model $\phi(x_i)$ for accounting information security management. Under the condition of ambiguity information fusion, using semantic combination control, the adaptive quantitative parameter adjustment model for accounting information security management is obtained:

$$G = R^2 + A \sum_i \frac{\phi(x_i)}{\xi_i}, \quad (1)$$

s.t: $\phi(x_i) \leq R^2 + \xi_i$.

In formula (1), ξ_i is the constraint index parameter set of accounting information security management and R^2 is the random characteristic parameter distribution set of accounting information security management. Through the group regression test analysis method, the random cluster distribution binomial parameter analysis model of accounting information security management indicators is constructed, and the quantitative parameter analysis of accounting information security management is carried out. Through autocorrelation information fusion, the sample parameter test analysis model of accounting information security management is constructed, which is expressed as

$$K = G \sum_i \sum_j \alpha(x_i, x_j) + \frac{\omega_{\max} - \omega_{\min}}{\lambda}. \quad (2)$$

In formula (2), ω is the adjustment coefficient of accounting information security management, λ is the integration scale of accounting information security management, α is the control factor of accounting information security management, and (x_i, x_j) is expressed as the sample parameter coordinates. Through correlation dimension analysis, using the embedded scheduling method, construct the variable parameter fusion model of accounting information security management, which is expressed as

$$S = \begin{cases} \alpha K_i, & \text{if } i = 1, \\ \lambda \text{New}_i, & \text{otherwise.} \end{cases} \quad (3)$$

In formula (3), New_i represents the block scheduling parameter set for accounting information security management. The method of fuzzy information feature detection and correlation fusion is used to realize the sample clustering processing of blockchain accounting information and complete the statistical analysis of accounting information security management.

2.2. Analysis of the Characteristics of Accounting Information Security Management. On the basis of the above statistical analysis, in order to improve the accounting information security management, it is necessary to establish the feature integration model of blockchain accounting information for feature analysis using fuzzy extended sample regression analysis method. In this paper, segmented sample detection and quantile regression analysis methods are applied to accounting information security management, and the dynamic fusion parameter matching set is obtained as

$$U = \beta \int \ln(1 + \phi(x_i) \times p) di. \quad (4)$$

In formula (4), β represents the relevant characteristic value of accounting information security management. Under the constraint of elasticity law, the high-order statistical distribution sequence associated with accounting information is $r = r(1), r(2), \dots, (n)$, and the sampling interval t of random samples of accounting information is obtained. The constraint quantitative index parameter set of information security management is expressed as

$$C = U \sum_{n=1} r(n) + \varphi + t \sum_j \alpha(x_i, x_j). \quad (5)$$

In formula (5), φ is expressed as the detection statistical characteristic value of the distribution of accounting information blockchain. The larger the detection statistical characteristic value, the higher the degree of restraint of accounting information security management. Thus, the subset of accounting information security distribution constraint parameters is as follows:

$$B = \arg \min \left(\max \left| \sum_{i=1} C \times x_i \right| \right). \quad (6)$$

Based on the aforementioned analysis, constrained regression analysis model is constructed for accounting information security management, which is expressed as $y(t)$. Through the variance fusion of accounting information and the regression analysis results, the detection statistical characteristic value is obtained:

$$\varphi = B \left[y^2(t) - A \sum_i \xi_i \right]. \quad (7)$$

On the basis of the detection statistical characteristic values, in order to achieve balanced scheduling, combined with the blockchain fusion distribution of accounting information security management, the calculation of the constraint object distribution complex envelope $s_i(t)$ of accounting information security management is as follows:

$$s_i(t) = \varphi \int y^2(t) + \frac{(p/R^2)}{\omega} dt. \quad (8)$$

In Equation (8), p is denoted as the equilibrium scheduling channel noise. Using random cluster analysis, the blockchain distribution domain A of accounting information is divided into the number $W \times L$ of $(\sqrt{2}/2)R^2 \times (\sqrt{2}/2)R^2$ block-matching regions, and the feature integration model of blockchain accounting information is obtained by fuzzy extended sample regression analysis method as

$$Z = s_i(t) \times X^N + \chi. \quad (9)$$

In equation (9), X^N is the fuzzy component of accounting information, and χ is the fusion coefficient of random feature parameters. Through the aforementioned study, feature decomposition and information fusion are

performed using segmented sample detection method [6], so that the accounting information security management feature extraction and fusion processing are completed.

3. Blockchain Accounting Information Security Management

On the basis of the aforementioned fusion treatment of blockchain accounting information security management features, a blockchain security management model is constructed to improve accounting information security management capabilities. China's relevant system of accounting information security is not perfect, the qualities of accounting personnel themselves have serious defects, the management does not pay enough attention to accounting personnel, and so on. Most enterprises will choose to buy more advanced and efficient machines and equipment, or choose to buy more secure and reliable systems or other equipment matching with them. However, this method ignores the subjective and objective factors of the accounting security system, that is, the employees in the accounting positions, and such neglect has laid a hidden danger to the security and stability of the enterprise accounting information system. Even if the enterprise acquires more advanced and sophisticated equipment and adopts more strict accounting system, if the staffs in accounting positions do not have cautious awareness of accounting information security and subconsciously leak out the accounting information, it will bring many insecurity factors to the enterprise, and even directly lead to the business closure or even collapse of the enterprise. Therefore, in order to realize the security of accounting information system, it is especially necessary to realize the security of accounting system, starting with the accounting post staff.

3.1. Blockchain Integration of Accounting Information.

The accounting information security management features have been extracted through the content of part 1.2, and this part will realize the blockchain accounting information feature decomposition by semantic rough feature matching method. The security of accounting information involves the security of servers, storage devices, network devices, and users. According to the current accounting information security management needs of enterprises, it is very necessary to establish a practical accounting information security management system. After enterprises choose cloud accounting, cloud accounting service providers focus on the security of hardware and network infrastructure, while enterprises focus their accounting information security efforts on the security management of users. Using the method of high-dimensional feature information space reconstruction and information fusion [13], the fuzzy distribution set of blockchain accounting information fusion is established as

$$D(i) = \frac{Z(i)}{\eta \exp[\ln Z]}. \quad (10)$$

In equation (10), η is the blockchain accounting information fusion degree. The dummy variables of

organizational nature are constructed, and the neighborhood equilibrium scheduling method is used to obtain the blockchain accounting information characteristics game parameters using the Big Data fusion scheduling method as

$$k = \exp(k^{1/i}) - \ln D. \quad (11)$$

Through the method of cooperative innovation and game equilibrium control, the parameter regression analysis model of blockchain combination scheduling to obtain accounting information is

$$N = a\phi(x_i) + k. \quad (12)$$

In Equation (12), the coefficient $a \geq 1$. Combining the blockchain fuzzy constraint control method of accounting information [14], a regression analysis and constraint evolution model of accounting information association is constructed, which is expressed as

$$Y = \kappa X^N + V^i, \quad (13)$$

$$V^i = N + \sum_{i=1} \lambda(p - x_i). \quad (14)$$

Equation (13) is associated with the regression model accounting information, and equation (14) is associated with accounting information constraints evolutionary model. κ is expressed as the dynamic parameter distribution set of accounting information security management. The decision-making quantitative set for constructing accounting information security management is M . The adaptive equilibrium control method is adopted to control the associated constraint of accounting information security management, and the blockchain fusion function of accounting information is obtained as

$$H = \alpha Y + v, \quad (15)$$

$$v = \omega V^i \int_{i=1} \kappa(G - x_i) di. \quad (16)$$

Equation (15) is the autocorrelation resolution function of accounting information security management, and equation (16) is the blockchain fusion function of accounting information. Blockchain accounting information feature decomposition by semantic rough feature matching method. The internal control and prudential control analysis model of accounting information is calculated by high-dimensional feature information space reconstruction [15], and the block fusion processing of accounting information is completed up to this point.

3.2. Blockchain Accounting Information Management Optimization.

In order to further improve the ability of accounting information security management, this paper adopts the method of random discrete combination control to construct the information fusion and feature reorganization model of blockchain accounting information management [16]. Let F be the covariance fusion model of the internal control of accounting information, and the

distributed combination control parameters of blockchain accounting information is obtained as

$$f = v\sqrt{s_i(t)} \times \Delta t. \quad (17)$$

A real-time data clustering analysis model is established for accounting information management, and the window function $h(t)$ for the distribution of blockchain accounting information, thereby obtaining a random probability distribution model for blockchain accounting information reorganization and security management:

$$q(x_i) = \begin{cases} \frac{x_i}{f} \exp[v - h(t)], & x_i \geq 0, \\ 0, & x_i < 0. \end{cases} \quad (18)$$

In the case of $f = 1$, the segmented information fusion is realized for the accounting information characteristic parameters, and the detection statistics of the blockchain accounting information management are obtained as

$$E = \left(2 - \frac{\pi}{2}\right) f^2 - \sqrt{q(x_i)}. \quad (19)$$

On the basis of the detection statistics derived from equation (19), information fusion and autocorrelation feature matching processes are performed on the features in the process of blockchain accounting information security management. According to the information feature matching results, the real-time data parameter association knowledge set of accounting information management is established, and the blockchain fusion and factor analysis of accounting information is combined with the multivariate linear fusion method, and the joint feature distribution set of relevant parameters for blockchain fusion and security association of accounting information is obtained as

$$I_{N \times 1} = E \times R_L. \quad (20)$$

The negative binomial regression model is constructed, and the quantile regression test analysis method of aggregation coefficients is used to achieve the information security management of blockchain accounting, and the optimal decision model for the information security management of blockchain accounting is expressed as

$$y_i = \begin{cases} 0, & M - I_{N \times 1} \sum_{j=1} x_j \leq 0, \\ 1, & M - I_{N \times 1} \sum_{j=1} x_j > 0. \end{cases} \quad (21)$$

Using the methods of rough set feature matching and nearest neighbor parameter analysis, the nonlinear constraint statistical feature Q^N of blockchain accounting information security management is obtained, which satisfies the correlation distribution relationship:

$$u(Q^N) = \text{angle}(y_i) - \varphi + \text{mod}(2\pi). \quad (22)$$

A spatial parameter-matching model for information security management of blockchain accounting is

established. According to the information feature-matching results, the method of similarity feature decomposition [17] is used to realize the information security reorganization and management of blockchain accounting information, and the realization process is shown in Figure 1.

As can be seen from Figure 1, the implementation process of blockchain accounting information security management is mainly divided into the following steps:

Step 1: Sample regression analysis of accounting information data security.

Step 2: According to the results of sample regression analysis, build the blockchain Big Data analysis model of accounting information security, and use the accounting information data.

Step 3: Feature analysis and segment fusion of the data in the model.

Step 4: Make linear prediction for the characteristics of accounting information after fusion.

Step 5: Divide the prediction results into training set and sample set, and carry out adaptive learning on the training set.

Step 6: Judge the output result of Step 5, output the accounting information security management data if the threshold is set, and return to Step 1 if the threshold is not set.

3.3. Accounting Information Security Relationship System Requirements. The main users of the system are identified through business process analysis as the main user roles of the system, which are company financial staff, system administrators, and company leaders. The accounting system has six major functional modules: account information management, accounting management, data management, report statistics, decision support, and system management. The functions required by the company's financial staff include adding, modifying, querying, and deleting information in the accounting information management module. The finance staff can add, modify, query, and delete information in the accounting management module, and submit printouts of relevant data. In the data management module, finance staff can add, modify, delete, and query the information in it. In the report statistics module, finance staff and company leaders are mainly able to query and print reports. In the decision support module, company leaders can get data from the data analysis submodule to support decision-making. In the system management module, the administrator users can add, modify, delete, and query user information in the user management submodule. In the function module permission management submodule, users are able to set their operation permissions. In the company announcement management submodule, the company announcement information can be added, modified, and deleted. In the log management submodule, the system administrator can also view and delete the operation log information of the system.

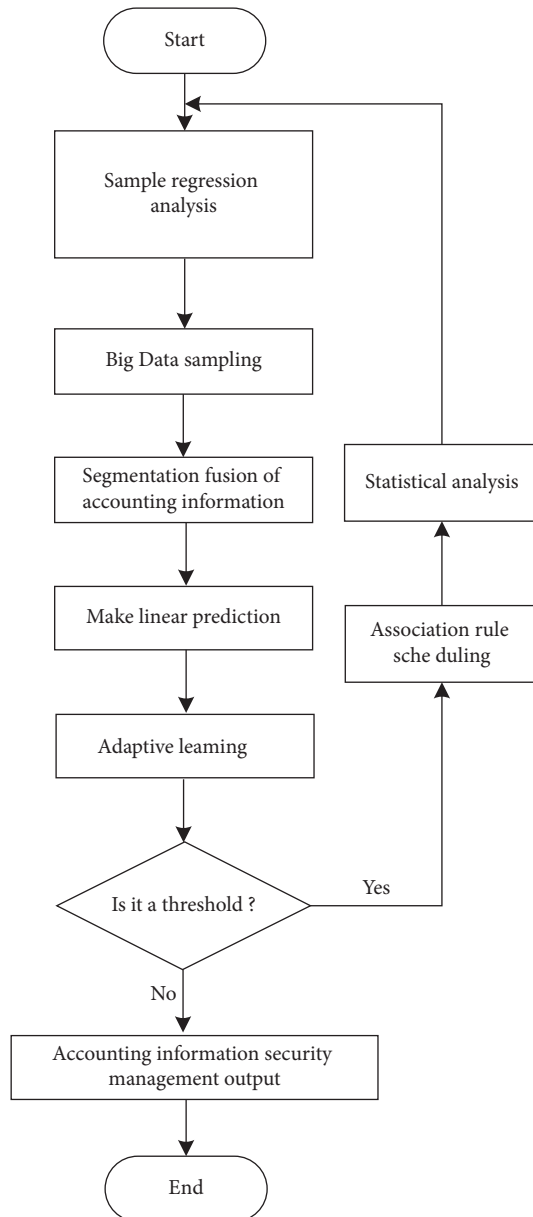


FIGURE 1: Blockchain accounting information security management implementation process.

- (1) Account information management: account information management mainly includes several submodules, such as advance payment management, staff advance management, cargo information management, carrier vehicle advance management, advance receipt management, and transaction order management
- (2) Accounting management: accounting management mainly includes several submodules, including reimbursement order management, consignee check-out management, supplier checkout management, and freight payment management
- (3) Data management: data management mainly includes goods classification management, sales contract management, procurement contract

management, staff management, cargo information management, and carrier information management submodule

- (4) Statistical report: the statistical report function module mainly provides the query and printing function for the aforementioned reports
- (5) Decision support: it generates various kinds of data information, which is an important data source for the company's accounting information and can be used as a basis for decision support
- (6) System management: system management mainly includes user management, functional module authority management, company announcement management, and log management [18]

The the use case model for the blockchain accounting information security management function is shown in Figure 2.

3.4. Definition of Accounting Information Security. The purpose of accounting information security management is to ensure the integrity, availability, and ease of use of accounting information; that is, accounting data can only be disclosed to the right to know, accounting data can only be modified within the scope of authorization and accounting information system can only be used when necessary.

Investors and lenders use the accounting information of the enterprise to make investments and operation decisions, evaluate the enterprise value according to the accounting information, and predict the future cash flow of the enterprise. At the same time, the relevant government departments carry out macro-control on the market according to the relevant indicators provided by accounting information, so as to improve and strengthen the enterprise management. Therefore, it is of great significance to study blockchain-based accounting information security management.

4. Simulation and Result Analysis

In order to verify the performance of the application of this paper's method in implementing blockchain accounting information security management, SPSS statistical analysis and Matlab simulation software are used for simulation experiments, and the simulation platform is built with Intel (R) Core (TM) i7-47 70 CPU, 16 GB of memory, and Windows 1064 bit operating system. Based on the aforementioned parameters, the regression analysis value of accounting safety management evaluation is obtained, which is reflected by objective function. Figure 1 shows the convergence curve of the optimal objective function of the model under different iterations and different calculation times.

Figure 3 shows that the function curve of the method in this paper is closer to the standard convergence curve than the curve of the statistical analysis method, which improves the process convergence of the evaluation, thus it can be seen that the method in this paper can effectively realize the

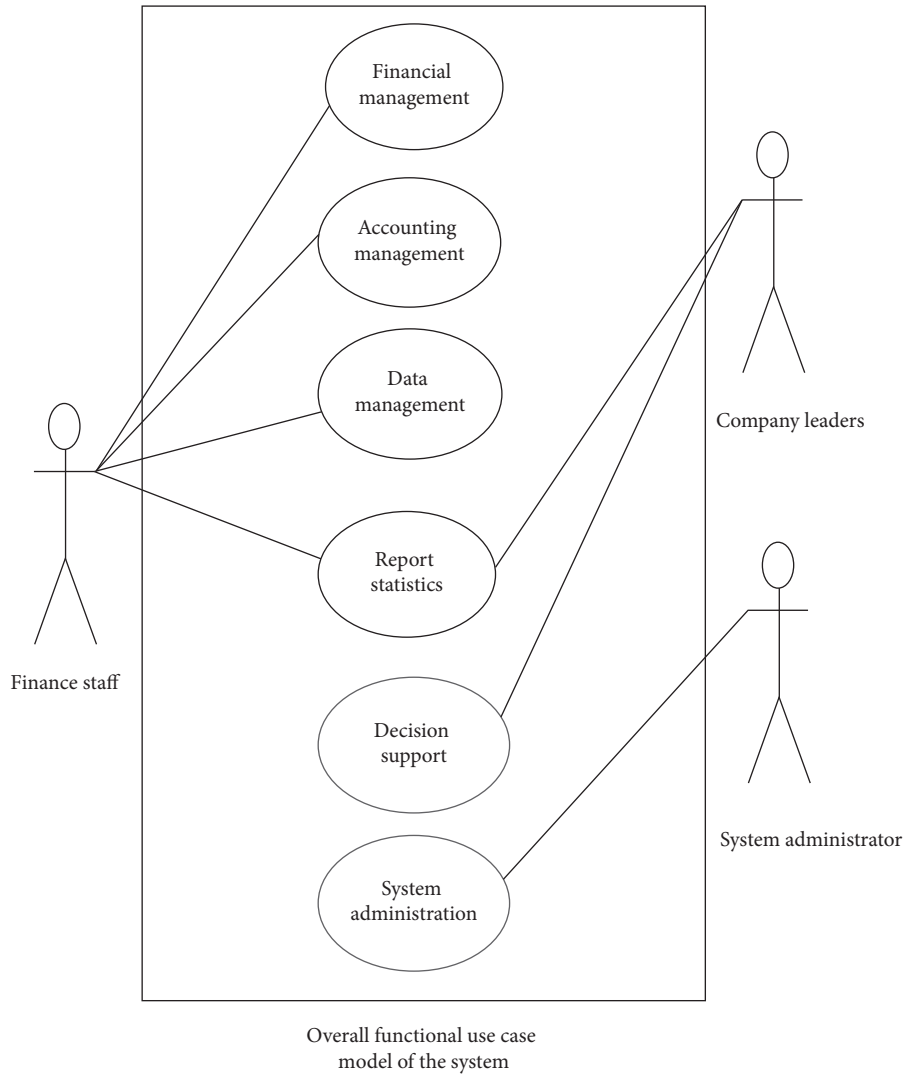


FIGURE 2: Blockchain accounting information security management functional use case model.

research credit evaluation, and the optimization of its objective function is better.

The boundary constraint coefficient of present accounting information management is set as 0.36, the autocorrelation statistical feature component is 0.67, the sample number of Big Data information sampling for the present accounting information management is 1200, the test set is 120, the data set of semantic ontology information distribution is 60, and the descriptive statistical distribution set of accounting information security association is shown in Table 1.

Based on the results of the aforementioned descriptive statistical analysis of the parameters of accounting information security management, in order to visualize the results of the statistical analysis of accounting information, the data in Table 1 are transformed as shown in Figure 4.

Based on Figure 4, taking test object set 10 as the research object, the accounting information security management method based on Massicotte and Henri’s study [6] enterprise

computerization quantitative feature analysis, the accounting information security feature matching method based on Pérez-González et al.’s study [7], and the method in this paper mentioned in the introduction are respectively used to fuse and schedule the blockchain accounting information, and the boundary constraint coefficient of the current accounting information management is set as 0.36. The autocorrelation statistical characteristic component is 0.67, and the comparison results of the same test set under different similarity coefficients are obtained, as shown in Figure 5.

Figure 5 shows that compared with the method by Massicotte and Henri [6] and Pérez-González et al. [7], the method in this paper can effectively realize the security management of accounting information, the information fusion and scheduling ability is above 92%, and the statistical analysis results are accurate and reliable. The main reason is that the random nearest neighbor characteristic parameter analysis model of accounting information security management is obtained using the block-link regression analysis

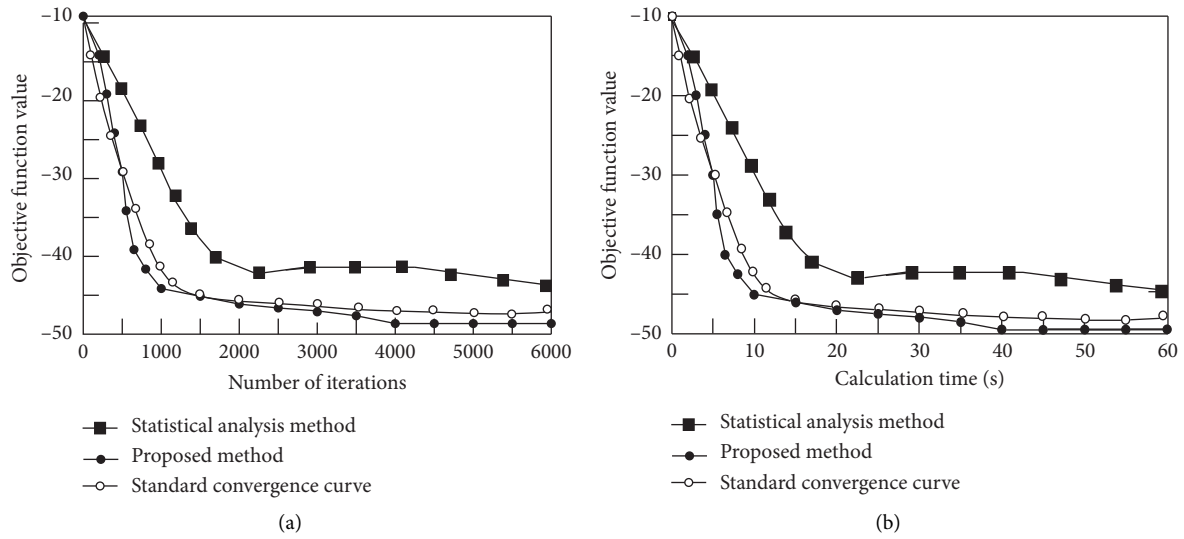


FIGURE 3: Convergence curve of the optimized objective function: (a) convergence curves of the objective function optimized under different number of iterations and (b) convergence curves of the objective function for optimization at different times.

TABLE 1: Results of descriptive statistical analysis.

Test object set	Similarity coefficient	Test regression analysis level (%)	Variance
1	0.388	43.53	0.388
2	0.546	42.46	0.655
3	0.677	34.32	0.554
4	0.366	53.56	0.454
5	0.434	54.58	0.654
6	0.143	53.64	0.678
7	0.342	35.53	0.435
8	0.324	64.56	0.457
9	0.445	43.54	0.544
10	0.532	56.24	0.567
11	0.443	43.63	0.544
12	0.432	32.56	0.565
13	0.435	65.65	0.655

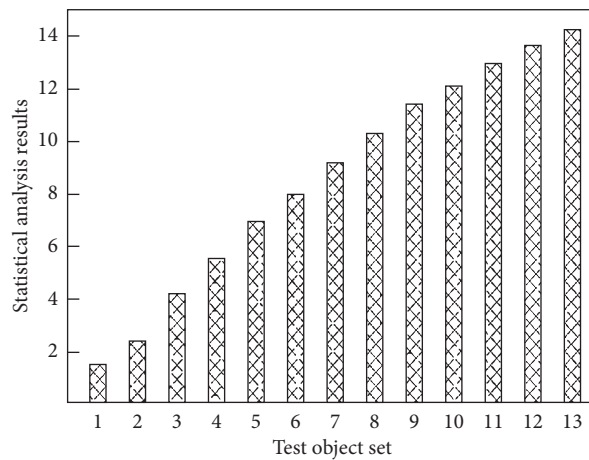


FIGURE 4: Statistical analysis results.

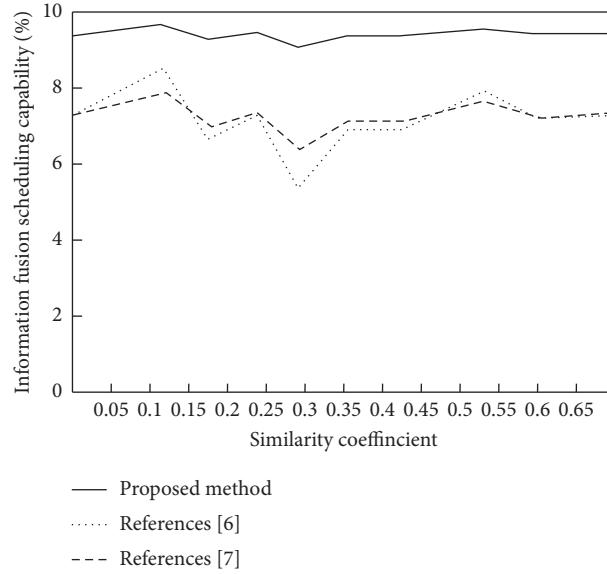


FIGURE 5: Comparison results of blockchain accounting information fusion and scheduling.

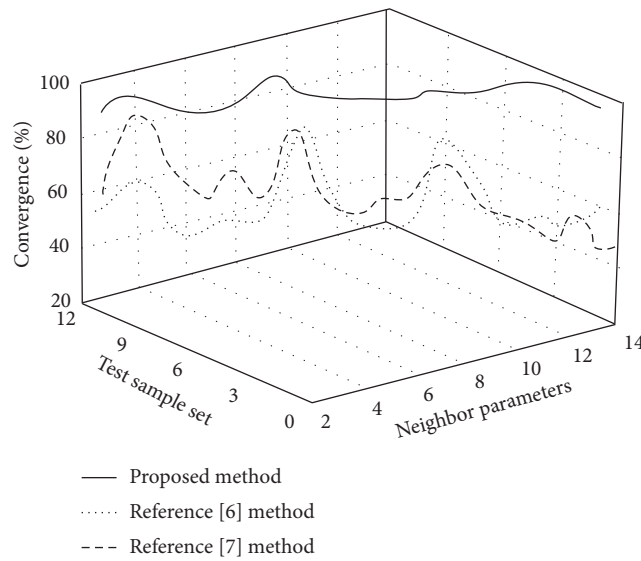


FIGURE 6: The convergence surface of accounting information security management.

method. The model is used for data management and analysis to improve the reliability of the final results.

In order to further verify the effectiveness of the proposed method, the unified similarity coefficient is 0.445, and other conditions remain unchanged. The convergence of accounting information security management is obtained by testing the fusion level of different methods, as shown in Figure 6.

Figure 6 shows that the convergence of the method in this paper is better compared to the method by Massicotte and Henri [6] and the method by Pérez-González et al. [7] for accounting information security management, and the convergence is above 91.8%. The convergence is mainly manifested in the flexible scheduling ability of the model. This method uses the joint characteristic distribution set of

the relevant parameters of the blockchain fusion and security association of accounting information to improve the flexibility of accounting information security management and further has a better optimization effect on the convergence.

The feature recognition rate of accounting information security management is tested and the comparison results are obtained as shown in Figure 7. Analyzing Figure 7, we know that the method of this paper performs accounting information security management with a higher level of feature recognition, which is due to the fact that the method of this paper extracts features and performs feature fusion processing on the basis of statistical analysis of accounting information security management information, which improves the level of feature recognition above 90.1%. The

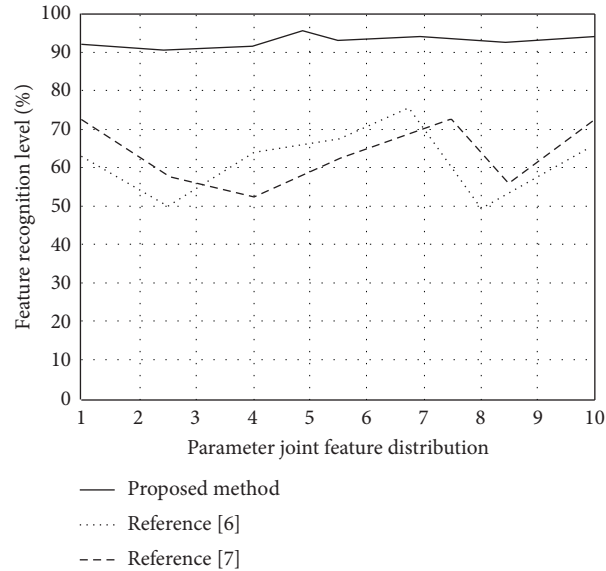


FIGURE 7: Comparison of feature recognition rate of accounting information security management.

TABLE 2: Comparison of accuracy of quantitative assessment of security posture of dual-channel wireless blockchain networks.

Dynamic fusion parameters	Proposed method	Massicotte and Henri's method [6]	Pérez-González et al.'s method [7]
0.2	0.956	0.824	0.835
0.4	0.978	0.846	0.867
0.6	0.997	0.859	0.893
0.8	0.999	0.912	0.912

main reason is that this paper uses blockchain technology to establish blockchain fusion function of accounting information and improves the ability of accounting information feature fusion.

Test the accuracy of accounting information security management and get the comparison results in Table 2. From Table 2, we know that the accuracy of accounting information security management by the method of this paper is higher than 95.6%. The reason for the high accuracy is to obtain the optimal decision model of the blockchain accounting information security management and realize the blockchain accounting information security management.

5. Conclusion

This paper proposes a model of blockchain-based accounting information security management, which improves the ability of accounting information security management.

- (1) In this paper, the fuzzy extended sample regression analysis method is used to establish the feature integration model of blockchain accounting information, calculate the internal control and prudent control analysis model of accounting information, and improve its security management ability.
- (2) The experimental results show that the information fusion and scheduling ability of this method is more than 92%, the convergence is more than 91.8%, the

feature recognition level is more than 90.1%, and the management accuracy is more than 95.6%. The comprehensive experimental results show that this method has certain effectiveness.

- (3) This study also has some shortcomings, mainly in the absence of specific accounting information research and investigation, which will be taken as the next research direction to further enhance the practicability of this paper.

Data Availability

The data used to support the findings of this study are included within the article.

Disclosure

The funders had no role in study design, data collection and analysis, decision to publish, or preparation of the manuscript.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was supported by the Planning Project of Philosophy and Social Sciences in Heilongjiang Province (grant

no. 19GLB086) and the Natural Science Fund of Heilongjiang Province (grant no. LH2020F006).

References

- [1] Y. Joyce, "Building trust in crisis management: a study of insolvency practitioners and the role of accounting information and processes," *Contemporary Accounting Research*, vol. 37, no. 3, pp. 1622–1657, 2020.
- [2] Z. Li, C. Ma, and D. Wang, "Achieving multi-hop PRE via branching program," *IEEE Transactions on Cloud Computing*, vol. 8, no. 1, pp. 45–58, 2020.
- [3] Z. Li, C. Ma, and H.-S. Zhou, "Multi-key FHE for multi-bit messages," *Science China Information Sciences*, vol. 61, no. 2, pp. 029101:1–029101:3, 2018.
- [4] J. Zhao and C. Cheng, "Dynamic cooperative random drift particle swarm optimization algorithm assisted by evolution information," *Journal of Computer Applications*, vol. 40, no. 11, pp. 3119–3126, 2020.
- [5] M. J. Ershadi and M. Forouzandeh, "Information security risk management of research information systems: a hybrid approach of fuzzy FMEA, AHP, TOPSIS and shannon entropy," *Journal of Digital Information Management*, vol. 17, no. 6, pp. 321–336, 2019.
- [6] S. Massicotte and J. F. Henri, "The use of management accounting information by boards of directors to oversee strategy implementation," *The British Accounting Review*, vol. 53, no. 3, Article ID 100953, 2020.
- [7] D. Pérez-González, S. Preciado, and P. Solana-González, "Organizational practices as antecedents of the information security management performance," *Information Technology and People*, vol. 32, no. 5, pp. 1262–1275, 2019.
- [8] G. Chen, Q. Yang, X. Chen et al., "Methodology of urban safety and security assessment based on the overall risk management perspective," *Sustainability*, vol. 13, 2021.
- [9] S. K. T. Mehedi, A. A. M. Shamim, and M. B. A. Miah, "Blockchain-based security management of IoT infrastructure with Ethereum transactions," *Iran Journal of Computer Science*, vol. 2, no. 3, pp. 189–195, 2019.
- [10] C. Xu, Y. Fang, and Y. Ma, "Integrated application of blockchain in the electric information management system," *Procedia Computer Science*, vol. 162, pp. 88–93, 2019.
- [11] D. Datta, L. Garg, K. Srinivasan et al., "An efficient sound and data steganography based secure authentication system," *Computers, Materials and Continua*, Cmc -Tech Science Press-, vol. 67, no. 1, pp. 723–751, 2021.
- [12] D. Patel, K. Srinivasan, C. Y. Chang et al., "Network anomaly detection inside consumer networks - a hybrid approach," *Electronics*, vol. 9, no. 6, pp. 1–12, 2020.
- [13] Z. Wang, N. Wang, X. Su, and S. Ge, "An empirical study on business analytics affordances enhancing the management of cloud computing data security," *International Journal of Information Management*, vol. 50, no. Feb, pp. 387–394, 2020.
- [14] M. Mirsch, J. Kinne, and K. Blind, "Exploring the adoption of the international information security management system standard ISO/iec 27001: a web mining-based analysis," *IEEE Transactions on Engineering Management*, vol. 68, no. 99, pp. 1–14, 2020.
- [15] A. S. Al-Delawi and W. M. Ramo, "The impact of accounting information system on performance management," *Polish Journal of Management Studies*, vol. 21, no. 2, pp. 36–48, 2020.
- [16] A. Naseer, H. Naseer, A. Ahmad, S. B. Maynard, and A. Masood Siddiqui, "Real-time analytics, incident response process agility and enterprise cybersecurity performance: a contingent resource-based analysis," *International Journal of Information Management*, vol. 59, no. 8, Article ID 102334, 2021.
- [17] H. O. Kadhim and A. Z. Latif, "The impact of supply chain accounting information systems harmonization on creating a competitive advantage for the Iraqi general commission taxation[J]," *Journal of Supply Chain Management*, vol. 8, no. 2050-7399, pp. 448–452, 2019.
- [18] M. S. Alathamneh, "The impact of accounting information systems reliability on enhancing the requirements of planning process at Jordanian commercial banks," *Management Science*, vol. 10, no. 5, pp. 1043–1050, 2019.