Research on the Design of Financial Management System Based on Blockchain

Fei Li

Dalian Vocational Technical College, Dalian, Liaoning, 116011, China
**Corresponding author's email: tg667788@xzcstudio.com*

ABSTRACT

In order to meet the various needs of the financial management system in the new era, in this research, based on the current emerging blockchain technology, starting from the overall structure, the functional modules, databases, encryption and security of the financial management system are many important components. Part of the design is carried out step by step, and the effect of the design is verified by testing. The test results show that the blockchain-based financial management system designed this time is excellent in performance and security, proving that the design to be initial success. Compared with the previous blockchain financial management system, the innovation of this design lies in the effective integration of blockchain, smart contract and encryption technology and other technologies, forming a set of data transmission mechanism that combines both openness, security and precision.

Keywords*-blockchain; financial management; system design*

1. INTRODUCTION

At present, as an emerging technology, the integration between blockchain technology and other fields is deepening, and the financial management field is no exception. Based on the application of blockchain technology, the operational efficiency and security of the financial management system will be further improved, and at the same time, it will help to ensure the authenticity of the data and information in the system, and its practical significance is particularly prominent. Therefore, further research should be done on the R&D and design of blockchain-based financial management systems.

2. SYSTEM BASIC REQUIREMENTS ANALYSIS

2.1 System functional requirements

In order to ensure that the financial management system designed this time can meet the actual needs, the following functions should be ensured. The first is to quickly retrieve financial information. The second is the statistics and inquiries on fixed assets and other information. The third is to record the daily work of financial management and related information of system operation and form a log. The last is the automatic backup of important data information.

2.2 System performance requirements

Considering that this system is a platform for financial management of enterprises and institutions, it involves massive data storage, uploading and downloading operations, and has high requirements for concurrency. Based on the above considerations, this design selects a high-performance server. The basic parameters are shown in table 1.

Table 1 Basic parameters of the high performance server

Project	Parameter
CPU	8 pit, 3.20GHz
Internal storage	512GB
Fixed disk	3×600G
Hard disk controller	SAS 6Gbps
Power pack	Redundant power supply

On the other hand, considering the high security requirements of the system, in order to avoid unnecessary information leakage based on hashing technology, part of the data is hashed and then transferred to the blockchain for storage. [1-2].

© The Author(s) 2023
S. A. R. Khan et al. (Eds.): ICMSSE 2022, AHCS 12, pp. 528–532, 2023.
https://doi.org/10.2991/978-94-6463-056-5_77

3. SYSTEM DESIGN

3.1 Overall architecture design of the system

Considering the needs of development speed, practical application and later access, in this system development, the development is based on the mainstream B/S architecture, and the four-tier architecture model is adopted, as shown in table 2.

Table 2 Software architecture of the financial management system

Layers	Major function
Presentation layer	Provide an intuitive interface for operators through HTML and JavaScript
Business logic layer	Achieve data retrieval, modification and other functions
Data access layer	Realize the system and user daily management and other functions
System access layer	Provide network access services for the management system

3.2 The overall functional module design of the system

Combined with the actual functional requirements of the financial management system, the overall functional module design of the system mainly includes the following parts.

One is the system management module. This module is mainly for the system administrator account, which can add, edit and delete other user accounts, and the relevant data are stored in the database. The user performs verification when logging in, and jumps into different operation interfaces according to the corresponding attributes.

The second is the data transmission module. Since the financial management system involves a large number of different types of data information in the daily use process, and involves the adaptation of a large number of software and hardware devices. The data transmission method based on the proxy network (figure 1) is selected, thereby improving the efficiency of data transmission. The data transmission is mainly divided into the following steps. The client sends a data request packet to the server. After the server receives it, it determines the legitimacy of the source and target. If both the source and target are legal, the server checks whether it has data that meets the requirements, and if it does not, it requests data from other devices in the network. After getting the data, the data back should be sent to the client.

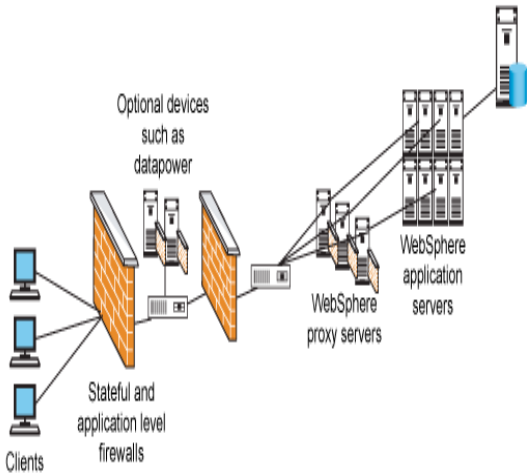

Figure 1. Basic schematic diagram of proxy network

The third is the domain name and access control module. This module is mainly based on the BonAcs system, which can quickly realize the configuration of the distributed computer network system, so as to obtain the absolute control over the financial management system based on the blockchain, and realize the demand support for different types of data formats.

The fourth is the user module design, which is mainly designed for ordinary financial managers to ensure that they can use this system to upload and retrieve financial information and other daily work. Among them, the financial information with a higher level of confidentiality involved in the work of the user account will be encrypted and stored in the super ledger.

The fifth is the system operating environment design. In this research, four peer nodes and one order node are designed as the underlying network of the blockchain. At the same time, considering that the information stored in the Hyperledger requires an MSP certificate for transmission, this experiment uses the Cryptogen tool and the Hyperledger Fabric CA component to configure the MSP certificate. In order to ensure the normal operation of related tool components, configure related nodes and files, specify the mapping relationship between the organization's network topology and the corresponding image file in the configuration file, and then write the SDK to complete the design of the operating environment.

The sixth is the design of data verification module, which is one of the important modules to ensure data integrity and improve data transmission, storage and application efficiency. In the design of this link, the OPT

adaptation module is introduced to realize comprehensive verification of data information, which can not only provide users with a data-centric trust system, but also use Hash value to verify data integrity [3]]. On the other hand, in order to prevent the data sender from stealing the data information in the blockchain by using the fake data Hash value, the researchers introduce a trusted proxy stage, and check the data Hash value when it enters the blockchain, which is for data security and the transmission lays the foundation.

3.3 Database design

In the database design of this system, the design is mainly based on MySQL2019, and the relevant data information is stored in the cloud server, and its information table is shown in table 3.

Table 3 The database information table

Field name	Chinese name	Data type
zlID	ID	Int
zlmc	Data name	varchar
bcdz	Save the address	varchar
jj	Brief introduction	varchar

On this basis, in order to further improve the comprehensive performance of the database, the following technologies are also applied. One is data integration technology. Considering that the financial management system involves data information from various sources, in order to achieve effective integration of diversified data information, researchers preprocess the data based on metadata and convert it into XML and further compress through the XCiot compression processing method (figure 2) to eliminate the redundancy problem [4-5].

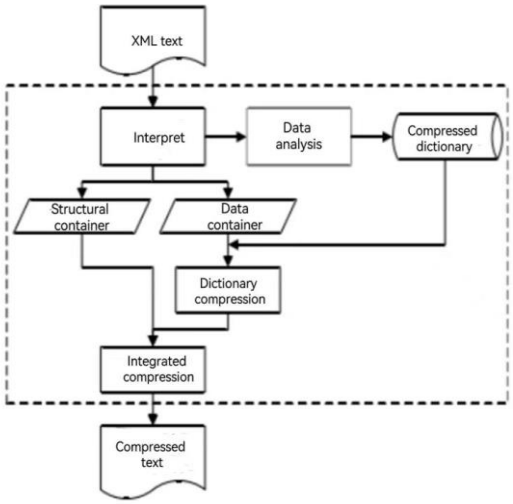

Figure 2. Basic flow chart of XCiot compression

The second is data mining technology, which is mainly based on the C4.5 algorithm for mining in this research. The third is data interaction technology, mainly using ADO NET technology, that is, the interaction technology in the data source network, to realize data interaction. In this technical mode, the interactive object SqlConnection is used to manage the data source, and the interactive object can satisfy the communication between the developer and the data source and send commands. The fourth is data visualization technology, which uses the combination of MySQL and Navicat data visualization tools for database design and management, which further improves the comprehensive performance of the database.

3.4 Data encryption design

In order to realize data encryption, in this system design, the encryption algorithm of RSA fusion AES is used for data encryption design, and its basic flow chart is shown in figure 3.

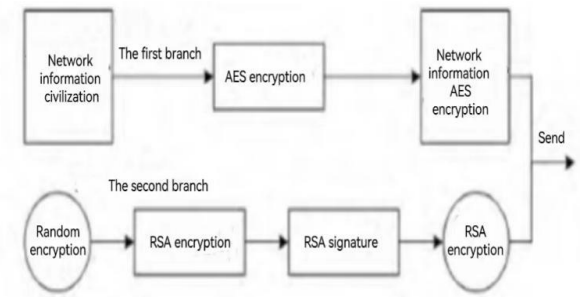

Figure 3. Flowchart of the R S A fusion AES encryption algorithm

As can be seen from the flow in figure 3, the first branch is to encrypt the plaintext of the network information to be encrypted using the AES algorithm to make it ciphertext. The second branch is to randomly generate a key, and then configure it on the information that needs to be encrypted based on the RSA algorithm. After the key configuration is completed, perform RSA signature and authentication processing on the key

information to transform it into RSA key. Finally, the ciphertext and key obtained by the two branches are sent to the receiver at the same time to complete the entire encryption process.

In this study, in order to ensure the effective application of the RSA-fused AES encryption algorithm, the researchers design the relevant software and hardware supporting the algorithm. Specifically, the first is to choose DS420j type storage to convert the relevant data to make it into a unified type of data, and then output the data through the conversion interface, and finally perform encryption processing based on this encryption algorithm. Secondly, the C5402 DSP chip is used to quickly transfer the data that needs to be encrypted, and it is also equipped with a signal blocker to avoid possible interference during data transmission.

3.5 Data security design

In order to realize the security of data in this system, a data classifier module is used in this research to realize fast and high-precision identification of possible external attack information. From a physical point of view, the classifier module contains a rule base, which stores the classification rules of data information. The rule base generates identification rules for attack codes according to the encryption algorithm designed above. According to the identification rules, the relevant data information is analyzed. After the suspicious attack code data is captured, it should simulate and quantify according to the unified mode of the database, set up a search engine in the process of simulation and quantization, and transmit the simulated and quantized data to the database. Only through the feature search function, various possible attack behaviors can be effectively identified, and necessary preventive measures can be given.

4. IMPLEMENTATION OF BLOCKCHAIN-BASED FINANCIAL MANAGEMENT SYSTEM

4.1 Formal Definition

In order to ensure that the financial management system based on blockchain can achieve the expected functions, the financial contract management of a mechanical engineering is taken as an actual case to study, which leads to the smart contract and its form definition. Specifically, the contract involved in this case contains a series of associations and agreements, which describe the obligations that both parties need to undertake. Therefore, in this section, the contract is defined as follows, the agreement in the contract is represented by a quintuple A (a, b, c, o, tl), the specific content of which is that the contract is made by party a to party b. If condition c is fulfilled, it can produce an action. Among them, the value of the condition c is Boolean. When the value is true, it means that the condition is established. If it is false, it proves that the condition is not established. tl indicates the time period of the agreement. If the value is true, the agreement is valid.

4.2 The Specific Implementation Process

After the formal definition is completed, the code is implemented for the financial management system integrated with the smart contract. Since the system includes states and a series of interface functions, the above-mentioned contract transaction is still used as an example for programming based on the solidity programming language. In this core code, the following parts are mainly included. Firstly, it should determine the buyer and seller and the contract's total price of the transaction. The second is to add modifiers to determine the identity of the buyer and the seller. The third is to use the condition function to determine the conditions for the establishment of the transaction. If the transaction conditions meet the requirements, the subsequent transaction process will continue. The fourth is to confirm the receipt of the transaction by the buyer. After the entity or service, it should unlock the ether and end the process.

4.3 Evaluation of Credibility

In order to ensure that all the data involved in the operation process of the blockchain-based financial management system, the credibility evaluation algorithm is introduced in the implementation process of the system to realize the quantitative evaluation of each project. This link mainly applies the following formula.

$$R_i^t = R_i^{t-\Delta t} + \alpha_i R_{\alpha i}^{\Delta t} + \beta_i \sum_{j=1}^{N} \delta_j R_{ij}^{\Delta t} + \chi_i \sum_{i=1}^{M} \varepsilon_l R_{il}^{\Delta t} \quad (1)$$

$$\alpha_i + \beta_i + \chi_i = 1 \quad (2)$$

In the above formula, R_i^t represents the credit score of node i at time t. $R_i^{t-\Delta t}$ indicates the credit score of the previous node. $\alpha_i R_{\alpha i}^{\Delta t}$ represents the credit given by the system after the node itself uploads the information. $\beta_i \sum_{j=1}^{N} \delta_j R_{ij}^{\Delta t}$ determines the information of node i at time t. $\chi_i \sum_{i=1}^{M} \varepsilon_l R_{il}^{\Delta t}$ represents the reward item obtained when the node i participates in the credit mechanism of other broadcast nodes.α_i, β_i, χ_i6 all represents the weight values of the different links.

5. SYSTEM TESTING AND ANALYSIS

5.1 System Performance Test

In order to ensure that the performance of the blockchain-based financial management system designed this time can meet the actual needs, after the system design is completed, the researchers test its main performance indicators, and the test results are shown in table 4.

Table 4 Results of the system performance test

Indexes	Parameters
Response time /s	1.6
Information transmission time/s	1.2
Maximum number of concurrent users	255

From the data in table 4, it is not difficult to see that the blockchain-based financial management system designed this time has excellent basic performance and can basically meet the actual needs of use.

5.2 System Security Testing

In order to test the security of the blockchain-based financial management system designed this time, the simulation experiment is carried out. Firstly, it should prepare two computers with the same hardware and software configuration, one of which is the experimental group, and the tampering program is set and implanted in it, and the other is the control group, and no operation is performed in this link. The second is to enter the same string of data information in the two computers. The third is to start the tampering program and check whether the data information enters in the two computers is consistent after a certain period of time. Through the experiments of the above several links, it is found that the information in the financial management system based on blockchain is still consistent with the data information initially input by the system, and the tampering program has no effect on it, which shows that the system has good security.

6. CONCLUSION

On the whole, in this research, a financial management system based on blockchain is designed and implemented based on blockchain technology and with the assistance of Internet computers and other related technologies. Through the test of the financial management system, it can be seen that its performance and security have been significantly improved, which shows that the blockchain technology has been fully utilized, and the financial management information system designed this time also has potential application value. Further in-depth research is still needed in the future work to continuously improve the design level of the financial management system.

REFERENCES

[1] Han Xu, Liu Zhihui, Yang Yan. Research on the application of blockchain technology in scientific research management [J]. Science and Technology Innovation and Application, 2022, 12(13): 14-19.

[2] Li Jie. Epidemic management system based on blockchain technology [J]. Software Guide, 2022, 21(04): 57-61.

[3] You Cong, Wang Lipeng, Pan Changchun. Data security management system based on blockchain [J]. Computer Times, 2022(04):34-37+42.

[4] Guo Lei, Li Cheng, Zhang Ya. Application of blockchain technology in state management of power transmission and transformation equipment [J]. Shanghai Energy Conservation, 2022(03):315-320.

[5] Zhang Wei, Xiao Huichen, Wei Qing. Construction and analysis of blockchain copyright management system for smart library [J]. Library Research, 2022, 52(02): 85-93.

Open Access This chapter is licensed under the terms of the Creative Commons Attribution-NonCommercial 4.0 International License (http://creativecommons.org/licenses/by-nc/4.0/), which permits any noncommercial use, sharing, adaptation, distribution and reproduction in any medium or format, as long as you give appropriate credit to the original author(s) and the source, provide a link to the Creative Commons license and indicate if changes were made.

The images or other third party material in this chapter are included in the chapter's Creative Commons license, unless indicated otherwise in a credit line to the material. If material is not included in the chapter's Creative Commons license and your intended use is not permitted by statutory regulation or exceeds the permitted use, you will need to obtain permission directly from the copyright holder.