Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.037756

Article

Research and Implementation of Credit Investigation Sharing Platform Based on Double Blockchain

Yanyan Han[1,2], Wanqi Wei[2,*], Kaili Dou[3] and Peng Li[2]

[1]College of Information Engineering, Xidian University, Xi'an, 710071, China
[2]Department of Electronic and Communication Engineering, Beijing Electronic Science and Technology Institute, Beijing, 100070, China
[3]Department of Cyberspace Security, Beijing Electronic Science and Technology Institute, Beijing, 100070, China
*Corresponding Author: Wanqi Wei. Email: cug_jason@126.com

Received: 15 November 2022; Accepted: 28 February 2023

Abstract: As the development of the modern economy is increasingly inseparable from credit support, the traditional credit investigation mode has yet to meet this demand. Because of the difficulties in conventional credit data sharing among credit investigation agencies, poor data portability, and centralized supervision, this paper proposes a data-sharing scheme for credit investigation agencies based on a double blockchain. Given the problems such as difficult data sharing, difficult recovery of damaged data, and accessible data leakage between institutions and users with non-traditional credit investigation data other than credit, this paper proposes a data-sharing scheme for credit investigation subjects based on the digital envelope. Based on the above two solutions, this paper designs a double blockchain credit data-sharing platform based on the "public chain + alliance chain" from credit investigation agencies' and visiting subjects' perspectives. The sharing platform uses the alliance chain as the management chain to solve the problem of complex data sharing between credit bureaus and centralized supervision, uses the public chain as the use chain to solve the problem of complex data sharing between the access subject and the credit bureaus, uses the interplanetary file system and digital envelope and other technologies to solve the problem of difficult recovery of damaged data, data leakage, and other issues. After the upload test, the average upload speed reaches 80.6 M/s. The average download speed of the system is 88.7 M/s after the download test. The multi-thread stress test tests the linkage port on the system package, and the average response time for the hypertext transfer protocol (HTTP) is 0.6 ms. The system performance and security analysis show that the sharing platform can provide safe and reliable credit-sharing services for organizations and users and high working efficiency.

Keywords: Dual blockchain; credit data sharing; truffle framework; digital envelope; ipfs

1 Introduction

In recent years, with the rapid development of the economy, the construction of social credit system has attracted more and more attention, and the credit scenarios and credit products derived from it have also increased sharply. Driven by computer technology and Internet technology, various countries have established their credit investigation platforms. In China, the credit investigation Center of the People's Bank of China is the most representative one [1], establishing China's largest personal user credit investigation database.

The development of the modern economic system is increasingly dependent on credit support, and the traditional credit investigation mode has yet to meet this demand. Therefore, many scholars have researched the sharing and supervision of credit investigation data. Furthermore, with the rapid development of the digital cryptocurrency represented by Bitcoin, blockchain, an emerging technology, has gradually entered people's vision and received significant attention.

Due to its advantages of decentralization and the impossibility of tampering [2], blockchain provides specific new ideas for the operation and development of the credit investigation industry, which may make up for the shortcomings of traditional credit investigation platforms and strengthen the protection and management of relevant data. Building a new credit data-sharing platform based on blockchain technology can effectively solve the current international credit shortage problem and reduce the risks and costs of data sharing [3].

Domestic research on credit investigation started relatively late. Still, in recent years, as the potential of blockchain has been continuously tapped, domestic scholars are also trying to apply blockchain technology to the credit investigation and sharing field. Li et al. [4] analyzed the existing problems in the Chinese credit investigation industry and the existing experiences of foreign credit investigation modes. They put forward the viewpoints of constructing Chinese credit investigation mode according to the technological advantages of blockchain. Ju et al. [5] proposed a multi-source data-sharing framework based on the blockchain based on the big data credit investigation platform of multi-source heterogeneous data fusion. Still, the framework did not give a corresponding description of data security. Wang et al. [6] proposed a safe and high-performance sharing and multi-party computing model, which enables users to control data independently while ensuring the security of data calculation and sharing. Guo et al. [7] proposed the trading mode of data-sharing under different levels of supervision from the perspective of supervision. Chen et al. [8] proposed a credit investigation system model based on the blockchain storage structure and decentralized features, aiming at the problems of data storage being too centralized and easy to forge. Chen et al. [9] proposed a privacy protection scheme based on personal credit investigation by combining blockchain smart contracts with homophobic encryption technology. Shen et al. [10] proposed an SVM (support vector machine) training mechanism for securely sharing credit investigation data to ensure data privacy and security. Ding et al. [11] started by analyzing the shortcomings of the traditional personal credit investigation system and built an individual credit scoring model from the perspective of blockchain by using the analytic hierarchy process. Yuan et al. [12] combined blockchain smart contract technology to create a multi-party trusted computing framework for enterprise credit data, providing expansion space for future efficient and trusted data exchange. Zhang et al. [13] proposed an SVM training mechanism based on data security sharing. Based on the construction of the data security sharing model, this method adopted the method of the data encryption operation, which ensured the security of credit data to the maximum extent.

Compared with China, foreign research on credit investigation started earlier and was more often applied to commercial examples [14]. In addition, most foreign scholars also used blockchain technology in other sharing fields. Zyskind et al. [15] proposed a decentralized personal data protection system to achieve fine-grained access. The system model gives the strategy and description of fine-grained access control and suggests that this model can be applied to more mature distributed trusted computing platforms after extension. Zyskind et al. [16] designed a distributed computing framework based on storing and managing separated data, which can better ensure data security. They store data through a distributed hash table (DHT) [17,18], which makes data open and transparent and protects data privacy, thus ensuring data security. Azaria et al. [19] designed a medical data-sharing platform based on smart contracts and access control to consider large amounts of information, low sharing efficiency, and strong privacy of medical data to manage and integrate the permission of the medical data information. Chowdhury et al. [20] designed a blockchain technology data-sharing framework applied in the field of notarization, using an alliance chain to confirm the real identity of data users and increasing the durability and volume of data through off-chain storage. At the same time, through the audit of personal data traceability to achieve the security protection of data information. Feng [21] designed an alliance chain for the failure of effective information-sharing enterprises. Qiao et al. [22] designed a credit rating system that effectively guaranteed personal privacy. Kairaldeen et al. [23] designed an intelligent home network architecture that virtually ensures data integrity and security while ensuring the validity of blockchain transactions. Chen et al. [24] proposed a method to measure the user's credit degree by obtaining data before it is stored on the blockchain and builing a credit rating system based on the analytic hierarchy process. Basu et al. [25] effectively integrated blockchain technology with a multi-institutional business network carbon supply chain through a unique architecture, improving supply chain transparency and enabling all parties to obtain reliable carbon output information. Kairaldeen et al. [26] efficiently optimized user authentication times using efficient user signature encryption algorithms in a peer-to-peer decentralized network blockchain network. Zhou et al. [27] designed a new spectrum trading framework based on Blockchain consisting of an access, distribution, and core layer. They proposed a spectrum trading matching scheme that maximizes user benefits, which solves the problems of high delay and high resource consumption when introducing traditional blockchain technology into spectrum management. Sun et al. [28] designed a 5G message log credit management and verification system based on blockchain, which realized the decentralization, trust, and tamper-proof capabilities of rich communication suite logs, enabling users to track and authenticate rich communication suite logs. Liu et al. [29] designed and implemented a financial management platform based on integrating blockchain and supply chain, which realized the automatic flow of monetary funds and supplied chain finance process supervision. Ren et al. [30] proposed an anti-fraud protection approach to blockchain technology based on a gradient lifting decision tree that addresses the market's vulnerability to parasitic credit card fraudulent transactions accompanying economic growth.

By combing domestic and foreign research on credit sharing, it is found that although the current scheme solves the security and trust problems existing in credit sharing by utilizing the characteristics of decentralization and de-trust of blockchain technology, However, there are still some other problems :(1) Digital credit data is stored in the form of the bit stream in the centralized database, and the data is easy to be tampered with; (2) There are problems of isolated credit investigation data and complex data sharing among major credit investigation agencies. Centralized storage and its supervision mode need to be improved; (3) It is also difficult to share data among institutions with non-traditional credit investigation data other than credit. Meanwhile, the data these institutions store is easy to leak and hard to recover after data damage.

This paper proposes the following solutions to solve the above problems based on critical technologies such as the truffle framework, interplanetary file system, and digital envelope.

1) A data-sharing scheme for credit investigation agencies based on double blockchain is proposed to solve problems such as difficulty in sharing traditional credit data among credit investigation agencies, poor data portability, and centralization of supervision.

2) To solve the problems of difficult data sharing, difficult recovery of damaged data, and accessible data leakage between institutions and users with non-traditional credit investigation data other than credit, a data sharing scheme of credit investigation subject based on the digital envelope is proposed.

3) As for the problems existing in traditional credit investigation platforms, blockchain, IPFS, digital envelopes, and other technologies are used to ensure the safe sharing of a credit investigation.

4) Based on the above schemes and technologies, a double blockchain mode credit data-sharing platform is designed and implemented from the perspective of visiting subjects and credit investigation agencies. This effectively makes up for the shortcomings of traditional credit investigation platforms.

2 Related Technologies

Here, the technology used in this paper will be described from four aspects: blockchain technology, truffle framework, interplanetary file system, and digital envelope.

2.1 Blockchain Technology

The blockchain infrastructure model can be divided into six layers, including a data layer, network layer, consensus layer, incentive layer, contract layer, and application layer from bottom to top [2], as shown in Fig. 1.

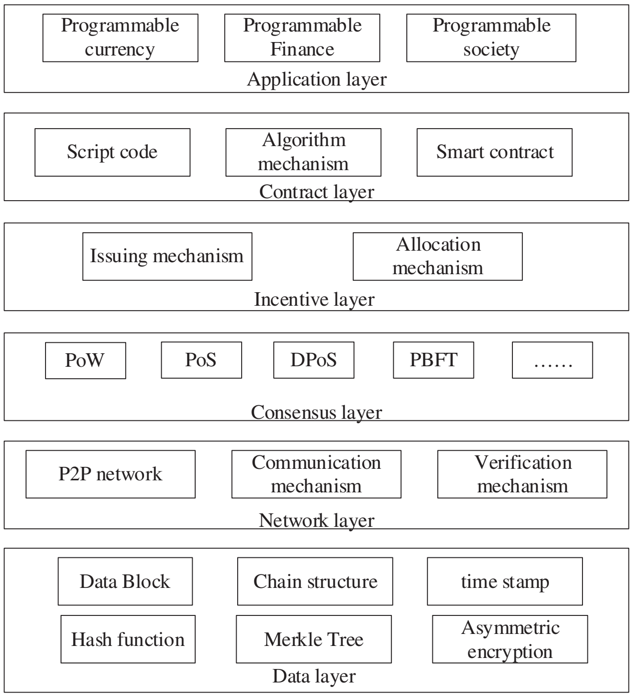


Figure 1: Blockchain infrastructure model

The data layer is the lowest in the blockchain infrastructure model. The layer encapsulates the underlying data block, related data encryption, Merkle Tree, and timestamp technology. The network layer includes a point-to-point network mechanism, a data transmission mechanism, and a data verification mechanism. The consensus layer solves the problem of making the system reach a consensus when faulty nodes are under the premise of reliable network communication. The incentive layer is an incentive mechanism to ensure that the accounting node can add blocks to the chain. It provides specific incentive measures to encourage nodes to actively participate in the security verification and maintenance of the blockchain. The contract layer encapsulates various basic codes, algorithmic mechanisms, and smart contracts, giving the blockchain programmable properties. Finally, the application layer encapsulates multiple application scenarios and cases of blockchain.

2.2 *Truffle Framework*

Truffle framework [31] provides a whole set of tools for compiling, deploying, and debugging smart contracts, which significantly simplifies the development process of decentralized applications and has the following advantages:

(1) The framework has a built-in Solidity compiler to automate the compilation of contracts written in the Solidity language and link to them during the compilation process. Once compiled, the framework will deploy to the corresponding blockchain network based on the configuration information.

(2) The framework supports automated testing, framework-related dependency libraries are managed through EthPM and NPM, and scripted network management supports all blockchain networks.

(3) To facilitate development and debugging, the framework also supports the console interaction mode, which can directly interact with the contract at the command line and output the caller results.

2.3 *Interplanetary File System*

The interplanetary file system [32] (IPFS) is a protocol and peer-to-peer network that stores and shares data in a distributed file system. The system absorbs some ideas of the existing peer-to-peer network protocols and systems, including DHT, BitTorrent, etc. It integrates the concepts and technologies of these systems to develop the system into a comprehensive file system that incorporates the excellent features of the above systems.

IPFS is also a distributed hypermedia transfer protocol, which no longer relies on the backbone network and centralized servers and connects all the devices in the network through a file system so that the files stored on the system can be quickly accessed anywhere in the world. IPFS uses content-based addressing instead of HTTP's traditional domain name-based addressing. The user does not need to care about the server's location or worry about the file store's name and path. IPFS also uses a general-purpose infrastructure with few storage limitations. Large files are split into smaller chunks that can be downloaded from multiple servers simultaneously. IPFS network is not a fixed, fine-grained, distributed network. It can adapt well to the content distribution network requirements and share data.

2.4 *Digital Envelope*

The digital envelope (DE) is a way to distribute symmetric keys through asymmetric encryption [33]. DE adopts secure encryption technology to ensure if and only if the specified recipient has permission to decrypt data information and read the content of communication data. DE not only inherits the advantages of a symmetric encryption algorithm but also incorporates the advantages of an asymmetric encryption algorithm, such as better security and convenient key management. Fig. 2 describes the specific process of encrypting and decrypting data information using DE.

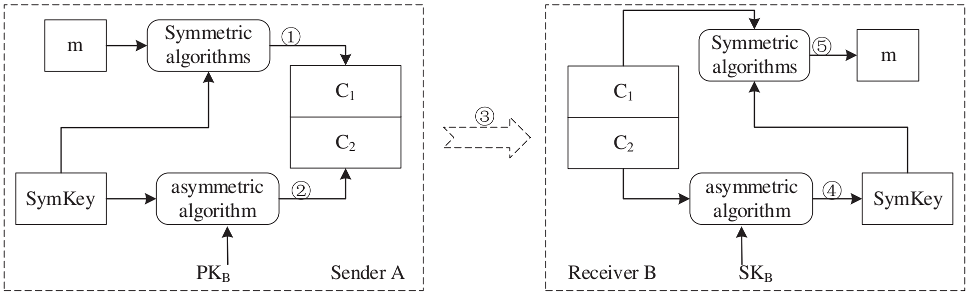


Figure 2: DE encryption and decryption flow chart

3 System Scheme Design and Overall Structure

This chapter will detail the system's consensus design, scheme design, overall architecture, and contractual framework. Among them, the scheme design includes two models. The data-sharing model based on credit investigation agencies proposed in Section 3.2 mainly aims at problems such as difficulties in sharing traditional credit data among credit investigation agencies, poor data portability, and centralized supervision. The data-sharing model based on the digital envelope proposed in Section 3.3 mainly aims at such problems as difficult data-sharing, difficult recovery of damaged data, and accessible data leakage among institutions and users with non-traditional credit investigation data other than credit.

3.1 IDPoS Consensus Design

Delegated proof of stake (DPoS) consensus mechanism [34] is a consensus algorithm similar to the voting election. Compared with the proof of work (PoW) algorithm that solves mathematical problems based on its calculation power and obtains the node accounting right, DPoS solves the problem of a large amount of energy consumption of PoW and improves work efficiency. For the proof of stake (PoS) algorithm that solves the same mathematical problem and obtains the bookkeeping right through the shares held by the nodes, DPoS takes a much shorter time to reach a consensus than PoS and solves the problem of unfair bookkeeping caused by the uneven distribution of shares of PoS.

Based on the reference of commercially distributed design blockchain operating system and Byzantine fault-tolerant algorithm [35] and considering the actual scenarios of credit investigation, this paper suggests improvements to the DPoS consensus mechanism. In addition, it proposes improved delegated proof of stake (IDPoS).

Firstly, IDPoS ranks the credit rating of credit investigation agencies, according to the Credit Center of the People's Bank of China. Secondly, select 33 super and 200 standby nodes according to their credit scores. Then choose two nodes from the 33 super nodes, one as the data supervision node and the other as the data link node; Finally, when data needs to be stored or shared, the corresponding node becomes the outgoing node and generates blocks to broadcast to the other 32 nodes. In addition, ten blocks are generated in each round to ensure sufficient validity. The block is valid when at least 23 other nodes pass the verification. The IDPoS consensus is shown in Fig. 3.

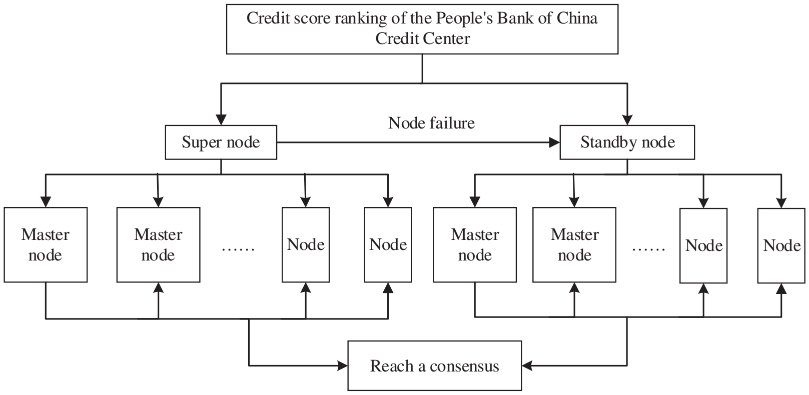


Figure 3: IDPoS consensus process

If a super node fails, you can set it again from the standby node and select it again at intervals. Furthermore, since the selection of nodes depends on the level of credit scores, credit investigation agencies can improve the ranking of credit scores by improving the quality and quantity of data to promote the realization and sharing of consensus.

3.2 Data Sharing Model Based on Credit Investigation Agencies

This section aims at the problems such as the difficulty of traditional credit data-sharing among credit investigation agencies, poor data portability, centralized supervision, etc., combined with blockchain technology, and based on the shared transaction model designed in references [35,36], proposes a data sharing model based on credit investigation agencies. Through the double-link setting, the data access of participants with different identities is controlled. The alliance chain is used as the management chain to solve the problem of difficult data sharing and centralized supervision among credit investigation agencies. The public chain is used as the use chain to solve the problem of complex data sharing between the access subject and the credit investigation agency. It not only ensures the diversity and traceability of shared data sources but also protects the personal privacy of credit investigation users and the interests of credit investigation agencies.

This model divides all subjects into four categories: credit reporting agency (CRA), credit provider (CP) and, credit management agency (CMA), credit interview agency (CIA). Among them, CRA plays the role of the data link, which stores the relevant data of credit investigation users provided by CP. CP plays the part of the data provider, responsible for collecting and collating credit user data; CMA plays the role of data regulator, which is responsible for the appraisal of CIA data access authority and the search and feedback of credit data. Finally, the CIA is an individual or enterprise that needs credit user data. CRA and CMA are elected through the IDPoS consensus mechanism, and every CP can become a CRA or CMA through an election. Fig. 4 shows the data-sharing model based on credit investigation agencies.

Under this sharing model, different credit investigation agencies share credit investigation data through the "management chain" network, eliminating the trust problem between agencies. In addition, the "use chain" network is used to realize data sharing between the credit investigation agency and the visiting subject to facilitate the credit evaluation of individuals and enterprises.

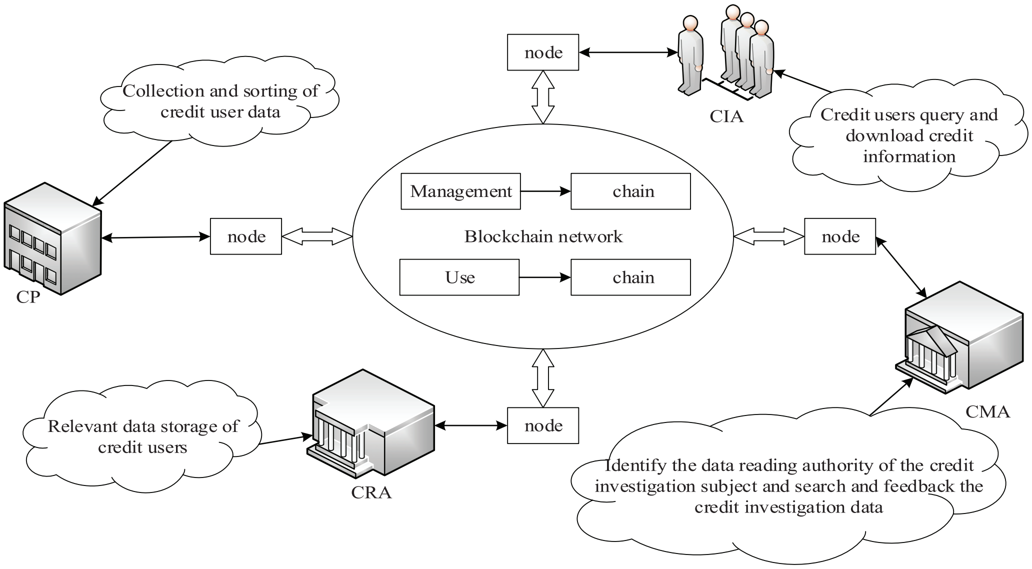

node
CIA
Collection and sorting of credit user data
Credit users query and download credit information
Management
chain
Blockchain network
Use
chain
CP
node
node
CMA
Relevant data storage of credit users
CRA
node
Identify the data reading authority of the credit investigation subject and search and feedback the credit investigation data

Figure 4: Data sharing model based on the credit bureau

3.3 Data Sharing Model of Credit Investigation Subject Based on Digital Envelope

This section, aiming at the problems of data sharing difficulty, data damage difficulty recovery, and data leakage among institutions and users with non-traditional credit investigation data other than credit, combines blockchain, DE, and IPFS technologies and based on the data-sharing model designed in reference [35–37], a credit investigation subject data sharing model based on the DE is proposed.

The main subjects of this sharing model are credit investigation agencies, users, digital envelope encryption agencies (DEEA), and IPFS storage institutions (IPFSSI). IPFSSI, as an offline database, saves the credit information of all users. DEEA is the encryption agency responsible for generating and distributing critical pairs. Fig. 5 shows the data-sharing model of credit investigation subjects based in DE.

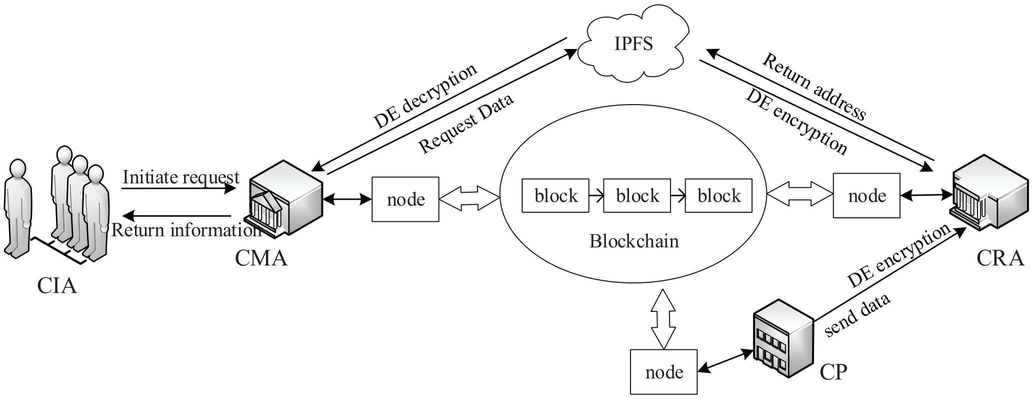


Figure 5: Data sharing model of credit information subject based on DE

Under this sharing model, CRA encrypts the credit investigation data collected by CP through DEEA and uploads it to IPFSSI. IPFSSI returns the address information to the CRA and uploads it to the blockchain network through CRA. When the CIA has a need, it sends an access request to CMA, which retrieves the data information address associated with the user Hash of the blockchain network and requests IPFSSI to download the data, which is then decrypted by DEEA and returned to the CIA, thus completing the process of data sharing.

3.4 Overall System Framework

The design of the credit data-sharing platform involves the data interaction of multiple business organizations, and trust and data security among the organizations are the priority issues. Based on this, this paper designs a credit data-sharing platform based on double blockchain based on the scheme proposed in Sections 3.2 and 3.3. The platform system is composed of two blockchain networks, “public chain + alliance chain,” in which the public chain network serves as the “use chain” of the CIA, and the alliance chain serves as the “management chain” of other credit investigation agencies. Fig. 6 shows the overall framework of the credit data-sharing platform based on a double blockchain.

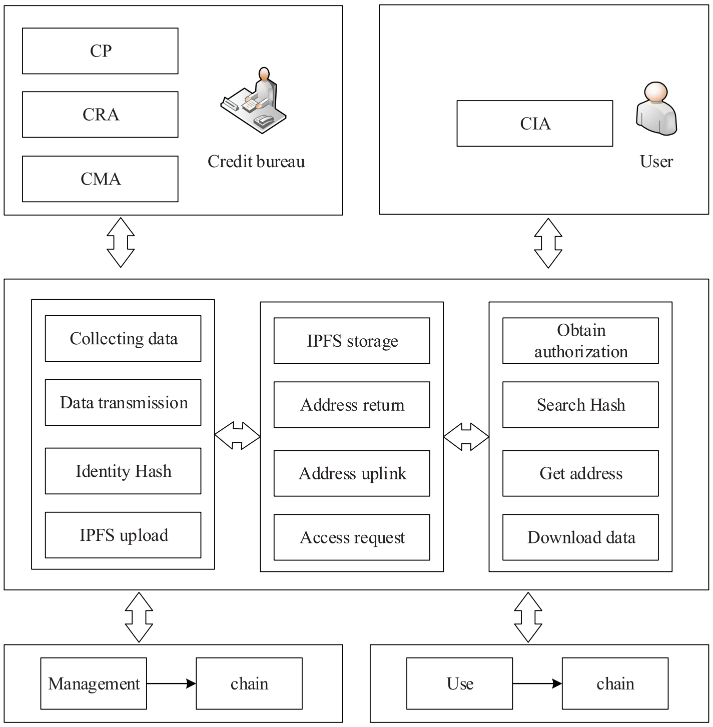


Figure 6: The overall framework of the dual-blockchain credit data-sharing platform

The CP in Fig. 6 can be a traditional financial credit institution such as a bank or an Internet financial institution capable of generating credit behavior like Jingdong, Taobao, and Alipay. The CP sends the collected information to the CRA. After receiving the data, the CRA encrypts the data into blocks, uploads the block addresses to the IPFS, and uploads the block addresses to the “management chain” using the identity Hash. When the CIA needs to apply for credit investigation, it sends a request to CMA through the “use chain.” After receiving the request, CMA searches the identity Hash through the “management chain” to obtain the address of the data block of the information of the credit user, and finally downloads the data from IPFS through the received data block address and returns it to the CIA.

3.5 System Contract Framework

Considering the actual scenario of credit investigation, the corresponding contract is designed in this paper. All users in the "management chain" and "use chain" must abide by the contract rules, all participants' information is safe, and the contract can be automatically executed.

The contractual framework of this system is shown in Fig. 7. The framework mainly includes a credit management contract (CMC) and a credit use contract (CUC). The CMC also consists of an identity management contract (IMC), a data transfer contract (DTC), and data on-chain contract (DOC), a data control contract (DCC); CUC also includes a data query contract (DQC), and a data sharing contract (DSC).

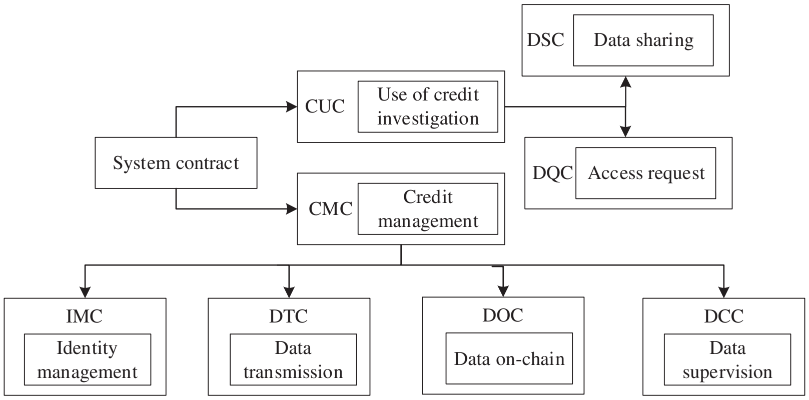


Figure 7: System contract framework

(1) DQC stipulates that the CIA can initiate an access request to CMA and return corresponding data content according to CIA identity. In addition, DSC specifies how CRA and IPFSSI, IPFFSI and CMA, and CIA and CMA interact in data sharing to ensure data security.

(2) IMC stipulates which subjects are oriented to the credit data sharing platform based on double blockchain and provides different services for different subjects; DTC ensures that data will not be stolen during the upload or download process. DOC ensures that data stored on an off-chain database is associated with the identity of the user digest in the blockchain network; DSC supervises all the subjects in the system and eliminates the malicious nodes to ensure the system's regular operation.

4 System Prototype Design

This section describes the detailed implementation of the system prototype.

4.1 Identity Generation and Permission Management

To better manage the credit data-sharing platform and improve the platform's efficiency in providing services to users and organizations, the system uses the super management node to generate identities for other organizations and users, and based on this, the role-based authority control strategy is designed. This strategy has four types of nodes: CRA, CMA, CIA, and CP. First, different permissions are granted to these four types of nodes, respectively, forming a credit node permission table (CNPT). Then, the system invokes IMC according to the identity role of the credit node and searches for the credit node permission granted by CNPT.

4.2 Data Processing and Data Storage

Data processing is mainly for CP (credit provider). CP divides the credit behaviors generated by users into three categories, namely delinquent behaviors, non-overdue behaviors, and temporary non-overdue behaviors, and assigns them different marker influence bits. The marker influence bits represent the event records under the three categories of behaviors with numbers. After the CP completes the data processing, it sends the data to the CRA (credit reporting agency) for data on-chain and storage. CRA in received CP data immediately after the user identity is extracted from data and information, and according to the user's identity in the chain of blocks in the network, users search the user identity hash table (UIHT) of the hash value, store the data to the user of the hash IPFSSI (IPFS storage institution), then IPFSSI address information to the CRA to return to the user data, CRA will return address information Chain. The system searches the user hash in UIHT through the user identity to obtain the corresponding off-link database address of the user and calls DOC (Data On-chain Contract) to complete the data linking and storage.

4.3 Data Encryption and Data Decryption

Data encryption and decryption mainly occur in the interaction between CP and CRA, CRA and IPFSSI, and CMA and IPFSSI. The system uses DE technology and invokes DTC to complete the encryption and decryption of credit investigation data. Considering the amount of data in the credit investigation business and the actual service scenario, the system uses the SM4 algorithm to encrypt the credit investigation data symmetrically and the SM2 algorithm to encrypt the symmetric key. It not only ensures the integrity and security of credit-sharing data but also improves the working efficiency of the system.

4.4 Data Query and Data Sharing

When the CIA needs access, the CIA sends the requested information to the CMA through the "use chain" network. After receiving the requested information, the CMA will analyze the information to obtain information about the CIA and the information of the credit user. After determining the authority of the identity group to which the CIA belongs, CMA will retrieve the identity Hash of the credit user from the "management chain" network. When the identity Hash is retrieved, the address value of the IPFS data block will be returned. By using the obtained address value and calling DSC, CMA will download the user's data information from IPFSSI. Finally, the corresponding data information is returned according to the CIA authority to complete the data query and sharing.

5 System-Specific Implementation

Based on the model proposed in Sections 3.2 and 3.3, this paper designs and implements a credit data-sharing platform based on a double blockchain. The platform will be divided into blockchain intelligent contract development, off-chain IPFS database construction, decentralization application (DAPP) design, and DE technology-based data-sharing.

(1) Blockchain Smart Contract

This paper uses the truffle framework to build a blockchain platform based on Ethereum. We use Solidity language to develop CMC, CUC, and other contracts and complete contracts' compilation, operation, and deployment through the truffle framework. The platform uses a *Puppeth* program to generate the initial block and its related information *Creation.json*. The alliance chain super management node is created on this basis, and other management nodes and common nodes are created through the IDPoS consensus mechanism. Through the use of a go-Ethereum client to achieve the Ethereum alliance chain and public chain synchronization, successful contract invocation.

(2) Off-chain IPFS Database

Aiming to establish an off-chain IPFS database, this paper uses a *go-ipfs* client to complete the establishment of a local off-chain database. Privatize the cluster by setting the environment variable *LIBP2P_FORCE_PNET* to 1, and generate the group-shared vital *swarm.key* simultaneously to restrict access to the database to only the institution or user that obtained the shared key.

(3) DAPP Design

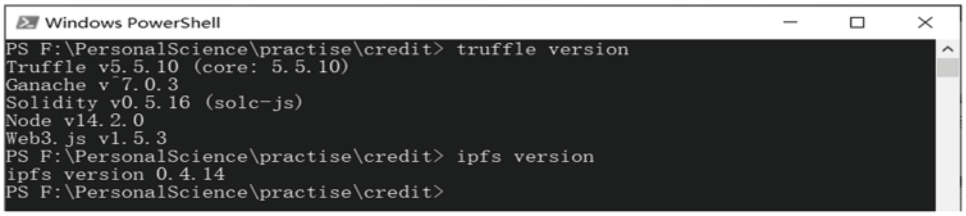
For the design of DAPP, based on the truffle framework, this paper uses *Node.js* Web framework Express to realize the development of the system application layer, uses *Web3.js* to recognize the call of various smart contracts in the system, and combines *js-ipfs-api* to learn the interface call of IPFS database.

(4) Data Sharing Based on DE Technology

In this paper, DE technology is used to ensure the security and privacy of data in the process of data sharing and transmission. Considering the actual scenario of the credit investigation business, the SM4 algorithm is used to encrypt the credit investigation data symmetrically, and the SM2 algorithm is used to encrypt the symmetric key, ensuring the security of the data but also improving the working efficiency of the system.

6 System Performance Test and Safety Analysis

The experimental environment of the system designed in this paper is a Windows 10 system, its version number is 19042.1645, and the system processor is Intel(R) Core(TM) i5-7200U CPU @2.50 GHz 2.70 GHz with 8.00 GB RAM. The environment and IPFS configuration information about the truffle framework are shown in Fig. 8.



```
PS F:\PersonalScience\practise\credit> truffle version
Truffle v5.5.10 (core: 5.5.10)
Ganache v^7.0.3
Solidity v0.5.16 (solc-js)
Node v14.2.0
Web3.js v1.5.3
PS F:\PersonalScience\practise\credit> ipfs version
ipfs version 0.4.14
PS F:\PersonalScience\practise\credit>
```

Figure 8: Truffle framework environment configuration and IPFS configuration information

6.1 System Main Function Test

This section tests the main functions of the system. Therefore, only the data upload function of the system is tested here. For example, assume that there are two institutions, A and B, and the specific process of system data uploading is shown in Fig. 9.

Firstly, add the blockchain addresses of institutions A and B under the authority of the super administrator, and authorize institution A as CP and institution B as CRA. Secondly, when agency A obtains the authorization to become CP, it can send the collected data information to Agency B as a CRA. Similarly, authorized Agency B can upload data information to IPFSSI after receiving it.

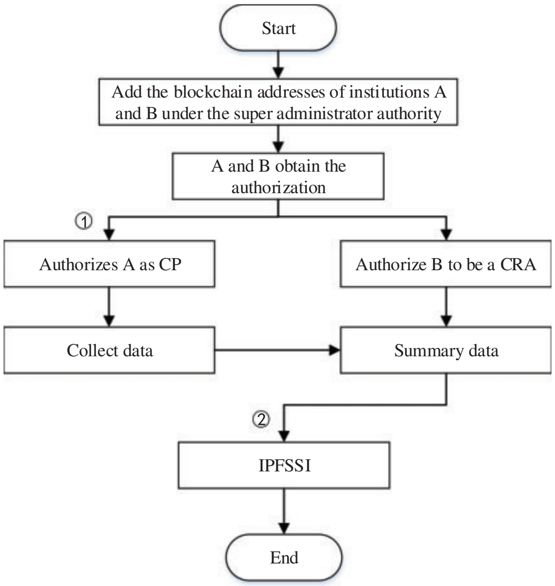
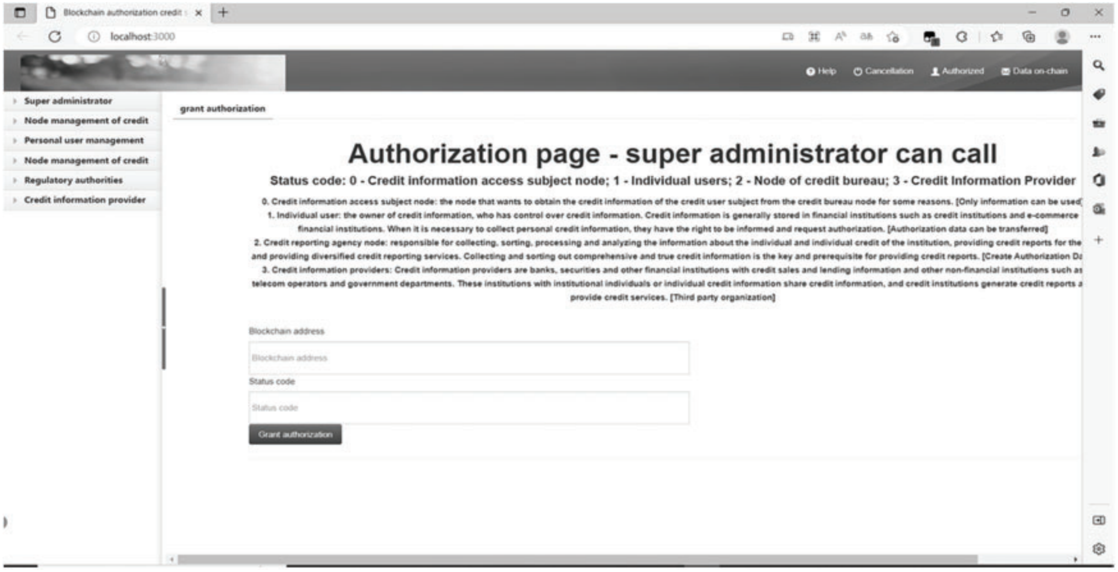

Start
Add the blockchain addresses of institutions A and B under the super administrator authority
A and B obtain the authorization
①
Authorizes A as CP
Authorize B to be a CRA
Collect data
Summary data
②
IPFSSI
End

Figure 9: Procedure for uploading system data

As mentioned above, the specific data upload process in Fig. 9 mainly involves two steps. First, the system authorization interface corresponding to Step 1 (as shown by ① in Fig. 9) is shown in Fig. 10, which shows that the super administrator authorizes organization A as CP. The system upload interface corresponding to Step 2 (as shown by ② in Fig. 9) is shown in Fig. 11, indicating that organization B, as a CRA, uploads data information to IPFSSI.



Authorization page - super administrator can call

Status code: 0 - Credit information access subject node; 1 - Individual users; 2 - Node of credit bureau; 3 - Credit Information Provider

0. Credit information access subject node: the node that wants to obtain the credit information of the credit user subject from the credit bureau node for some reasons. [Only information can be used

1. Individual user: the owner of credit information, who has control over credit information. Credit information is generally stored in financial institutions such as credit institutions and e-commerce financial institutions. When it is necessary to collect personal credit information, they have the right to be informed and request authorization. [Authorization data can be transferred]

2. Credit reporting agency node: responsible for collecting, sorting, processing and analyzing the information about the individual and individual credit of the institution, providing credit reports for the and providing diversified credit reporting services. Collecting and sorting out comprehensive and true credit information is the key and prerequisite for providing credit reports. [Create Authorization Da

3. Credit information providers: Credit information providers are banks, securities and other financial institutions with credit sales and lending information and other non-financial institutions such as telecom operators and government departments. These institutions with institutional individuals or individual credit information share credit information, and credit institutions generate credit reports a provide credit services. [Third party organization]

Blockchain address

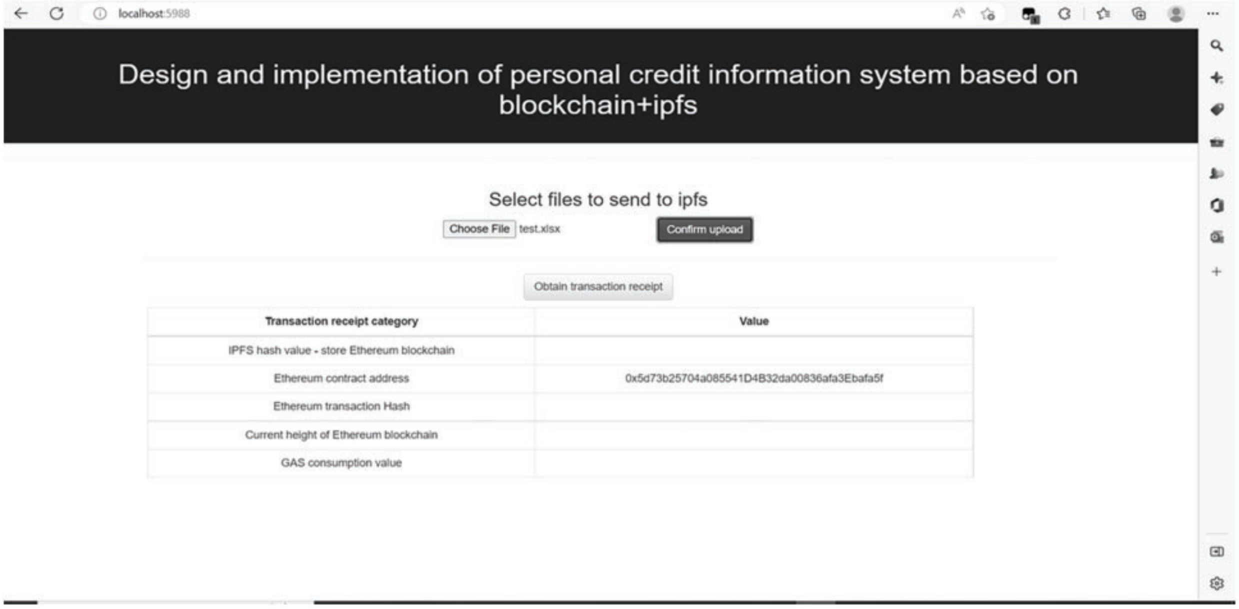
Blockchain address

Status code

Status code

Grant authorization

Figure 10: CP obtains authorization



Design and implementation of personal credit information system based on blockchain+ipfs

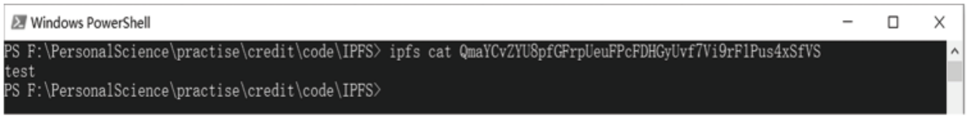
Select files to send to ipfs

test.xlsx

Transaction receipt category	Value
IPFS hash value - store Ethereum blockchain	
Ethereum contract address	0x5d73b25704a085541D4B32da00836afa3Ebafa5f
Ethereum transaction Hash	
Current height of Ethereum blockchain	
GAS consumption value	

Figure 11: CRA uploads data information to IPFS

To verify whether Organization B, as a CRA, has successfully uploaded data information to IPFSSI, open the Powershell window in the project folder directory and run the IPFS file view command to query the uploaded files. Fig. 12 shows the query results, verifying that the CRA has successfully uploaded the data file and that the uploaded file is consistent with the file shown in Fig. 11.



```
PS F:\PersonalScience\practise\credit\code\IPFS> ipfs cat QmaYCvZYU8pfGFrpUeuFPcFDHGyUvf7Vi9rF1Pus4xSfVS
test
PS F:\PersonalScience\practise\credit\code\IPFS>
```

Figure 12: Verify that the CRA successfully uploaded the data information

6.2 *System Function Analysis*

This section makes a functional analysis of the designed credit data-sharing platform based on double blockchain. It compares it with other blockchain-sharing schemes from the aspects of blockchain type, consensus mechanism, shared data management, etc. The results are shown in Table 1.

The scheme proposed by reference [7] in Table 1 only provides an idea for industry data-sharing. However, it still needs to be realized, and there are still some areas for improvement in data management. Although the decentralized credit information system model proposed in the literature [8] prevents data from being tampered with, it is implemented at the expense of system performance. Although literature [15] has achieved the off-chain management of data, it cannot guarantee security in data-sharing. Literature [38] only discusses the application of blockchain technology in the credit investigation industry without further exploration. Literature [19] has realized a blockchain system oriented to the medical field, but adopting PoW consensus causes the system to consume a lot of resources. Compared with the literature [19], the literature [39] uses DPoS consensus to solve the problem of system resource consumption but does not solve the problem of recovery after data damage.

Table 1: Comparison table of shared platform functions

Scheme	Alliance chain + public chain	Shared areas	Consensus mechanism	IPFS	DE
Literature [7]	No	Credit investigation	PBFT	No	No
Literature [8]	No	Mobile app	—	No	No
Literature [15]	No	—	—	No	No
Literature [19]	No	Medical care	PoW	No	No
Literature [38]	No	Credit investigation	—	No	No
Literature [39]	No	Medical care	DPoS+VSF	No	No
This paper	Yes	Credit investigation	IDPoS	Yes	Yes

To sum up, the above documents have realized the blockchain systems facing different fields. Although these systems ensure the security of the data by utilizing the characteristics of blockchain technology, they cannot realize the data recovery when the credit investigation data is damaged, nor can they ensure the security in the transmission and sharing process of the credit investigation data. Based on this, this paper builds a dual blockchain sharing platform of “alliance chain + public chain” based on the actual needs of credit investigation scenarios and improves the DPoS consensus mechanism to a certain extent. In addition to off-chain management of data, IPFS and DE technologies are also applied. Among them, IPFS guarantees that files can be quickly recovered when they are damaged or lost. DE ensures that files will not be stolen or tampered with in the file-sharing process, improving the system’s anti-attack.

6.3 System Performance Analysis

This section analyzes the efficiency of the system. Only the number of signatures in identity generation, the number of verified signatures in identity permission identification, and the number of hash operations are compared with other schemes, and the transaction cost is not taken into account. Details are shown in Table 2.

Table 2: Comparison table of shared platform functions

Scheme	Number of signatures	Number of verifications	Hash operation (get)	Hash operation (storage)
Literature [15]	$O(n)$	$O(n^2)$	$O(n)$	$O(n)$
Literature [16]	$O(n^2)$	$O(n^2)$	$O(n)$	$O(n)$
This paper	$O(n)$	$O(n)$	$O(n)$	$O(n)$

As shown in Table 2, compared with the schemes proposed in the literature [15,16], the plan designed in this paper reduces the number of signatures and the number of hash operations in the process of storage and query. This further indicates that the double blockchain credit sharing platform designed in this paper not only solves the problems existing in the traditional credit investigation system but also considers the working efficiency of the system.

After the upload test, the average upload speed reaches 80.6 M/s. After the download test, the average download speed of the system is 88.7 M/s, as shown in Table 3.

Table 3: System upload and download performance test

File size (byte)	Upload time (ms)	Upload spee (M/s)	Download time (ms)	Download speed (M/s)
671,999,132	9401	68.1	7563	84.7
331,789,963	4756	66.5	3625	87.2
204,125,475	2098	92.7	2064	94.3
138,365,248	1384	95.3	1483	88.9

Jmeter tool was used to conduct a multithreaded stress test on the on-chain interface on the system packaging, and the average HTTP response time was about 0.6 ms, as shown in Fig. 13.

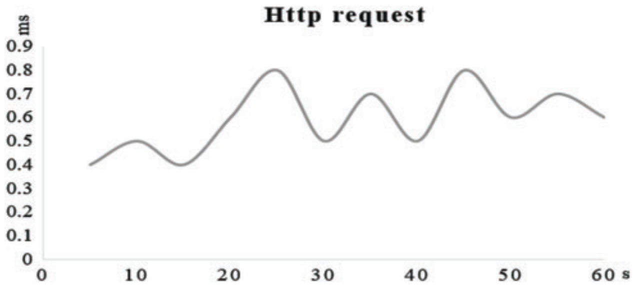


Figure 13: System multithreaded stress test diagram

6.4 System Safety Analysis

To ensure the system's security, the shared system designed in this paper also adopts DE encryption and IPFS technology based on blockchain technology to further ensure the integrity and security of data.

(1) Blockchain Security Analysis

Blockchain technology proposes four technological innovations aimed at the trust and security of transactions. The first is distributed ledger. Unlike traditional centralized accounting schemes, distributed ledger, on the one hand, avoids the possibility that a single account may be controlled or bribed to record false reports. On the other hand, it ensures the security of accounting data because there are enough accounting nodes. The second is asymmetric encryption and authorization technology. Transaction information stored in the blockchain is public, but account-identifying information is highly encrypted and can only be accessed with authorization, thus ensuring data security and personal privacy. The third is the consensus mechanism, which determines a record's validity and provides a means to prevent tampering. The fourth is smart contracts, which automate the enforcement of predefined rules and terms based on trusted but immutable data.

(2) DE Safety Analysis

DE is a technology that utilizes the advantages of symmetric encryption and asymmetric encryption to transmit information securely. Symmetric encryption technology is high-speed in encryption and decryption, which is suitable for processing large amounts of data, but the key management is tedious and easy to leak. However, the asymmetric cryptographic algorithm is ideal for key distribution and control, but the operation speed could be faster and more suitable for processing large amounts of data. Therefore, the combination of symmetric and asymmetric encryption technology can not only deal with large quantities of data but also distribute the management key efficiently. This paper uses the SM4 algorithm to encrypt data and the SM2 algorithm to encrypt the symmetric key, which not only guarantees the security of platform data but also improves the working efficiency of the platform.

(3) IPFS Security Analysis

IPFS is a globally oriented, point-to-point distributed file system. It is a single BitTorrent cluster using git-distributed, decentralized storage, mainly through the Merkle Tree data structure to build the version file system. There is no single point of failure. Nodes do not need to trust each other, so the information in the IPFS network is stored permanently with no 404 error.

7 Conclusion

Currently, the credit evaluation information collected by the credit investigation system managed by the credit investigation centers of the central banks of various countries is mainly the credit data of enterprises or individuals in financial institutions, supplemented by public information about social management. Although the central bank's nationwide coverage of credit reporting users has been enough, the traditional data collection method still needs to be improved. Weak data sharing, confidentiality, and portability have been the standard credit reporting system. The problem in decentralized blockchain technology is very good for solving these problems. This paper designs an "alliance chain + public chain" credit data sharing platform based on blockchain technology, in which the public chain network serves as the "use chain" of the CIA, and the alliance chain serves as the "management chain" between credit investigation agencies. The truffle framework realizes the underlying structure of this platform, and the integrity and security of data are guaranteed by DE encryption and IPFS technology. The proposed IDPoS improves the working efficiency of the system and provides reliable credit-sharing services for organizations and users. At the same time, it also provides some ideas for the government and institutions to build a broader application of the credit investigation platform in the future.

Funding Statement: This research was supported in part by the Advanced and High-level Discipline Construction Fund of Universities in Beijing (No.3201023), in part by the Beijing Electronic Science and Technology Institute of Basic Research Funds Outstanding Master Training Project (No. 328202233), in part by the National First-class Undergraduate Discipline Construction of ”Communication Engineering" and "Electronic Information Engineering," and in part by the National Cryptography Science Foundation of China.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

[1] Credit Information Center of the People's Bank of China, *Basic Knowledge of Credit Information*. http://www.pbccrc.org.cn/zxzx/zxzs/201401/a01d28731de24b1192402cd7889e11a3.shtml

[2] S. T. Guo, R. J. Wang and F. L. Zhang, "Overview of the principle and application of blockchain technology," *Computer Science*, vol. 48, no. 2, pp. 271–281, 2021.

[3] X. F. Huang, L. Xu and Q. Yang, "A blockchain cloud computing electronic forensics model," *Journal of Beijing University of Posts and Telecommunications*, vol. 4, no. 6, pp. 120–124, 2017.

[4] Q. M. Li, F. Dong and S. Dong, "New thoughts on China's credit reporting model," *Credit Reporting*, vol. 35, no. 8, pp. 33–36, 2017.

[5] C. H. Ju, J. B. Zou and X. K. Fu, "Research on the design and application of big data credit reporting platform integrated with blockchain technology," *Computer Science*, vol. 45, no. S2, pp. 522–526 + 552, 2018.

[6] T. Wang, W. P. Ma and W. Luo, "Blockchain-based information sharing and secure multi-party computing model," *Computer Science*, vol. 46, no. 9, pp. 162–168, 2019.

[7] S. X. Guo and Z. Q. Song, "Research on the design and application of the blockchain model for credit reporting," *Journal of Network and Information Security*, vol. 4, no. 4, pp. 63–71, 2018.

[8] C. L. Chen, Y. Shen and H. Yu, "Research on decentralized credit reporting system model," *Computer Technology and Development*, vol. 29, no. 3, pp. 122–126, 2019.

[9] L. Y. Chen, T. X. Rui and G. J. Lv, "Personal credit information privacy protection scheme based on blockchain smart contract," *Computer Engineering*, vol. 46, no. 7, pp. 30–35, 2020.

[10] M. Shen, J. Zhang, L. H. Zhu, G. Xu, K. X. Zhang *et al.,* "SVM training mechanism for credit data security sharing," *Journal of Computer Science*, vol. 44, no. 4, pp. 696–708, 2021.

[11] L. Ding, D. Duan, J. P. Han, Z. Y. Ma and J. L. Mai, "Research on the optimization of personal credit indicator system and information sharing mechanism from the perspective of blockchain," *Credit Research*, vol. 40, no. 5, pp. 1–7, 2022.

[12] J. Yuan, W. Zhang, J. C. Jia and Y. C. Fu, "Multi-party trusted computing framework of enterprise credit data based on blockchain," *Credit Investigation*, vol. 40, no. 12, pp. 58–63, 2022.

[13] P. Zhang and Z. M. Li, "SVM training mechanism analysis based on secure sharing of credit data," *China New Communications*, vol. 24, no. 18, pp. 40–42, 2022.

[14] M. Brown, T. Jappelli and M. Pagano, "Information sharing and credit: Firm-level evidence from transition countries," *Ssrn Electronic Journal*, vol. 18, no. 2, pp. 151–172, 2007.

[15] G. Zyskind, O. Nathan and A. Pentland, "Decentralizing privacy: Using blockchain to protect personal data," in *2015 IEEE Security and Privacy Workshops*, vol. 32, pp. 180–184, 2015.

[16] G. Zyskind, O. Nathan and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *Computer Science*, vol. 21, no. 5, pp. 1–14, 2015.

[17] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in *Revised Papers from the First Int. Workshop on Peer-to-Peer Systems*, Heidelberg, Springer Press, pp. 53–65, 2002.

[18] H. G. Do and W. K. Ng, "Blockchain-based system for secure data storage with private keyword search," in *2017 IEEE 13th World Congress on Services*, Honolulu, USA, pp. 90–93, 2017.

[19] A. Azaria, A. Ekblaw and T. Vieira, "MedRec: Using blockchain for medical data access and permission management," in *2016 2nd Int. Conf. on Open and Big Data (OBD)*, Vienna, Austria, pp. 25–30, 2016.

[20] M. J. Chowdhury, A. Colman and M. A. Kabir, "Blockchain as a notarization service for data sharing with the personal data store," in *2018 17th IEEE Int. Conf. on Trust, Security and Privacy in Computing and Communications*, New York, USA, pp. 1330–1335, 2018.

[21] X. Feng, "Enterprise's credit information sharing model based on consortium blockchain," in *2021 IEEE 9th Int. Conf. on Information, Communication and Networks (ICICN)*, Xi'an, China, pp. 440–444, 2021.

[22] Y. C. Qiao, Q. J. Lan, Z. D. Zhong and C. Q. Ma, "Privacy-preserving credit evaluation system based on blockchain," *Expert Systems with Applications*, vol. 4, no. 7, pp. 110–124, 2022.

[23] A. R. Kairaldeen, N. F. Abdullah and A. Abu-Samah, "Data integrity time optimization of a blockchain IoT smart home network using different consensus and hash algorithms," *Wireless Communications and Mobile Computing*, vol. 3, no. 5, pp. 1–23, 2021.

[24] C. Chen, H. Huang and B. Zhao, "The research of ahp-based credit rating system on a blockchain application," *Electronics*, vol. 12, no. 4, pp. 887, 2023.

[25] P. Basu, P. Deb and A. Singh, "Blockchain and the carbon credit ecosystem: Sustainable management of the supply chain," *Journal of Business Strategy*, vol. 11, no. 6, pp. 19–24, 2023.

[26] A. R. Kairaldeen, N. F. Abdullah and A. Abu-Samah, "Peer-to-peer user identity verification time optimization in IoT blockchain network," *Sensors*, vol. 23, no. 4, pp. 2106, 2023.

[27] Y. Zhou, L. Yu and Z. Jiang, "An improved spectrum trading design based on dynamic credit aggregate-signature blockchain," *IEEE Wireless Communications Letters*, vol. 19, no. 3, pp. 63–71, 2023.

[28] S. Sun, J. Yu and Z. Lu, "5G message log credit management and verification system based on blockchain," in *Human Centered Computing: 7th Int. Conf.*, Bern, Switzerland, pp. 242–251, 2023.

[29] H. Liu, B. Yang and X. Xiong, "A financial management platform based on the integration of blockchain and supply chain," *Sensors*, vol. 23, no. 3, pp. 1497, 2023.

[30] Y. Ren, Y. Ren and H. Tian, "Improving transaction safety via anti-fraud protection based on blockchain," *Connection Science*, vol. 1, no. 1, pp. 1–18, 2023.

[31] H. H. He, "Design and implementation of ownership based traceability anti-counterfeiting system on the blockchain," M.S. dissertation, Zhejiang Gongshang University, China, 2019.

[32] S. Q. Qiao and J. S. Wang, "Data decentralized secure sharing scheme based on threshold agent re-encryption and IPFS," *Journal of Tianjin University of Technology*, vol. 37, no. 3, pp. 45–50 + 57, 2021.

[33] Z. Y. Deng, "Research on digital envelope technology and its application," *Journal of North China Institute of Water Resources and Hydropower*, vol. 12, no. 1, pp. 77–79, 2006.

[34] S. He, X. N. Huang, Q. B. Liu and Y. J. Yang, "Research on improvement of dpos blockchain consensus mechanism," *Computer Application Research*, vol. 38, no. 12, pp. 3551–3557, 2021.

[35] Y. Cheng, "Research on credit information sharing scheme based on blockchain," M.S. dissertation, Chongqing University of Posts and Telecommunications, China, 2020.

[36] J. Q. Zuo and X. J. Zhang, "Design and application of double blockchain electronic archives management System based on information security," *Archives Research*, vol. 11, no. 2, pp. 60–67, 2021.

[37] L. Li, Q. X. Zeng, Y. H. Wen and S. C. Wang, "Data sharing scheme based on blockchain and proxy re-encryption," *Information Network Security*, vol. 20, no. 8, pp. 16–24, 2020.

[38] Q. Wang, S. D. Qing and J. R. Ba, "Discussion on the application of blockchain in the credit information industry," *Telecommunication Network Technology*, vol. 6, no. 6, pp. 44–48, 2017.

[39] T. F. Xue, C. Q. Fu and Z. Wang, "Research on medical data sharing model based on blockchain," *Journal of Automation*, vol. 43, no. 9, pp. 1555–1562, 2017.