Security Encryption Control Method of Trading Platform Information Network Based on Blockchain Technology

Boyu Shan[1], Lihua Song[2,*], Tianhao Gao[3]

{by117@mail.ncut.edu.cn[1], songlihua@ncut.edu.cn[2], 22101110225@mail.ncut.edu.cn[3]}

North China University of Technology, Beijing, China[1]
North China University of Technology, Beijing, China[2]
North China University of Technology, Beijing, China[3]
*corresponding author

Abstract. The conventional encryption control method for information network security of trading platform is mainly based on complex ciphertext. Although the information security is high, it adds a burden to decryption. Therefore, the security encryption control method of trading platform information network based on blockchain technology is designed. Authenticate the information access identity of the trading platform, verify the identity of each visitor, generate an identifier from the verified identity information, and distribute the platform key, so that only visitors who have the key can make a second access, thus ensuring the security of the trading platform information. Based on blockchain technology, the intelligent contract for information network security encryption control of trading platform is deployed, the preset encryption contract terms are executed by computer programming, and the integrity of information network encryption of trading platform is ensured by decentralization, transparency, non-breach, automation, non-tampering and anonymity. The comparison experiment shows that the encryption control effect of this method is better and can be applied to real life.

Keywords: Blockchain technology, Trading platform, Information network, Secure encryption, Control method,

1 Introduction

The trading platform is a third-party trading security platform, and its main function is to ensure the security and integrity of both parties to the transaction. The two parties will move the offline transaction to the online trading platform through a third party to complete the transaction; Online trading is that customers find the products they need in the trading platform and complete the transaction[1-3]. Trading platform information includes platform basic information, trading information, user information, financial institution information, trading security information, trading supervision information and other information. In the trading platform, the accuracy, integrity and security of information are very important, which directly affects the trading experience and interests of users. The platform needs to establish a perfect information management mechanism to ensure the privacy and security of user information[4-6]. At the same time, the platform also needs to publish relevant information in a timely and transparent manner to increase users' trust and satisfaction. With the development of network technology,

CONF-MLA 2024, November 21, Adana, Turkey

DOI 10.4108/eai.21-11-2024.2354640

the information network security of trading platform is threatened, and the problems of single encryption algorithm and low security are difficult to meet the information security requirements of trading platform. The main feature of blockchain technology is decentralization, which does not depend on any central organization or third-party trust[7-8]. Each node has the same rights and responsibilities, and participates in transaction verification and recording together, forming a distributed account book. This decentralized structure avoids the occurrence of a single point of failure and improves the reliability and security of the system. This technology uses cryptography to ensure the security and credibility of the transaction[9-11]. Each block contains certain information, including transaction data, time stamp, chain address and so on, and each block is protected by digital signature and encryption algorithm to ensure its integrity and authenticity. Therefore, this paper uses blockchain technology to design a secure encryption control method for trading platform information network.

2 Design of security encryption control method for trading platform information network based on blockchain technology

2.1 Authentication trading platform information network access identity

In the process of information network identity authentication of trading platform, it includes static password authentication, dynamic password authentication, secret protection problem authentication, image verification code authentication, certificate authentication and so on[12-14]. In this paper, the identity of each visitor is verified, the verified identity information generates an identifier, and the platform key is distributed. Only visitors who have the key can make a second visit, thus ensuring the security of the trading platform information. The authentication process is shown in Table 1 below.

Table 1. Transaction Platform Access Identity Authentication Flow Sheet

Step	Describe
Register an account	Provide user name, password, phone number, and other information on the trading website
Submit ID documents	Submit scanned copies or photos of identity documents to verify their true identity
Verify identity information	Verify the identity documents submitted by users to ensure the authenticity of their identity information
Improve personal information	Identity information verification has been passed, and personal information such as contact address and bank account number has been improved
Waiting for Review	Review the real name authentication materials submitted by users to ensure their authenticity and legality
Certification result notification	After passing the authentication review, the trading website sends a notification of the authentication result to the user; Certification failed, the trading website informs the reason for the failure and provides an opportunity for re certification

As shown in Table 1, in the authentication process of the trading platform, the identity key can only be obtained after the steps of identity document submission, identity information verification, personal information perfection and personal information review, so as to facilitate the next user access[15-17]. Assuming that the visitor's identity is G, CA performs identity authentication, and outputs public parameters to obtain the identity identifier. Identifiers are expressed as:

$$G(\lambda) \rightarrow (GP, aid, uid) \tag{1}$$

In the formula (1), λ is the identity identifier; $G(\lambda)$ is the identity identifier of the visitor; GP is a public parameter; aid is the identity information of the visitor;$uid$is the visitor authority identifier. According to $G(\lambda)$ output the master key and public key, and the expression is:

$$A(GP, aid) \rightarrow (M_{aid}, P_{aid}) \tag{2}$$

In the formula (2), A is the encrypted ciphertext of GP、aid; $M_{aid}$is the master key; P_{aid} is the public key. Perform the key generation process with AA, and input GP、P_{aid}、$G(\lambda)$ and output to the cloud proxy server M_{aid}, get the private key[18] . Convert$aid$to$uid$to generate a decryption key M_{uid}. When M_{uid} and M_{aid}can be converted and get the same secret text, the accuracy of identity authentication and visitor identity information security can be ensured.

2.2 Deploy the intelligent contract of information network security encryption control of trading platform based on blockchain technology.

The transaction reached by the blockchain has a high degree of transparency, but both parties to the transaction are anonymous. This mainly depends on the combination of intelligent contract with zero knowledge proof, ring signature, blind signature and other technologies, and the asymmetric and dense information network of trading platform is adopted to ensure the security of trading platform[19-21]. In this paper, computer programming is used to implement the pre-set intelligent contract terms, and decentralization, transparency and non-breach, automation, non-tampering and anonymity are used to ensure the integrity of information network encryption of trading platform. The operation of smart contracts on the blockchain is shown in Figure 1 below.

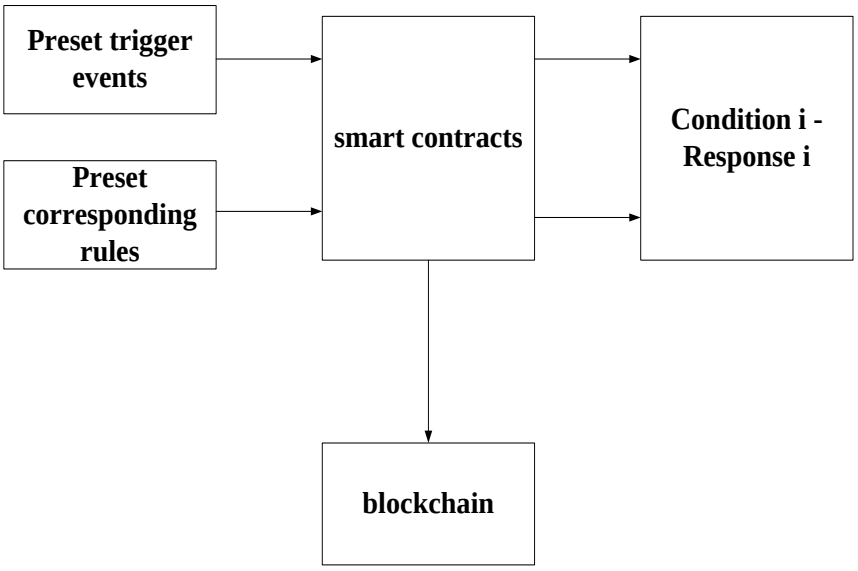

Fig. 1. Schematic diagram of smart contract running on blockchain

As shown in Figure 1, the preset trigger events include events such as authentication failure and authentication failure of trading platform identity information, and the preset corresponding rules include authentication failure → re-authentication until authentication passes; Authentication failed → no access to the trading platform information network; Authentication of the identity identifier succeeded → allow the trading platform information network access[22-23]. If any of the above trigger conditions are met, the smart contract will be automatically executed without external assistance. Under the encryption control of smart contract, the balance, information entropy, confusion and diffusion of ciphertext are analyzed. The calculation formula of ciphertext balance is as follows:

$$\delta = \frac{|K_1 - K_2|}{n} \tag{3}$$

In the formula (3), δ is an index of ciphertext balance, K_1、K_2 are the number of 0 and 1 in the cipher text; n is the sum of the number representing ciphertext 0 and the number representing ciphertext 1. δ is between 0 and 1, the closer δ to 0, the better the balance of ciphertext, indicating that the randomness of ciphertext is good and the encryption control effect is better [24] . The information entropy calculation formula is as follows:

$$H(S) = -\sum_s P(s_i) log_2 P(s_i) \tag{4}$$

In the formula (4), $H(S)$ represents information entropy for the security encryption control of the trading platform information network; S_i is the i-th encrypted character; $P(S_i)$ is the probability of occurrence for each in the secret text S_i. The ciphertext distribution of trading platform network information is mainly based on statistical units. If the ciphertext s_i is the equal probability distribution, the information entropy can get the ideal value of "1", which means that the ciphertext is the most uncertain and the encryption security of ciphertext is higher. Therefore, a secure encryption control method can ensure the security of ciphertext by making the

ciphertext information entropy as close to "1" as possible. The completeness calculation formula is as follows:

$$d_1 = 1 - \frac{1}{sk}\#\{(i,j)a_{ij} = 0\}, \begin{pmatrix} i = 1,2,\ldots s \\ j = 1,2,\ldots,k \end{pmatrix} \quad (5)$$

In the formula (5), d_1 represents every bit of ciphertext or plaintext that is affected by all bits of the input vector, indicating the encryption completeness of the encryption control method; a_{ij} is the input vector; i and j are bits;$s$is an input bit;$k$is the output bit. Simply say, d_1 can reflect the complex encryption relationship between plaintext and key, so that the key information obtained by attackers is confused and the original information cannot be judged. d_1 is in the range of 0-1. The closer d_1 to 1, the higher the completeness of encryption, which can confuse the attack range of attackers and ensure the security of trading platform information. Avalanche effect is expressed as:

$$d_2 = 1 - \frac{1}{s}\sum_{i=1}^{s}\left|\frac{1}{\#X \times k}\sum_{j=1}^{k} 2jb_{ij} - 1\right| \quad (6)$$

In the formula (6), d_2 is the inversion of any bit of ciphertext or plaintext input vector will affect the vector bit, indicating the diffusion characteristics of ciphertext encryption; X is the input vector; b_{ij} represents the input vector is inverted in the i bit and the corresponding output vector is inverted, the difference between the output vectors is j numbers. Simply say, d_2 can reflect the random characteristics of plaintext and key. When every plaintext bit changes, it will have a diffusion effect in the whole ciphertext, making it impossible for attackers to infer the information of the original data from the ciphertext.$d_2$also varies in the range of 0-1. Whend_2≈1, the avalanche effect of encryption control algorithm is good, and the encryption control effect is better.

3 Experiment

In order to verify whether the method designed in this paper meets the requirements of information network security encryption control of trading platform, this paper makes experimental analysis on the above methods. The final experimental results are presented in the form of comparison between the conventional trading platform information network security encryption control method based on memristive neural network, the conventional trading platform information network security encryption control method based on Ethereum and IPFS encryption algorithms, and the trading platform information network security encryption control method designed in this paper based on blockchain technology. The specific experimental preparation process and the final experimental results of encryption control performance are as follows.

3.1 Experimental preparation

This experiment includes coordinator, terminal equipment, host computer and other equipment, and forms an information network with the trading platform. The data is sent to the host computer through UART interface, and the terminal equipment senses the ambient temperature and humidity by sensors, and sends the relevant information to the coordinator through the RF chip. The upper computer is connected with the coordinator and displays the data collected by

the terminal equipment. The information network architecture of the trading platform is shown in Figure 2 below.

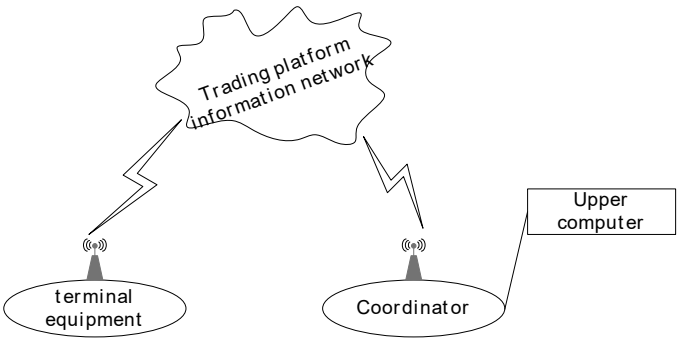

Fig. 2. Information Network Architecture of Trading Platform

As shown in Figure 2, the CPU of the upper computer is AMD Ryzen 2700 x 3.7 GHz, the RAM is 48GB, the operating system is 64-bit Windows 10, and the development environment is IAR Embedded Workbench 8.10.3. In the network architecture, MCU is 8-bit enhanced 8051, Flash is 128KB, RAM is 8KB, and RF chip is CC2591. The application layer of the terminal node adopts encryption contract, and the deployment cost of encryption contract is shown in the following table 2.

Table 2. Deployment Cost Table of Encryption Contract

Function	Caller	Transaction cost	Execution cost	Amount of money
Controller Contract deployment	Mediator	2949305	2193165	$2.70
DataOwnerFiles Contract deployment	DO	2123595	1566639	$1.93
Shared Library deployment	Public	76925	17297	$0.02
addDataOwner()	DO	48166	26894	$0.03
addDataRequester()	DR	151604	129756	$0.16
addMPA()	MPA	69054	47782	$0.06
addOracle()	DOF	57227	35955	$0.04
addFile()	DO	91901	68261	$0.08
setMPAAuthReqCount()	MPA	48295	26703	$0.03
authenticateDR()	MPA	72748	50068	$0.06
reuquestFile()	DR	113550	91190	$0.11
requestResponse()	DOF	32832	11176	$0.01
addOracleResponse()	Oracle	72355	48587	$0.06
submitDROracleRating()	DR	49640	24656	$0.03

As shown in Table 2, the functions with the lowest calling cost are selected in this experiment. The deployment costs of the requestResponse () contract, the Shared contract, the addDataOwner () function, the setMPAAuthReqCount () function and the submitDROracleRating () function are low, and the contract can be deployed by any node. By defining a common data structure, the authentication of MPA to DR is completed. The requestResponse () function handles the access request of the DR file. This function involves fewer parameters and has relatively low running cost, which is more in line with the encryption requirements of the trading platform information network.

3.2 Experimental results

Under the above experimental conditions, this paper randomly selects a variety of trading platform information types, and the ciphertext length is 5000 and 10000 respectively. In different ciphertext length types, the ciphertext balance index, ciphertext information entropy, confusion and diffusion are analyzed. The performance indexes of the conventional trading platform information network security encryption control method based on memristive neural network, the conventional trading platform information network security encryption control method based on Ethereum and IPFS encryption algorithms, and the performance indexes of the trading platform information network security encryption control method designed in this paper are compared. The experimental results are shown in Table 3 below.

Table 3. Experimental results

Trading platform information type	Ciphertext length /bit	Cryptographic control indicators		Plaintext		Ciphertext	
		δ	$H(S)$	d_1	d_2	d_1	d_2
Conventional Security Encryption Control Method for Trading Platform Information Network Based on Memory Resistive Neural Network							
Basic information of the platform	5000	0.060	0.854	0.852	0.843	0.854	0.862
	10000	0.096	0.674	0.864	0.864	0.862	0.854
Transaction	5000	0.058	0.843	0.832	0.852	0.873	0.873
	10000	0.084	0.762	0.782	0.867	0.854	0.862
Conventional Ethereum and IPFS encryption algorithm based control method for network security encryption of trading platform information							
user information	5000	0.014	0.943	0.896	0.948	0.896	0.909
	10000	0.021	0.885	0.903	0.928	0.885	0.894
Financial Institution Information	5000	0.028	0.892	0.885	0.893	0.902	0.927
	10000	0.045	0.864	0.932	0.886	0.896	0.886
The information network security encryption control method based on blockchain technology designed in this article for trading platforms							
Transaction security information	5000	0.003	0.997	0.999	0.998	1.000	1.000
	10000	0.004	0.999	0.998	0.997	1.000	1.000
Transaction regulatory information	5000	0.002	0.998	0.999	0.998	1.000	1.000
	10000	0.001	0.999	0.998	0.997	1.000	1.000

As shown in Table 3, the basic information of the platform includes the name, website, establishment time and location of the trading platform. Transaction information includes transaction type, quantity, price, time, method and other information; User information includes user's name, gender, age, occupation, location and other information; The information of financial institutions includes the names, locations, qualifications and other information of financial institutions such as banks and payment institutions; Transaction security information includes transaction password, security issues and identity authentication login information; Transaction regulatory information includes regulatory agencies, policies, compliance requirements and other information. All other conditions being the same, after using the conventional security encryption control method of trading platform information network based on memristive neural network, the ciphertext balance index is within 0.1, the ciphertext information entropy is above 0.65, and d1 and d2 are around 0.85. It can be seen that after using this method, the information encryption control effect of the trading platform is not good, which is not conducive to the trading security of the platform. After using the conventional security encryption control method of trading platform information network based on Ethereum and IPFS encryption algorithms, the ciphertext balance index is within 0.05, and the ciphertext information entropy, d1 and d2 are within the range of 0.85~0.95. It can be seen that after using this method, the encryption control performance is better than the conventional method based on memristive neural network, but there is still the problem of transaction information leakage, which needs to be further optimized. After using the security encryption control method of trading platform information network based on blockchain technology designed in this paper, the ciphertext balance index is within 0.005, and the ciphertext information entropy, d1 and d2 change in the range of 0.995~1.000. Most plaintext and ciphertext can meet the requirements of confusion and diffusion, thus ensuring the information security of trading platform.

4 Conclusion

In recent years, with the rapid development of the digital age, blockchain technology has gradually become a hot field of information network security. With the advantages of decentralization, high security, high transparency and traceability, the trading platform combined with blockchain technology has gradually become an important infrastructure in the digital economy era. With the expansion and complexity of the trading platform information network, the security threats and challenges faced by the trading platform are becoming increasingly serious, and it is urgent to deal with and optimize them. Therefore, this paper uses blockchain technology to design a secure encryption control method for trading platform information network. From the aspects of identity authentication, encryption control intelligent contract, etc., the encryption mode of blockchain is optimized, the encryption length is shortened, and the environment of ciphertext confusion and diffusion is changed. Even if the attacker gets the ciphertext, it can't be deciphered, which really improves the security of the trading platform information network.

References

[1] Zhong J , Zhou J , Gao S ,et al.Secure orthogonal time-frequency multiplexing with two-dimensional encryption for optical-wireless communications[J].Chinese Optics Letters, 2021, 19(5):050603.

[2] Bo Li. Research on dynamic searchable symmetric encryption with strong forward and backward security[D]. Nankai University,2020.DOI:10.27254/d.cnki.gnkau.2020.000156.

[3] Sheng Ye,Tu Guangsheng. An efficient fully homomorphic encryption scheme for CCA1 security[J]. Network Security Technology and Application,2024,(10):24-28.

[4] Deng Junhua,Zhao Lei,Dai Lulu,et al. Secure communication scheme based on encrypted trust management[J]. Journal of China Academy of Electronic Science,2019,14(10):1006-1010.

[5] Sadeghikhorami L , Safavi A A .Secure distributed Kalman filter using partially homomorphic encryption[J].Journal of the Franklin Institute, 2021, 358(5):2801-2825.

[6] Han M , Zhu M , Cheng P ,et al.Implementing an Efficient Secure Attribute-Based Encryption System for IoV Using Association Rules[J].Symmetry, 2021, 13(7):1177.

[7] Panda S K .Secure Dynamic Groups Data Sharing with Modified Revocable Attribute-Based Encryption in Cloud[J].International Journal of Nano and Biomaterials, 2021, 8(4):9508-9512.

[8] Acharya K , Dutta R .Constructing provable secure broadcast encryption scheme with dealership[J].Journal of Information Security and Applications, 2021, 58(4):102736.

[9] Watanabe Y , Nakai T , Ohara K ,et al.How to Make a Secure Index for Searchable Symmetric Encryption, Revisited[J].IEICE Transactions on Fundamentals of Electronics, Communications and Computer Sciences, 2022, E105.A(12):1559-1577.

[10] Morampudi M K , Prasad M V N K , Verma M ,et al.Secure and verifiable iris authentication system using fully homomorphic encryption[J].Computers & Electrical Engineering, 2021, 89(1):106924.

[11] Panwar K , Purwar R K , Srivastava G .A Fast Encryption Scheme Suitable for Video Surveillance Applications Using SHA-256 Hash Function and 1D Sine–Sine Chaotic Map[J].International Journal of Image and Graphics, 2021, 21(02):50-54.

[12] Kumar S , Nagarathinam K .Attribute-Based Proxy Re-encryption for Health Record Maintenance in Cloud Environment[J].Turkish Journal of Computer and Mathematics Education (TURCOMAT), 2021, 12(12):797-803.

[13] Wang Y , Miao M , Wang J ,et al.Secure Deduplication with Efficient User Revocation in Cloud Storage[J].Computer Standards & Interfaces, 2021, 78(5):103523.

[14] Rahmad C , Syulistyo A R , Sumari A D W .Securing the electronic medical record by implementing Advanced Encryption Standard (AES) on the information system of a health service place[J].IOP Conference Series: Materials Science and Engineering, 2021, 1073(1):012057 (6pp).

[15] Saurabh K , Rani N , Upadhyay P .Towards blockchain led decentralized autonomous organization (DAO) business model innovations[J].Benchmarking: An International Journal, 2023, 30(2):475-502.

[16] Bali S , Bali V , Mohanty R P ,et al.Analysis of critical success factors for blockchain technology implementation in healthcare sector[J].Benchmarking: An International Journal, 2023, 30(4):1367-1399.

[17] Qi Y , Wang X , Zhou Q ,et al.Research of Energy Consumption Monitoring System Based on IoT and Blockchain Technology[J].Journal of Physics: Conference Series, 2021, 1757(1):012154 (5pp).

[18] Uddin M , Memon M S , Memon I ,et al.Hyperledger Fabric Blockchain: Secure and Efficient Solution for Electronic Health Records[J].Computers, Materials and Continua, 2021, 68(2):2377-2397.
[19] Aldabbagh G , Bamasag O , Almasari L ,et al.Blockchain for Securing Smart Grids[J].International Journal of Distributed Sensor Networks, 2021, 21(4):255.
[20] Gupta S , Sethi S , Chaudhary S ,et al.Blockchain Based Detection of Android Malware using Ranked Permissions[J].International Journal of Engineering and Advanced Technology, 2021, 10(5):68-75.
[21] Ko H , Praca I .Design of a Secure Energy Trading Model Based on a Blockchain[J].Sustainability, 2021, 13(4):1634.
[22] Treiblmaier H .Exploring the Next Wave of Blockchain and Distributed Ledger Technology: The Overlooked Potential of Scenario Analysis[J].Future Internet, 2021, 13(7):183.
[23] Osei R K , Medici M , Hingley M ,et al.Exploring opportunities and challenges to the adoption of blockchain technology in the fresh produce value chain[J].AIMS Agriculture and Food, 2021, 6(2):560-577.
[24] Han B , Qian H X . Concurrent Access Control Method of Mainstream Knowledge Graph Storage System [J]. Computer Simulation, 2023, 40(3):333-337.