Digital Financial Transaction Security Based on Blockchain Technology

Huitong Song¹, Yansheng Chen²

¹Macau University of Science and Technology School of Business, 999078 Macau China;
²Guangdong Industry Polytechnic, 510300 Guangzhou, China;

*Corresponding author e-mail: robert.song@must.edu.mo

Abstract: Blockchain technology is currently recognized as the most potential new key technology, it can bring earth shaking changes, it is expected to trigger a new round of technological innovation and industrial change, and cause market attention. The purpose of this paper is to study the security of digital financial transactions based on blockchain technology. Firstly, the security of sdte is analyzed, and the DoS attacks that each role may launch, the attacks that a single role may send, and the attacks that can be launched by multiple roles in collusion are analyzed. It shows that sdte can resist these attacks and has strong security. Then, the related environment of the system test is described. Then, the performance test and analysis are carried out from the key security transmission, the execution of smart contract in the trusted environment SGX and the total running time. The experimental results show that the extra time consumed by using the k-nearest neighbor (KNN) algorithm to process data is less than 0.45s, At the same time, the additional cost brought by the system is also acceptable.

Keywords: Blockchain Technology, Digital Finance, Transaction Security, Digital Currency

1. Introduction
With the change of concept brought about by the development of science and technology, data storage and processing are gradually turned to online operation[1]. Although the work efficiency is improved, the fatal attack of the attacker may cause irreparable loss [2-3]. Financial, medical and management work can not do without the support of information technology [4]. Data leakage incidents occur from time to time. A large number of private data are stored in Internet connected devices. In order to protect the security of these data, many companies have begun to explore new storage methods, and are committed to building a trusted network ecosystem, and blockchain is one of the hot spots [5-6].

The emergence of bitcoin has brought about a turning point for the embarrassing social
phenomenon, gradually turning the focus from the traditional database to the safe storage of blockchain [7-8]. A lot of applications based on blockchain technology have emerged. Simply introducing blockchain from the perspective of security has been unable to meet the needs of daily work. Therefore, it is worth thinking about how to develop the application of blockchain with low consumption, high convenience and flexibility on the basis of blockchain security [9-10].

The innovation of this paper is mainly reflected in the following two aspects: first, the subject is relatively new, and the technical analysis is more detailed. At present, the research on blockchain and its application is still in the initial stage. In this paper, the technical framework of blockchain technology, asymmetric encryption technology and blockchain security response mechanism are analyzed and introduced in detail as far as possible, which are rarely seen in the current academic articles. Second, the experimental analysis is clearer. With the deepening of the research on blockchain technology, its experiments in many fields are gradually launched, and more and more cases are analyzed and studied. Based on the test and analysis of key security transmission, the application of blockchain technology has greater practical significance for the improvement of traditional mode.

2. Security of Digital Financial Transactions Based on Blockchain Technology

2.1 Blockchain Technology

(1) Blockchain technology framework

Narrow definition of blockchain: a kind of data in the blockchain is a data block structure linked in the way of continuous combination of time series, which ensures non-encrypted tampering to a certain extent. Broad definition of blockchain: the so-called blockchain technology is a new distributed infrastructure and computing method, which uses the construction of blockchain data to verify and save data. Distributed node consistency algorithm is used to generate and change data, and cryptography is used to ensure security.

(2) Asymmetric encryption technology

The key generation and digital signature algorithm of bitcoin is ECDSA, which comes from ECC. The elliptic curve calculation method satisfies the Weierstrass equation

\[ y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \]  

Elliptic curve points are continuous discrete points, and F is defined on the finite field. There are p elements in F.

Where p is a particularly large prime, P can be obtained from the following formula:

\[ p = 2^{256} - 2^{224} - 2^{192} - 2^{96} - 2^6 - 2^4 - 1 \]  

Let K and G be the points on the elliptic curve EP and satisfy the properties of discrete points. N is the order of G and K is an integer less than n. Given K and G, it's easy to calculate K. However, given K and G, it is very difficult to get K. Let G be the initial point on the ellipse, that is, the first discrete point. K is the public key and K is the private key. The following formula can be obtained:

\[ K = k \cdot G \]  

The public key is generated by the private key by the above method.

2.2 Mechanism for Dealing with Block Chain Security Problems

We define such a group of components \( \{g_1(x), g_2(x), \ldots, g_n(x)\} \), which is Out = \{O_1, O_2, ..., O_m\} with the external incentive set defined in the original isomorphic system logic, and Out' = \{O'_1, O'_2, ..., O'_3\}, which is not defined in the logic.

\[ g_1(O_1) = g_2(O_2) = \ldots = g_n(O_n), O_i \in \text{Out} \]  

The final output of the component set to stimulation is the multiple decision of all outputs. The isomerization transformation of the blockchain system can make the use of single vulnerability in the component be identified by the system, and the single vulnerability can not have a destructive impact on the system, thus greatly improving the security and stability of the blockchain system.
3. Digital Financial Transaction Security Experimental Research Based on Blockchain Technology

3.1 Test Environment

In sdte, it implements the blockchain platform based on Ethereum and sgxsdk to realize SGX related functions. Two machines are used to simulate the roles in sdte. One of the machines represents users (including data buyer and data seller, and roleuser is used to represent them). This machine is used to perform various operations of data buyer or data seller according to different test contents. The other one represents a trusted node (roletrust) with SGX security hardware and installed with sgxsdk. Among them, roletrust can create multiple enclaves to replace multiple trusted nodes in SDTP. Its main function is to perform remote authentication or create SGX security environment to ensure the whole execution process. The configuration of roletrust is shown in Table 1.

**Table 1. Configuration of Roletrust**

| CPU       | 2.40GHz |
|-----------|---------|
| Memory    | 64GB    |
| Hard disk | 1TB     |
| Network speed | 1Gbps |
| SGX SDK   | Intel SGX Linux 2.0 Release |

The above are roleuser and roletrust test environments. In the actual test, because sgxsdk does not support some library functions called by EVM, EVM cannot process 256 bit integers. Therefore, sdte extends the libraries supported by sgxsdk to implement 256 bit integer operation manually.

4. Digital Financial Transaction Security Experiments Based on Blockchain Technology

4.1 Secure Key Transmission and Storage

In the test process of key security transmission, 1000 enclaves are created in roletrust to execute data analysis smart contracts on behalf of 1000 nodes. The process can be divided into three parts. First, roleuser initiates remote authentication with n enclaves in roletrust, and the second is that roleuser establishes a secure channel with 1000 enclaves in roletrust and transfers keys, Finally, roletrust seals the received key. When testing the security transmission time of the key, a total of 100 tests are conducted, and then the average time is taken. The test results are shown in Table 2.

**Table 2. Time of key secure transmission**

| node | 1   | 2   | 3   | 4   | 5   | 6   | 7   | 8   | 9   | 10  |
|------|-----|-----|-----|-----|-----|-----|-----|-----|-----|-----|
| time(s) | 0.8 | 0.9 | 1.2 | 1.3 | 1.38| 1.45| 1.69| 2.36| 2.5 | 2.72|

![Graph showing the relationship between Number of trusted nodes and time](graph.png)
4.2 Data Analysis Smart Contract Execution
The process of running the data analysis smart contract in SGX can be divided into four parts: the first part is to read the source data of the data seller into enclave and decrypt it with the unsealed key; the second part is to read the byte code of the smart contract into enclave; the third part is to run the smart contract in EVM to process the source data and obtain the data analysis results; The fourth part uses the data buyer's key to encrypt the data analysis results. The first part and the fourth part use AES-256 bit encryption algorithm specially provided by wolfssl for SGX. In the third part, each data set contains 80 (x, y, z) points. For example, when there are 8 data sets, it represents that 800 (x, y, z) points have been processed. During the test process, the above process is executed 8000 times in roletrust and its average value is calculated. The test results are shown in Figure 2.

4.2.1 Experimental Results

As shown in Figure 2, the additional time consumed by SGX protected EVM increases linearly with the growth of data sets compared with the traditional EVM environment. The reason is that SGX itself is a CPU based security hardware, and the time consumed in the third step is basically the same as that in the traditional EVM environment. The process time of the second step is to copy the bytecode into enclave, which increases the length of the data set rather than the byte code itself. Therefore, the time of this step will not increase with the increase of data sets. The extra time is mainly concentrated in the first step and the fourth step. When enclave copies and decrypts the source data, its speed is certain, so the increase of data sets will lead to the increase of this part of time. In the same way, when the input data is more, the output results will become more, so the time for encrypting the results will also increase. In the process of linear growth of input data, the additional time consumed is no more than 0.45s, which is within the acceptable range of data copying, encryption and decryption. To sum up, the performance loss of SGX protected EVM virtual machine is less than that of traditional EVM virtual machine, which is within the acceptable range.

5. Conclusions
This paper is based on the basic theory of blockchain and cryptography to carry out the relevant work in the field of information security. The research content starts from the application of block chain key security transmission and storage, data analysis and intelligent contract execution. Firstly, this paper introduces the transaction risk of online payment. Under this background, the birth of blockchain
solves the dilemma, and expounds the research background and significance of blockchain. Secondly, it describes the research status of internal mechanism and application scenarios of blockchain. This paper introduces the important basic theory and key technology of the research topic. This paper summarizes the theory of blockchain technology and asymmetric encryption technology. The cryptography knowledge of blockchain including elliptic curve calculation is analyzed. Starting from the safe block height, the whole chain is stored in groups, and the data copies are released according to the proportion after the block height reaches a certain degree.

References

[1] Sikorski J J , Haughton J , Kraft M . Blockchain technology in the chemical industry: Machine-to-machine electricity market[J]. Applied Energy, 2017, 195(JUN.1):234-246.
[2] Zhang Y , Wen J . The IoT electric business model: Using blockchain technology for the internet of things[J]. Peer-to-Peer Networking and Applications, 2017, 10(4):983-994.
[3] Benchoufi M , Ravaud P . Blockchain technology for improving clinical research quality[J]. Trials, 2017, 18(1):335.
[4] Yeoh, Peter. Regulatory issues in blockchain technology[J]. Journal of Financial Regulation & Compliance, 2017, 25(2):196-208.
[5] O'Dair M , Beaven Z . The networked record industry: How blockchain technology could transform the record industry[J]. Strategic Change, 2017, 26(5):471-480.
[6] Eyal, Ittay. Blockchain Technology: Transforming Libertarian Cryptocurrency Dreams to Finance and Banking Realities[J]. Computer, 2017, 50(9):38-49.
[7] Yuan Y , Zhou T , Zhou A Y , et al. Blockchain Technology: From Data Intelligence to Knowledge Automation[J]. Zidonghua Xuebao/Acta Automatica Sinica, 2017, 43(9):1485-1490.
[8] Luisanna C , Andrea P , Michele M . Banking on Blockchain: Costs Savings Thanks to the Blockchain Technology[J]. Future Internet, 2017, 9(3):25.
[9] Mansfield-Devine, Steve. Beyond Bitcoin: using blockchain technology to provide assurance in the commercial world[J]. Computer Fraud & Security, 2017, 2017(5):14-18.
[10] Joshi A P , Han M , Wang Y . A survey on security and privacy issues of blockchain technology[J]. Mathematical Foundations of Computing, 2018, 1(2):121-147.