Data Security Ledger based on Blockchain Technology

Anna Li[1*], Shaohua Jiang[1], Yifeng Ma[2]
[1]School of Finance, Anhui Finance and Economics University, Bengbu, 233030, China
[2]School of Business Administration, Anhui Finance and Economics University, Bengbu, 233030, China

Abstract: The development of Internet technology is accompanied by the generation of online banking, and at the same time has opened the era of exploration of online banking security issues. Blockchain technology has been committed to solving the new trust problem of information security, introducing it into the data security problem of online banking, and improving the security and business capability of online banking. Blockchain 3.0 technology and alliance chain technology introduced into online banking has produced data security ledger fintech products. Data security ledger is a new type of intangible fintech products, with blockchain distributed ledger, smart contract, consensus mechanism, asymmetric encryption and authorization technology and based on blockchain alliance chain technology, to achieve data storage security is not easy to break, clearing business manpower and material savings, data transmission is not easy to change, Six important functions of data encryption security and effectiveness, credit rating authorization, and interoperability between data security ledgers.

Keywords: Online banking; Blockchain 3.0; Alliance chain technology; Data security ledger

1. Introduction

In December 2018, the China Financial Certification Center (CFCA) released the 2018 China e-banking survey report. According to the data in the report, the proportion of individual online banking users in 2018 reached 53% of the total urban residents, up 2% compared with 2017, and the proportion of individual online banking users in 2018 was 51%. These data are enough to prove that there are a wide range of customer groups in cities and towns, and the customer groups are still growing. With the increase of online banking function and the improvement of the system, online banking will become an indispensable financial tool for more and more users. However, we need to pay attention to the fact that Internet banking is the product of the integration of traditional banking and Internet technology, and it is a virtual bank. All the contents of traditional banks will be converted into data operation and circulation. Online banking can provide more convenient services, at the same time, it needs to face not only liquidity risk, market risk, interest rate risk of traditional banks, but also data risk from Internet technology.

Liu Yizhong and Liu Jianwei proposed that consensus mechanism is the core of blockchain [1], and analyzed the consensus mechanism model in depth. Anqingwen conducts research on blockchain in the form of alliance chain [2], realizing decentralized task allocation system and reward transaction of smart contract. Wang Shuo analyzes the differences between traditional payment methods and blockchain payment methods [3], aiming to achieve a flat global integrated clearing system. Liu Peng and Zhou Shuang proposed to use financial technology to accelerate the transformation of banking business [4] and strengthen regulatory design. Based on the security analysis of online banking, this paper improves the efficiency and supervision of online banking business according to the consensus mechanism of blockchain technology, asymmetric encryption and authorization technology, smart contract and distributed ledger.

2. Analysis on the Current Situation of data Security Management of Online Banking

Because the business of online banking is carried out on the network, there are various uncertain factors, i.e. risks, in which the online data are not safe. The risk is objective and has a certain threat to the development of data security ledgers. Only by correctly identifying and avoiding risks can we avoid the losses caused by risks and achieve the expected business objectives. Therefore, this paper analyzes the security management of online banking from the aspects of technology, operation, reputation, management and law.

2.1. Technology risk

Under the background of the rapid development and continuous innovation of electronic information and network technology, online banking does not adopt the matching related technology or the adopted technology fails to keep up with the pace of the times, which brings security risks and affects the normal operation of online banking. Technical risks mainly include:

2.1.1. Network transmission risk

The business carries out a series of complex data transmission and multiple intermediate transactions between the bank and all transaction participants through the network. For example, opening an account, closing an account, querying, reconciling, intra bank transfer, interbank transfer and other businesses require multiple authentication and payment processes. The continuous confirmation process of authentication information and payment information is also the continuous exposure process of information. If the network transmission system and environment of the business transmission link are broken, or the encryption algorithm is attacked by hackers, the funds, account numbers and passwords of online banking customers will be transmitted as clear text in the network transmission, resulting in the leakage of customer information and seriously affecting the information security of online banking users.

2.1.2. Security authentication risk of internet banking client

Cloud computing, Internet of things and other new technologies have created intelligent banking outlets, enabling customer business self-service processing and information processing to achieve seamless docking, and business to achieve unmanned automatic processing. Internet banking business breaks the geographical and time limit of traditional banking business, with 3A characteristics, that is, it can provide financial services to customers at anytime, anywhere and in any way. As long as you have an account password, you can conduct online banking transactions through the Internet all over the world. But when the business is not face-to-face, it is impossible to determine the physical spatial identity of all the people involved in the transaction, which makes it difficult to identify the authenticity of the client. Once hackers invade the bank's computer security system, disrupt the bank's computer system and steal the customer information of the files. The user information will be stolen to the designated server. If lawbreakers take the opportunity to fake users for trading activities, it will greatly threaten the safety of users' property.

2.1.3. Data security risk

The normal operation of online banking requires absolute security and confidentiality of data as the premise. But if the bank computer hardware resources are damaged by natural disasters or man-made, it may lead to the loss, leakage and tampering of the bank software resources and data information. Bring immeasurable loss and trouble to banks and users.

The existence of technology risk is a serious threat to the survival of online banking, and it is also one of the most concerned issues of online banking and all transaction participants. If this hidden danger can not be eliminated, the further development of online banking will be seriously hindered.

2.2. Operational risk

It refers to the risk of direct or indirect loss caused by imperfect or problematic internal operation process, personnel, system or external events. Operational risks mainly include:

2.2.1. Risk of authorized use of online bank account

The emergence of super online banking realizes the cross bank query and transfer of multiple bank cards in an online banking account. However, according to a major security alert issued by 360 Internet Security Center on May 28, it said that the "super online bank" cross bank account management function has become the target of malicious use by hackers. Once the lawbreakers obtain the authorization of other people's accounts, they can steal all the user account balance. It brings great threat to the property security of users.

2.2.2. The risk of management system of internet bank

If there is illegal communication and cooperation among managers, operators and regulators within the bank. It will lead to the phenomenon that similar audit departments and personnel do not report the problems found in the inspection, report the false situation or fail to perform the inspection, supervision and rectification. The internal management system of the Internet banking has some problems, which will lead to the collapse of the whole system, and then affect the continued operation of the Internet banking.

2.3. Reputation risk

In the information age of rapid development of Internet and information globalization, customers pay more and more attention to the security and operation experience in the process of online banking transactions. According to the 2018 China e-banking survey report, in the process of customers choosing online banking, the most important is the security of the system. Customers' experience of the security and convenience of the online banking operating system will be spread through various channels and directly affect the bank's reputation. The bad experience of customers is likely to lead to the trust crisis of online banking. The reputation risk of a bank mainly comes from its customers. The trust crisis of customers to the bank can be roughly divided into two aspects:

2.3.1. Lack of security of online banking operating system

At present, online banking has experienced a rapid development of the expansion stage, the development trend tends to be stable. In the period of rapid development of online banking, there are many unsolved technical problems. However, the popularity of online banking is high, the scope of business is wide, the volume of capital transactions is large, every small security risk may bring huge security risks, and bring economic losses to customers. Economic losses are likely to be widely spread through new media, affecting the bank's reputation.

2.3.2. Complex operating system

The establishment of online banking saves a lot of human resources and spreads business operations to various customers. But because the operating system also needs a certain amount of time and energy, customers have a demand for convenience of the operating system, and the operation of some transactions has a certain complexity that may affect customer experience, bring credit risk to the bank, and make customers choose other online banks or other online third-party transaction platforms.

2.4. Management risk

2.4.1. Customer information management risk

At present, it is not easy to manage the number of customers in online banking. No matter how strong the firewall is, it may be broken from the center. The customer's information and key are not in the customer's own hands, but are unified by online banking. On the one hand, online banking should bear the risk of customer information disclosure, on the other hand, it needs to spend too much human and material resources. As a database builder, it is not realistic that online banking does not carry out unified management. How to deal with the risk of information management is an important problem for online banking.

2.4.2. Internal personnel management risk

There are a lot of information and transaction data in the internal staff of online banking. Once the staff misoperate or are infiltrated by lawbreakers, it will bring great economic loss to online banking.

2.5. Legal risk

The existing online banking has one or several databases, the transaction information is easy to be intruded and deleted. Criminals may use Internet banks to engage in money laundering activities, which makes banks passively violate the laws and regulations of anti money laundering; some hackers may also use Internet loopholes to damage network connections, or even steal data for illegal transactions. These network crimes have a lot of concealment, a little carelessness will let criminals go unpunished. The transaction information of lawbreakers is not easy to monitor, which makes it difficult to track down and brings unnecessary risks to banks.

3. Blockchain Foundation and Data Security Ledger Application Design

Based on the principle of cryptography, blockchain technology is a kind of chained data structure which combines data blocks in chronological order, can't be changed, can't be forged, and has many advantages such as decentralization, encryption, consensus mechanism, etc. This paper uses the advantages of blockchain to design the data security account book of online banking [5-10].

3.1. Principles and characteristics of blockchain Technology

Blockchain comes into being together with bitcoin. Its original intention is to protect the transaction security of bitcoin. In order to solve the trust and security problems in the process of bitcoin transaction, it puts forward four technological innovations.

3.1.1. Distributed ledger

Distributed ledger technology uses multiple nodes distributed in different locations to complete transaction bookkeeping, and each node will keep a complete account. Therefore, distributed ledger technology can be used to monitor and prove the legitimacy of transactions.

Different from the traditional distributed storage, the uniqueness of the blockchain distributed storage is mainly reflected in two aspects: one is that each node of the blockchain stores complete data according to the block chain structure, and the traditional distributed storage generally stores the data in multiple parts according to certain rules; the other is that each node of the blockchain stores independently and in the same position Consensus mechanism is used to ensure the consistency of storage, while traditional distributed storage usually synchronizes data from the central node to other backup nodes.

In the whole system, no single node has the right to record the ledger data independently, thus avoiding the possibility of single bookkeeper being controlled or being bribed to record false accounts. Because there are enough accounting nodes, in theory, unless all nodes are destroyed, accounts will not be lost, thus ensuring the security of account data.

3.1.2. Asymmetric encryption and authorization technology

Although the transaction information stored in the blockchain is public, the account information is highly encrypted, and the core data can only be accessed after receiving the management authorization, so as to ensure the security of the information.

3.1.3. Consensus mechanism

The consensus mechanism is to determine the accuracy and effectiveness of records through each single accounting node that has reached an agreement. The consensus mechanism has the characteristics of minority subordinate to majority and each individual data node is equal. Taking bitcoin as an example, if you want to tamper with or forge a nonexistent transaction information, you need to master at least 51% of all nodes. When there are enough data nodes, this is almost an impossible task, so consensus mechanism can maintain data security.

3.1.4. Smart contract

Smart contract technology is based on the characteristics of blockchain data authenticity and non tamperability, through which some pre-set rules and terms can be automatically executed. Taking the bank's clearing and settlement business as an example, if the data information of each business object is authentic, it will save a lot of manpower and material resources for the online banking system and reduce the operational risk caused by the operator's misoperation.

3.2. Application design of data security ledger

Blockchain technology has a unique data security function, which has a promising application prospect in many fields. Through the analysis above, there are many hidden dangers of data security in the current online banking, which cannot be ignored. Online banking urgently needs a data security system that can effectively solve the existing data security risks of various types of online banking, and guarantee the safe operation of existing business and the expansion and upgrading of future business of online banking. Data security ledger system is a data security system based on alliance chain technology, which uses distributed ledger, consensus mechanism, smart contract, asymmetric encryption and authorization technology to provide three functions of data processing, authority management and data supervision. The data security ledger system can realize the differentiation of different customers and different bank's authority scope by controlling the authorization strength, which can meet the needs of transactions between banks and customers.

3.2.1. Data processing module design

The data processing module is the core module in the data security account book. There are two major problems in the data processing module. One is how to realize the safe storage of data, prevent data loss and data island. The other is how to realize the safe communication of data, prevent unnecessary operation risks and save human and material resources.

3.2.1.1. Data storage

Data security ledger uses distributed ledger technology to complete the safe storage of data. Each entity joining the data security ledger will generate an independent node with an independent account. The transaction data generated in the data security ledger will be stored in each node, that is, the ledger is not central.

The transaction data between accounts will not be directly stored in the node database, and the transaction data will be put into the blockchain for transaction legitimacy judgment. If the judgment is legal, it will be stored in each node database added to the blockchain. Since the data is stored in each node database, there is no central database, which avoids the data loss problem caused by the failure of the central database; on the other hand, because each account and transaction information will be put into each database after the legitimacy judgment in the alliance chain, the data change in any database will affect all databases, within each database The capacity is completely consistent to avoid data island.

3.2.1.2. Data exchange

Data exchange of online banking is the data flow generated by transaction activities. Traditional online banking is prone to inconsistency. The inconsistency of accounting data improves the operational risk caused by improper operation of employees in the business and increases the waste of human and material resources. In the data security ledger system, the pre-set rules and terms can be automatically executed by using the contract certificate after obtaining the authorization of the relevant subjects, so as to minimize the operational risk and the cost of human and material resources.

3.2.2. Authority management and encryption module design

The authority management module includes two types: principal level authorization and key authorization of encrypted transaction. As the traditional blockchain system is a public chain system, any subject can join and view any information at will. The data security ledger will be based on the alliance chain technology, using asymmetric encryption and authorization technology to realize the security and controllability of the blockchain and protect the trade secrets in the transaction. In the data security account book, the blockchain system construction bank can assign the authority level according to the credit level of each entity joining the alliance chain, and different authority levels will have different rights and get the service of level by level improvement.

As each customer has the need to protect their own information security and trade secrets, in addition to some information that must be disclosed, customers can decide whether to choose to disclose the rest of the information. For non-public data, customers can authorize some entities to view, and customers have strong management autonomy on their own data. In each transaction, the customer can create a private key and a public key. The private key can be used as decoding and the public key can be used as encryption. The private key can also be used as encryption and the public key can be used as decoding. The customer may choose to use according to the actual situation. For example: the customer can hand over the public key to the trader, the trader writes the necessary information and uses the public key to encrypt the information into a password and then transmits it to the customer, and the customer uses the private key to decode. By using asymmetric encryption technology, the security of personal information and transaction is greatly improved, and the risk of information leakage and transaction is reduced.

3.3. Data verification module design

The data security ledger will use pool validation pool technology to achieve consensus and data supervision. The core purpose of data supervision is to verify the legitimacy of data exchange process. The transaction data generated in each transaction is firstly verified by the validation pool data, and more than 51% of nodes reach a consensus that the transaction is legal before the transaction is successful, and the transaction information will be stored in the database.

3.4. Extensible module design

Data security ledger is a blockchain system based on alliance chain technology. Its service scope includes the transaction between online banking and customers who build the system and the transaction between customers who use the online banking who build the system. Although other financial institutions can create accounts as customers, they are likely to build their own data security account systems with different algorithms due to the need for their own data protection and the limited role of a single account. In order to realize the effective exchange of data and improve the effectiveness of data processing of online banking, the data security account system provides an external interface to facilitate the exchange of information between banks. When each data security account book needs to be interconnected, each data security account book can put forward the need to audit the data validity. The system checks whether the database information in a single data security account book is consistent and legal. If it passes the test legally, it can access other database information that passes the test after algorithm conversion, so as to realize data interoperability. If the data validity test fails, the system will solve the problem Explain the reasons for failure and reject the application, and apply for inspection again after modification, so as to protect the authenticity of each data account information and effectively avoid the problem of information island, and realize the information exchange between online banking and other financial institutions.

4. Analysis of Advantages and Application Prospects of Data Security Account Book

Data security account book is a new type of intangible financial technology product, which further solves the current online banking security problem. It is based on the current online banking data security system and blockchain technology 3.0, and has its own innovation breakthrough [11-15].

4.1. Advantages of data security ledger

4.1.1. Data exchange is safe and effective

At present, asymmetric encryption technology is the best and effective technology for data communication, and asymmetric encryption technology is used in data security account book. On the one hand, it ensures the security in the process of data communication and transmission, on the other hand, double encryption improves the effective security of data communication and transmission password. The security and efficiency of data exchange is the most basic advantage of data security account book, which makes up for the defects of symmetric encryption technology of online banking.

4.1.2. Data storage security is not easy to break

The data security ledger adopts the distributed ledger to realize the data security storage of online banking. Legitimacy judgment is the first barrier of data storage. Physical security of data storage: legal data exists in parallel and independent databases to avoid accidental data loss caused by central database. Each independent database is parallel, and the data information is consistent. And each database node is a member of the legitimacy judgment, which ensures that the data storage is not easy to break. The security of data storage is the core content of data security account book. In this content, data security account book breaks through the current data storage of online banking to make it more secure.

4.1.3. Data supervision is not easy to change

The data security ledger adopts pool verification pool technology to supervise the transaction data. Only when more than 51% of the parallel database nodes approve the transaction data, can the transaction be considered as a successful transaction and included in the new independent database node, as one of the members of the new transaction data to judge the legitimacy. Otherwise, the transaction is rejected and fails until the legitimacy judgment is passed. The more transactions there are, the more parallel databases there are, the more members there are to judge the legitimacy, and the more reliable the legitimacy is. Data supervision is an important part of online banking transactions. The consensus mechanism of data security account book is a better technology of transaction data supervision, which breaks through the current data supervision of online banking users and makes it more difficult to be changed.

4.1.4. Reduce human and material resources in liquidation business

The data security ledger adds the intelligent contract technology in the blockchain technology, uses the contract certificate recognition, and reduces the operational risk and the use of human and material resources in the clearing business through the automatically set rules and terms. It reflects the innovation and advantages of data security ledger compared with the current online banking, realizes further automation and meets the requirements of the current society.

4.2. Application prospect analysis of data security account

Firstly, alliance chain technology is added to the data security ledger based on blockchain 3.0 to realize data exchange among multiple security ledgers. Data security ledgers are judged according to the results of data security inspection. Only the safety ledgers that pass the data security inspection can communicate through the external interface provided by the data security ledgers. The convenience of safe communication between banks and customers is the unique advantage of data security account book. Secondly, based on blockchain technology 3.0, credit rating system is added. The current credit level authorization technology is applied to various fields of life, such as Alipay, small bicycle and mobile phone number. However, block chain technology 3 does not require credit rating. The design of data security account has done a good job in the credit rating system of block chain technology.

5. Acknowledgment

National Undergraduate Innovation Project "analysis of the elderly care needs of the rural left behind -- Based on the field survey of Lixin County, Bozhou, Anhui Province" (201910378097).

References

[1] Liu Yizhong, Liu Jianwei, Zhang Zongyang, Xu tongge, Yu Hui. A review of blockchain consensus mechanism. Journal of Cryptography. 2019, (04), 395-432.

[2] An Qingwen. Research and application of key technologies of decentralized transaction based on blockchain. Tutor: Huang Qiubo. Donghua University. 2017.

[3] Wang Shuo. Research status and innovation trend of blockchain technology in financial field. Shanghai Finance. 2016, (02), 26-29.

[4] Liu Peng, Zhou Shuang. Attach great importance to the important role of financial technology in financial reform. China Price. 2019, (11), 59-62.

[5] Fang Yu. Research on the application of blockchain technology in joint stock commercial banks -- Taking China Merchants Bank as an example. Hangzhou: Zhejiang University of Industry and Commerce. 2018

[6] Huang Xingyue. Application of Blockchain Technology in Traditional Business Innovation of Commercial Banks. Journal of Changchun University of finance. 2019, 5, 1-5

[7] Hu Ying. Case study and reference of developing digital Inclusive Finance in urban commercial banks based on the perspective of bill blockchain. Finance and Economy. 2019, (04), 78-82.

[8] Li Jiaqian. Baidu Encyclopedia: blockchain [EB / OL]. Https://baike.baidu.com/item/blockchain/134656662019.

[9] Li Xingxin. Research on application of blockchain technology in bank payment and clearing in China. Beijing: Beijing University of Posts and telecommunications. 2018.

[10] Tian Yu. Research on risk management of online banking in China. Shenyang: Liaoning Normal University. 2017.

[11] Xu Ruzhi, Bai Peidong, Zhao Huawei. Research on the application of blockchain in commercial banks. Corporate Finance Research. 2017, (z1), 128-153.

[12] Yang Yuan. Design and implementation of bank information interconnection platform based on blockchain. Beijing: Beijing Jiaotong University. 2018.

[13] Zhu Chao. Research on risk prevention measures of online banking of Kunshan rural commercial bank. Nanjing: Nanjing Agricultural University. 2012.

[14] China financial certification center. 2018 China e-banking survey report. Beijing: China Financial Certification Center. 2018.

[15] Satoshi Nakamoto. Bitcoin:A Peer-to-Peer Electronic Cash System. Metzdowd.com. 2008.