Asian Social Science; Vol. 14, No. 2; 2018
ISSN 1911-2017 E-ISSN 1911-2025
Published by Canadian Center of Science and Education

Study on Internet Finance Credit Information Sharing Based on Block Chain Technology

Maoran Zhu[1] & Xin Liu[1]

[1] School of Economics and Management, Tongji University, Shanghai, China

Correspondence: Xin Liu, School of Economics and Management, Tongji University, Shanghai, 200092, China. Tel: 86-150-0183-8907. E-mail: liuxin0918@tongji.edu.cn

Received: December 1, 2017 Accepted: December 13, 2017 Online Published: January 29, 2018

doi:10.5539/ass.v14n2p81 URL: https://doi.org/10.5539/ass.v14n2p81

Abstract

With development of Big Data technology these years, Internet financial companies in China started trying using big data technology to do credit investigation instead of traditional methods. But there is some limitation and problem in terms of data acquisition channel, information asymmetry and data privacy protection, etc. Block chain, characterized in unalterability and decentralization comes into people's sight. This paper will introduce block chain technology, explore the use of block chain technology in Internet financial credit investigation, and put forward an internet financial credit data sharing model based on block chain, which mainly composed by the Fin-tech Federate Servers group (FFS), the user data storage structure and a distributed database system (DDBS). By combining DPoS and re-encryption technology, the model has the characteristics of non-tampering, authorized access and convenient accountability. Through this model, the user data is recorded by the trusted agent, encrypted by asymmetric encryption technology, and anchored to the chain of the block periodically.

Keywords: block chain, information sharing, internet finance credit

1. Introduction

The key to the survival and development of financial institutions is risk control, and credit mechanism is the basis of risk management and control. With development of Big Data these years, Internet financial companies started trying adopting big data technology to solve the credit investigation problem. The big data technology has played more and more important role in this field and gradually replaced the traditional manual investigation method. But the technology still has limitation in terms of data acquisition channel, information asymmetry and data privacy protection, etc. Block chain, a new technology characterized in distributed storage, peer-to-peer transmission, and consensus mechanism and encryption algorithm comes into people's sight.

As the underlying technology of BitCoin and other digital currency, block chain technology has the characteristics of unalterability and decentralization with the use of encryption algorithm, consensus mechanism, incentives and other mechanisms to realize peer-to-peer transaction in a distributed network, which provides more possibility for online transactions, payment, and intelligent contract. It was considered as fifth disruptive paradigm that may bring credit revolution to society after large computers, personal computers, the Internet, mobile social networking, and is likely to become the next generation of global credit authentication and value Internet infrastructure agreement. Block chain as a new solution to the trust problem, has especially caught the attention of the financial science and technology field. The research on the application of block chain in the financial field has become a hot spot in the research of block chain.

This paper will introduce block chain technology, explore the block chain technology and Internet financial credit model, and put forward an internet financial credit data sharing model, Fin-tech Federate Data Bank (FFDB), based on block chain.

2. Actuality and problems of Internet Finance in China

2.1 Actuality of Internet Finance in China

With deep integration of Internet technology and finance, many new Internet financial business and services are emerging. China's Internet financial platform can be divided into four types as (Li, 2016):

2.1.1 Payment Platform

The payment platform refers to the platform on which currency trading can be completed by internet terminals, such as Alipay and WeChat. The use of mobile payment has become a considerable part of people's preferred way of payment. The Great Wall securities research data show that the total scale of China's mobile payment market transactions in 2012 was 140 billion Yuan, and rose to 9.31 trillion Yuan in 2015, increasing about 65 times. By 2017, it is expected to reach 15.4 trillion Yuan.

2.1.2 Financing platform

Internet financing platform is designed to meet the investment and financing needs of individuals and small and medium-sized enterprises, including P2P credit, the crowd financing and small loan.

2.1.3 Financial Platform

Such pattern refers to a variety of financial or non financial institutions that provides products and services of insurance, funds, foreign exchange, futures and others to investors through the Internet, such as Yu E Bao, Li Cai Tong etc..

2.1.4 Service Platform

This kind of platform provides investors with financial information services, so that they can make more efficient decision by more convenient information acquisition, sorting, comparison and analysis, such as 360rong, Copper Street and so on.

2.2 Present Internet Finance Credit Reporting Mechanism in China

Credit is the cornerstone of financial transactions. Investors, financing users and institutions that are no matter under traditional or the Internet financial system, need mutual trust relationship to achieve transaction. If basic trust and credibility is lack, both sides will face enormous risks, and it will be highly possible to fail. The main participants of China's Internet finance are small and medium-sized micro enterprises, and the financing difficulties caused by the asymmetric information and the credit evaluation system are the obstacles to the development of these enterprises.

Internet financial credit refers to that in order to alleviate or eliminate the problem of asymmetric information of Internet financial transactions, and reduce the adverse selection and moral hazard as much as possible, to evaluate the user credit through collecting, sorting, storing and processing personal internet transaction information and data (Ping, Chen, Li, Feng & Zhao, 2015).

The Internet financial credit system belongs to the social credit system. Its essence is information integration and resources sharing: the industry agencies share, integrate and process their customers' credit data and information, in order to achieve the comprehensive customer credit evaluation. At present, there are two basic models of Internet financial credit reporting in China:

2.2.1 Big Data Credit Model

Big data credit refers to the use of technology to manipulate diversified information that obtained from diversified credit providers, e-commerce and social network, etc. and unstructured data, through information cleaning, effective matching, data integration and deep mining so as to acquire accurate and predictive credit data and evaluation reflecting the credit status. E-commerce platforms and P2P network loan platforms mainly use this model, such as Ant Fin-tech using e-commerce transaction data from Alibaba and Sesame Credit System to evaluate user credit.

2.2.2 Business credit reporting model

Business credit reporting model, represented by Microfinance Credit Information Sharing Platform (MSP) and Network Finance Credit System (NFCS) is another type. MSP provides P2P companies, small amount loan companies, guarantee corporations and other microfinance institutions with services including credit information query and reporting, borrower blacklist and bad information sharing, etc. NFCS collect and organize five kinds of credit transaction information generated by natural human subjects in internet finance processes, including basic personal information, loan application information, loan repayment information, loan open information, and special transaction information. Combined with credit information obtained from other fields, these information is integrated into a credit report.

2.3 Problems of Present Internet Finance Credit Reporting

There are still some problems in present Internet financial credit reporting systems.

2.3.1 Low efficiency and High Cost of Manual Audit

Manual verification is still the main way of Internet financial credit audit by collecting information and verify by manual. At present, the core technology of the Internet financial risk control is similar to the IPC model, including anti fraud, pre loan risk review, credit risk management, post loan risk assessment and collection etc. (Wu & Wang, 2016). As no third party takes part in, there is no guarantee of credibility, so the enterprise must further confirm the authenticity of information off-line. Specialized audit staffs make phone call or do on-site investigation to confirm, which greatly increases the manpower cost and reduce efficiency. Because of the limitation of manual check, it cannot completely ensure the authenticity of information either.

2.3.2 Serious Isolated Island Problem

Many Internet financial institutions cooperate with credit information platforms, such as MSP or NFCS, to obtain credit information. However, the amount of information that can be obtained by these platforms is limited. The information isolation between platforms and platforms is serious. Information is held respectively by various agencies and is rarely shared, which leads to the result that information has not been effectively utilized. Other credit information is held by other agencies such as telecom operators, government departments and courts (Li, Li & Zhu, 2016). If Internet financial institutions want to get more information, they have to cooperate with multi credit platforms and as a result risk control cost will increase.

In addition to that credit institutions are not willing to actively share data, safety of data sharing between institutions is also a problem based on the traditional architecture. The data isolated island problem remains unresolved in the credit reporting field.

2.3.3 Data Source Battle

User privacy protection must be paid attention during client information sharing. Ensuring authenticity and safety of credit data sharing concerns vital interests of enterprises and individuals and still remains to be a problem because of limitation of technology. Therefore, the allowance of being a formal credit data collection channel is strict. Traditional credit agencies need to actively strive for allow authorization from relevant departments and integrate data from limited scenes to take the initiative and opportunity of development in credit reporting industry. As a result, competition for data sources is particularly fierce.

3. Block Chain

Block chain is first known as the basic support technology of BitCoin, a digital encryption currency. Satoshi Nakamoto described the decentralized peer-to-peer trading system in BitCoin: a Peer-to-Peer Electronic Cash System. The 8 years' operation of BitCoin has proved the feasibility of block chain technology. In recent years, the application of block chain began to be independent of BitCoin.

3.1 Concept of Block Chain

At present, there is no widely accepted definition of Block Chain. In a broad sense, block chain technology is a new decentralized infrastructure and distributed computing paradigm using encrypted chain block structure to verify and store data, using the distributed consensus algorithm to generate and update data, using automated script code (intelligent contract) to program and manipulate data. In the narrow sense, block chain is a data structure according to the time sequence of valid data blocks to form chain combinations, and a decentralized shared ledge that is undeniable, unalterable and attachable through cryptography (Xue, Fu, Wang & Wang, 2017). Its essence is to collectively maintain a reliable database through a centralized approach. Block Chain contains three major components.

Transaction record. Block chain technology is a distributed safe ledger. Any transactions that occur in this network are recorded on the block chain system with agreed algorithms and structures. All transaction information will be encrypted to ensure its accuracy and authenticity (Yuan Yong & Feiyue Wang, 2016).

Block. A block is a data structure that stores transaction information, and it is the basic storage unit of the block chain. A block records all transaction information of all nodes that happened in 10 minutes. Blocks are chained sequently and form a block chain.

Chain. When a node initiates a transaction, it needs to broadcast the information to other nodes, and other nodes use the backup information to verify the legality of the transaction. After successful verification, the information is stored in the last block, and the timestamp is connected to the block chain.

Generally speaking, block chain is a complete transaction information chain composed of blocks connected according to time sequence.

3.2 Characteristics of Block Chain

Block chain is a new database scheme, which has the characteristics of decentralization, unalterablility, security and trustworthiness, and robustness.

3.2.1 Decentralization

Decentralization means that, in a system with many nodes, each node has a high degree of autonomy, and nodes can be connected freely with each other to form a new connection unit. Block chain using pure mathematical methods to establish the trust relationship between the distributed nodes, forming a trustworthy distributed network. Any node can create and verify transaction. All the activities are based on distributed network.

3.2.2 Unalterability

All transaction information on block chain, which is a distributed network, will be publicly recorded. Each transaction will be broadcast to other nodes, and must be verified by other nodes. When the node is verified, a timestamp is stamped as a proof of the transaction time so that the uniqueness of each transaction is guaranteed. The transaction data uses hash algorithm to generate hash value. Once the transaction information is changed, the hash value will alter and cannot be verified by other nodes. This mechanism makes the cost and difficulty of rewriting data very large, so the block chain technology has the characteristics of security and trustworthiness, and is suitable for applications that need to ensure the authenticity of information (Yao, Wu & Yu, 2016).

3.2.3 Robustness

As each node in the distributed ledger stores a complete data backup, it can effectively prevent the data loss caused by server failures and network paralysis. Malicious attack on a single node cannot affect the whole block chain system and data sharing, unless someone can control more than 51% of the nodes in the system, which is basically impossible (Li & Ren, 2016).

4. Application of Block Chain in Internet Financial Credit Reporting

Based on the current problems of Internet financial credit and the characteristics of block chain technology, this paper introduces a design of data sharing model Fin-tech Federate Data Bank (FFDB) using the block chain technology, in order to achieve decentralized, unalterable, safe and reliable credit data sharing mechanism between internet financial institutions.

4.1 Basic Composition

The FFDB model includes three main modules: the Fin-tech Federate Servers group (FFS), the user data storage structure and a distributed database system (DDBS).

4.1.1 Fintech Federate Servers (FFS)

The server of each Internet financial institution is the node of the model, which generates, verifies and records the user transaction information. Delegate Proof of Stake (DPoS) is used as the consensus mechanism among the Internet financial institutions.

Consensus mechanism is a rule that each node in distributed network agrees. Early BitCoin uses Proof of Work (PoW) to ensure the consistency of the network distributed ledger. Proof of Stake (PoS) is an improved mechanism based on PoW, that recording rights are obtained by the node with highest equity. DPoS is a more effective and flexible consensus mechanism, which reduces the number of participating nodes and improves the efficiency of consensus verification.

The working process of DPoS is that: first an initialization starts, all nodes separately vote for the delegates that they trust. The first 101 nodes with highest scores that are willing become the representative nodes will take turns to produce new blocks; once the authorized representative makes mistake when sign a new block or miss its turn to produce a block, the next representative node will do the sign job instead. The node making mistake may be cast on behalf of shareholders node seats; representative nodes need to register a unique 32 bit public key which will be cited in the header of a record. All representatives' action will be indicated by a performance indicator. If one of them makes error several times, the indicator will suggest changing the delegate (Wang, Gao, Dong, Guo, Chen & Wei, 2017).

4.1.2 User Data Storage Structure

In order to ensure user data needed for credit investigation, especially user's personal information and financial behavior information, be true, unalterable with effective dissemination, a hierarchy of storage structure should be designed.

Block chain does not directly save user data in plaintext. The nodes add the timestamp, operate the hash algorithm and acquire a certain length of the hash value. The hash value will be organized in accordance with binary tree structure, namely Merkle tree and stored in blocks.

The generation of Merkle tree is to divide data block into hash function, and then take out two data to do the hash operation, and go recursively until the only Merkle root is made.

The characteristics of the Merkle tree is: (1) each non-leaf node is the hash value of its leaf node; (2) the Merkle tree has good scalability; (3) it's easy to find the source from bottom of the Merkle tree. The time complexity of this process is low, which greatly improves the efficiency of the node; (4) nodes do not need to save all the user data but only need to keep the header that contains the Merkle root contains and the legitimacy of the data can be verified.

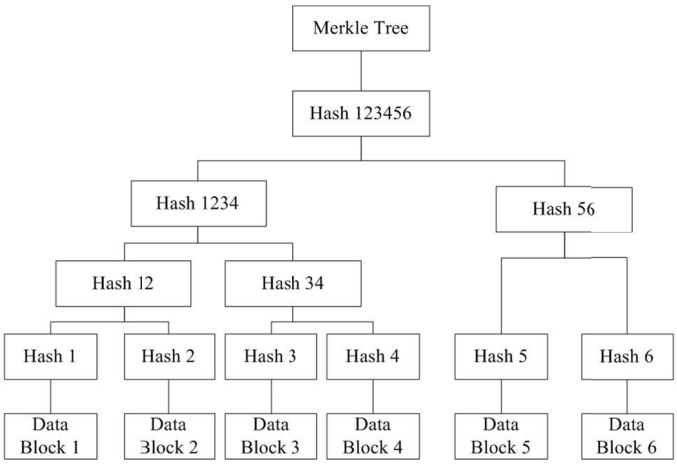

Figure 1. Merkle Tree, the User Data Storage Structure

4.1.3 Distributed Database System (DDBS)

The user data is encrypted and stored in the distributed database, which decreases the possibility of data loss because of hardware failure, disasters and so on. By a distributed database, users can index the distributed database system when there is need to access files in the data block. This helps reduce the pressure of data storage and high frequency access to the block chain.

4.2 Mechanisms of FFDB

4.2.1 Data Block Grouping

The hash value of the user's original data is stored in the data block after the hash algorithm. Each data block contains the hash value of 10 pieces of user data and header information. Each piece of user data consists of three parts: metadata, data owner's public key and data digest. The composition of the data block is shown in Figure 2.

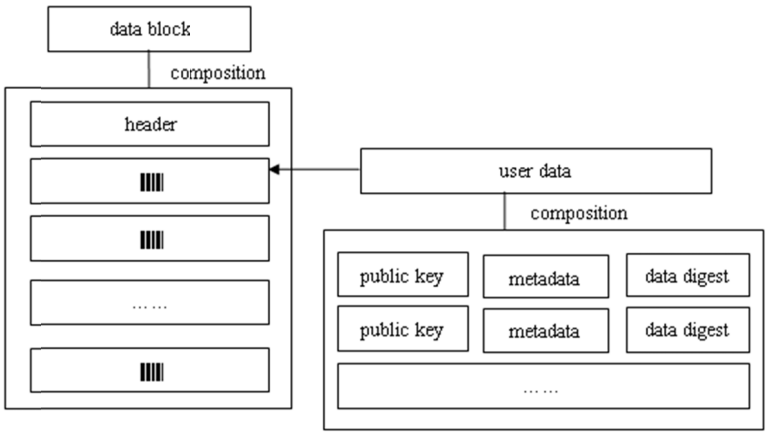

Figure 2. Composition of Data Block

FFDB uses a block structure similar to BitCoin. Each block stores no more than 100K data. For small data that

does not need to be encrypted, the original information can be stored directly in the abstract. For encrypted or large data, the data digest will be calculated and stored in the data block, and meanwhile, the original data will be stored in the distributed database system. The data digest in the data block can complete the integrity check, and can also be used as the index to find the data in the database. The data block of this form improves the efficiency of each block in the peer-to-peer transmission of the distributed network, and reduces the cost of data verification.

4.2.2 DPoS and Rewarding

The initialization of the DPoS consensus mechanism is to select 101 representatives by voting. These 101 representatives are usually large Internet financial institutions, and have the ability of data recording and inquiry. These nodes are responsible for recording requests submitted to the data block and signing with the private key.

FFS nodes will obtain reward points if they complete a data service. If the node produces error blocks or miss signing a new block, points will be deducted. When one node's score is below the threshold, it will be replaced by the node ranked behind the representative. The points as a reward mechanism encourage Internet financial institutions to share data and provide data services.

4.2.3 Re-Encryption for Data Sharing and Protection

Re-encryption mechanism is used to realize the sharing and access control of the user data. The characteristics of decentralization enables the system do not need the only proxy to do re-encryption Any node in the FFS can act as a proxy to complete the re-encryption operation, will be rewarded points through this operation.

When a Internet finance institution has a demand to query the user credit information, the user will encrypt the data on his terminal and then will generate a corresponding proxy re-encryption key from him and to the institution. The proxy re-encryption power will competed by nodes in the FFS competition, and the user should select one from the competition list to become the service node. His re-encryption key will be sent to the node. After the proxy re-encryption node encrypts the ciphertext by the re-encryption key. The ciphertext will be stored in the database, and the institution's public key who has the query requirement is the index identifier. The institution can access the database and decrypt the user data with its own public key. Through proxy re-encryption, data sharing and privacy protection can be easily realized.

4.3 Model Structure and Working Process

The structure and composition of the FFDB model are shown in Figure 3.

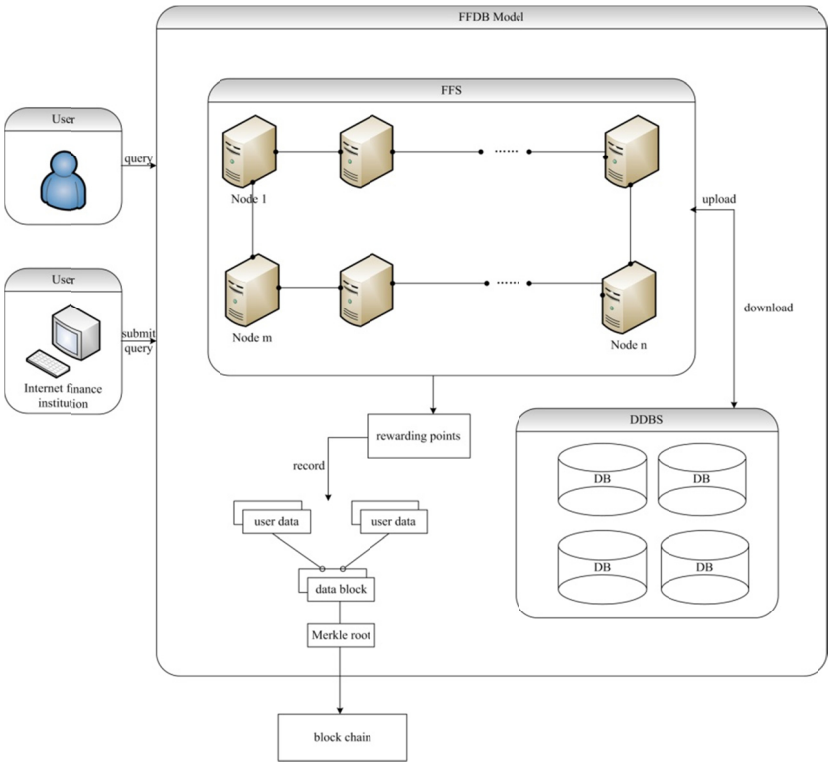

Figure 3. FFDB Model Structure

Similar to BitCoin, data will be frozen about every 10 minutes. The representative node in the FFS will submit Merkle root to the blocks in the chain, so every 10 minutes a new block will be generated. This process repeats and thus forms an unalterable block chain.

5. Summary

The rapid development of block chain technology provides new possibilities for various fields, and it becomes a hot topic in academic research field. This paper puts forward an idea of Internet financial credit reporting mechanism based on block chain, in order to realize the safe and reliable data sharing between Internet financial institutions. Through this model, the user data is recorded by the trusted agent, encrypted by asymmetric encryption technology, and anchored to the chain of the block periodically, so that the data cannot be tampered. Compared with the traditional data sharing technology, because of the use of rotation responsibility system, it's easy to track down to the responsible node and can prevent abuse or fraud. Each organization can obtain the unified and credible results quickly. All parts are thus connected and work with interoperability. User information can be stored immediately, and users can manage their own behavior data, through proxy re-encryption to authorize the trustworthy organization.

The combination of FFS and DPoS builds a foundation platform for the realization of Internet financial credit data, but there is also limitation in this design. For example, as long as a deal is verified by more than half of all nodes, then it is valid. There is still possibility, although highly unlikely, a whole network is maliciously controlled, which means more than half on all nodes are controlled. In this regard, the model can be further studied.

References

Ping, L., Chen, L., Li, Q., Feng, Y., & Zhao, H. J. (2015). Review of Research and Industry Development of Internet Finance. *Journal of University of Electronic Science and Technology of China, 44*(2), 245-253. https://doi.org/10.3969/j.issn.1001-0548.2015.02.015

Li, R. J. (2016). Internet Financial Credit Reporting Model Selection. *Credit Reference, 34*(9). https://doi.org/10.3969/j.issn.1674-747X.2016.09.006

Wu, Y. M., & Wang, Q. (2016). The Impetus of Evolution of Internet Finance: from the Perspective of Co-evolution of Technology and Finance. *Research on Economics and Management, 37*(3). https://doi.org/10.13502/j.cnki.issn1000-7636.2016.03.006

Xue, T. F., Fu, Q. C., Wang, C., & Wang, X. Y. (2017). Study on Medical Data Sharing Model Based on Blockchai. *Acta Automatic Sinica, 43*(9), 1555-1562. https://doi.org/10.16383/j.aas.2017.c160661

Yong, Y., & Wang, F. Y. (2016). Blockchain：The State of the Art and Future Trends. *Acta Automatica Sinica, 42*(4). https://doi.org/10.16383/j.aas.2016.c160158

Yao, G. Z., Wu, C. H., & Yu, X. (2016). Financial industry reform driven by block chain. *Journal of Nanjing University of Posts and Telecommunications (Natural Science), 36*(5). https://doi.org/10.14132/j.cnki.1673-5439.2016.05.001

Li, Z. D., & Ren, X. C. (2016). The Impact of Block Chain on the Internet Finance and its Future Prospects. *Technoeconomics & Management Research,* (10). https://doi.org/10.3969/j.issn.1004-292X.2016.10.014

Wang, J. Y., Gao, L. C., Dong, A. Q., Guo, S. Y., Chen, H,, & Wei, X. (2017). Block Chain Based Data Security Sharing Network Architecture Research. *Journal of Computer Research and Development, 54*(4). https://doi.org/10.7544/issn1000-1239.2017.20160991

Li, X. L., Li, J., & Zhu, P. A. (2016). *Study on Information Technology Innovation and Internet Finance. Technoeconomics & Management Research,* (12). https://doi.org/10.3969/j.issn.1004-292X.2016.12.014

Copyrights