



Block-Chain Will Lead to Innovation in Financial System

Ying Su^{a,b*}, Meng Sun^a, Yitong Zhai^a

^a College of Economics and Management, Yanshan University, Qinhuangdao 066004, China

^b Regional Economic Development Research Center of Yanshan University, Qinhuangdao 066004, China

Abstract

Because its data structure creates a digital transaction ledger, block-chain will build a more transparent and publicly verifiable system that will fundamentally change the way of our transaction activities, asset value, contract performance, and sharing data across industries. Since 2015, “block-chain” has become the hottest topic to the world’s major financial giants. This paper first introduces the principle and characteristics of block-chain technology. The block-chain technology based on encryption algorithms builds a global distributed secure network database that records and updates transaction information through decentralized chain connections and block chronological arrangement. Secondly, it focuses on the technological innovation of block-chain in financial systems. Block-chain technology solves the problems of decentralization, information security, and information disclosure in financial transactions. Thirdly, we put the emphasis on the block-chain technology application prospect in the field of finance. The block-chain technology will be used in digital currency, payment and clearing, smart contracts, as well as financial transactions. At last, we lead a warning that the application of block-chain technology could bring financial risks, which includes a technical problem, resource problem, and competition problem. Our conclusion is that block-chain will change the credit management mode of the traditional financial system. But due to the shortcomings of technical maturity, resources reserve, and the regulation of competition, the application value of block-chain in financial field will face risk. Therefore, monetary authorities should reserve talents and technologies of block-chain, and strengthen the basic research, practical application and standardization research of block-chain. According to the domestic and international situation, the authorities should issue legal digital currency, build internationally competitive Chinese block-chain products, and continuously explore effective regulatory model block-chain to secure a healthy and sustainable development of the chain block industry.

Keywords

block-chain technology; financial system innovation; ledger data structure; decentralization

* Corresponding author at: College of Economics and Management, Yanshan University, Qinhuangdao 066004, China
E-mail address: suying@ysu.edu.cn

1. Introduction

Since the second half of 2015, “block-chain” has become one of the hot topics of most concern to the world’s major financial giants. In December 2015, the National Association of Securities Dealers Automated Quotations (NASDAQ) took the lead in launching the block-chain-based securities trading platform “Linq”, which became an important milestone in the decentralization trend of the financial securities market. Then, professional audit service companies such as *Deloitte* and *Ernst & Young* established block-chain research and development centres. The team is committed to improving the quality of its client audit services. Based on the BaaS (*Block-chain as a service*) service launched by *Microsoft’s* cloud service platform *Azure*, the capital market start-up *3CEV* has signed agreements with more than 40 large banking institutions around the world, such as *Bank of America* and *Citibank* in the beginning of 2016. The Block-chain cooperation project is committed to formulate block-chain industry standards and protocols for the banking industry (Yuan and Wang, 2016). In October 2015, *The Economist*, a well-known British economics journal, published a ten-page article titled “*Behind Bitcoin will be the driving wheel of the future economy.*” With virtual currency and block-chain technology, it is believed that block-chain technology will change our future economy and life (Wang, 2016). From the perspective of value scale, only some mainstream encryption currencies (such as Bitcoin) can set prices for other currencies, and most of them can be priced with legal tender (such as US dollar) (Dyhrberg et al., 2016). Since May 2018, encryption currencies have entered the price downward channel, and the pricing power of legal tender against encryption currencies. The liquidity proportion of stable currency anchored by legal tender (such as USDT and TUSD) has also gradually increased. In order to overcome excessive fluctuations in the price of encryption currencies and promote the development of cross-border payments, *Facebook* published a *Libra* white paper targeting global digital currencies in June 2019, aiming to anchor a basket of bank deposits and short-term *Treasury* bills to achieve price stability. In addition to the stability currencies that anchor the legal tender, the price fluctuation range of encryption currencies is larger than that of traditional financial assets, which makes it unable to perform the function of value measurement (Zhang and Wu, 2019). Xu (2018) studied the functions of block-chain from the perspective of economics. Based on the economic explanation of block-chain technology, he summarized the “*Token paradigm*” adopted by the mainstream block-chain system at present, clarified the two basic concepts of consensus and trust related to block-chain, and sorted out the functions of intelligent contract (Xu and Zou, 2018). Luo (2018) pointed out Bitcoin and other new forms of finance based on block-chain technology have exerted a profound influence on the development of Internet finance and the reform of other financial fields. The application value of block-chain in the financial field can be realized through the security, credibility and uniqueness of the data supported by block-chain technology (Luo, 2018). Ouyang (2018) analysed the working principle of block-chain technology to promote the development of inclusive finance. He summarized the challenges that may be faced, and put forward corresponding policy suggestions which included financial knowledge education and infrastructure construction, industry application standards, talent reserve, and cooperative innovation (Ouyang and Li, 2018). Zhai (2018) started from the pain points in the field of securities market segmentation and analysed the advantages of block-chain technology to bring innovative solutions and promote the reform of business model. Taking the digital assets as the core and referring to the elements of the traditional securities market, he analysed the new segment of the digital assets-oriented securities market (Zhai et al., 2018).

At present, there is a lack of systematic analysis on the application scenario of block-chain in the financial field. This article first introduces the principles and characteristics of block-chain technology;

secondly proposes that block-chain technology will lead a new round of financial system innovation; thirdly focuses on the application prospects of block-chain technology in the financial field; then warns that attention should be paid to the financial risks arising from the application of this technology; and finally puts conclusion and implications.

2. Principles and Characteristics of Block-chain Technology

Strictly speaking, the block-chain is a data structure that creates a digital transaction ledger. The ledger is in a shared state in a distributed computer network, rather than a single provider. Sharing data will build a more transparent and publicly verifiable system. It will fundamentally change the way we think about transaction activities, asset value, contract performance, and sharing data across industries. The block-chain will eliminate the uncertainty in human transactions by technical means. Through the block-chain, logical data records will be connected in time series; coupled with cryptography technology, all parties to the transaction will have a copy that changes with the completion of the transaction.

From a technical point of view, the block-chain system consists of six core layers: data, network, consensus, incentive, contract and application. The data layer encapsulates the underlying data block, chain structure, timestamp, hash function, Merkle tree, and related data encryption technologies; the network layer includes distributed networking mechanism, data transmission mechanism and data verification mechanism, etc.; the consensus layer mainly encapsulates various consensus algorithms that can support the operation of network nodes; the incentive layer integrates economic factors into the block-chain technology system, mainly including economic incentives such as issuance and distribution mechanisms *Elements*; the fifth layer of the contract layer mainly encapsulates various script codes, algorithms and smart contracts as the basis of the programmable features of the block-chain; the sixth layer of application layer encapsulates various application scenarios and cases of the block-chain, and its operation. The principle is shown in Figure 1.

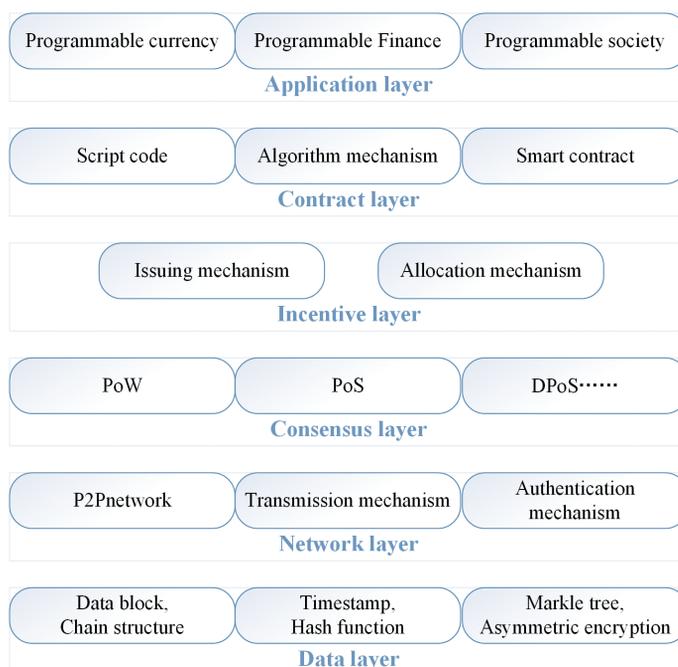


Fig. 1 The infrastructure model of Block-chain

Source: Collecting and drawing by authors

The following focuses on the key technology, the chain block structure based on timestamp (see Figure 2). As it can be seen from the figure, each data block is composed of four elements: including the hash value of the previous data block (*Bits*), the timestamp of this data block (*Timestamp*), Random number (*Nonce*) and Merkle root (*Merkle-root*). Among them, the hash value of the previous data block builds a corresponding relationship with this block, and connects up and down to form a chain; the timestamp records and stores the time period during which the block runs, solves the nonce value of the random number, and all verified miners will obtain the accounting rights of the current block, form incentives, and provide the computing power required by the system; the Merkle root of this block includes the array of secret keys for storing various information in this block, and only the password can allow the customer to obtain the data information of the block chain. Each block body includes the number of transactions in the current block and all verified transaction records generated during the block creation process. In short, the block-chain technology based on encryption algorithms builds a global distributed secure network database that records and updates transaction information through decentralized chain connections and block chronological arrangement.

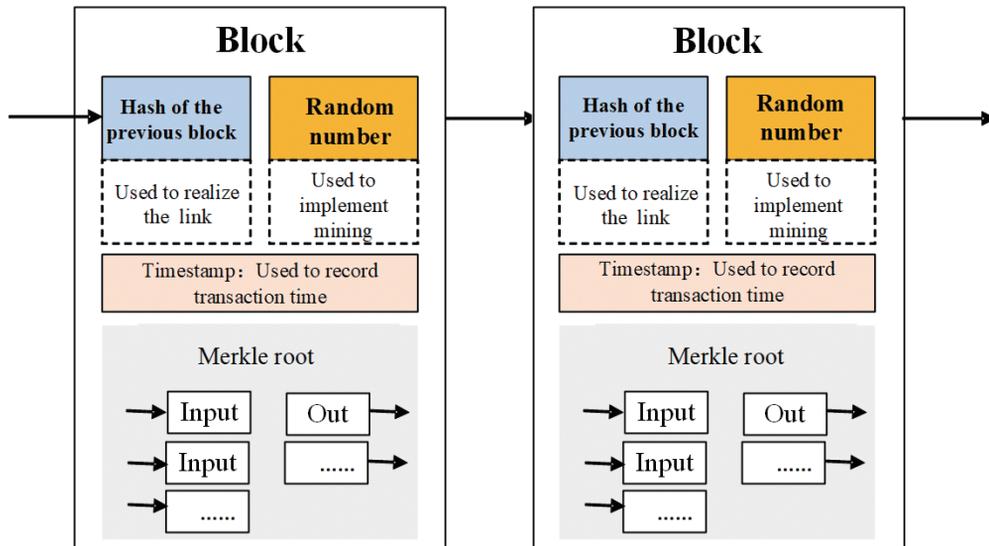


Fig. 2 The structure of Block
Source: Collecting and drawing by authors

In the design of block-chain technology, the chain block structure is based on timestamp, while the economic incentive design is based on consensus algorithm. The consensus mechanism of distributed nodes and the flexible and programmable smart contract are the most unique innovations of block-chain technology. Block-chain technology solves the data problems of decentralization, privacy protection, and non-tampering of data information through distributed accounting design (Yi, 2016).

The following paragraphs take financial business as an example to introduce the specific characteristics:

One of the specific characteristics is the decentralized structure. The trust mechanism of block-chain technology is established on the basis of asymmetric cryptography. With the help of open-source algorithms, each node can automatically reach a consensus when data is exchanged. The operation of the entire system is open and transparent, ensuring information security at the same time. In other words,

this system does not support the central core system, and there is no central payment clearing institution. Information exchanges between network nodes are directly carried out. Any node damage will not affect the operation of the entire network, and the continuity of financial services is adequately guaranteed, greatly improving the efficiency of transaction operation, while reducing transaction costs.

The second special characteristic is that the data cannot be tampered with and are safe. Since the accounting and storage functions of the block-chain are allocated to each participating network node, a series of risks that may be caused by server crashes in the centralized storage mode are avoided. At the same time, a super large database formed by all nodes of block-chain technology not only stores all transaction data (including account opening, payment, transactions, etc.), but also has strong fault tolerance. In theory, as long as there is no control with more than 50% of the computing power of the entire system, the data cannot be tampered with. The more nodes involved and the stronger the computing power, the more secure the data.

The third character is complete anonymity protection while information is open and transparent. Block-chain technology uses public key addresses to replace the identity information of bank users, enabling bank users to complete anonymity protection while disclosing information. In other words, any piece of financial transaction data on the block-chain is open and transparent, but the corresponding financial transaction data is not tied to an individual, so it is impossible to know who the specific trader is, which greatly protects the financial transaction of personal privacy of activists.

3. Block-chain Technology Leads to Financial System Innovation

Block-chain technology solves the problems of decentralization, information security, and information disclosure in financial transactions. In theory, it can fully optimize the financial market environment and change the payment and settlement system, credit management mode, and IT system technology in the traditional financial system. The architecture and the financial Internet of Things are further intelligent to create a faster financial system with lower transaction costs.

3.1. The underlying technical foundation of payment and settlement will be completely changed

At present, the bank's payment and settlement relies on the completion of the central institution. The entire process includes multiple steps such as initiation of payment, information feedback, bookkeeping, transactional hedging, and balance reconciliation. The process is very cumbersome and complex, and the payment and settlement of a single fund costs more time and expense cost. If the entire system of the central bank adopts the block-chain technology architecture, commercial banks will conduct peer-to-peer payment and clearing, eliminating the need for a payment clearing centre, making payment and clearing services faster, and greatly reducing operating costs. Companies such as *Ripple*, *A-bra*, *Bit-spark*, and *Circle* are currently actively developing various payment and clearing applications, but so far only the *Ripple* system has achieved commercial applications. The comparison between traditional payment and settlement systems and block-chain payment and settlement systems is shown in Figure 3.

3.2. Credit risk management model will undergo major adjustments

The credit risk management work in the existing financial system is accomplished through the unified management of credit data through the central bank's credit investigation centre, while sharing data with financial institutions, and providing users with credit data inquiries. The credit investigation

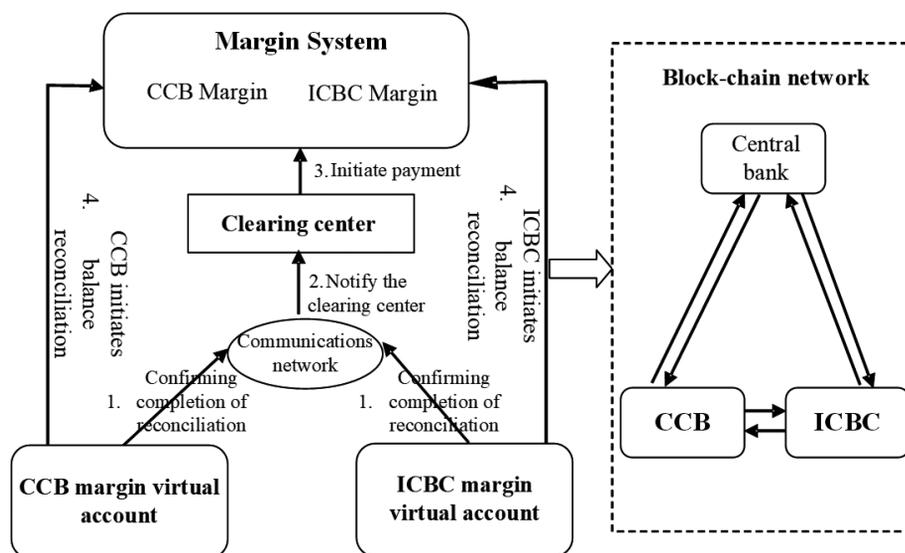


Fig. 3 Changes in the underlying technical foundation of payment and settlement
 Source: Collecting and drawing by authors

system based on the block-chain will directly deploy the financial transaction data and other related credit data of individuals and enterprises in the data block. Financial institutions can directly complete the credit investigation activities through the block-chain, which overcomes the problems of incomplete information, delayed data update and high cost caused by the central organization. At the same time, with the application of block-chain technology in the field of asset authentication, the physical assets in society will complete the digital asset management model in the form of codes, which means that commercial bank asset mortgage management, settlement processing and other business adjustments will be made to the processes. Due to the networking of credit management, the Internet will transform from an information network to a value network, and the credit risk management model is bound to face significant adjustments.

3.3. The technical architecture of the IT system in the financial system will be subverted

At this stage, the IT support system of financial institutions relies on infrastructure such as *PC server, Windows Server/LINUX* and *NET/J2EE*. The structure requires a large number of middle and back-office personnel to perform transactions such as account registration, payment and settlement. Part of the work requires manual operations. This kind of IT architecture is not only inefficient, but its operation and maintenance costs are very high. Block-chain technology will change the situation of traditional IT systems in the financial service industry. For example, in many complex transaction projects, multiple transaction entities will be involved, and the conditions for transaction triggering are more complicated. If multiple signatures of the block-chain are used through smart contract technology, it can automatically execute the work processes of transaction registration, accounting, payment and settlement, which greatly improves work efficiency and effectively reduces operation and IT system maintenance costs. It can be predicted that the entire organizational structure of financial system will be completely subverted (Swan, 2015).

3.4. Financial Internet of Things will be more intelligent

The financial Internet of Things will undoubtedly be the most potential and broad application

prospects for the development of the financial industry. If block-chain technology joins, it will prompt the Internet of Things to establish a low-cost trading platform based on a large number of smart devices, and improve the security and privacy of the overall system through centralization and consensus mechanisms. The smart contract setting in the block-chain enables the financial Internet of Things to achieve automatic management processes, ensuring information security and privacy, and at the same time, it can better promote the autonomy of financial equipment, which means that block-chain technology can promote the optimization and improvement of the financial Internet. It makes the application of block-chain technology extend to a wider field.

4. The Application Prospects of Block-Chain Technology in the Financial Field

Due to its above-mentioned technical characteristics, the main research and application fields of the block-chain are carried out in the financial field. At present, the block-chain technology is being used in digital currency, payment and clearing, smart contracts, and financial transactions. There are relatively broad application prospects in many fields, such as Internet finance.

4.1. Digital currency

In the current monetary system, digital currencies represented by Bitcoin are slowly coming. The digital currency system created by block-chain technology has typical characteristics of decentralization. Taking Bitcoin as an example, unless more than half of the nodes are supported (meaning more than 51% of the nodes in the network system are supported), no node can independently modify the total amount of bitcoin production, distribution methods and trading rules. In terms of supply, according to the Bitcoin system algorithm, 10.5 million Bitcoins will be produced in the first four years; every 4 years, the Bitcoin contained in each new data block is reduced by half. In other words, in the fifth to eighth years, only 5.25 million bitcoins will be made, and in the ninth to twelfth years, only 2.625 million bitcoins will be made. Theoretically speaking, the cumulative total of Bitcoin is the sum of a decreasing geometric sequence in mathematical principles. Then by 2140, the cumulative total of Bitcoin will reach the highest value of 21 million (Wenker, 2014). This property of Bitcoin is similar to gold. Gold reserves determine the total amount of money, avoiding the problem of spamming that may be caused by paper money. It is an ideal currency expectation (Wang, 2016).

4.2. Payment and settlement

At present, the basic mode of global commercial and financial transactions is a centralized mode. In this traditional mode, the payment and settlement of any commercial transaction must be completed through the banking system. In other words, when a transfer transaction occurs, either through online banking or mobile phones, the transaction information must be transmitted to the headquarter data centre of the bank account processor. Then, the data recording and fund transfer will be completed. The customer funds and account information will be stored in a core system server during this process. Each institution must establish a financial accounting system and an agency relationship, for which the entire process will take a high cost of time and expense.

Compared with traditional bank centralized payment and clearing, block-chain technology can realize the point-to-point direct payment and clearing business of both parties to the transaction, without the need for intermediaries, which greatly reduces the time and expense costs. Especially for cross-border

payments, if a financial transaction system is built through distributed block-chain technology, users can make real-time payments and clearing services on a global scale, and cross-border payments will be fast and low-cost. If a universal distributed inter-bank financial transaction system is constructed based on block-chain technology, it can provide users with global cross-border, real-time payment and clearing services in any currency, as well as cross-border payments will become convenient and inexpensive. In the field of international payment, the experimental application of the payment system based on block-chain technology developed by *Ripple* in 2012 has begun, mainly to provide member commercial banks and other financial institutions with foreign exchange transfer solutions based on block-chain protocols. At this stage, *Ripple* provides software for different financial institutions to connect to the *Ripple* network. Member banks can maintain the original accounting method. *Ripple's Inter ledger protocol* can be used as long as minor system changes are made. And transaction and payment information between banks is passed while the encryption algorithm hides the details of the transaction, which means that the details of the transaction will not be seen by the counterparty. Only the bank's own accounting system can track the transaction details, which fully guarantees the security of payment and transaction activities of financial institutions (He and Mao, 2016).

4.3. Smart contract

Smart contracts were first proposed by cryptographer *Nick Szabo* in 1994. They were originally defined as: "a set of digitally defined promises (promises), including agreements on which contract participants can execute these promises." Smart contracts were originally designed to be written into computer-readable code for creating various flexible and controllable smart assets. However, due to the backward calculation methods and the lack of application scenarios, the research and application of smart contracts were restricted.

However, the emergence of block-chain technology redefines the smart contract, which is the core component (contract layer) of the block-chain. Specifically, a smart contract is a set of scenario-responsive procedural rules and logic, and it is a decentralized, trusted and shared program code deployed on the block-chain. Smart contracts have the general characteristics of block-chain data, such as distributed records, time series, immutability and forgery, etc. The parties who signed the contract reached an agreement on the contract terms, breach clauses, liability for breach of contract, verification and audit and

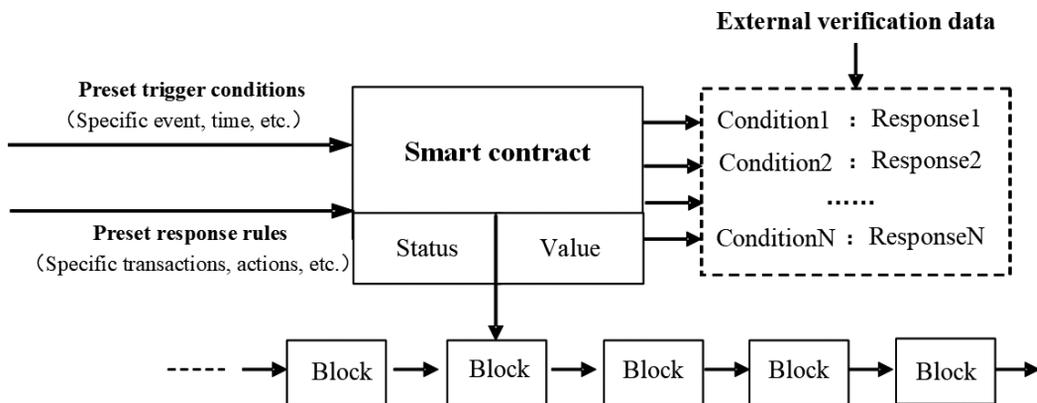


Fig. 4 The operating mechanism of smart contract

Source: Collecting and drawing by authors

other data sources, and after they passed the contract code test successfully, they were deployed on the block-chain in the form of smart contracts, so they did not rely on any intermediary agencies. The contract will be automatically executed on behalf of each signatory, and the programmable feature of the smart contract allows the signatory to add arbitrary complex clauses.

Block-chain and smart contracts have broad application prospects in the field of Internet finance. For example, business models such as equity crowd funding or P2P network lending can be realized through them. The traditional mode of equity crowd funding or P2P lending is to complete fund raising, fund management and investment through intermediary institutions such as exchanges or online platforms. In actual operation, it is prone to financial risks caused by the moral hazard or adverse selection of intermediary institutions. Using smart contracts, the operations can be automatically executed on the block-chain through decentralized code design (see Figure 4 for the operating mechanism). The data block can record each financing according to the time series through time-stamp and other elements. It can calculate the equity share of each investor when a specific financing quota is set, or automatically return the funds to the investor when the financing quota is not reached within a period of time. For another example, in the transaction process of physical assets such as houses or vehicles, asymmetric encryption technology can be used to embed physical assets such as houses or vehicles into smart contracts with specific access rules and deploy them on the block-chain. Access rights can use these assets, which can effectively solve the difficulties of asset handover and licensing delays in the physical asset leasing business model.

4.4. *Financial transactions and audit*

Block-chain can automatically generate credit in a decentralized system, establish a financial market without a central institution, and realize a market environment in which financial transactions can be independent of third-party credit. This requires intermediary agencies for third-party payment and fund custody. The business model is a disruptive change. There is also a high degree of fit between block-chain technology and financial transactions. For example, securities and banking are also important application areas of block-chain. Traditional securities transactions need to go through central institutions such as central clearing institutions, banks, securities companies, and exchanges. The need for multiple coordination, and the use of block-chain automated smart contracts and programmable features, avoiding the cumbersome centralized clearing and delivery process, and realizing convenient and fast financial product transactions; at the same time, the features of block-chain and digital currency are instant arrival. It can enable banks to achieve faster, more economical and safer cross-border transfers than the *SWIFT* code system. This is also an important reason why financial giants such as *R3CEV* and *NASDAQ* have successively invested in the research and development of block-chain technology.

In addition, because block-chain technology can guarantee the integrity, permanence, and immutability of all data, it can effectively solve the difficulties of the audit industry in transaction forensics, tracking, association and backtracking. Deloitte has established a dedicated team to study the application of block-chain technology in auditing since 2014. At present, it has cooperated with some commercial banks and enterprises to successfully create experimental solutions for block-chain applications. *Price Water House Coopers* has entered the field of block-chain technology research since 2016, and currently has dozens of outstanding researchers in this field. At the same time, it cooperates with block-chain professional technology companies *Block-stream* to seek providing security for various enterprises around the world fast economic and financial audit services (Melanie, 2016).

5. Financial Risk Expectations and Countermeasures in the Application of Block-chain Technology

5.1. Financial risks and countermeasures that may be caused by technical problems

Block-chain technology is based on timestamp-based chain block structure, consensus algorithm-based economic incentive design, distributed node consensus mechanism and flexible and programmable smart contracts. Block-chain technology solves data problems such as decentralization, privacy protection, and non-tampering of data information (Dyhrberg *et al.*, 2016).

But even so, there are still some technical problems in block-chain technology. Among them, the block-chain based on the Proof of Work (PoW) consensus process mainly faces the 51% attack problem. Taking Bitcoin as an example, according to statistics, the computing power of China's large mining pools has accounted for more than 60% of the total computing power of the entire network. In theory, these mining pools can cooperate to implement 51% attacks to achieve double payments in Bitcoin (Ding, 2015). Secondly, due to the development and popularization of mathematics and computing technology, the asymmetric encryption mechanism of the block-chain will also become more and more risky. Furthermore, the privacy protection of the block-chain is not absolutely secure. Each node in the block-chain system is not completely anonymous while it realizes data transmission through address identification (such as Bitcoin public key address). Although the address is identified that it is not directly associated with real-world character identities, block-chain data is completely open and transparent, with the development of various anti-anonymity identification technologies, it is still possible to achieve the positioning and identification of some key targets. The above-mentioned technical security will cause systemic risks to the financial system. For this reason, banks and other financial institutions are required to promote experimental application projects, conduct scenario exercises, and do sufficient technology before advancing the block-chain technology system. The practice of reserve and application projects achieves an understanding of the in-depth principles and technical problems of block-chain technology to find and solve those problems.

5.2. Financial risks and countermeasures that may be caused by resource problems

The achievement of the PoW consensus process mainly relies on the contribution of the computing power of each node of the block-chain network. These computing powers are mainly used to solve the hash value and random number search. In addition, there is no other economic value, which is usually considered as a waste of computing power. At the same time, in order to maintain huge computing power, a large amount of power resources is needed. Taking Bitcoin as an example, with the increasing popularity of Bitcoin and the emergence of professional mining equipment, the Bitcoin ecosystem has shown a clear arms race in terms of capital and equipment, and has gradually become a capital-intensive industry with high energy consumption. The problem of resource consumption is becoming more and more serious (Zhang *et al.*, 2016). It is an important issue that how to effectively pool the network computing power of distributed nodes to solve practical problems in the financial field. At present, major financial institutions are making large-scale investments and designing efficient interaction mechanisms to gather and use the swarm intelligence of distributed consensus nodes. The investment of Chinese financial institutions in this field is very limited, and the technological observation is urgently needed to make timely adjustments to advance the technological level of China's financial institutions.

5.3. Financial risks and countermeasures that may be caused by competition issues

As a decentralized distributed system, the block-chain network inevitably has a game relationship of mutual competition and cooperation during the interaction process. Let's take Bitcoin as an example too, Bitcoin mining pools can cooperate with each other to maintain their own stable income, but there are often mining pools blocked by block with holding attacks, and the operators of the corresponding nodes disguise themselves as opponent mines. Miners in the pool can enjoy the revenue of the opponent's pool and reduce the revenue of the opponent's pool. When the mining pool's revenue function meets certain conditions, this attack and competition will result in the "Prisoner's Dilemma" game ending (Wang et al., 2015). How to design a reasonable penalty function to suppress irrational competition and make cooperation a stable and balanced solution for repetitive mining pool games is a problem that still needs to be solved when block-chain technology is applied in practice. In addition, the block-chain consensus process is essentially a multi-person participation process. It is key problems that how to design an incentive-compatible consensus mechanism so that self-interested nodes in a decentralized system can spontaneously implement block data verification and financial transactions.

In summary, the security of data in the decentralized structure of block-chain technology cannot be tampered. But due to its broad application prospects in the financial field, we should not ignore that the basic theory and technical application research of block-chain in its infancy. There are many fundamental scientific and technical issues that are critical to develop the block-chain industry and the application industry.

6. Conclusion and Implications

Due to its decentralized data structure, non-tampering data, openness, transparency, and autonomy, block-chain will change the credit management mode of the traditional financial system. But it has such shortcomings as technical maturity, resources, reserves, and of the regulation of competition, therefore further studies need to be done. The following suggestions were about how to do block-chain technology application prospect in the field of finance.

Firstly, explore the application of block-chain technology to improve the level of financial services. The cost of integrating block-chain technology into the existing financial system is high, and large-scale input and application will involve the remodeling of IT architecture and business processes. Therefore, it is a safe way to start from small scale pilot exploration and gradually expand the application scope. Only by continuously testing and evaluating the stability and scalability of the technical framework through the pilot, constantly summarizing and finding problems, and testing the feasibility and effectiveness of the application framework in the pilot, can it provide reference basis for further promotion in more fields. From the perspective of financial regulatory institutions, they can make full use of the convenience of block-chain technology to improve the way of supervision and improve financial infrastructure, such as considering the establishment of a controlled and authorized block-chain application system at a certain level and improving the financial service system. From the perspective of financial institutions, block-chain technology can be used to make breakthroughs in some businesses. For example, small-scale experiments can be carried out in areas such as auditing and asset management.

Secondly, gradually establish a regulatory system with flexible supervision. The application of block-chain technology in the financial field can be understood as the embodiment of "finance + cryptography + distributed accounting technology + consensus mechanism + other technologies". The regulation of

its technology application is relatively complex for the combination of technology and finance, relevant enterprises and institutions, and cross-industry, cross-field innovative technology. In view of this, it is suggested that in the early stage of the application of block-chain technology, flexible supervision should be given priority. While controlling risks and protecting consumers' rights and interests, incentive measures and trial-and-error rules should be introduced to encourage qualified financial institutions to innovate and use block-chain technology to carry out their own businesses.

Thirdly, improve the formulation of relevant standards for block-chain technology. We should explore standards for the application of block-chain technology in the financial industry, and actively promote the pilot application of block-chain technology standardization in the financial industry. The block-chain standard design needs to strengthen the top-level design of the standard architecture, and focus on the compatibility with the existing basic standard protocols to support the interconnection and interworking of the system. For example, as the basic protocol in the domestic interbank market, the current IMIX protocol was used as the application promotion of digital currency based on block-chain. It can be extended based on IMIX protocol to reduce the subversive transformation of the existing standard system.

References

- Ding, W., 2015. An innovation system for instrument data management based on block-chain technology. *China Instrumentation*, 10, 15-17. (In Chinese)
- Dyhrberg, A.H., Foley, S., Svec, J., 2016. How investible is Bitcoin? Analyzing the liquidity and transaction costs of Bitcoin markets. *Applied Economics*, 19, 1799-1815.
- He, M., Mao, J.H., 2016. Block-chain: Changing the financial industry infrastructure. *CICC Research Report*, 1(29), 7-14.
- Luo, W., 2018. The innovation and application of block-chain technology in the financial field. *Journal of Technical Economics & Management*, 8, 90-95. (In Chinese)
- Melanie, S., 2016. *Block-chain: New economic blueprint and guide*. Beijing, New Star Press.
- Ouyang, H.B., Li, W., 2018. Application research of block-chain technology in China's inclusive finance field. *Wuhan Finance*, 4, 36-40. (In Chinese)
- Swan, M., 2015. Block-chain thinking: The brain as a decentralized autonomous corporation. *IEEE Technology and Society Magazine*, 34(4), 41-52.
- Wang, F. Y., Wang, X., Yuan, Y., et al., 2015. Social computing and computing society: The foundation and necessity of a smart society. *Chinese Science Bulletin*, 60(5-6), 460-469.
- Wang, S., 2016. Analysis of the research status and innovation trend of block-chain technology in the financial field. *Shanghai Finance*, 2, 26-30. (In Chinese)
- Wang, S., 2016. Research on block-chain legal tender system. *Economist*, 9, 77-86.
- Wenker, N., 2014. On line currencies, real-world chaos: The struggle to regulate the rise of Bitcoin. *Texas Review of Law & Politics*, 19(1), 145-197.
- Xu, Z., Zou, C.W., 2018. What can and cannot block-chain do? *Journal of Financial Research*, 11, 1-16. (In Chinese)
- Yi, Y., 2016. The status quo of the development of block-chain-analysis of the challenges and countermeasures facing the banking industry. *Financial Accounting*, 4, 46-51. (In Chinese)
- Yuan, Y., Wang, F.Y., 2016. Blockchain: The state of the art and future trends. *Acta Automatica Sinica*, 42(4), 481-494. (In Chinese)
- Zhai, C.X., Xu, W., Xu, K. et al., 2018. Application and regulatory research of block-chain in China's securities market. *Financial Regulation Research*, 7, 33-54. (In Chinese)
- Zhang, L.Q., Wu, T., 2019. The application of block-chain in the financial field: Theoretical Basis, Realistic Dilemma and Cracking Strategy. *Reform*, 12, 65-75. (In Chinese)
- Zhang, N., Wang, Y., Kang, C.Q., et al., 2016. Block-chain technology in the energy internet: A preliminary study of research framework and typical applications. *Proceedings of the CSEE*, 15, 4011-4023. (In Chinese)