Technical Analysis and Application Scene of Blockchain Society

Wen Si, Jiankang Zhang*
School of International Economics and Tourism Management, Zhejiang International Studies University, Hangzhou, Zhejiang310012, China
693295009@qq.com,88018456@163.com
*Corresponding author

Abstract. There are many problems in the current social, it’s urgent to build blockchain society. As a distributed consensus system, blockchain can effectively solve four problems: storage, transmission, expansion and consensus. Especially the blockchain system has the characteristics of decentralization, its information is open and can not be tampered with. Its data exchange is based on cryptography to ensure the accuracy of the data. Blockchain technology can also enhance the efficiency of notarization and certification. These advantages make the blockchain society a necessity for the development of blockchain technology and a model for the transformation of social production and life style. Its application scenarios include payment of remittances, free trade, equity settlement, intelligent contracts, authentication, audit profession, crowd-funding, bill business, asset-confirming and intelligent Internet of things, etc.

1. Introduction
Blockchain technology has been widely used in big data era. Besides the financial field, the technology of blockchain decentralization, irrevocable and highly transparent has been found to be able to be applied in many fields. Its technology development from the first stage of virtual currency, to the second stage of intelligent contract derivative, will develop to the third section of the blockchain society, to provide solutions for many problems in the social field. The whole social system is based on a blockchain.

2. Physical structure of blockchain technology: distributed consensus system
Building a blockchain society requires a distributed consensus system, which is a common decision, operation and maintenance system for all participants. It can effectively solve four problems, such as storage, transmission, expansion problem and consensus problem, which lays the foundation for the construction of blockchain society.

2.1 Storage problems in distributed consensus systems
The data in the blockchain is stored in the storage medium of the computer, based on the application of cryptography, the stored data is encrypted and processed, which ensures the security and privacy of the user data[1].

2.2 Transmission of distributed consensus systems
How to realize the fast and safe transmission of data information? The solution of transmission problem is due to the improvement of Internet transmission speed and stability. With the continuous upgrading of the network transmission speed and the continuous improvement of the communication infrastructure of various countries, the global rapid and stable transmission of data will gradually become a reality.

2.3 Extension of distributed consensus systems
How to scale up the system? Nakamoto uses economic incentives to encourage people to participate in the system, in which every qualified participant (decision maker, operator) can reap the economic benefits of bitcoin, which is called a node. The number of nodes in a distributed consensus system basically represents its size.

2.4 Consensus issues in distributed consensus systems
The consensus problem comes to first. When the consensus system is running on a small scale, we think that each node is basically credible, so it doesn’t require many complicated conditions to reach a consensus. However, when the application scope of the system is extended to the whole world, the honesty of each node can’t be guaranteed, how to prove the authenticity and reliability of the node becomes a difficulty. In response to this, people have developed a variety of consensus proof mechanisms, including workload proof (PoW), equity proof (PoS), share authorization proof (DPoS), Byzantine fault-tolerant algorithm (Pbft).

In general, blockchain is a distributed consensus system based on the idea of decentralization.

3. Social problems require blockchain society
At present, the payment system is inefficient, credit data sources are narrow, anti-money laundering supervision is difficult, audit work is expensive, the cost of notarization certification is high. It needs to be solved urgently through the construction of blockchain society.

3.1 Inefficiency of the payment system
In the process of completing a cross-bank payment business, the capital data flow has to go through complicated intermediate links, such as the commercial bank's internal system, the people's Bank of China's inter-bank clearing and so on, and the inter-bank expenses incurred during the process, the delay of large transaction can lead to the problems of high cost and low efficiency of payment and settlement[2]. There will be some potential risks of system failure and a few disputes with fuzzy boundary of power and responsibility.

3.2 Narrow sources of credit data
The credit data of individuals and enterprises in China mainly come from the financial credit data of the credit information system of Bank of China. When commercial banks handle credit business, they obtain credit information data from credit information system after authorized by customers, which is more authoritative. However, at present, the credit system of centralized data management has not realized the sharing of resources and information with the Internet financial data platform, and the scope of application is limited, so it is difficult to solve the problem of asymmetric credit information. Compared with the rapid development of Internet data platform in recent years, the coverage of credit data sources is small and the information is incomplete, which helps to judge the non-financial information, such as water, electricity, gas, communication and so on, without being included in the credit system.

3.3 Difficulties in regulating anti-money-laundering
Besides ID number and telephone number, the authenticity of other information is difficult to verify. Customers are engaged in financial activities through online banking, mobile banking, WeChat, Alipay and other network payment methods, financial institutions are difficult to supervise the sources
and uses of customers' funds effectively. China's relevant system, laws and regulations and technical means still need to improve.

3.4 Audit work is costly
In the field of auditing, auditors need a lot of manpower and material resources to verify the authenticity of transactions. In theory, there can be no interest dependence or management relationship between CPA and manager. The problem is that the decision-making power of a company to choose a CPA is in the hands of the management. The cost of hiring and the way of payment may have an impact on the interest relationship between the audited enterprise and the CPA. There is no effective separation between the independence and the paid service.

3.5 The cost of notarization is high
Traditional authentication system is slow, can’t find, upload, download the corresponding data. In existing cases, records are done manually, and the protection of recorded data, synchronous updates, and verification of authenticity are of a great difficulty. Computer records are easily change after computer automation. Therefore, the cost of authentication system is high, storage is complex, there are great risks. Once a unified electronic escrow is damaged, much of the data cannot be restored[3]. It is necessary to mention that in today's economic conditions, trust is rare. The lack of trust has resulted in a significant amount of resources, which is being devoted to audit and record verification. These reduce productiveness and mercantile rate of return.

4. Blockchain Society: scientific and technological change production and life style

4.1 Blockchain system is characterized by decentralization
The transaction behavior of any node requires all nodes in the block network, to pass the verification and update the account book before it can take effect, so as to realize the mutual supervision between nodes and the self-certification function in the whole network. This model subverts the traditional trust model which needs the help of the bank, Alipay and other trusted third parties. It builds the mutual trust model between the two sides of the transaction and solves the credit problem in the financial activities effectively. At the same time, the point-to-point data and information interaction mode can avoid the complicated system transaction intermediate link, break through the current situation of separation of the existing systems. It can set up a low cost and fast payment way and build flat global integrated clearing body department.

4.2 Blockchain information is open and untampered
Each node in the blockchain network can participate in the bookkeeping and maintain the book data through competitive calculation. In addition to private information is encrypted, blockchain data is open to public, the system information is transparent. On the other hand, the information that is verified and stored on the blockchain cannot be modified by a single or a few nodes, unless more than half of the nodes in the system confirm the modification of the data. Therefore, the data on the blockchain are of a great stability and reliability. Relevant institutions can record and keep credit information of all kinds of financial activities on the node of blockchain, widen the coverage of information and increase the time limit of information by taking advantage of openness. By using its non-tampering advantage, it can effectively prevent credit fraud events and ensure the integrity of the data[4]. According to demand, financial institutions can seek information and obtain relevant credit data, which can reduce the negative impact caused by asymmetric information and further improve the construction of credit information system to some extent.

4.3 Blockchain data exchange is based on cryptography
Digital signature technology ensures that each transaction can be traced back. Financial institutions provide the private key of electronic identification for the entity in the transaction, match the user
address to the electronic identification information. Each transaction must be verified by the private key and the public key which is held by bank. Only when the two are matched, can the transaction be facilitated. That means, the authenticity and legitimacy of the data in the blockchain are guaranteed. Therefore, reliable technical support for anti-money laundering can be provided.

4.4 Blockchain technology improves efficiency of notarization and certification
Each block is like an account book, where the "account book" generated by the transaction is linked to other books, the details of which are recorded and anyone can verify the transaction. At the same time, the blockchain will use distributed accounting to build an immutable record of property rights, providing a higher level of transparency and accountability.

5. Application scenario of blockchain society
Blockchain society consists of public chain, alliance chain and private chain. As the three major forms of blockchain society, they construct payment of remittances, free trade, equity settlement, intelligent contracts, authentication, audit profession, crowd-funding, bill business, asset-confirming and intelligent Internet of things and so on.

5.1 Payment of remittances and free trade
At present, people are subject to a variety of conditions when dealing with cross-border remittance transactions, such as the must to provide relevant certificates and pay high fees, the must to process cross-border remittance transactions at a specific time and provide all kinds of information. Procedures are cumbersome and time is wasted. Users can complete cross-border transfers faster and at a lower cost with the help of blockchain technology. Instead of relying on a central payment system to liquidate funds and store all transaction information, both parties can transfer value directly based on a consensus mechanism that doesn't require trust coordination[5].

As we all know, Alibaba provides consumers with direct access to small businesses, while its other major shopping scene, Tmall, provides consumers with links to larger brand retailers. Alibaba's profit model is based on the paid service to merchants, which is a successful third party intermediary essentially. Based on the development of block-chain technology, we have a "open market". It uses the open source point-to-point technology to realize the direct transaction between the buyer and the seller, without a centralized platform[6]. Trust, security and dispute resolution are all handled by the system. You can connect directly to other users of the network and trade only by running a program on computer. The network is not controlled by a company, nor is it managed by an organization. It goes to a central mall, so you don't have to pay for advertising.

5.2 Equity settlement and intelligent contracts
The present situation "two networks" are separate, which increases the cost burden of securities firms, increases the risk of capital turnover. It is not conducive to the flow of securities firms and investors, limits the overall development of the national market finally. What's worse, the system is limited to provide services for the venue, only for member organizations. However, blockchain technology can not only realize the core function of banking value storage and transfer center, but also solve the problems of securities clearing and settlement effectively. Blockchain accounts can achieve digital management of securities registration, equity management and securities issuance. In essence, it is "decentralization" in the process of securities settlement and clearing, neglecting middleman and backstage, reducing the high cost of third party audit, accounting and verification, thus reducing transaction cost. The securities exchange settlement system modified by blockchain technology can enable the buyer and seller to realize the automation directly with the intelligent contract. What's more, it can pair and automatic settlement through a distributed digital system.

At present, traditional contracts refer to two or more parties to hold an equivalent exchange by agreement, both or parties must trust each other, so that they can make the transaction. With the help of blockchain technology, contracts are defined by code and enforced by code. Here comes smart
contracts. It’s digital protocol for assets that include where the underlying asset is and how it will be executed without human intervention. It is a replicable, shared account book, proving loyalty to the other side is unnecessary. As a result, it can reduce commercial transactions fraud, but also reduce law enforcement costs. In addition, smart contracts have the potential to help the one who has no advantages to open the door of the justice system. It can also be a financial boon for low-income people, helping them gain more access to credit.

5.3 Authentication and audit profession
In today's society, there are times when we need to prove who we are, to prove our family, to prove our real estate and so on. Going to government agencies for a long and cumbersome process of proof is a real headache, sometimes we don't even know how to do it. You can see a smart identity system as an "electronic identity card" that contains your name, year of birth, email, contact information, e-mail wallet address, key creation date, which can solve the problem of information loss conveniently. Because this authentication system allows you to hold your information completely in your own hands, never lose, never be tampered with. In the event of being an unfortunate refugee, even if you don't have a bank account, you can use this QR code to apply for a Bitcoin credit card and receive emergency relief from family and friends[7].

The present situation is that there can be no interest dependence or management relationship between CPA and manager. The decision-making power of a company to choose CPA is under the control of management, the choice of CPA, the cost of hiring and the way of payment may have an impact on the interest relationship between the audited enterprise and the CPA. With blockchain technology, the reliability of the blockchain ensures the accuracy of the transaction records of economic activity, the transparency of the blockchain solves the problem that a great deal of manpower and material resources are required to collect the audit evidence in the audit work. It also reduces the audit profession the corresponding cost greatly. At the same time, it avoids the possible moral hazard of auditing by third-party auditors and benefits users as well as regulators.

5.4 Crowd-funding and bill business
Nowadays, stock raising has the characteristics of low threshold, difficult to solve start-up financing, relying on mass power to promote social innovation and entrepreneurial development. With the introduction of relevant domestic regulatory regulations, stock raising and other industries will usher in a more standardized development. The crowd-funding project supports the transfer of funds to the crowd-funding platform accounts. The platform transfers the funds to the project sponsors' accounts when the funds raised by the projects meet the standards. With blockchain technology, blockchain based crowd-funding platforms can raise money by creating their own digital money or distributing their digital equity to early backers, giving investors credentials to support the shares of startups. Blockchain unique identity account system can record the equity as an electronic certificate of equity registration. The ownership of equity is registered in the blockchain, and the ownership transaction must be verified by the signature of the owner's private key. After the transaction is confirmed, the change of ownership will also be recorded in the blockchain, so as to protect the interests of both parties. At the same time, blockchain technology can store crowd-funding contracts in the form of smart contracts, it ensures that the contract can't be tampered with in performance.

At present, large banks pay more attention to the development of buy-and-resale paper business, electronic bill business has been rapid development, paper financing, note asset management and other cross-market business has become a new profit growth point of institutions; Various types of Internet platforms appear continuously. Thanks to the blockchain has the irrevocable time stamp and the whole network open characteristic, there will be no debt phenomenon no matter the paper ticket or the electric ticket; The distributed high fault-tolerant and asymmetric encryption algorithm in the blockchain doesn't have any risk of artificial operation. The blockchain can collect and evaluate the credit of all the participants and it can be controlled in real time. With the help of the programmability of blockchain, not only can the balance between the asset side and the liability side of the participants
be effectively controlled, but also the truthfulness of the whole market price response to the capital demand can be urged by the transparent nature of the data. A more realistic price index can be formed, in favor of controlling the market field risk[8].

5.5 Asset-confirming and intelligent internet of things

Nowadays, the right of confirmation needs to be declared to the relevant departments, investigated, examined and approved, registered, issued certificates and other registration procedures, to confirm the ownership of an object, the right to use the subordinate relationship and other rights. It also need to use third-party authority in accordance with the relevant provisions of the law to be clear. It will use distributed accounting to build an immutable record of property rights, provide a higher level of transparency and accountability. At the same time, the blockchain technology will also contribute to the safe construction of smart city facilities. It will enhance the transparency of the construction process and save the cost while clarify the main responsibility.

There are many problems with the Internet of things nowadays. It’s mainly the high cost, the lack of trust from users, the lack of practical use value, the absence of predictable business models and so on. Thousands of participants in the Internet of things are untrustworthy, some even malicious, so they need some form of verification and consensus mechanism. Luckily, with the blockchain, we can record every transaction of each participant. Cryptography is used to confirm transactions and ensure the privacy of information on the blockchain. Participants confirm each transaction, provide highly redundant confirmation. At the same time, they are rewarded for their computational effort. The blockchain eliminates the need for trust by using a decentralized consensus to confirm the transaction.

6. Conclusion

The blockchain technology provides new ideas and technical support for the transformation of production and life style. To some certain extent, it can make up for the defects existing in various fields at present. However, as a new thing, blockchain technology also has its own shortcomings, which need to be optimized and perfected in continuous research and practical application. At the level of blockchain technology, the processing performance and network security need to be continuously improved. First, the blockchain technology occupies a large number of computing and storage resources. The data processing capacity cannot meet the speed and scale requirements of most transactions at present, so it is still necessary to continuously explore innovative technological means. Reduce the generation time and transaction confirmation time of data block. Optimize the algorithm to improve the utilization of resources. Second, the blockchain technology is based on distributed accounting, open sharing, traceability and other characteristics, which may lead to risks such as customer privacy security, sensitive data disclosure. What we need to do is to strengthen security measures to plug up security vulnerabilities in a timely manner. To find the balance between the convenience of transaction activity and the security of information network. Third, the Bank of China has absolute leadership in the field of financial management, which is the core force to formulate monetary policy, maintain financial stability and prevent financial risks. The decentralization of blockchain technology will weaken the management of financial management functions to a certain extent. Fourth, it’s about the institutional level. At present, China's banks, securities, insurance and other forms of financial industry must abide by the corresponding laws and regulations, accept the "one line three sessions" management and supervision. Regulatory laws and regulations are clear, supervision system is strict. Innovative areas such as blockchains will largely move away from traditional regulatory systems, with laws and regulations still blank. When the continuous penetration of blockchain technology into various fields, legislation lags behind, the defects of supervision and regulation are bound to bring new challenges, which need to be constantly explored by the vast number of practitioners, for the establishment of a sound system of relevant laws and regulations to provide the basis.
References
[1] Zhai Sheping. Blockchain Technology: applications and problems[J]. Journal of Xi'an University of Posts and Telecommunications, 2018,(1):1-13(in Chinese).
[2] Maang. Review on the basic and application of blockchain technology[J]. Information Security Research, 2017, (11): P969(in Chinese).
[3] Wang Mao Lu. Research on blockchain technology and its application in government governance[J]. E-government, 2018,(2): 2-14(in Chinese).
[4] Wang Zhenzhen. Can blockchains really upend the world-connotations, application scenarios, reforms and challenges[J]. China Science and Technology Forum, 2018,(2): 112(in Chinese).
[5] Chen Xiaojing. The challenge and strategy of blockchain technology to the construction of Shanghai Kechuang Center[J]. Shanghai Insurance, 2018,(3): 44(in Chinese).
[6] Shao Qifeng. Blockchain Technology: architecture and Progress[J]. Journal of Computer Science, 2017, (11): 970(in Chinese).
[7] Hou Heng. Application of blockchain Technology in E-government: advantages[J], Constraints and Development. E-government, 2018,(6): 22-30(in Chinese).
[8] Yuan Yong, Wang Leap. Development and Prospect of blockchain Technology[J]. Journal of Automation, 2016,(4): 481(in Chinese).