

Research on the Application of Blockchain Technology in the Management of Financial Transfer Payment

Zhang Jiangen¹, Xing Shuxia^{2*} and Qi meng³

¹ Information Center, Finance Department of Hebei Province , Shijiazhuang, Hebei, 050051,China

² Huaxia Bank Co.,Ltd. Shijiazhuang Branch ,Shijiazhuang , Hebei, 050051,China

³ Hebei Caihua Information Technology Co.,Ltd, Shijiazhuang , Hebei, 050051,China

Abstract. Blockchain technology is considered to be a subversive innovation of computing mode after mainframe, personal computer and Internet. In the financial, medical, supply chain and other industries show great development potential. As an important part of financial management, financial transfer payment system is an important part of modern financial system. This paper combines blockchain technology with the management of financial transfer payment, analyzes the adaptation scenarios of blockchain technology, summarizes the status and development bottleneck of financial transfer payment informatization, tries to establish a financial transfer payment system based on blockchain technology, describes the advantages of blockchain technology in supporting the management of financial transfer payment, and puts forward suggestions on the possible problems.

1 Introduction

The report of the 19th National Congress of the Communist Party of China[1] pointed out that the establishment of a modern fiscal system should be accelerated, and the central and local fiscal relations should be established with clear powers and responsibilities, financial coordination, and regional balance. The fiscal transfer payment system of China is an important part aspect for clarifying the fiscal powers and expenditure responsibilities of the central and local governments.

In recent years, on the one hand, the amount of central transfer payment funds has keeps growing larger and larger. So the central transfer payment funds has played an extremely important role in narrowing the financial gap between regions, optimized the allocation of resources between regions, and implemented specific policy goals.

On the other hand, transfer payment funds from higher levels have greatly ensured the basic financial resources of local governments, effectively enhanced the ability of grassroots governments to "guarantee wages, ensure operations, and protect people's livelihood", and fully ensured the normal operation of grassroots governments.

In view of the huge scale of financial transfer payment funds, a relatively high proportion of expenditures, and the important role it plays in ensuring the smooth implementation of central policies and effectively improving the governance capabilities of local governments, the Budget Law [2] requires that financial

transfer payments should be normative, fair and open. However, in actual management, there is no unified national budget management information system. Instead, administrative divisions at all levels have independent systems. Any system only stores the usage data of financial funds within its administrative division. The work of data collection and information disclosure is mainly relied on data submission and government affairs disclosure. Therefore, any administrative division can't grasp the usage data of financial transfer payment funds in time and lacks the means to supervise the whole process.

The process of financial transfer payment fund management involves financial department and budget departments at all levels, which fits the characteristics of blockchain, such as multi-party participation, decentralization, openness and transparency. However, there is no literature that integrates blockchain and fiscal transfer payment. This article will try to explore "blockchain + financial transfer payment", which builds a financial transfer payment system based on blockchain technology, analyses the advantages of that system, and puts forward countermeasures and suggestions for the difficulties in promotion and application.

2 Related works

Blockchain has attracted wide attention within the popularity of Bitcoin[3]. It can be regarded as an encrypted distributed instant ledger system, which uses a clever combination of distributed storage, asymmetric encryption, peer-to-peer transmission, consensus

*Corresponding author's e-mail: xing0213@126.com

mechanism and other technologies to ensure that the data on the chain cannot be tampered with, and the operation traces can be traced throughout. Blockchain has changed the trust mechanism endorsed by third-party organizations in social interactions, and formed a social trust mechanism supported by information technology and guaranteed by rigorous mathematical algorithms, where everyone endorses me and I endorses everyone. Blockchain can complete the fair allocation of resources and achieve the goal of ensuring that all participants have the same goals and standard behavior. According to the degree of openness of access rights, blockchains are mainly divided into three categories: public blockchain, alliance blockchain, and private blockchain.

In the public blockchain, all participants are anonymous. Generally, Proof of Work (PoW) [3] or Proof of Stake (PoS) [4] is introduced as the basis of the consensus algorithm. In the permission blockchain, (alliance blockchain, private blockchain), all participants are identified and have consistent goals, but lack of trust between each other. On the basis that all participants are open and transparent, consensus algorithms based on Byzantine fault tolerance [5], Kafka [6], RAFT or PAXOS [7] can be introduced.

At present, the more popular permission blockchain projects in the world include the multiple blockchain platforms proposed by Hyperledger[8], Corda proposed by the Financial Blockchain Alliance[9] CCF[10] proposed by Microsoft, and Enterprise Ethereum Alliance[4]. Among them, Fabric[11] the most popular blockchain architecture.

3 Financial transfer payment system based on blockchain Technology

In the financial transfer payment system based on blockchain technology, the national, provincial, municipal, and county financial departments and supervision departments are connected in the form of nodes. Transfer payment transaction information is transmitted point-to-point among all nodes, and stored by every node. The anonymity of the public blockchain makes it difficult to confirm the true identity of the access node, so it is not suitable as a carrier for financial transfer payments. The alliance blockchain has a strict identity access mechanism, which makes it easy for joining nodes to have a consistent goal. Therefore, this article adopts a technical solution based on the alliance blockchain. The overall system model is shown in Figure 1.

The agency management service approves all levels of financial departments to join or exit the blockchain financial transfer payment system, creates a unique identity ID and issues e-certificates for each participant. Because of the alliance blockchain mode, the message transmission between nodes is all through electronic signature and electronic encryption. The agency management service is also used for signature verification and transaction verification.

In the technical structure, the blockchain financial transfer payment system is divided into a network layer, a data layer, a consensus layer, a contract layer, and an application layer (as shown in Figure 2).

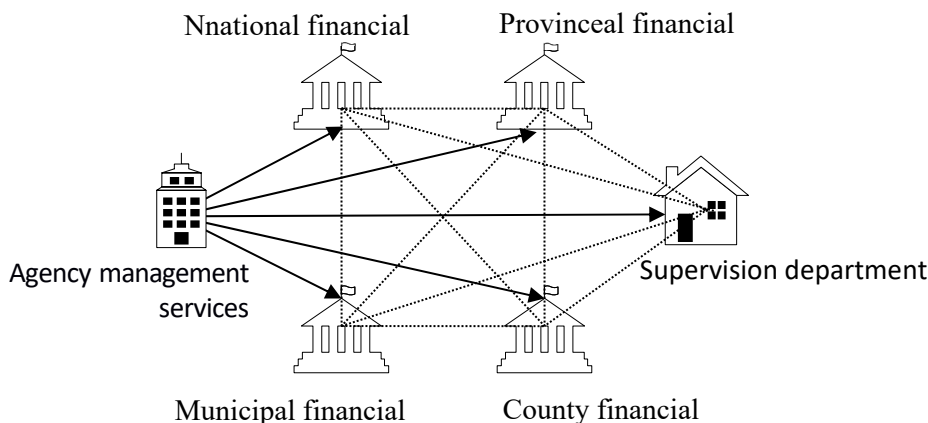


Fig 1. The overall system model.

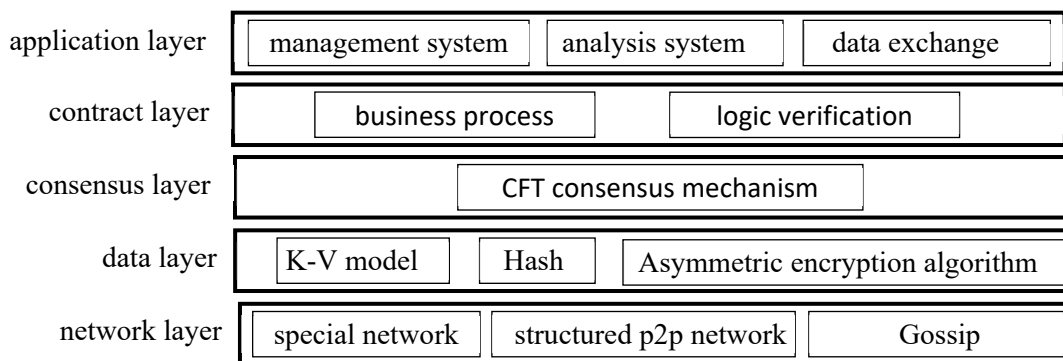


Fig 2. The technical structure of the blockchain financial transfer payment system.

3.1 The network layer

The financial transfer payment data requires high security, so it is not suitable to run in public network. So the existing special network of financial system can be fully utilized to construct a structured peer-to-peer network. The Gossip agreements[12] is adopted to realize TLS encryption transmission.

3.2 The data layer

The key value information model is used to store key elements of transfer payment business. Hash function and asymmetric encryption algorithm are used to ensure the strong correlation and security of the data.

3.3 The consensus layer

The strong authentication of organization management service makes the nodes in the access system have clear identity information. Therefore, CFT consensus mechanism [6] is used to complete the confirmation and verification of transfer payment business, and effectively solve the problems caused by node failure, network congestion and other abnormal conditions.

3.4 The contract layer

The script encapsulating the transfer payment business process and logic verification is executed according to the predetermined rules, which ensures that the transfer payment business can be automatically and completely executed, and the execution results of all nodes are consistent, so as to ensure the fairness of the transfer payment business process.

3.5 The application layer

The management system standardizes the data structure and processing process of the transfer payment business, the statistical analysis system establishes a comprehensive data analysis index system to reflect the value of data in a timely and rapid manner, the data exchange services develops standardized data exchange interfaces to provide services for system interaction, information resource sharing, etc.

4 Conclusions

Blockchain technology is in the ascendant and in the stage of vigorous development. It has profoundly changed the traditional transaction mode, provided a new solution for the restructuring of business processes and the improvement of regulatory level, and has shown great potential in finance, supply chain, medical treatment and other aspects. In the financial management system, the transfer payment business is only a small part of the whole business. Looking to the future, with the continuous development and improvement of blockchain technology and the in-depth study of financial business scenarios, the blockchain technology will be better integrated into financial management business, and the application of blockchain technology in financial management business will be continuously expanded, so as to provide more solid technical solutions for financial governance and financial reform.

References

1. Book writing group. (2014)The report of the 19th National Congress of the Communist Party of China. people's Publishing House, Beijing.
2. Book writing group. (2014)Budget Law of the People's Republic of China. China legal Publishing House, Beijing.
3. Nakamoto S. Bitcoin: a peer-to-peer electronic cash system[EB/OL]. (2008-10-31)[2020-08-19]. <https://bitcoin.org/bitcoin.pdf>.
4. Ethereum. Ethereum Whitepaper[EB/OL].(2020-08-06)[2020-08-06]. <https://ethereum.org/en/whitepaper/>.
5. Castro M, Liskov B. Practical byzantine fault tolerance and proactive recovery[J]. ACM Trans. on Computer Systems, 2002,20(4):398–461.
6. Sax M.J. (2018) Apache Kafka. In: Sakr S., Zomaya A. (eds) Encyclopedia of Big Data Technologies[EB/OL].Springer,Cham.(2018-02-10)[2020-08-06]. https://doi.org/10.1007/978-3-319-63962-8_196-1.
7. Ongaro D, Ousterhout JK. In search of an understandable consensus algorithm: In: Proc. of the

- 2014 USENIX Annual Technical Conference, Philadelphia PA, June 19-20 2014[C]. (ATC). 2014.
8. Hyperledger. An Introduction to Hyperledger[EB/OL].(2018-08)[2020-08-06].https://www.hyperledger.org/wp-content/uploads/2018/08/HL_Whitepaper_IntroductionToHyperledger.pdf.
 9. Corda. The Corda Platform:An introduction[EB/OL].(2018-05)[2020-08-06].<http://www.corda.net/content/corda-platform-whitepaper.pdf>.
 10. M. Russinovich, E. Ashton, C. Avanesians, et al. CCF: A Framework for Building Confidential Verifiable Replicated Services[EB/OL].(2017-04)[2020-08-06].<https://ashamis.github.io/files/CCF-A-Framework-for-Building-Confidential-Verifiable-Replicated-Services.pdf>.
 11. E.Androulaki, A. Barger, V.Bortnikov, et al. Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains:Proceedings of the 13th EuroSys Conference, Porto Portugal, April 23-26 2018[C]., ACM,2018.
 12. DEMERS A,GREENE D,HOUSER C,et al.Epidemic algorithms for replicated database maintenance [J]. ACM SIGOPS Operating Systems Review,1988,22: 8-32.