Multi-Chain Model and Cross-Chain Communication Protocol for Financial Transactions

Chao Li[1,2,*], Guigang Zhang[1,4], Xiangke Mao[1], Jian Zhang[1], and Chunxiao Xing[1,2,3]
[1]Tsinghua University Beijing National Research Center for Information Science and Technology, Beijing, China
[2]Department of Computer Science and Technology, Tsinghua University, Beijing, China
[3]Institute of Internet Industry, Tsinghua University, Beijing, China
[4]Institute of Automation Chinese Academy of Sciences, Beijing, China
li-chao@tsinghua.edu.cn, guigang.zhang@ia.ac.cn, xiangkemao@tsinghua.edu.cn, zhangjian05@tsinghua.edu.cn,
xingcx@tsinghua.edu.cn
*corresponding author

***Abstract*—Aiming at the cross-chain problems faced by financial transactions, study the cross-chain communication protocols of the financial-oriented autonomous panda model and golden monkey model, and study the construction of a new scalable and credible multi-chain model that supports homogeneous blockchains and heterogeneous blockchains. The models and protocols that support financial transactions in the blockchain environment need to be able to meet the SSL or SET security protocols similar to traditional Internet transactions, and meet various requirements such as transaction integrity, reliability, and privacy protection.**

***Keywords*—Multi-chain model; cross-chain communication; data lake; financial transaction**

I. Introduction

With the development of blockchain technology, more and more homogeneous or heterogeneous blockchains are running on the Internet. Different from various business activities based on the Internet environment, whether it is the entire open Internet or various internal networks connected to the Internet, they all use the same connection protocol TCP/IP, whether it is a company's internal network transactions, and between companies. Internet transactions, or transactions across the entire Internet, all commercial activities are not affected. Financial settlement between countries only needs to be easily completed based on the Internet and the SWIFT system. Unlike the Internet, business activities based on the blockchain have not formed a unified agreement, so it is difficult to achieve a unified transaction on a global scale. Different companies have their own blockchains, and their own company businesses run on their own unique blockchain architecture. In this way, due to the use of different underlying blockchain architectures for transactions between companies, it is difficult to achieve interconnection between them, and business activities are greatly affected.

Running a variety of different chains on the Internet and requiring cross-chain transactions between different chains including homogeneous chains and heterogeneous chains, especially the realization of its financial settlement is whether the blockchain technology can truly be realized from the experiment. key steps towards the application of the chamber. This paper attempts to explore a multi-chain model based on financial transactions and its corresponding cross-chain transaction protocol to solve this problem.

II. Related Work

There are lots of research about the multi-chain model and cross-chain communication protocol. Paper [1] proposed a multi-chain communication layer between the blockchain and application layer and give a router blockchain model. Paper [2] do some research on the consensus protocol and propose the "Hub-parachain" model for blockchain based on interoperability architecture. Paper [3] gives a kind of cross-chain transactions methods. This kinds of model used the hashed time-lock contracts. Paper [4] proposed the cross-chain protocol, especially the cross-chain smart contracts. Paper [5] proposed the multi-chain model-based 5G network. Paper [6] proposed the web3.0 from the cross-blockchains perspective view.

The Tiande Chain Technology White Paper provides two kinds of models, which are panda model and golden monkey model[7].

The panda model shows in figure 1 is proposed to improve the efficiency of transactions, a double-chain transaction information. The structure that separates interest from account balances was born. Panda Chain uses a double-chain architecture. Any financial institution can join the chain network at any time.

The golden monkey model shows in figure 2 is a heterogeneous chain network model, which is a fully distributed, multi-chain network without a central node or architecture. Committed to creating a distributed financial architecture that enables efficient and trustworthy transactions between different financial institutions without going through a central institution.

A good cross-blockchain transaction protocol [8], [9], [10], [11], [12], [13] must consider the integrity. In traditional financial transactions, in order to ensure the correctness, security, privacy protection, etc. of all transactions, there will be corresponding transaction protocols, such as SSL protocol or SET protocol. Specifically, it is implemented using technologies such as digital digests, digital signatures, and digital envelopes. With the development of blockchain technology,

2693-9371/22/$31.00 ©2022 IEEE
DOI 10.1109/QRS-C57518.2022.00087

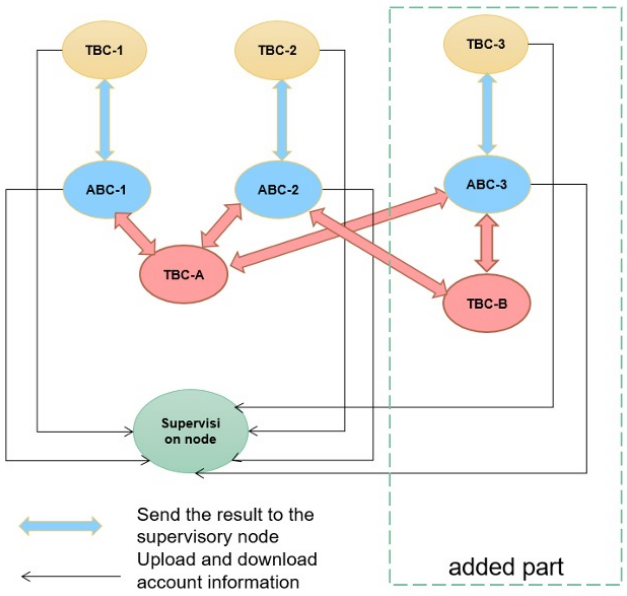

Figure 1. Panda model

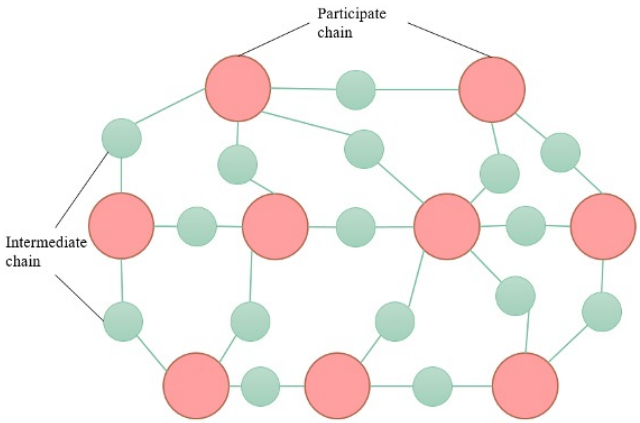

Figure 2. Golden monkey model

many future transactions will be based on the blockchain architecture. Accordingly, various transaction protocols based on the blockchain transaction environment need to be studied to meet the validity of the transaction.

Data lake technology will be a development trend of blockchain technology. The following figure shows the future data semantic extraction mechanism based on blockchain data lake environment, and the following figure 3 shows the future cross-chain multi-model blockchain application trading mechanism based on blockchain data lake environment. Different from traditional blockchain, future blockchain applications not only need to extract semantic information such as transactions from relational databases, but also need to directly extract massive semantic information from the data lake to support or assist the intelligent analysis and mining of block transactions.

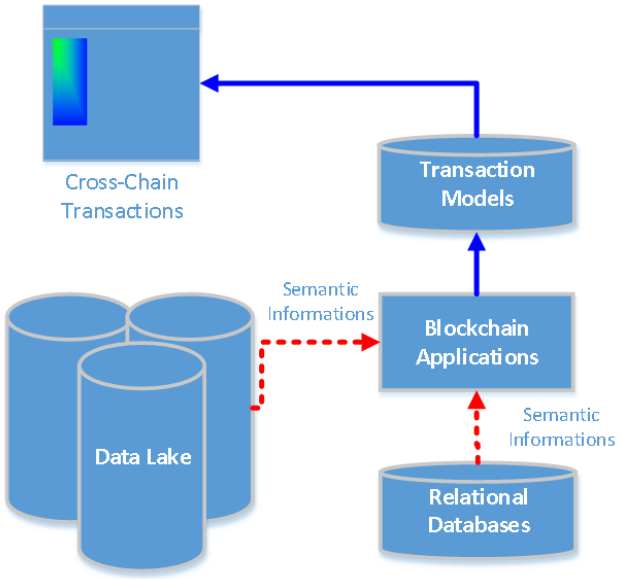

Figure 3. Blockchain semantic information come from the data lake

III. A Multi-chain Model for Financial Transactions

With the development of blockchain technology and data lake technology, blockchain applications based on data lakes will become more and more important in the future. However, the current blockchain environment is very complex, and there are various public chain systems, private chain systems, and enterprise alliance chain systems on the market. At the same time, all application data will be gradually migrated to a special storage environment such as the data lake. How to create a blockchain environment that supports cross-chain and alliance chain trusted transactions and transparent supervision in this environment will face a huge difficulty and challenges. In order to solve these difficulties, we designed a system architecture method and system that supports trusted transactions and transparent supervision of cross-chain and alliance chains. The method and system simultaneously support all users from different public chain systems, private chain systems, and enterprise alliance chain systems to use various blockchains from enterprise private chains and enterprise alliance chains completely transparently and seamlessly through the blockchain data lake application platform. Blockchain application system. The rise of this method will greatly promote the cross-platform and cross-chain application of blockchain technology. With the future data lake as the storage cornerstone, it will satisfy and drive the vigorous development of the blockchain industry under the entire data lake. The figure 4 shows the multi-chain model based on data lake. It will support the financial transactions in the future.

The blockchain data lake application platform also includes an application integration module, which is used to integrate blockchain applications and provide a unified interface for application services. The blockchain data lake application

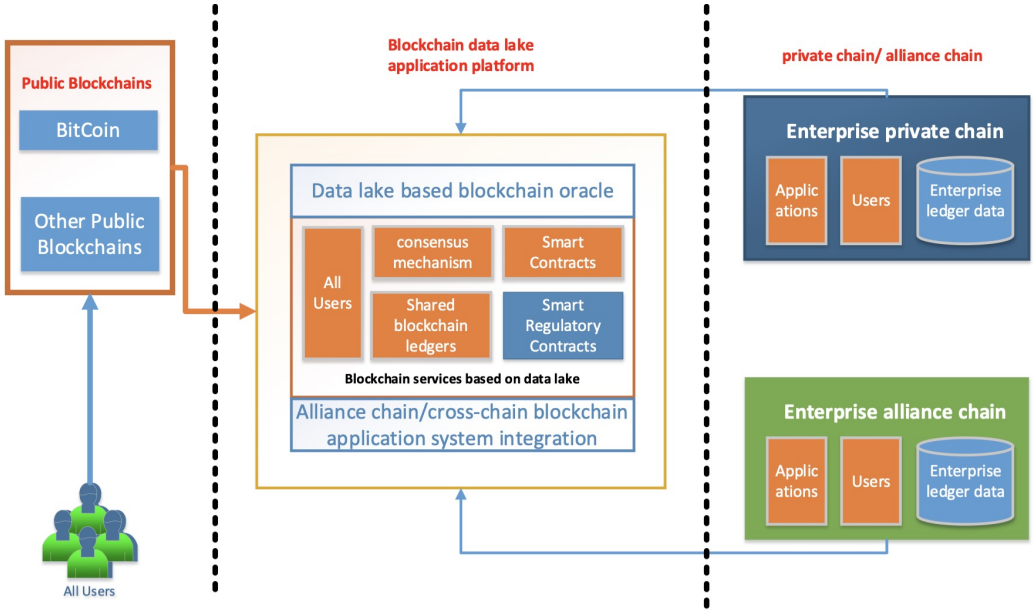

Figure 4. Multi-chain model based on data lake

platform also includes a data lake-based blockchain service unit. The participants of the data lake-based blockchain service unit integrate blockchain application users and blocks from the blockchain public chain. Blockchain participants of the private chain/consortium chain. The data lake-based blockchain service unit includes a smart contract module, which is used to manage the transaction process according to the set smart contract. Smart contracts include smart supervision contracts, which are used to intelligently supervise the legality of transactions by using preset smart technologies; wherein, the preset smart technologies include semantic rule compliance judgment technology. The blockchain service unit of the data lake also includes an accounting module, which is used to share the ledger of the blockchain private chain/consortium chain and record the generated transactions. The blockchain service unit based on the data lake also includes a consensus module, which is used to provide a consensus mechanism for transactions of blockchain applications from blockchain private chains/consortium chains in the data lake environment. A blockchain system that supports cross-chain transactions under the data lake architecture, and the blockchain public chain includes blockchain application users. Blockchain private chain/consortium chain includes enterprise private chain and enterprise alliance chain; enterprise private chain includes first enterprise ledger data, enterprise private chain blockchain participants and enterprise private chain applications; enterprise alliance chain includes second enterprise ledger data, enterprise alliance chain blockchain participants and enterprise alliance chain applications. The blockchain system that supports cross-chain transactions under the data lake architecture provided by this model can format the deployed blockchain applications by setting a data lake-based blockchain oracle on the blockchain data lake. To achieve users of blockchain applications on the public chain or participants from private chains and consortium chains can seamlessly use blockchain application systems from private chains and consortium chains on the blockchain data lake, and serve the needs of blockchain applications better.

IV. A CROSS-CHAIN COMMUNICATION PROTOCOL FOR FINANCIAL TRANSACTIONS

A. Security communication protocol for financial transactions based on the same blockchain

Figure 5 shows the security communication protocol for financial transactions based on the same blockchain.

In Figure 5, user A needs to conduct business transactions with user B through the blockchain. A and B belong to two different users on the same blockchain. The transaction between them can be completed directly through the traditional SET protocol. At the same time, all information of user A, all information of user B, and all ledger and transaction information on blockchain X will be gathered in the financial supervision big data center. All data in the financial supervision big data center can be analyzed by big data, and the analysis results can be submitted to AML or KYC applications.

B. Security communication protocol for financial transactions based on the homogeneous blockchain

Figure 6 shows the security communication protocol for financial transactions based on the homogeneous blockchain.

Figure 6 shows user A and user B conducting business transactions. User A belongs to blockchain X, and user B belongs to blockchain Y. But both blockchain A and blockchain B belong to two blockchains running under the same architecture (Bitcoin), and they belong to homogeneous

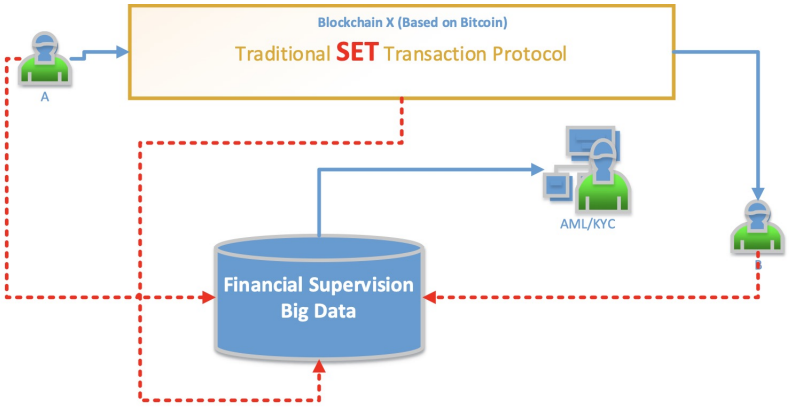

Figure 5. Security communication protocol for financial transactions based on the same block-chain

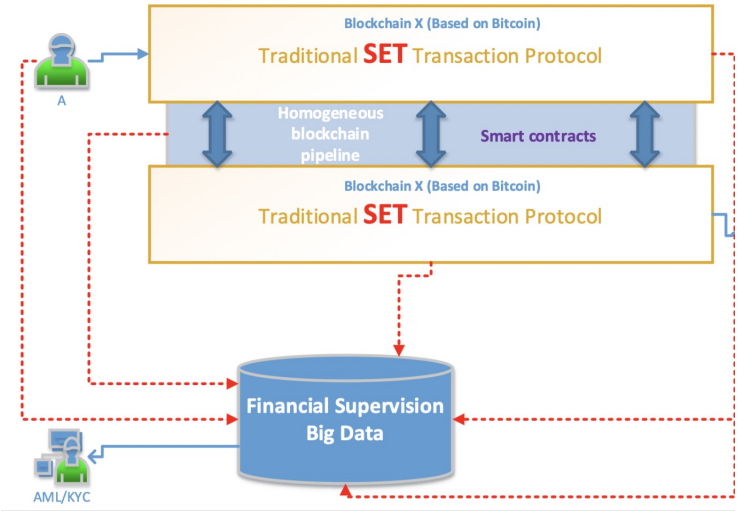

Figure 6. Security communication protocol for financial transactions based on the homogeneous blockchain

blockchains. Since user A and user B belong to different blockchains, a homogeneous blockchain pipeline needs to be established between them and follow the smart contracts between homogeneous blockchains that meet the communication requirements. The Financial Supervision Big Data Center will collect all the information of user A, user B, blockchain X, blockchain B, and the isomorphic blockchain pipelines and smart contracts between blockchain A and blockchain B. The Financial Supervision Big Data Center conducts big data and artificial intelligence analysis on all data for AML or KYC applications.

C. Security communication protocol for financial transactions based on the heterogeneous blockchain

Figure 7 shows the security communication protocol for financial transactions based on the heterogeneous blockchain. Figure 7 shows user A and user B conduct business transactions. User A belongs to blockchain X, and user B belongs to blockchain Y. However, both blockchain A and blockchain B belong to two blockchains running under different architectures (one is Bitcoin, the other is ETH), and they belong to heterogeneous blockchains. Since user A and user B belong to different blockchains, they need to establish a heterogeneous blockchain oracle (including heterogeneous blockchain communication pipelines, and follow the communication requirements between homogeneous blockchains) smart contract). The Financial Supervision Big Data Center will collect all the information of user A, user B, blockchain X, blockchain B, and the heterogeneous blockchain oracles between blockchain A and blockchain B. The Financial Supervision Big Data Center conducts big data and artificial intelligence analysis on all data for AML or KYC applications.

V. Conclusion

This paper proposed a kind of multi-chain model and cross-chain communication protocol for financial transactions. Through this model and transaction protocol, all homogeneous or heterogeneous blockchain systems running on the Internet can achieve interconnection and conduct business activities with transaction behavior. In the future, we will give this model

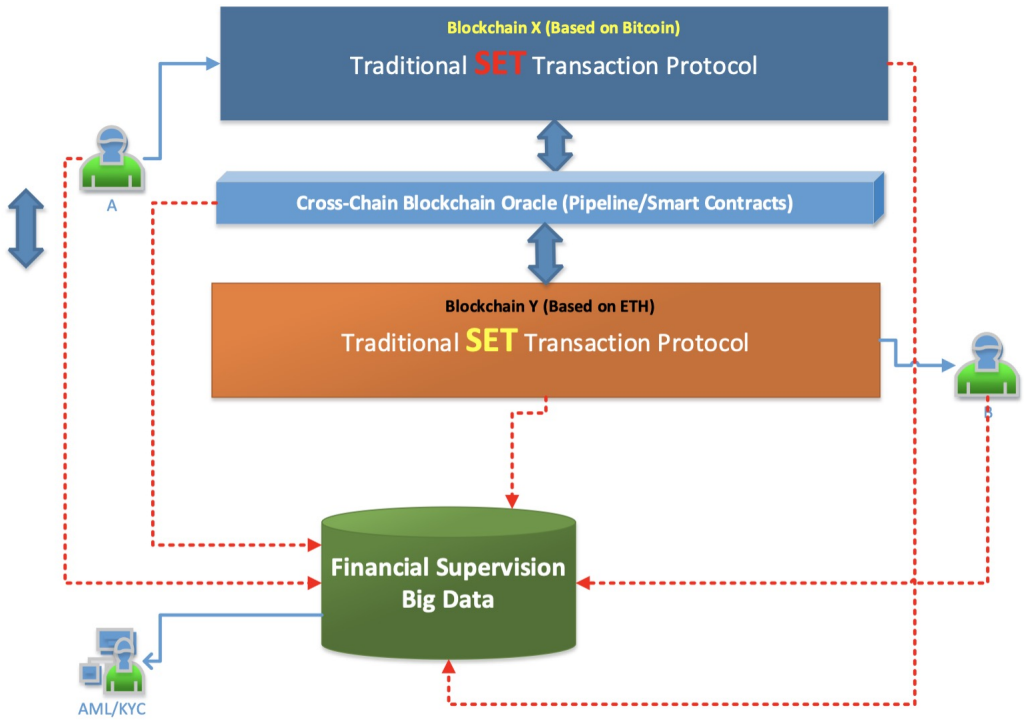

Figure 7. Security communication protocol for financial transactions based on the heterogeneous blockchain

and secure transaction protocol to develop a corresponding prototype system.

ACKNOWLEDGMENT

This research was funded by the National Key R&D Program of China (2018YFB1402701).

REFERENCES

[1] L. Kan, Y. Wei, A. Hafiz Muhammad, W. Siyuan, L. C. Gao and H. Kai. A Multiple Blockchains Architecture on Inter-Blockchain Communication. 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C), Lisbon, Portugal, 2018, pp. 139-145.

[2] Y. Pan. A New Consensus Protocol for Blockchain Interoperability Architecture. IEEE Access, vol. 8, pp. 153719-153730, 2020.

[3] N. Shadab, F. Houshmand and M. Lesani. Cross-chain Transactions. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-9.

[4] L. Cao and B. Song. Blockchain cross-chain protocol and platform research and development. 2021 International Conference on Electronics, Circuits and Information Engineering (ECIE), Zhengzhou, China, 2021, pp. 264-269.

[5] Y. He, C. Zhang, B. Wu, Y. Yang, K. Xiao and H. Li. Cross-chain Trusted Service Quality Computing Scheme For Multi-chain Model-based 5G Network Slicing SLA. IEEE Internet of Things Journal.

[6] Liu, Zhuotao, et al. "Make Web3. 0 Connected." IEEE Transactions on Dependable and Secure Computing (2021).

[7] Tiande Chain Technology White Paper. www.tdchain.cn

[8] J. Rueegger and G. S. Machado. Rational Exchange: Incentives in Atomic Cross Chain Swaps. 2020 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Toronto, ON, Canada, 2020, pp. 1-3.

[9] B. Pillai, K. Biswas, Z. Hóu and V. Muthukkumarasamy. The Burn-to-Claim cross-blockchain asset transfer protocol. 2020 25th International Conference on Engineering of Complex Computer Systems (ICECCS), Singapore, 2020, pp. 119-124.

[10] A. Garoffolo, D. Kaidalov and R. Oliynykov. Zendoo: a zk-SNARK Verifiable Cross-Chain Transfer Protocol Enabling Decoupled and Decentralized Sidechains. 2020 IEEE 40th International Conference on Distributed Computing Systems (ICDCS), Singapore, Singapore, 2020, pp. 1257-1262.

[11] H. Tian et al.,. Enabling Cross-Chain Transactions: A Decentralized Cryptocurrency Exchange Protocol. IEEE Transactions on Information Forensics and Security, vol. 16, pp. 3928-3941, 2021.

[12] A. Zamyatin, D. Harz, J. Lind, P. Panayiotou, A. Gervais and W. Knottenbelt. XCLAIM: Trustless, Interoperable, Cryptocurrency-Backed Assets. 2019 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2019, pp. 193-210.

[13] R. Belchior, A. Vasconcelos, M. Correia and T. Hardjono. Enabling Cross-Jurisdiction Digital Asset Transfer. 2021 IEEE International Conference on Services Computing (SCC), Chicago, IL, USA, 2021, pp. 431-436.