A Multiple Blockchains Architecture On Inter-Blockchain Communication

Kan Luo
School of Computer Science and Engineering
Beihang University
Beijing, China
looken@buaa.edu.cn

Wei Yu
School of Computer Science and Engineering
Beihang University
Beijing, China
yuwei@buaa.edu.cn

Hafiz Muhammad Amjad
School of Computer Science and Engineering
Beihang University
Beijing, China
amjadphool@ buaa.edu.cn

Siyuan Wang
School of Computer Science and Engineering
Beihang University
Beijing, China
wsy17@buaa.edu.cn

LingChao Gao
Beijing China Power Puhua Information Technology Co.Ltd
Beijing, China
gaolinchao@sgitg.sgcc.com.cn

Kai Hu
School of Computer Science and Engineering
Beihang University
Beijing, China
hukai@buaa.edu.cn

***Abstract*—Blockchain is a new technology for data sharing between untrusted peers. However, it does not work well with massive transactions. Besides, there are high barriers between heterogeneous blockchain systems. In this paper, we proposed an innovative component-based framework for exchanging information across arbitrary blockchain system called interactive multiple blockchain architecture. In our architecture, a dynamic network of multi-chain is created for inter-blockchain communication. We propose the inter-blockchain connection model for routing management and messages transferring. Additionally, our proposed protocols provide transactions with atomicity and consistency in crossing-chain scene. In the end, our experiment results based on a network of private multiple blockchain systems show that the throughput is increased by a number of chains parallel running.**

Keywords—Blockchain, Multi-chain, Scalability, Routing

I. INTRODUCTION

Recently, more and more applications are created based on blockchain technology. It is used for sharing decentralized and transactional data among a network of unreliable participants[2]. There is no central point that is trusted by other components in a blockchain system. With the distrust between all participants, blockchain system applies blockchain data structure and consensus algorithm. The data structure is a list of blocks, which records each hash value of finished transaction in order. This determines the history of assets movement and offers an unforgeable time ordering records. Furthermore, the list of blocks will be consented among participated nodes in system. In this way, the whole blockchain system reaches a consensus on the list. With the unanimous list of hash blocks, the transactions are stored immutably for the reason that the digest will only changes with the original content of a certain transaction. Taking advantages of the special data structure and consensus mechanism, blockchain makes a distributed tamper-proof ledger.

Although a reliable ledger can be set up based on a blockchain system, a single blockchain system is not a suitable solution for an inter-ledger applications. Compared to Internet, blockchain is more like a local area network(LAN). Heterogeneous blockchain systems cannot trust or communicate with each other. They are incapable of securely exchanging value with each other. However, the movement of assets between different ledgers brings convenience. Users become more interested in information exchanging between blockchains. Connecting the activity in different chains is meaningful, For example, an institution may want the arrival of funds on one blockchain to trigger a corresponding transfer of funds on another. Actually, there are few connectors facilitating payments between these ledgers and there are high barriers to entry for creating new connections[1]. In addition, global consensus mechanism in blockchain brings that the speed of dealing with the transaction cannot be improved by adding extra nodes. So a single blockchain has limited performance. It is unable to meet the requirements of large-scale application. For instance, Bitcoin shares all transactions results between all nodes in blockchains. It can only deal with no more than 400,000 transactions per day but the Visa network handles 150 million transactions per day in the USA[7].

Not satisfied with the benefits brought by a single blockchain system, Gideon[13] proposed a configurable multichain, which is easy to configure and can work with different blockchains. In addition, it is able to create connection between the activity in chains. Pegged sidechains, proposed in Blockstream [1], enables bitcoins and other ledger assets to be transferred between multiple blockchains. However, those technology concerning blockchain interaction focus on homogeneous blockchain system. In this paper, aiming at lowering the barrier of between heterogeneous decentralized ledger, we proposed an extensible blockchain architecture called interactive multiple blockchain architecture. Besides, we design an inter-blockchain connection model as routing management of multiple systems. In this model, router blockchain maintains routing information of involved blockchain system, making heterogeneous blockchain systems interoperate. Based on the router blockchain, two involved

978-1-5386-7839-8/18/$31.00 ©2018 IEEE
DOI 10.1109/QRS-C.2018.00037

chains can establish a connection and trade through crossing chain protocol. Our protocol guarantee atomic and consistence crossing-chain transactions by utilizing three-phase commit[14] and escrow transfer. Our contributions can be summarized as follows:

1)Our architecture enables heterogeneous blockchains to communicate according to inter-blockchain connection model;

2)We propose a protocol for reliably exchanging information without third party in a multiple blockchains system;

3) We improve the throughput of the blockchain system by parallel executing transactions.

This paper are organized as: Section II discusses the related work on multiple blockchain. Section III describes our proposed extensible blockchain architecture; In Section IV, the inter-blockchain connection model is stated, followed by the crossing chain protocol in Section V. Section VI represents and analyzes the experiment before Section VII concludes the paper.

II. Related Work

A. Pegged Sidechains

Side-chain is an addition to the Bitcoin protocol, making trustless communication between Bitcoin and side-chains. pegged sidechains are able to transfer of Bitcoin and other ledger's assets between multiple Blockchains. Users can easily access to new cryptocurrency systems with already-own asset in another system. these systems can communicate with each other by using Bitcoins, eliminating the liquidity shortages and market fluctuations. Furthermore, sidechains are separated, but the technical and economic innovation is not distinguished. Although Bitcoin and sidechains are bidirectional for assets movement, they will not interference each other. In other word, if one chain is break down, the damage will totally confined to itself.

B. Cosmos

Cosmos[5] is a novel blockchain network architecture. It allows parallel blockchains to interoperate while retaining their security properties. a network of many independent blockchains is called zones. Those zones are powered by a high-performance, consistent ,secure consensus engine. The first zone on Cosmos is the hub of the network. It works as the government of the whole system, enabling the network to adapt and upgrade. In addition, the Hub can be extended by connecting other zones. Zones allow for future-compatibility with new blockchain because any blockchain system can connect the hub Cosmos Hub. It also is able to isolates each one from the failure of other zones. Cosmos make blockchains communicate via protocols, like a kind of virtual UDP or TCP. Tokens can be transferred from one zone to another, securely and quickly, without the need for exchange liquidity between zones. In order to keep track of the total amount of tokens held by zones, all tokens go through the Cosmos Hub.

C. Polkadot

Polkadot is a scalable multi-chain framework. It unlike previous blockchain implementations which have focused on providing a single chain of varying degrees of generality over potential applications. Polkadot is a set of independent chains with pooled security and trust-free interchain transactability. The application to be deployed on Polkadot should be parallelized over parachains. Each parachain is conducted by a different segment of the Polkadot network. Polkadot leaves much of complexity to be addressed at the middleware level. Further, it outlines a scalable multi-chain protocol with the potential to be backwards compatible to blockchain protocol.

D. MultiChain Private Blockchain

MultiChain is designed for communicating of private blockchains, either within or between companies. To overcome the obstacle to the deployment of blockchain technology in the institutional financial department, it provides the privacy and control required in a portable package. It has API and command-line interface and supports any common operation system, like Windows, Linux and Mac. MultiChain solves the problem of mining, privacy and openness via integrated management of user permissions. MultiChain can be configured easily and work with different blockchains at the same time. The benefit is enabling private blockchain to be configured and deployed by administrators rather than specialized developers. the mining node and the mining process are limited to a manageable range to avoid the monopoly of the mining process called "diversity mining". Diversity mining asks the miners executing transactions in a random poll. MultiChain is compatible with Bitcoin, so assets held in the Bitcoin can be imported into the MultiChain. Since it can be configured to simultaneously supports different heterogeneous Blockchains in the same network.

III. Interactive Multiple Blockchain Architecture

Based on existing blockchain architecture[9], a new architecture called interactive multiple blockchain architecture, as a solution to communicate different blockchains, is proposed in the paper.

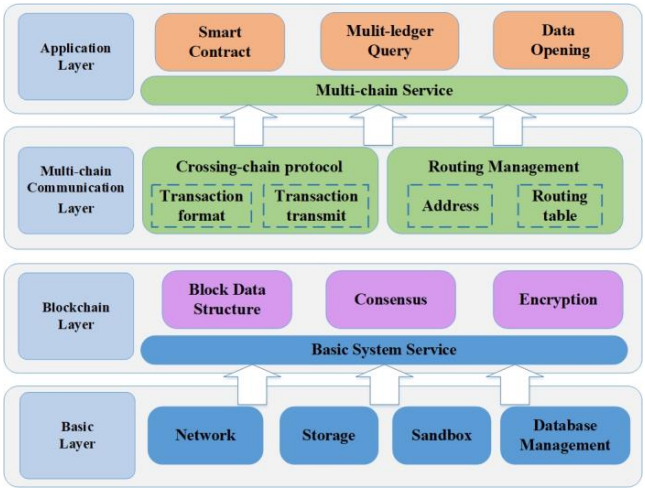

Fig.1. Interactive multiple blockchain architecture

It is a hierarchical framework, services are encapsulated in different layers. all services are component-based and modules are pluggable. In this way, we can swiftly construct a blockchain application by substituting encryption module or consensus module. Our architecture is unlike previous blockchain implementations which couples the applications directly. To be specific, an application involving two organizations can be constructed with the provided service of blockchain layer. The developer even do not need to know the consensus algorithm and data structure of the blockchain.

Figure 1 shows the brief overview of the whole architecture. this architecture consists of four layers: basic layer, blockchain layer, multi-chain communication layer and application layer. details regarding the four layers are given below.

A. *Basic layer*

In this layer, there are foundation of the system operation, containing network module, storage module, sandbox module, database management module. Particularly, in Sandbox modular, virtualization technology is utilized to sandbox the smart contract execution, for providing "locked down" and secured container.

B. *Blockchain layer*

Blockchain systems have different underlying implementation but these three parts are essence: basic data structure, consensus mechanism and encryption. In blockchain layer, blockchain data structure and the format of transaction are defined in basic data structure modular; the chain will be consensus in blockchain system with consensus algorithm specified in consensus module; and encryption algorithm are specified in encryption module.

C. *Multi-chain cmmunication layer*

To make transaction swiftly confirmed and assets reliably circled, a blockchain network is set up according to multi-chain communication layer. This layer consists of crossing-chain protocol and routing management.

- Routing management: arbitrary blockchain system can join the blockchain network with a router. A inter blockchain model is designed for routing management[18].
- Crossing chain protocol: Rules for secure crossing-chain transaction execution are defined in protocols. Three phase commit and escrow transfer are used to provide atomicity and consistency for crossing-chain transactions

D. *Application layer*

On the top of this architecture, smart contract, multi-ledger query and data opening are based on multi-chain system with the service of the chain-crossing layer. Smart contacts[6] is a key emerging use case of blockchain technology. With services of multi-chain communication layer, it become accessible to carry out complex combination query through multiple ledgers. As for data opening, heterogenous systems join up, making information exchanged swiftly and shared securely with the service of multi-chain layer.

IV. INTER-BLOCKCHAIN CONNECTION MODEL

A blockchain is a network of a set of peer-to-peer nodes. After initialized by users, transactions are delivered from node to node and recorded into ledger. Only nodes in network can handle the transactions proposed by users. In this way, blockchain system is isolated. To lowering the barriers to facilitating blockchains communication, inter-blockchain connection model is designed for heterogeneous blockchains by creating a network of multiple blockchains. In this model, a blockchain system is able to establish connections with other blockchain system. After two systems connected, data and message are shared.

A. *Overview*

We make heterogeneous blockchain system interoperable by creating a dynamic blockchain network called router blockchain. In figure 2，router blockchain contains a group of router nodes. A chain attends to join the blockchain network, before making one of its nodes becomes a router node, which is a member of router blockchain. All router nodes with details of different chains become a blockchain system, maintaining router information. Once the router information is updated, all router nodes consent the newest routing table. In this way, the router blockchain system records the validated address of each participating blockchain. When a transaction between chain A and chain B is generated, chain A can establish a connection with chain B, transferring the data according to the routing information written in router blockchain.

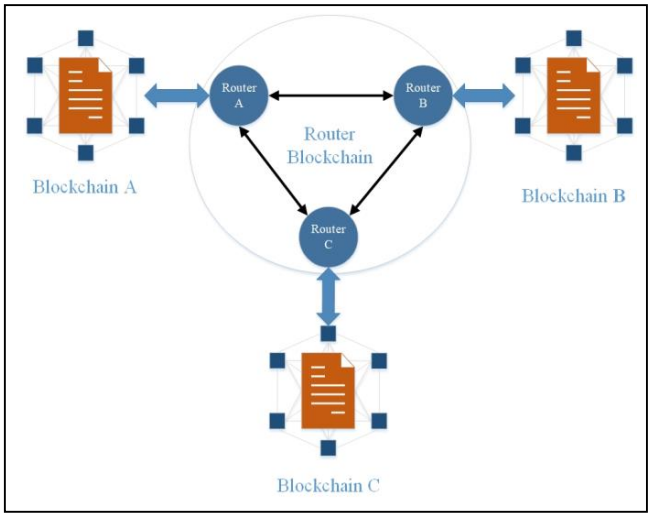

Fig.2. Inter-blockchain connection model

In all, the inter-blockchain connection model has the following features:

- Heterogeneous blockchains communicate with each other through standard crossing-chain transactions.
- Crossing-chain transactions are transferred by nodes in router blockchain.

- Transactions are transferred in peer-to-peer way without participation of any third party.
- Routing table are credible for being maintained in blockchain system.

B. Standard Crossing-chain Transactions

The router blockchain helps to create connections between two blockchains. Based on those connections, it is still infeasible to communicate them without a unified transaction format. In general, different blockchains have different transaction formats. There is no unified transaction format among blockchains. We design a unified crossing-chain transaction format which can be adaptively transited into the local transaction of arbitrary blockchain system. While crossing-chain activities happens, chains communicate with each other through standard crossing-chain transactions. The unified transaction fomat is given below:

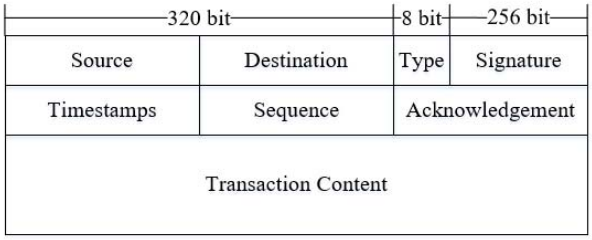

Fig.4. Unified transaction format in inter-blockchain connection model

- Source: the sponsor of the transaction will be recorded with 20 bits. It can be the identification number of a certain blockchain.
- Destination: it presents the receiver of the transaction.
- Type: classification of transaction properties, such as payment, authorization and information sharing.
- Signature: the transaction will be signed by participants.
- Timestamps: the time of starting the transaction.
- Sequence: the unique identification number of the transaction.
- Acknowledgement: it is used for receiver to confirm the transaction.
- Transaction Content: details of the transaction.

We define the process of conversion between a local transaction and a standard crossing-chain transaction as two functions. They are package function and unpack function. The package function is to wrap up a local transaction to a standard inter-chain transaction. The unpack function is to resolve a standard transaction into a local transaction. Considering two isolated blockchain S1 and blockchain S2, we use an expression indicating transferring value from address A1 in S1 to address A2 in S2 are defined as:

$$TRANSFER(A_1, A_2, value) \quad (1)$$

T_{s1} and T_{s2} are intra-chain transactions in S1 and S2 respectively. the assets are transferred between S1 and S2 through τ , τ is collection of crossing-chain standard transactions, T is one of standard crossing-chain transactions, and $T \in \tau$. We have the functions of mutually converting intra-chain transactions and crossing-chain transactions.

$$\forall\ T_{s1}\ ,\ PACKAGE_{s1}(T_{s1})=T,\ \ T \in \tau \quad (2)$$

$$\forall\ T \in \tau\ ,\ UNPACK_{s2}(T)= T_{s2} \quad (3)$$

The process of transferring contains packing the local transaction into a standard transaction in S1 which will be unpacked into the local transaction of S2.

V. Crossing Chain Protocol

When a blockchain system receives the transactions from users, it will carry out transactions and write down the results into the ledger. In the above scenario, assets are transferred among accounts inside the system. However, it is different to handle the transaction that requires moving the assets between two different blockchains. For one thing, the source system need to know how to make the transactions get to the target chain system. For another, two involved chains must keep the same results after finishing the crossing-chain transaction. We present a protocol for inter-chain assets movement that enables account on two chains to transfer value reliably. We record the blockchain address information in form of the standard format. In the process of executing crossing-chain transactions, three phase commit are used to keep the consistency of two systems. Escrowed transfer allows secure payments through untrusted participants. Each blockchain has their own public escrow address which is the authentic intermediary between inter-chain payment. More details about our protocol will be discussed in this section.

A. Routing Messege Format

Transactions are transmitted by router node according to the routing table written in router blockchain. Routing information are formatted as following:

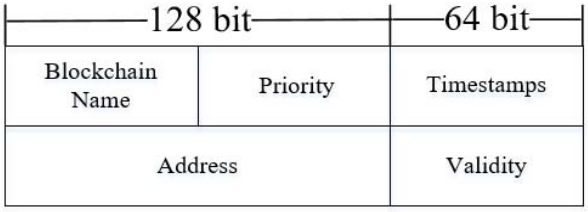

Fig.3. Routing information format

- Blockchain name: the unique identifier of a certain blockchain system. It is recorded with 64 binary bit, The first 16 bits are used to represent the country, the city are marked in the next 16 bits. The last 32 bits indicates the sequence of blockchain.
- Priority: the priority of routing information. routing message with the highest priority contains the newest

blockchain address. The out-to-date information is invalid but will not be deleted. the routing table is updated incrementally in router blockchain and routing message will never be deleted once recorded.

- Timestamps: the generation time of a certain routing message.
- Validity: the validity of a certain routing message.

B. Crossing Chain Protocol

Assets can be moved from chain to chain, by connecting blockchain systems through transactions. In our inter-blockchain connection model, transaction must be a group of atomic, consistent, isolated and durable operations. For durability, after a transaction finished, it is noted in ledger and will survive a system crash. For isolation, write and read operation in transaction are required to be serializable, which means transactions are completely isolated from one another. To guarantee the atomicity and consistence of the transaction, crossing chain protocol is designed. In our proposed protocol, we adopt three phase commit to consensus result between two peers. In this way, the receiver can make final decision to commit or abort in the extra phase. Especially, ledger-provided escrow is also used to eliminate the need of third party. The process of protocol is described briefly below:

1) Transation successful execution: after the transaction is executed successfully, the sender will get an acknowledgement then write down the result into ledger. concerning executing *TRANSFER(A_1 ,A_2,value),* the steps of transferring value from blockchain S1 to blockchain S2 are described as following:

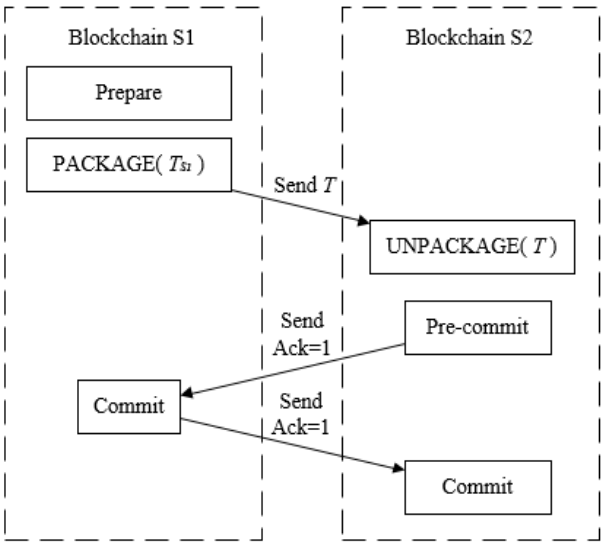

Fig.5. Committing process

- S1 launches an intra-crossing transaction T_{s1}, then gets into prepare stage where the escrow address A_{s1} of S1 is involved and *TRANSFER(A_1, A_{s1}, value)* is executed. And T_{s1} are forwarded to R1, a node in the router blockchain, which is adjacent to S1.
- T_{s1} will be packaged into T by R1, and T are transmitted to node R2 in router blockchain which is close to S2. Once receiving the T, R2 will unpack T into T_{s2}, then send T_{s2} to S2.
- After receiving the T_{s2}, S2 step into the phase of pre-commit, deal with the transaction, check the balance, confirm the signature and consensus the result. However, the result will not be written into block before the result is confirmed by S1. Then the acknowledgement of T_{s2} is sent to S1 through router blockchain.
- After S1 get the acknowledgement message, the result of transaction T_{s1} will be consented and written down in the commit stage. Finally, S1 send the ACK message to S2.
- S2 gets the reply from S1, goes into commit stage, executing *TRANSFER(A_{s2}, A_2, value)*, A_{s2} is the escrow address of S2 and the final result of transaction T are recorded into the chain.

2) Failed transaction execution: the transaction can fail at any stage. So all operations in transaction must be undone whenever the transaction is interrupted. The step of transaction failed in S2 is presented:

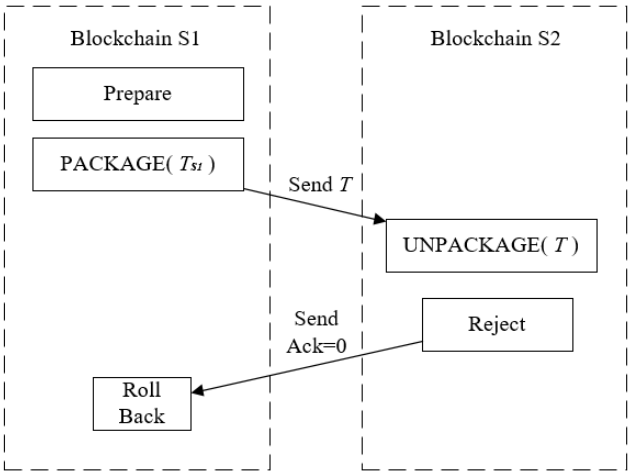

Fig.6. Rolling back process

- S2 receives the transaction T from S2 through router blockchain, then carry out T_{s2} after unpack T.
- Transaction failed for a certain reason, such as insufficient balance, incorrect signature. S2 response S1 with a rejection message through router blockchain.
- After get the rejection, S1 need to undo all operation of transaction T to roll back.

3) Retranmmision protocol: all communications between chains based on peer-to-peer transmision. In this way, transaction delivering will be interfered by packet loss, data transmission error or other network problem. To avoid failing transaction caused by instable network, the strategy of retransmission is designed. The steps of retransmission are given below:

- After finishing the stage of pre-prepare and packaging, S1 sets a timer.
- While counting down to zero and not getting any reply from S2, S1 resend the transaction *T* to S2 and reset the timer.
- S1 will reset the timer three times maximum, which means retransmission will happen three times at most. If S1 still cannot get the reply from S2, S1 roll back and undo all operation of transaction *T*.
- If gets the acknowledgement, S1 steps into commit stage, and send the ACK message to S2.

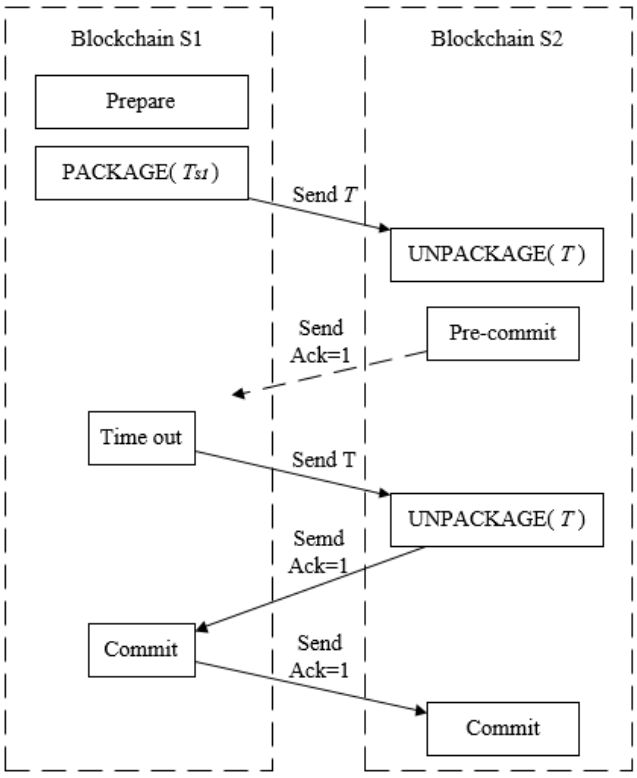

Fig.7. Retransmission process

VI. Experiments And Analysis

To verify the feasibility of our inter-blockchain connection model and test the performance of multiple blockchains system, two experiments are carried out. In the first experiment, a multiple chains system is implemented, executing crossing-chain transactions. Further, in the second experiment, we measure the overall performance of multiple blockchains systems where a quantity of parallel chains deal with transactions.

A. Experiment I

We create a network of our own parivate multiple blockchains and construct a transaction simulater which is able to deliver inter-chain transactions or inter-chain transactions to the blockchain system. Firstly, the simulater only sends intra-chain transactions to one of chain in the chains network. Then, intra-chain transactions mixed with inter-chain transactions are sent to the chain. The total amount of transaction is the same in the two process. The proportion of inter-chain transactions and total transactions is initially set to 20%.

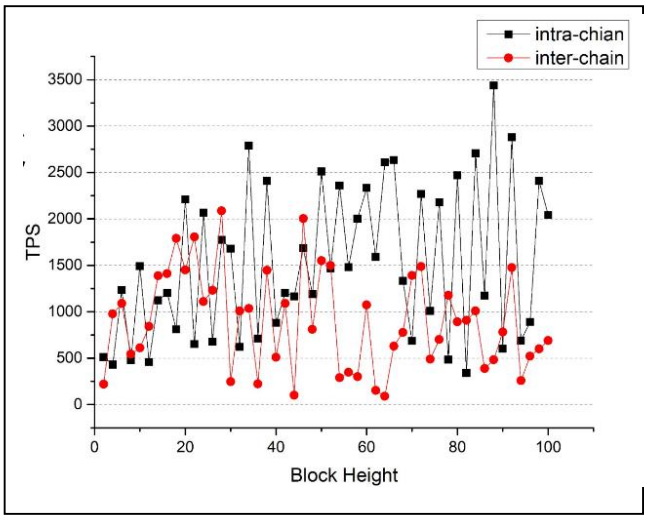

Fig.8. TPS in executing different transactions

In figure 8, the result shows that the performance of a single chain executing intra-chain transactions is better than that of executing mixed transactions. the average transaction per second(TPS) reaches 1520.56 with only handling intra-chain transactions in a blockchain while it is 899.81 maximum with mixed transactions. The reduction is mainly caused by the three commit phase in the process of confirming crossing-chain transactions.

B. Experiment II

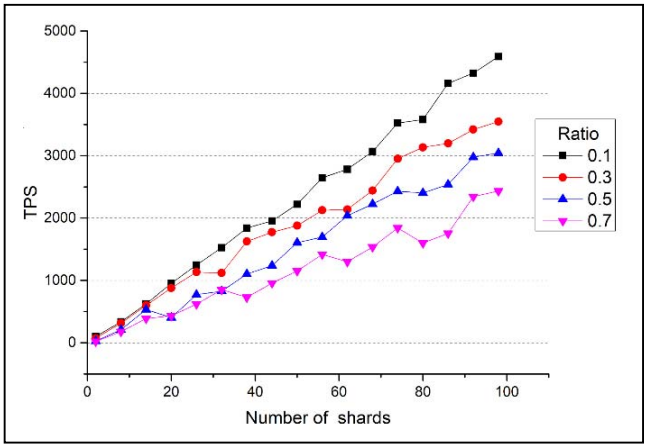

Fig.9. TPS of different chain systems

The second experiment is simulated to test the trend of the system performance with different crossing-chain transaction proportion and the number of chains. a multi-chain system is constructed, containing a group of blockchain systems. Each blockchain system is regarded as a shard. the transaction per second of a single blockchain system varies from 20 to 60. In the experiment, the variable are the number of shard in multi-chain and the complexity of transaction, which is the

proportion of crossing-chain transactions and total transactions. The output is the TPS of the whole multi-chain system.

The experiment result is shown in figure 9, representing the TPS in multiple blockchain system with different amount of shards. Ratio stands for the proportion of crossing-chain transactions and total transactions, varying from 10% to 70%.The result of experiment shows that the performance of multi-chain system increases with the number of shard. For a multi-chain system, the throughout is influenced by the ratio of chain-crossing transaction, while the ratio increasing, the throughout decreases steadily, for the reason that crossing-chain transactions are more time consuming corresponding with the result of experiment I.

VII. Conclusion

In this paper, we proposed an interactive multiple blockchain architecture for reliable exchanging information across arbitrary blockchain system. In our architecture, inter-blockchain connection model was designed for routing management in multiple blockchains. In our proposed protocols, three phase commit is used for confirming the communication result. Escrow transfer of crossing-chain transactions can eliminate the third party. Our protocol also provides atomicity and consistency for crossing-chain transactions. In this way, it is capable of accelerating transaction execution and increasing the throughput of blockchain. Our future work focus on adding encryption and access control into inter-blockchain connection model, improving the security of the multiple blockchain system. We also need to verify our inter-blockchain connection model with formal methods[19][20].

Acknowledgment

This work was supported by National Natural Science Foundations of China (No. 61672074,91538202). Funding of Ministry of Education and China Mo-bile MCM20160203, Project of the State Key Laboratory of Software Development Environment of China under Grant SKLSDE-2016ZX-1

References

[1] Stefan Thomas, Evan Schwartz. A Protocol for Interledger Payments.

[2] X. Xu *et al*., "The Blockchain as a Software Connector," *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)*, Venice, 2016, pp. 182-191.

[3] Hope-Bailie A, Thomas S. Interledger: Creating a Standard for Payments[C]// International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee, 2016:281-282.

[4] S. Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. bitcoin.org, 2008.

[5] Cosmos. [EB/OL].2017[2017-08-01].https://cosmos.network/whitepaper

[6] Michael Crosby, Nachiappan,et al.blockchain technology beyond bitcoin, air Applied Innovation Review[J] ,June 2016. Issue No.2

[7] www://usa.visa.com/merchants/industry-solutions/retail-visa-acceptance.jsp

[8] Aitzhan N Z, Svetinovic D. Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams [J]. IEEE Transactions on Dependable and Secure Computing, 2016.

[9] Chinese Blockchain Technology Application and Development White Paper

[10] Chen Z. Research on Private Blockchain Based on Crowdfunding[J]. Journal of Information Security Research, 2017, 3(3): 227-236.

[11] Back A, Corallo M, Dashjr L, et al. Enabling Blockchain Innovations with Pegged Sidechains. White paper, Blockstream, 2014[J].

[12] Hope-Bailie A, Thomas S. Interledger: Creating a Standard for Payments[C]// International Conference Companion on World Wide Web. International World Wide Web Conferences Steering Committee, 2016:281-282.

[13] Greenspan G. MultiChain Private Blockchain—White Paper [J]. 2015.

[14] Henry Robinson, Consensus Protocols: Three-phase Commit, Henry in computer science, Distributed systems, 2008

[15] Ann-Router.[EB/OL].2017[2017-03-01].http://7i7ifh.com1.z0.glb.clouddn.com/whitepaper.pdf

[16] Lamport L, Shostak R, Pease M. The Byzantine Generals Problem [J]. ACM Trans on Programming Languages & Systems, 1982, 4(3):382-401

[17] Castro M. Practical byzantine fault tolerance and proactive recovery [J]. ACM Trans on Computer Systems (TOCS), 2002, 20(4):398-461.

[18] Mcquillan J, Richer I, Rosen E. The New Routing Algorithm for the ARPANET [J]. IEEE Transactions on Communications, 1980, 25(5):711-719.

[19] Wang Z, Hu K, Xu K, et al. Structural Analysis of Network Traffic Matrix via Relaxed Principal Component Pursuit[J]. Computer Networks, 2011, 56(7):2049-2067.

[20] Hu K, Zhang T, Yang Z, et al. Exploring AADL Verification Tool through Model Transformation[J]. Journal of Systems Architecture, 2015, 61(3–4):141-156.