Inter-Blockchain Communication

Zhi-dong CHEN¹, Zhuo YU², a*, Zhang-bo DUAN¹ and Kai HU¹

¹School of Computer Science and Engineering, Beihang University,
Beijing China 100191

²Beijing China Power Puhua Information Technology Co.Ltd, Beijing China 100192

a*yuzhuo@sgitg.sgcc.com.cn

*Corresponding author

Keywords: Blockchain, Inter-blockchain communication, Routing.

Abstract. With the rapid development of Blockchain technology, researchers have devoted much to it, and many exciting achievements have been made in industry. However, it doesn’t work well with the massive transactions, leading to islands of redundant and inconsistent information arising. Therefore, a mechanism on how to make different Blockchain systems communicate with each other better, and the Inter-Blockchain communication (IBC) will be proposed in this paper. In IBC, the nodes between the Blockchain systems use the efficient routing algorithm to update the routing path dynamically. It will analysis the transaction and pack the transaction into a specific form to adapt to the destination Blockchain system. In this way, IBC can make different Blockchain system communicate without any intermediaries. The experiment results show that the use of IBC does not have much impact on throughput of Blockchain system.

Introduction

The Blockchain is a new technology derived from Bitcoin, which constructs a new value transfer model on the Internet. A Blockchain is a chronologically ordered chain of blocks protected by solving a proof-of-work. The chaining is built by adding the hash of one block to its following block. Consecutive nested blocks guarantee transactions to come in a chronological order. Hence a transaction cannot be changed backdated without changing its block and all the following blocks. In the narrow sense, Blockchain is a chained data structure combining data blocks in chronological order and is crypto logically guaranteed for non-tampering and unforgeable distributed ledger. Broadly speaking, the Blockchain technology is a new distributed infrastructure and computing paradigm which contains using Blockchain data structure to verify and store data, taking advantage of distributed node consensus algorithm to generate and update data, using cryptography to ensure data transmission and access security, using smart contract, which is composed, to program and manipulate data.

In the process of continuous development of Blockchain technology, the emergence of a lot of creative progress is encouraging. Ethereum gives a Turing-complete smart contract under the protection of the Blockchain architecture; Truth coin has invented a tool for making oracle on the Blockchain; Name coin gives a distributed domain name system based on Bitcoin; Factom uses Blockchain to store the hash value of the data to protect the digital assets. However, all solutions lack at least one of the following: regulatory, scalability, script security, and easy access to real-world data. Even if they have all the characteristics, the Blockchain is still isolated.
Our Contribution. 1) Combining Blockchain technology and routing algorithm to connect different Blockchain systems. 2) Proposing the Inter-Blockchain communication to make different Blockchain systems communicate without any intermediaries.

Organization. Section II discusses the recent studies on multi-chain. Section III provides the core protocol component. Whereas section IV describes the IBC in detail. Section V describes the technical implementation, and concluding remarks can be found in section VI.

Related Work

Pegged Sidechains
Blockstream 0 uses pegged side chains to achieve the transfer of Bitcoin and other ledgers’ assets between multiple Block chains. This allows the user to transfer the assets on the Bitcoin to the new Blockchain to generate new and innovative cryptocurrency systems. By exchanging money, it is possible to interact with each other and with the Bitcoin, which increases the application and the flow of Bitcoin. That the sidechains are independent of the main chain and other sidechain systems makes it unimpeded by other factors in terms of technology and currency circulation. Although the system on the side chain can be redeemed and transferred with the Bitcoin system, it does not affect the main chain when a malicious attack occurs on the sidechain.

Interledger Protocol
Ripple proposed an Interledger protocol 0 (ILP), whose primary goal is to serve all distributed ledgers (Blockchains), transactions between ledgers, and value transfers. ILP is not a ledger, and does not require any consensus process. It provides a top-tier cryptographic custodian system that allows funds and currencies to flow between accounts. As a result, with the help of such top-tier cryptographic custodian systems, the security of the ledgers can be guaranteed. However, this way of capital flows requires the managed system as an intermediary to complete.

MultiChain Private Blockchain
MultiChain 0 is an off-the-shelf platform for the creation and deployment of private Blockchains, either within or between organizations. It aims to overcome a key obstacle to the deployment of Blockchain technology in the institutional financial sector, by providing the privacy and control required to use package easily.

The platform limits the mining node and the mining process to a manageable range to avoid the monopoly of the mining process called “diversity mining”. Diversity mining does not use proof of work, or plenty of computing resources to achieve its correctness and effectiveness, which allows miners dealing with transactions to recognize and process 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 and also support a lot of third-party assets, you can make the private Blockchain and Bitcoin block between the assets of mutual conversion.

Ann-Router
Ann-Router 0 provides a method of interworking message distribution and proposes a communication protocol between the Blockchains so that different Blockchain systems
can exchange information as a communication device in the network. In an Ann-Router based network architecture, a part of the Blockchain systems can function as a router in a network-like configuration, distributing request information according to the agreed transport protocol. And in the meantime, update and maintain the entire Blockchain network topology. Ann-Router can also fragmentize the Blockchain to improve the throughput of the entire system. Compared to a single Blockchain system, the Ann-Router can be increased linearly in transactional throughput by using multiple sub-chains. The transaction request is distributed into different Blockchain systems through the mechanism. This method can effectively avoid the problem that the overload of the same Blockchain system is too heavy.

In addition to the Blockchain fragmentation, Ann-Router’s another function is the interconnection between the various Blockchain systems to establish a trusted transmission medium.

Components
Inter-Blockchain communication (IBC) gives a way that different Blockchain systems can communicate without any intermediaries. In this section, we will discuss the core components of the protocol.

Blockchain
The Blockchain in IBC is replicated at every node and assists nodes in reaching the consensus on the state and calculation results. A Blockchain contains series of blocks, as shown in Figure 1. Each block has an identifier of their predecessor in the chain, a number denoted as the generation of the Blockchain, as well as a list of transactions consistent with the state of the ledger represented by the chain they extend. However, transactions are not stored in Blockchain directly, because the block head only stores the merkle root of the transactions. To avoid creating the monopoly on the approval of transactions, all nodes have chances to create blocks. Once a block (Supposing its generation is $h$) is created, it is distributed to the rest of the network, which is denoted as $B_h$.

![Blockchain diagram](image)

Figure 1. Blockchain.

Transactions
A transaction is a cryptographically-signed instance of changing ownership of tokens through digital signing portion of data and broadcasting it to the network. The structure of transaction $Tx$ can be defined/quantized by the equation 1:

$$Tx = nVersion || vin || vFrom || vout || vTo || vNum || nFlag$$  \hspace{1cm} (1)
where \( \text{vin} \) and \( \text{vout} \) are vectors of input and output measured by tuples of elements used for transferring ownership of tokens from the previous owner to the current. \( \text{vFrom} \) and \( \text{vTo} \) denote Blockchains that \( \text{vin} \) and \( \text{vout} \) belonging to respectively. \( \text{vNum} \) shows the number of transaction inputs. \( \text{nFlag} \) denotes whether the transaction has been broadcasted to others. Tokens are transferred in the consecutive or non-consecutive order in transactions \( T_n, T_m, T_k \) of blocks \( B_{h1}, B_{h2}, B_{h3} \), such that \( T_n \in B_{h1}, T_m \in B_{h2} \) and \( T_k \in B_{h3} \), where \( n < m < k \) and \( h1 < h2 < h3 \).

**Consensus**

The block calculated by the verification point (VP) needs to be broadcasted in the network. When VPs receive the block, they have to decide whether agree on this block through the consensus algorithm. The algorithm is based on Practical Byzantine fault tolerance (PBFT [8, 9]). IBC is a token-based protocol which allows users to transfer their belongings without any intermediaries. The consensus algorithm is shown in Figure 2.

**Algorithm:** Inter-Blockchain Consensus algorithm

<table>
<thead>
<tr>
<th>Algorithm: Inter-Blockchain Consensus algorithm</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Input:</strong> transactions ( \text{tx} ),</td>
</tr>
<tr>
<td>height ( h ),</td>
</tr>
<tr>
<td>round ( r )</td>
</tr>
<tr>
<td>BEGIN</td>
</tr>
<tr>
<td>1  leader ( \leftarrow \text{proposer}(h,r) )  //get leader</td>
</tr>
<tr>
<td>2  IF ( \text{self} ) is leader THEN</td>
</tr>
<tr>
<td>3     //compute block</td>
</tr>
<tr>
<td>4     block ( \leftarrow \text{processBlock}(\text{tx}) )</td>
</tr>
<tr>
<td>5     broadcast(block)  //broadcast the block</td>
</tr>
<tr>
<td>6     IF block is received THEN</td>
</tr>
<tr>
<td>7     vote ( \leftarrow \text{verify(block)} )  //vote for the block</td>
</tr>
<tr>
<td>8     broadcast(vote)  //broadcast the vote</td>
</tr>
<tr>
<td>//count votes</td>
</tr>
<tr>
<td>9     IF +1/3 reject vote received THEN</td>
</tr>
<tr>
<td>10    ( r \leftarrow r + 1 )  //over 1/3 opposes then round + 1</td>
</tr>
<tr>
<td>11    IF +2/3 approve vote received THEN</td>
</tr>
<tr>
<td>12    ( h \leftarrow h + 1 )  //over 2/3 approves then height + 1</td>
</tr>
<tr>
<td>END</td>
</tr>
</tbody>
</table>

Figure 2. Inter-Blockchain Consensus algorithm.

**Inter-blockchain Communication**

IBC makes every verification point maintain a routing table that can communicate with other Blockchain systems. Network scenarios in the work are assumed that there are a lot of Blockchain systems and the topology is complicated, and not all the systems can communicate with each other directly.

When a transaction involving two different Blockchain systems is generated, IBC does some analysis and deliver the transaction in different systems as follows (Figure 3). The transaction is divided into two parts according to whether this operation belongs to the system. The first part belonging to it makes a pre-commit in the system \( S1 \). Meanwhile IBC pack and deliver the second part to the other system \( S2 \). When \( S2 \) receives the second part, it will make a commitment and reply. \( S1 \) will make the final commitment. As an atomic operation, both parts are either successful or failed. Once the network failure occurs, system \( S1 \) will retransmission the 2\textsuperscript{nd} part (Figure 4).
Implementation and Analysis

A scenario with two Blockchain systems is simulated in implementation in which tokens are used for transferring data. The main software components of the IBC infrastructure are:

*The platform client.* The platform client is a reactor managing transaction execution, validation, signing, node observation and messages encryption and propagation.

*P2P network and points.* To simulate and validate IBC, two different Blockchain systems are designed in experiments and each one has four verification points. All points are connected in a p2p network 0 and propagate transactions and messages to each other.

*Blockchain.* The private Blockchain is generated by creating unique merkle hash root and a new genesis block.

IBC’s P2P network can be described as an undirected connection graph $G = (V, E)$, where $V$ is the set of all eight points and $E$ is denoted as the set of connections cost between the points. Point $v_i \in V (0 \leq i \leq 3)$ maintains the Blockchain in system $S1$ and point $v_i \in V (4 \leq i \leq 7)$ maintains the Blockchain in system $S2$. Point $v_i \in V$ propagates...
block $B_h$ and transaction $T_n$ where $T_n \in B_h$. The timestamp of the transaction $t_{in}$ is determined by the transaction generation time and $t_h$ is determined by the time that the block including the transactions are accepted. Therefore, we consider that transaction processing time is $\delta_t = t_h - t_{in}$.

In simulation, we assume that there is a lot of users who want to transfer their tokens from $S1$ to $S2$. When there is just one user transferring tokens from $S1$ to $S2$ and it costs 231 milliseconds to finish, it needs 231 milliseconds to confirm this transaction. However, when it comes to the real world, there will be thousands of transactions generated at the same time. With IBC, our Blockchain system can deal with 1223 inter Blockchain transactions per second and dealing with 1431 inner Blockchain transactions. It shows that use of IBC does not have much impact on the throughput.

**Conclusion**

In this paper, we proposed the Inter-Blockchain communication that can make different Blockchain systems communicate with each other without any intermediaries. We implemented a token-based private decentralized system including two different Blockchain systems, and used Blockchain technology, routing algorithm and PBFT algorithm to make sure that users can use this system to fulfill the token circulate.

However, the throughput of the whole system is unsatisfactory. We found the different network topologies can bring different effects In the future, we will discuss different network topologies, study their characteristics to find a more appropriate one. In the other hand, IBC requires a formal verification method to verify its correctness.

**Acknowledgement**

This work was partially supported by the National Natural Science Foundation of China under Grant 61672075 and 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-16.

**References**


http://7i7ifh.com1.z0.glb.clouddn.com/whitepaper.pdf


