Good Governance by using Blockchain

Abhishek Gandhi[1], Mayur Dahake[2], Dhiraj Gadekar[3], Abhishek Bondage[4], P. P. Nimbalkar[5]
[1,2,3,4]*Student, Dept. of Computer Engineering, JSPM'S Imperial College of Engg. and Research, Pune, India*
[5]*Professor, Dept. of Computer Engineering, JSPM'S Imperial College of Engg. and Research, Pune, India*

***Abstract*: The Blockchain is a trustworthy digital ledger of economic transactions that can be programmed to record not just financial transactions but virtually everything of value. To transfer money outside to country its take three to four day to complete the process. The current banking system requires the use of multiple third-party verifications and transfer services in order to complete the transaction. There is no trust and transparency between the user and the bank system. To overcome these problems, in this paper we use Blockchain technology for faster payments than banks. Blockchain technology and distributed ledgers can decrease operational costs and bring us alongside real-time transactions between financial foundations. We use cross chain protocol for reliably exchanging information without third-party in multiple Blockchain systems.**

***Keywords*: Blockchain, Cross-chain, Three-Phase commit protocol**

1. Introduction

Now a day we see that money transferring from one donor to some organization, is a part of risk because there can take a lot of time and unacceptable risks in transferring money.

They incur a lot of risk and fraud when dealing with money changers and middlemen in areas where traditional banking. This avoids local government deception, possibility to employees carrying large amounts of cash, and easy repatriation of charity.

There is lack of transparency showing donors how funds are spent and obey with donor regulations. So to avoid these types of problem we made this project. By Utilizing smart contracts, Coin creates transparent records and real-time funds traceability of donations, expenses, and contracts with suppliers, eliminating the possibility of fraud and simplifying donor/foundation compliance regulations.

Blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology has three main features:

- Immutability: The inability of a block to be deleted or modified once it is in the Blockchain once data has been written to a Blockchain no one, not even a system administrator, can change it As a provider of data you can prove that your data hasn't been altered, and as a recipient of data you can be sure that the data hasn't been altered. These welfare are useful for databases of financial transactions.
- Verifiability: The ledger is decentralized, replicated and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.
- Distributed Consensus: A distributed consensus protocol to determine who can add the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any newly proposed block of entries becomes a permanent part of the ledger.

2. Multiple blockchain architecture

A new architecture called multiple Blockchain architecture, as a solution to communicate different blockchain, is proposed in the paper.

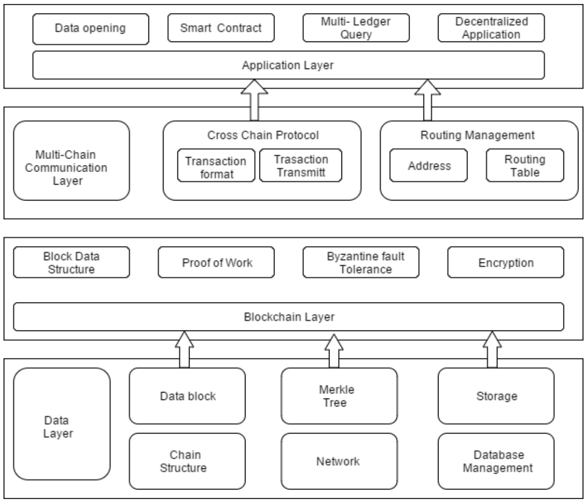

Fig. 1. Multiple blockchain architecture

- Data Layer: In this layer, there are foundation of the system operation, block chain data structure and physical storage, network, containing Data block, Chain structure, Merkle tree, Database Management.
- Blockchain Layer: In Blockchain layer, Blockchain data structure and the format of transaction are defined in basic data structure modular; the chain will be concurrence in Blockchain system with concurrence algorithm describe in concurrence module; and encryption algorithm are describe in encryption module.

- Multi-chain communication layer: To make transaction quick committed 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
  1) Routing management: Inconsistence Blockchain system can join the Blockchain network with a router. A inter Blockchain model is designed for routing management.
  2) 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.
- Application Layer: Provide application interfaces on top of Blockchain architecture, multi-ledger query, smart contract, and data opening are based on the multi-chain system with the service of the chain-crossing layer. Smart contacts are a key appear used case of Blockchain technology. With services of multi-chain communication layer, it becomes reachable to carry out complex mixture query through multiple ledgers. As for data opening, heterogeneous systems join up, manufacture information exchanged briskly and shared securely with the service of the multi-chain layer.

3. Cross chain protocol model

When a Blockchain system receives the transactions from users, it will carry out transactions and write down the results into the ledger, however, it is different to handle the transaction that requires moving the things between two different Blockchain. For one thing, the source system needs to know how to make the transaction 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 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 cross-chain transactions, the three-phase commit is used to keep the consistency of the two systems. Guarantee transfer allows secure payments through untrusted participants. Each Blockchain has their own public secured address which is the authentic intermediary between inter-chain payments. More details about our protocol will be discussed in this section.

A. Routing message format

Transactions are transmitted by router node according to the routing table written in router Blockchain. Routing information is formatted as follows:

- 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, and the city is 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 outdated 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.

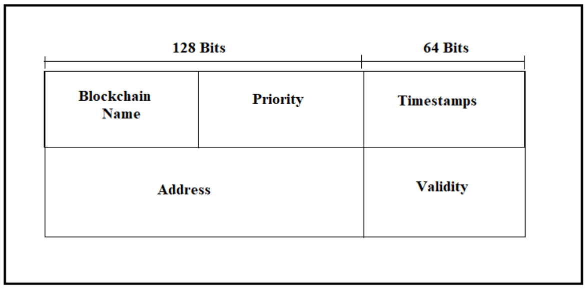

Fig. 2. Routing information format

B. Crossing chain protocol

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

1) Transaction successful execution

After the transaction is executed successfully, the sender will get an acknowledgment then write down the result into the ledger. The steps of transferring value from Blockchain 1 to Blockchain 2 are described as following:

- Block 1 launches an intra-crossing transaction T1, then gets into the prepare stage where the guarantee address A1 of block 1 is involved and is executed.
- T1 will be packaged into T, and T is transmitted to block which is close to Blockchain 2, through the router.
- Once receiving the T will unpack T into T2, then T2 send to Block 2. After receiving the T2, Block 2 step into the phase of pre-commit, deal with the

transaction, check the balance, confirm the signature. However, the result will not be written into the block before the result is confirmed by Block 1. Then the acknowledgment of T2 is sent back to Block 1 through router Blockchain.

- After Block 1 get the acknowledgment message, the result of transaction T1 will be approved and written down in the commit stage. Finally, Block 1 sends the ACK message to Block 2.
- Block 2 gets the reply from Block 1, goes into the commit stage, executing A2 is the guaranteed address of Block 2 and the final result of transaction T are recorded into the chain.

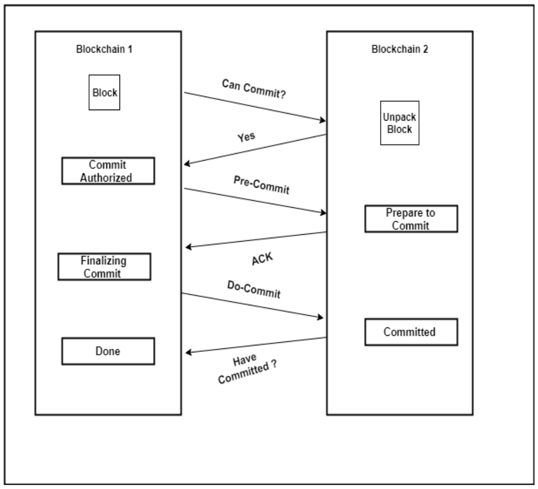

Fig. 3. Committing process execution

2) *Failed transaction execution*

The transaction can fail at any stage. The step of the transaction failed in Block 2 is presented:

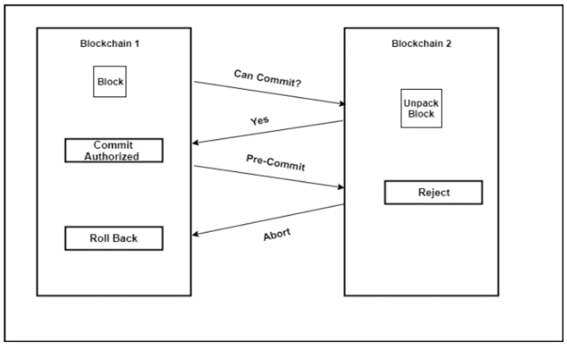

Fig. 4. Failed transaction execution

- Block 2 receives the transaction T from Block 1 through the router, then carry out T2 after unpacking T.
- Transaction failed for a certain reason, such as an incorrect signature. Block 2 response Block 1 with a rejection message through router Blockchain.
- After getting the rejection, Block 1 need to undo all operation of transaction T to roll back.

3) *Retransmission protocol*

Transaction delivering will be prevented by packet loss, data transmission error or other network problem. To avoid failing transaction, the strategy of re-transmission is designed.

A retransmission timeout (RTO), on the other hand, is quite a difference. An RTO occurs when the sender is lost too many acknowledgments and choose to take a time out and stop sending completely. After some amount of time, usually at least one second, the sender cautiously starts sending again, testing the waters with just one packet at first, then two packets, and so on.

- After finishing the stage of pre-prepared and packaging, Block 1 sets a timer.
- While counting down to zero and not getting any reply from Block 2, Block 1 resend the transaction T to Block 2 and reset the timer.
- Block 1 will reset the timer three times maximum, which means retransmission will happen three times at most. If Block 1 still cannot get the reply from Block 2, Block 1 rollback and undo all operation of transaction T.
- If gets the acknowledgment, Block 1 steps into the commit stage, and send the ACK message to Block 2.

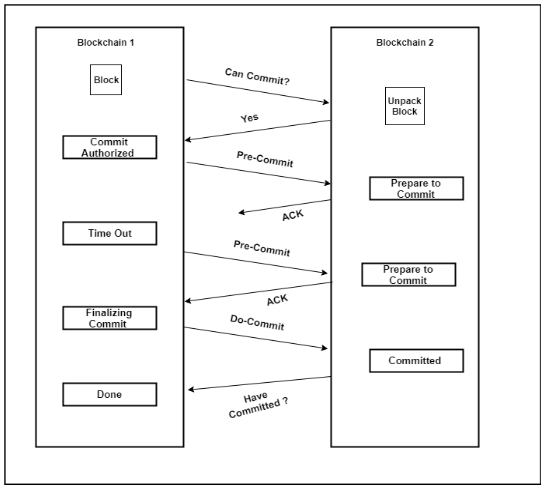

Fig. 5. Retransmission process execution

4. Network

The steps to run the network are as follows:

1) New exchanges are communicated to all peer.
2) Each peer gathers new transactions into a block.
3) Each peer works on finding a hard proof-of-work for its block.
4) When a peer finds a proof-of-work, it communicates the block to all peer.
5) Peer accept the block only if all transactions in it are valid and not already exhausted.

6) Nodes express their acquiring of the block by working on producing the next block in the chain, using the hash of the gained block as the previous hash.

5. Privacy

The conventional banking model accomplishes a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly prevent this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys unknown. The audience can see that someone is sending an amount to someone else, but without information connecting the transaction to anyone. This is the same as the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

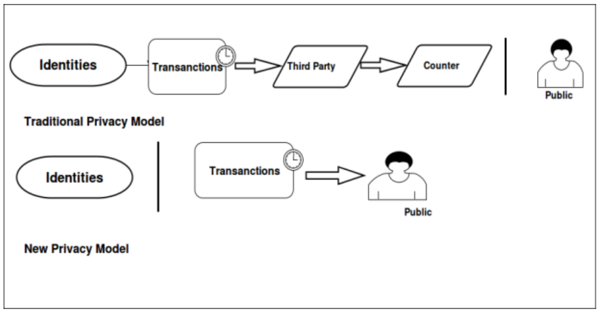

Fig. 6. Privacy transaction

6. Conclusion

In this paper, we proposed an, we use cross chain protocol for reliably exchanging information without third-party in a multiple Blockchain systems. In our proposed protocols, three-phase commit is used for confirming the communication result. Guarantee transfer of crossing-chain transactions can remove the third party. Our protocol also provides atomicity and consistency for crossing-chain transactions. Our future work focuses on adding encryption and access control into inter-Blockchain connection model, improving the security of the multiple Blockchain systems. We also need to verify our inter-Blockchain connection model with formal methods.

References

[1] Kan Luo, Wei Yu, Hafiz Muhammad Amjad, Kai Hu, LingChao Gao, (2018) “A Multiples Blockchain Architecture on Inter-Blockchain Communication”.

[2] Satoshi Nakamoto, “Bit coin: A Peer-to-Peer Electronic Cash System”.

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

[4] Henry Robinson, “Consensus Protocols: Three-phase Commit”, Henry in computer science, Distributed systems, 2008.

[5] Stefan Thomas, Evan Schwartz, “A Protocol for Interledger Payments”.

[6] Christopher Ehmke, Florian Wessling, Christoph M. Friedrich, “Proof-of-Property – A Lightweight and Scalable Blockchain Protocol” 2018 ACM/IEEE 1st International Workshop on Blockchain.

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

[8] J. Warren, “Bit message: A peer-to-peer message authentication and delivery system,” 2012.