International Research Journal of Engineering and Technology (IRJET) e-ISSN: 2395-0056
Volume: 08 Issue: 04 | Apr 2021 www.irjet.net p-ISSN: 2395-0072

Architecture and Design to Facilitate Cross-Chain Transactions on Blockchains

Harsh Wasan

Vidyalankar institute of technology, Maharashtra, India

Abstract--*Crypto currencies are becoming increasingly popular for executing transactions on the blockchain. The only drawback is that these blockchains do not allow cross-chain payments or exchange of crypto currency without use of having additional crypto funds or smart contracts to facilitate exchanges between the buyers and sellers. For converting one crypto currency into another, the buyers and the sellers of the crypto currencies are necessary on an exchange. This dependency of buyers for the crypto currency being sold will stall or hinder the exchange if the buyers are absent. The method proposed tries to bypass the need of having the buyers for any crypto currency being sold by directly converting the currencies into each other and storing the converted currencies into the new wallets of the individual who required the converted currencies. This allows anyone to directly convert their currencies eliminating the need for buyers. Thus, to facilitate the direct conversion of the currencies some new designs and architectures for these blockchains need to be introduced. The proposed method attempts to exchange currencies between 2 blockchains, i.e., to facilitate interoperability between blockchains. These blockchains follow a set of designs suggested in this paper which allow them to communicate with another blockchain called as buffer chain. This buffer chain facilitates the cross-chain transactions/payments by acting as a medium to store the transactions till the transactions are pushed onto both the blockchains. In this paper we illustrate how the proposed designs and architecture can work.*

Keywords—blockchain, cross-chain, interoperability, coin-exchanges, cross-chain transactions.

1. Introduction

Blockchain systems are increasingly getting adopted, yet there are issues which need to be addressed before they can be used to substitute the current monetary system [3]. Consider bitcoin, it has a self-regulating system which on certain intervals discovers new blocks. Currently in the bitcoin blockchain new blocks are added every 10 minutes on an average [4] yet all the transactions in these blocks are intra-chain transactions i.e. the transactions occur between wallet-addresses of the same chain. Blockchains which can allow users to create cross chain transactions with other can grant a lot of freedom to people which makes it easier to create a decentralized ecosystem. One of the main areas which interoperability can be a boon to is the crypto exchanges. Crypto exchanges carry out process of exchanging one crypto currency to another. To facilitate exchange of crypto-currencies current crypto-exchanges require the exchange to happen between a buyer and a seller. Hence, they have developed models based on smart contracts, mini chains etc. Also protocols such as inter-ledger protocols can be used. Additionally, centralized exchanges only allow the users to exchange or hold the currencies in wallet addresses owned by the company itself. This can also pose security problems and leave the users open to be victims of fraud.

This paper suggests that instead of locking the funds in escrow, one can use the proposed set of standards to design the newer upcoming blockchains which will allow them to communicate with each other using any central medium to synchronize the transactions/payments i.e. make the blockchains interoperable. This removes the dependency of any buyer of any currency since it enables one to convert the currencies directly instead of exchanging. The central medium is also a blockchain which is used as a ledger to maintain a record of the requested transactions/payments, which acts as a proof of the transaction and can be used to confirm and execute the transactions. The medium blockchain or the buffer-blockchain can be a public blockchain which different exchanges can connect to access and facilitate transactions.

Since the defining feature of blockchains is their decentralized system [7], directly facilitating transactions between the chains by converting the coins i.e. enabling the blockchains to be interoperable is the main aim of this paper.

2. Literature survey

This paper tries to suggest design changes and models to ensure interoperability of different blockchains enabling them to carry out cross chain transactions. Though there is a lack of vast research and papers with the motive of making the blockchains interoperable, some of the papers have succeeded to achieve and deploy such blockchains. “An interoperable blockchain architecture is a composition of distinguishable blockchain systems, each representing a distributed data ledger, where transaction execution may span multiple blockchain systems, and where data recorded in one blockchain is reachable and verifiable by another possibly foreign transaction in a semantically compatible manner.”[6].

This paper from the Massachusetts Institute of Technology also tries to address to this problem. They have defined 2 levels of interoperability- mechanical level and value level. This paper tries to propose some standards which allow the blockchains to partake in transactions at both the levels.

In a patent by Vijay K. Madisetti , Arshdeep Bahga [5] the inventors have designed a central blockchain with a bridge to facilitate cross-chain transactions, but the central blockchain was implemented as a private blockchain. The private blockchain introduces constraints on the interoperability and provides chances for middle ware to be introduced. This paper proposes to use a public blockchain or set up a group of public blockchains for cross-chain transactions.

Some protocols such as the inter-ledger protocol are also in use. This protocol is for inter-ledger payments that enables anyone with accounts on two ledgers to create connections between them It uses ledger provided escrow conditional locking of funds to allow secure payments through untrusted connectors [1].

3. Cross-chain transactions and interoperability

The future of the distributed web lies in the ability of blockchain networks to interact and integrate with each other [2]. This is the concept of Blockchain interoperability. A defining characteristic of interoperability are cross- chain transactions.

The cross-chain transactions/payments are different from cross-chain swaps or atomic swaps. The cross-chain swaps are used to facilitate exchange of currencies between 2 entities. On the other hand, cross-chain transaction in this paper is used simply to refer to a payment or a transaction between 2 entities having different wallet addresses on different blockchain. In cross-chain transactions conversion of the crypto-assets takes place instead of exchange.

When a transaction occurs between two addresses of different blockchains it suggests that the data transferred from one chain is easily accessible and readable in terms/format of the other blockchain [2]. The fact that the transaction should be readable in the format of the other blockchain is a very important aspect for the transaction to be valid.

Let us consider 2 blockchains without a limit on the maximum number of coins in existence.
Example – A wants to send 10$ worth of coins from blockchain 1. Blockchain 1 operates on coins whose unit value is 1 $
Hence A will send 10 coins of the blockchain 1
Whereas B must receive 10$ worth of coins on blockchain 2. Blockchain 2 operates on coins whose unit value is 2$ Hence B should receive 5 coins of the blockchain 2

The above example illustrates a simple cross chain transaction.
The current systems do not allow to convert one crypto currency to another directly hence one has to get their currencies exchanged using exchanges.

4. Proposed standards and working

To enable cross-chain transactions or interoperability between the blockchains, the design standards used commonly need to be updated. A medium to enable and add the cross-chain transaction to the chains is also required. Though the proposed design and architecture can work for any application, this paper mainly focuses on the implementation of the design to enable cross-chain payments.

The proposed architecture consists of 3 entities namely the blockchains, the buffer chain and the crypto-currency exchanges.

4.1 Blockchain design.

The blockchain is simply a chain of data blocks. Each block can be thought of as a page in a ledger. The individual blocks are composed of several transactions. These transactions can be a record of transfer of data between two addresses. Most of the current blockchains at least have the following parameters in their transactions –

- Sender's address
- Receiver's address
- Data.

These 3 are most common and necessary parameters which are used with other parameters to validate a single transaction. This paper suggests adding a few more parameters to make the blockchains interoperable. To send data from one chain to other, parameters such as the sender's chain and the receiver's chain are required since this can be used to identify on which chain the data is sent. The receiving and the senders address should point to the address of the wallets on different blockchains when a cross chain transaction is to be carried out. Another parameter which refers to the hash of the buffer chain is also required. This hash can be used to locate the transaction on the buffer chain for validation. The hash of the buffer-chain refers to the hash of the block in which the transaction is recorded on the buffer chain.

So, the required parameters are as follows

- Sender's address
- Receiver's address
- Data.

- Receiver's chain
- Sender's chain
- Hash of current block of the buffer chain

The constructor of the blockchain look like this

```
constructor(senderaddress ,recieveraddress ,amount,senderchain ,recieverchain,hash_of_bufferchain_block){
        this.senderaddress =senderaddress ;
        this.recieveraddress =recieveraddress ;
        this.amount=amount;
        this.senderchain =senderchain ;
        this.recieverchain =recieverchain ;
        this.hash_of_bufferchain_block=hash_of_bufferchain_block;

    }
```

After the transaction is recorded it can be encrypted and added to the blocks.

4.2 The Buffer chain

This paper proposes to deploy blockchain which will act as a proofing medium for the cross-chain transactions. This chain is a public chain which the coin exchanges can access data from. The blockchains which are designed using the standard parameters proposed above are synchronized with this chain.

Instead of trying to lock the funds or use swapping methods, the paper proposes to create a new transaction on this new buffer chain which can be referenced to create transactions on the sending and receiving chain with different chain addresses. The new transactions can be the proof of a transaction between the two chains even though there has not been any connection between the two chains. In this paper it is referred as the buffer-chain because it acts a buffer for the transactions i.e. till the transaction is added to both the blockchains the transaction is considered in the waiting phase. Even if the transaction gets pushed onto a block in one blockchain the transaction is not considered completed till the second blockchain also pushes the transaction. Till the time the transaction is not completed the record of the transaction is available on the buffer-chain. Fig-1 shows the process of confirmation of the transaction with respect to time.

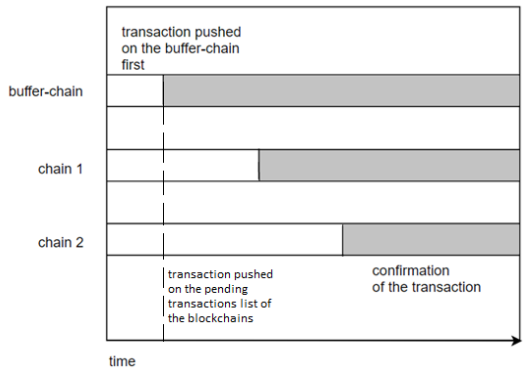

Fig 1- Confirmation of a transaction with respect to time

In the buffer chain the transactions have the similar standard parameters discussed above except for an additional parameter- The conversion factor.

The conversion factor refers to factor which needs to be multiplied to the amount transferred across the chains to ensure that the monetary value transferred from one chain to another is not changed even of the number of coins change from one chain to another.

Conversion factor (C_F) = V_s/ V_R

Where
$V_{s=}$ value of a unit coin of the sender's chain,
V_R =value of a unit coin of the receiver's chain.

To get the converted amount of coins which needs to be added to the receiving chain we need to multiply the amount of coins sent to the conversion factor

Amount of coins on the receiving chain= N_s * conversion factor.

Where
N_s =Number of coins sent

This makes the conversion factor an important parameter which cannot be overlooked.
So, the required parameters are as follows

- Sender's address
- Receiver's address
- Data.
- Receiver's chain
- Sender's chain
- Conversion factor

Also for validation purposes we can create hashes of both the transactions on the sender and receiving blockchain using the data on the buffer chain.
Hence 2 addition parameters can be added namely

- Sender chain transaction hash
- Receiver chain transaction hash

We used java-script to implement the buffer-chain and the transaction constructor of the chain is as follows

```
constructor(senderaddress ,recieveraddress ,amount,senderchain ,recieverchain, conversionfactor){
        this.senderaddress =senderaddress ;
        this.recieveraddress =recieveraddress ;
        this.amount=amount;
        this.senderchain =senderchain ;
        this.recieverchain =recieverchain ;
        this.conversionfactor=conversionfactor;

    }
```

The buffer chain also needs to return the hash and the converted amount to push the transactions on the sender's and receiver's chain. Hence another method is added to fetch the values upon request by storing it in a dictionary.

The sample code of the method is as follows

```
gettransactiondata(getsendertransactionaddress,getrecievertransactionaddress){
        var dict={
             amount:0,
             convertedamount:0,
         recieverchain:"",
         senderchain:"",
         recieveradd:"",
         senderadd:""

        };
        for( const block of this.chain){
            for(const trans of block.transaction)
            {
                if(trans.senderaddress==getsendertransactionaddress && trans.recieveraddress==getrecievertransactionaddress)
                {
                  dict.amount=trans.amount;
                  dict.convertedamount =trans.conversionfactor*trans.amount;
                  dict.recieverchain=trans.recieverchain;
                  dict.senderchain=trans.senderchain;
                  dict.recieveradd=trans.recieveradd;
                  dict.senderadd=trans.senderadd;
                }

            }
        }
        return dict;
    }
```

4.3.1 Working in Coin exchanges

Coin exchanges are businesses that allows customers to trade cryptocurrencies or digital currencies for other assets, such as conventional fiat money or other digital currencies. Following the launch of a decentralized cryptocurrency bitcoin in 2008 and the subsequent introduction of other cryptocurrencies, many virtual platforms were created specifically for the exchange of decentralized cryptocurrencies[9]. The main drawback of the exchanges is the threat of losing one's assets to the exchanges due to hacks or leaks as well as dependency of buyers and sellers.

A cryptocurrency wallet is a device, physical medium, program or a service which stores the public and/or private keys and can be used to track ownership, receive or spend cryptocurrencies.[10]

Both the wallets and the coin exchanges are accompanied by interfaces which can potentially become the medium required to facilitate communication between the blockchains.

The paper proposes that the coin exchanges/wallets carry out the transactions between the blockchains. As shown in Fig-2 when a cross chain transaction is accepted, the transaction is first pushed onto the buffer chain. The coin exchange/wallet receives the block hash of the block in which the transaction is pushed into as well as the converted amount. The coin exchange/wallets then push the same transaction onto the sender's blockchain after adding the hash of the block the transaction. It is also pushed in on the receiver's blockchain after the amount in the transaction is changed to the converted amount received by the coin exchange/wallets, and the hash of the buffer-chain block is added. Since the blockchains will most likely confirm and push the transaction on the block at different times the buffer chain acts as a proof or record of the transaction.

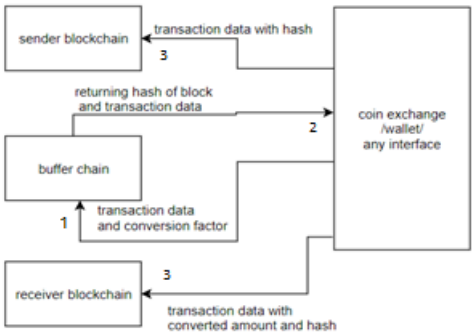

Fig 2- working example of a cross-chain payment/transaction

Consider two blockchains between which the inter-chain transaction must take place and let both add a new block at different intervals. Since the transaction is already recorded on the buffer blockchain and the transaction was pushed in the pending transactions list of the blockchains the transaction only needs to be pushed onto the newly created blocks. Once the transaction is pushed onto both the blockchains the transaction can be considered as completed.

4.3.2 Considering mining reward limits

There are blockchains which have an upper limit to how many coins can be circulated in the network [8]. Since in the proposed method one sends coins from chain to another chain using the receiving address of the wallet existing on another chain, the unintended result is invalidation of the assets of the sender and receiver blockchain. Hence, one needs to add the total amount of the assets transferred to another chain to the number of assets left to mine so that the invalidated assets can be mined again, and the limit also does not get affected. Similarly, for the receiver chain the count of the assets received should be subtracted from the total assets left to mine.

4.3.3 Ensuring valid transactions

The hashing process of any transaction can be like the one used in the current systems. When confirming the transaction, the interface can compare the transaction hashes of all the three chains to make sure the transaction is valid. The receiving chain will have a different amount than the sending change since the transaction was converted into terms of the receiving blockchain. Hence it is necessary to take the converted amounts and the original sent amounts into

consideration while creating the hash and signing the transaction.

Since the receiving and the sending addresses are same for all the chains unless the transaction is not tampered the signature will be valid for all the 3 chains.

4.3.4 Preventing fraud transactions

The main aim to include the transaction on a public buffer chain is so that there can be no fraud transactions. Since there is a time difference between pushing transactions on both the blockchains. One can create new transactions on different exchanges/wallets before the balance is updated once the transactions are added to the chains. Hence it is necessary that the coin exchanges/wallets also check the transactions listed for the wallet address on the buffer chain as shown in Fig-3. If there are any transactions which have not been added to the blockchains but are visible on the buffer chain the balance considered on the interface is updated accordingly. This prevents anyone to make invalid transactions by taking advantage of the fact that their previous transaction has not been completed. Since creating a transaction on the buffer-chain acts as a contract/ proof that the transaction is scheduled.

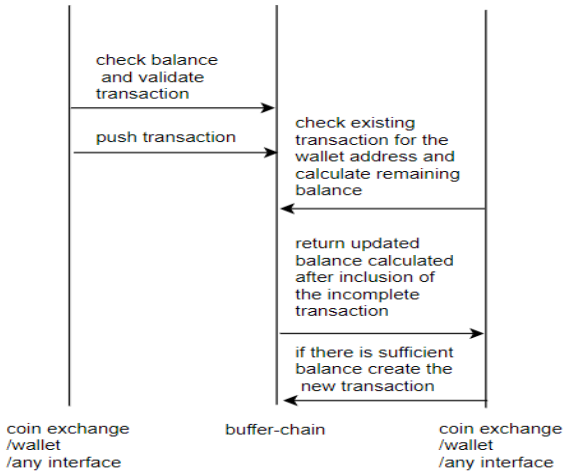

Fig 3- validation of the balance of any wallet address

4.4 Mining on the buffer-chain

In the proposed implementation there is no concept for any reward for mining the blocks on the buffer-chain, but an incentive is required to get miner to mine the block on the buffer-chain which will act as a proof of work mechanism. The mining function on the buffer-chain can be like other blockchains, but it becomes difficult to maintain the cross-chain transactions and the intra-chain transactions on the buffer-chain. Hence instead of creating a distinct crypto-currency for the buffer-chain one can simply dish out unit monetary value to the miners (for example-Dollars)

If the reward is decided the miner must select the blockchain on which the miner has its wallet and then the unit value is converted into the crypto equivalent of the chain using the conversion factor. This ensures that the mining reward for mining on the buffer-chains does not change in monetary value irrespective of the chain the reward is transferred to.

4.5 Scaling to real life applications

The proposed method works for a small number of transactions with two blockchains, to scale it up to the current standards of the blockchains it is necessary to manage the time required to add new blocks and the difficulty of the buffer chain accordingly. Since the buffer chain is a public blockchain in its roots there will be inevitable delays in adding transactions to the blocks.

Considering a new block is added every 1-unit time in the buffer-chain, the users will still have to wait for 1-unit amount of time before they get confirmation of their transaction being recorded in the buffer chain and can act as a proof of transaction.

Though this still reduces the waiting time for the users as the transaction has been at least recorded on the buffer chain and will be added to the blockchains participating in the transactions. This buffer chain can be designed to communicate with a limited number of trusted nodes which will ensure lower latency.

5. Scope

The standard parameters proposed in this paper allow any new blockchains designed by including the proposed standard parameters to communicate with the buffer-chain and execute cross-chain transactions. Coin exchange/wallets or interfaces are required to communicate between the buffer-chain and the other blockchains since buffer-chains need input for the conversion factor from the coin exchanges/wallets. There can be many public buffer-chains supported by coin-exchanges/wallets. The coin-exchanges/wallets can select the public-buffer-chain with the least latency for confirming transactions to facilitate fast confirmations from the buffer-chains.

The coin-exchanges/wallets can support cross-chain transaction only for the blockchains which are designed keeping the standards in mind. This implies that the buffer-chain can facilitate any transactions between different chains which are supported by the coin-exchanges/wallets for cross-chain transactions.

The coin-exchanges/wallets can also establish their own private buffer-chains to facilitate the transfer of data over different chains.

6. Conclusion

This paper attempts to establish some standards which will enable blockchains based of on the proposed designs to communicate and operate with each other. The necessary mediums such as coin-exchanges/wallets, and buffer-chains are required to complete the model. The paper also discusses the mining options for the buffer-chains. The coin-exchanges/wallets can provide freedom of choice to the payer and the receiver to pay and receive in the currency of their choice regardless of the chain the transaction occurred in. It also removes the dependency of the buyers and sellers and makes the system more secure.

References

[1] Stefan Thomas & Evan Schwartz. A Protocol for Interledger Payments. https://interledger.org/interledger.pdf. Pg-1 . 2019.
[2] #Meta hash. "What is Blockchain interoperability and why is it important?". https://medium.com/metahash/what-is-blockchain-interoperability-and-why-is-it-important-32e4db3bce84. Aug 2018.
[3] Joseph Poon ,Thaddeus Dryja. The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. https://www.weusecoins.com/assets/pdf/library/Lightning%20Network%20Whitepaper.pdf. Pg-1. Nov 2015.
[4] Kyle Croman, ETAL. On Scaling Decentralized Blockchains. http://fc16.ifca.ai/bitcoin/papers/CDE+16.pdf. Pg-1. 2016.
[5] Vijay K. Madisetti , Arshdeep Bahga. Patent no-US20180300382A1. https://patents.google.com/patent/US20180300382A1/en. Fig-14,15. 2018.
[6] Thomas Hardjono, Alexander Lipton, Alex "Sandy" Pentland. Towards a Design Philosophy for Interoperable Blockchain Systems. https://arxiv.org/pdf/1805.05934.pdf. Pg-15,16. May 2016
[7] Techracers. 4 Key Features of Blockchain. https://medium.com/techracers/4-key-features-of-blockchain-5a4aff025d38. Apr 2018.
[8] Controlled supply. https://en.bitcoin.it/wiki/Controlled_supply.2019.
[9] Cryptocurrency exchange. https://en.wikipedia.org/wiki/Cryptocurrency_exchange.2019.
[10] Cryptocurrency wallet. https://en.wikipedia.org/wiki/Cryptocurrency_wallet. 2019.