THE INTERBLOCKCHAIN ARCHITECTURE

Introduction

Actual blockchains are not interoperable. Different approaches are proposed with the intention to resolve the issue, partially or fully.

- **Sidechains**: A communication channel is established between a main network and an external one. Liquid—developed by Blockstream—and RSK are good examples of this type of technology.
- **Federated networks**: This type of architecture allows to transfer value across the boundaries of blockchains sharing the same technology, or, in some cases, allows the execution of code on any member of the federation. All the federation members share the same technology.
- **Inter-blockchain networks**: This solution enables the transfer of value across blockchains based on different technologies and different network structures. For example, the transfer of value from a blockchain network to a directed acyclic graph network (DAG).

The first approach (sidechains) is restricted to a binary relation between two networks having a different technology. The second approach (federated networks) does not permit inter-blockchain communication with other networks based on different technologies but allow communication between members of the federation. The third approach (the Interblockchain networks) is the only one that is a real solution for transferring value across heterogeneous blockchain networks, based on different technologies.

A full inter-blockchain solution would transfer value and code execution across network boundaries. However, the diversity of virtual machines used to execute code on the different platforms forces applications to be restricted to a subset, the trans-ledger communication. The trans-ledger communication involves the transfer of value across different implementations of ledgers.

Two trans-ledger complementary approaches hold the solution to transferring value across ledgers that are implemented with different ledger technologies. For example, these include relational databases, blockchain networks, or a directed acyclic networks (DAG). These last technologies (blockchains and DAG) are transparent by providing a public archive of all transactions performed in their networks. Some technologies, like centralized databases, are opaque to external scrutiny.

The first approach, which is based on the W3C interledger group, focuses on the internetwork connection. The second approach, led by Interblockchain.io, focuses on the accountability and security of transactions on public blockchain networks and directed acyclic graphs (DAG).

In this document, we present a unique trans-ledger architecture based on a peer-to-peer network that links different agents involved in the transfer of value across heterogeneous blockchain networks and directed acyclic graphs (DAG).

Current state of the art

Different market players are proposing different solutions to trans-ledger communication across blockchain networks. Some are ready to be used and some are still on paper without any working code.

Sidechain

As of this writing, RSK and Blockstream are proposing a sidechain connected to the Bitcoin network. In both cases a blockchain is connected through a bridge to the Bitcoin network. The RSK network offers a network the ability to execute smart contracts using Bitcoin as its main utility token. In other words, Bitcoins are used as network fees.

Liquid is produced by blockstream transferring Bitcoins into a replica to be transacted in a faster blockchain network, the liquid network. The latter does not support the execution of smart contracts and is solely used to host Bitcoins replicas on a faster network with lower fees. Liquid is bi-directional by permitting the transfer of value back and forth between the blockchain network and the liquid network.

Both RSK and Liquid are real working solutions and currently in the Beta testing stage.

Federated blockchains

In this solution, several blockchain networks sharing the very same technology are connected as a federation. As of this writing, none of the proposals is exists as more than a simple piece of paper or has gone through any real testing of their respective concepts. Among the proposals:

- Polkadot
- Cosmos
- EOS
- Wanchain

Wanchain claims to have a working solution but no public demo is available. The EOS network is most likely the network with greater market traction by attracting a lot of developers implementing solutions to its platform. Moreover, several fork networks based on the EOS technology appeared very soon after the introduction of the EOS main network. Several of these forks demonstrated the need to be connected into a common federation. This configuration leads to a greater opportunity to scale with specialized networks still connected to a common currency and main network, the EOS.

The inter-blockchains

Some of the federated network providers claim to offer connections or bridges to external blockchains but none of them actually offers concrete working code we can use on testnet or mainnet. The only one with a working code on the different testnets is the solution proposed by

Interblockchain.io. Currently, Interblockchain.io is connected to seven different blockchain networks, most of them having a different technology:

- Bitcoin
- Bitcoin Cash
- Litecoin
- Ethereum
- Ripple
- Stellar
- EOS

In fact, the Interblockchain.io technology can connect to networks other than just blockchain networks. It can also connect Directed Acyclic Graph (DAG) networks. Through a W3C interledger connection it can also connect to other ledgers that are either centralized or decentralized. Thus, the Interblockchain.io technology is based on a trans-ledger technology that is at the crossroad of several technologies and ways of interconnecting.

Today, more than 40 established financial organizations are already connected to the interledger network. The transledger-Interledger connection provides a connection to these financial institutions. For example, the Thailand's bank Krungsri offers a direct connection to the interledger network. The transledger technology can directly connect to banks like the one previously mentioned. Thus, the transledger mission is to connect different ledgers implemented with different decentralized technologies such as blockchains and directed Acyclic Graphs—or to connect with centralized financial institutions through the interledger protocol.

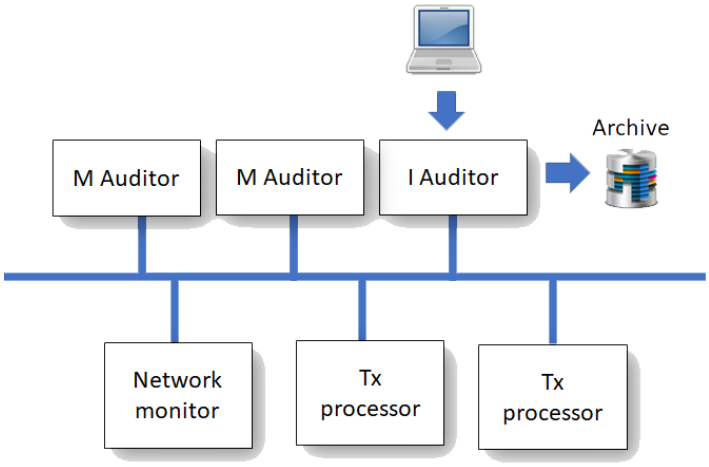
The Interblockchain network

The Interblockchain network is composed of these major elements:

- The Interblockchain network
- The Network monitors
- The auditors
- The transaction processors
- The blockchains

The auditors and the transaction processors are connected to the Interblockchain network. Both use the service of the Interblockchain augmented node interface. The latter provides a unique interface to the supported blockchain networks.

> **An Interblockchain network is NOT a blockchain**. It is an Interblockchain network based on different processes specific to the Interblockchain processes.



The Interblockchain network

The Interblockchain network is used to connect all Interblockchain agents through an encrypted messaging system. It is based on Kamdelia, a well-known peer-to-peer communication protocol. The encrypted messaging system is inspired by—but not identical—to the RLPx protocol from Ethereum. The network supports several channels. Three channels are actually implemented:

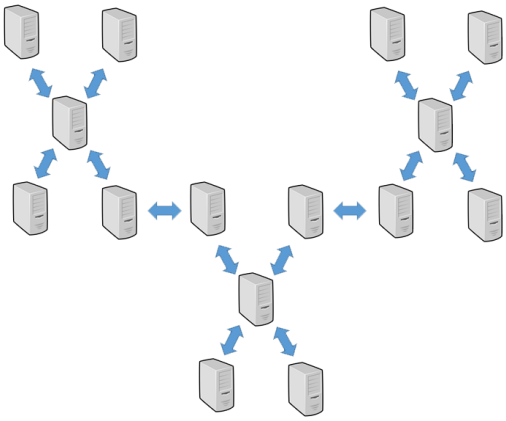
- A Production channel
- A Beta test channel
- An Alpha test channel

The Interblockchain network is composed of three layers:

1. The Distributed Peer Table layer. This layer is responsible for peer discovery and maintaining a table of Interblockchain peers.
2. The Messaging layer is responsible for validating and encrypting/decrypting messages.
3. The Application layer is for sending, receiving and processing messages.

Several network monitors are included in the network to check the overall health of the network. They provide statistics and other parameters about the network state in real time.

All connected nodes have a unique ID. Communication between nodes is based on UDP and can adapt to different ports in real time. Each node has a limited number of peers. Nodes exchange their list of peers to build the network. A set of filters is used to filter out unneeded connections. And a unique identifier identifies each channel.



As of this writing, the Interblockchain network is used to broadcast ***transfer requests*** to all attached agents. Transaction requests are signed and encrypted.

The Auditors

The auditors check the transaction balances in the source and the destination network, respectively. The auditors are performing an accounting audit. They verify that the amount transferred from the source network is identical to the amount received in the destination network. When a discrepancy between the two networks/ledgers is identified, a warning message is sent on the Interblockchain network to take appropriate actions.

Some auditors, called I-auditor nodes, fulfill several roles:

- Getting transaction requests from client applications through a REST API.
- Performing an accounting audit to check the accounts' balance in the source and destination networks.

The Interblockchain network presents several input nodes for a truly distributed system that starts from the entry points. This is in contrast to most actual blockchain systems in which their input node (for user interface) is highly centralized and limited to a single website—a single point of failure. These input nodes also audit every transaction—the ones submitted to them through received transfer requests and the ones received from other input nodes.

Other auditors named M-auditor nodes only perform an accounting balance audit. These nodes add redundancy to the network by increasing the number of auditors. The downloadable version of the client user interface includes an M-auditor. The more downloadable versions are running the more auditors are present to audit the transactions.

All auditors are used to audit any transaction broadcasted on the network. They broadcast a message when transactions are completed. The broadcasted message contains a reference to a transfer request and the result of the audit. Any agent connected to the Interblockchain network can receive these messages. Network monitor databases record each transfer request

and audit results. The messages sent by the auditors are collected for each transfer request as illustrated below.

TRANSFER REQUEST ID	POSITIVE AUDIT	NEGATIVE AUDIT
NSFT35-3HH367-277638-SHHT	26	0
37732-SHHDH3-27SIJJX2-WWT	26	0

M-auditor or I-auditors nodes can either connect to the *Interblockchain Augmented Node service*—a service that provides a single event-based interface—or use their own connections to the blockchains. However, the augmented node service offers the advantage of a single interface to several blockchains which tremendously reduces the software development time and costs. Several augmented nodes provide access to the blockchains. Currently, this online service supports the following blockchain networks:

- Bitcoin
- Bitcoin Cash
- Ethereum
- Litecoin
- Ripple
- Stellar
- EOS

M-auditors and I-auditors nodes can be standalone—which means they are not using the Interblockchain augmented node—or be considered as a full Interblockchain node, as long as they include the following elements.

- A full blockchain node for each of these networks
  - Bitcoin
  - Bitcoin Cash
  - Ethereum
  - Litecoin
  - Ripple
  - Stellar
  - EOS
  - *Note: several others will be added to the list in the future.*
- Access to the Interblockchain network and a capacity to react to messages broadcasted on this network.
- A valid HTTP certificate

A full Interblockchain node also conforms to trust constraints like having a digital certificate. The certificate must be linked to a person and cannot be anonymous. A KYC process must be

performed on that person. Also, the MAC address and IP are registered, the server's code cannot execute outside of the computer associated with these properties.

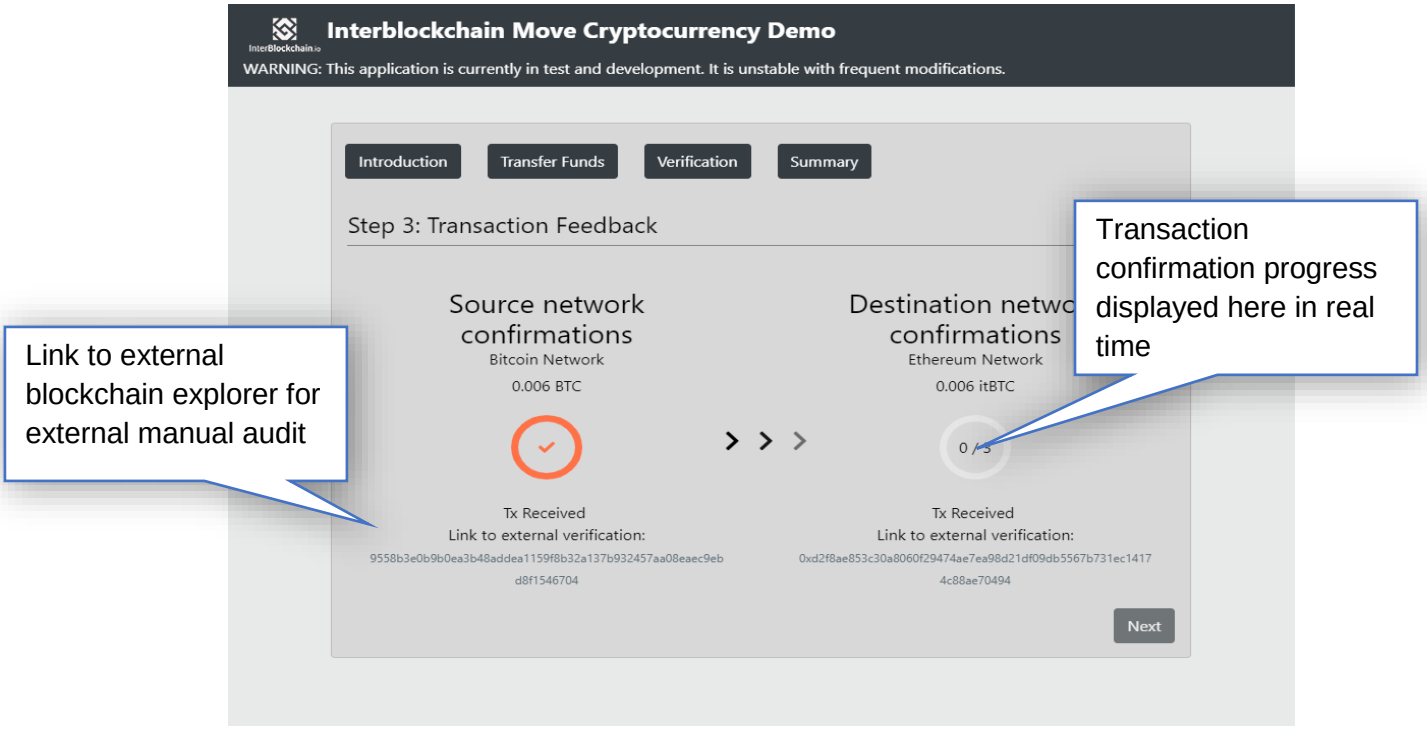
A light client version of an auditor is not required to go through this whole procedure and can execute code anonymously. This type of server will be connected to the *Interblockchain Augmented Node* (as a service client) and the Interblockchain network.

I-auditors nodes record all transfer request records into a replicated database implemented over the Tendermint blockchain. All transactions—validated or not—are stored in the archived blockchain. All transfer requests are stored as transactions in an Interblockchain blockchain network; any balance kept in each blockchain network reserve is registered into the distributed ledger. This feature increases the transparency of the network by helping any third party to audit the accounting of all transactions performed on the Interblockchain network.

Transactions from clients—either through the Interblockchain client (as an embeddable library or standalone) or through a REST API—are received by one of the network I-auditor node (input node). The latter verifies the conformance of the received transaction. It then sends the transaction to the Interblockchain network as an encrypted message and waits for the audit of a transaction from an accounting point of view. The amount transferred from the source network should be identical to the amount transferred to the destination network. The I-auditor node transfers request records in the Interblockchain archive network. The archive network is used solely to act as a distributed history audit trail in a distributed ledger. Anyone can install an Interblockchain history node to verify the processed transactions. It is also feasible for anyone to verify a transaction balances in the different blockchain explorer offered by third parties.

The Interblockchain network is fully transparent and offers several means to audit transactions.

The client user interface, which is provided by Interblockchain, includes a graphical interface displaying an accounting audit trail. Also, it displays a real-time feedback of the respective confirmation delays in both the source and destination networks/ledgers (as illustrated below). This feedback screen also includes a reference to networks explorers publishing the state of transactions on both the source and destination blockchains. This last feature provides an additional manual auditing feature.



Transaction processing

For network users, the whole process starts with filling a *Transfer Request* form. For a distributed application like, for example, a distributed exchange, an HTTP POST transaction is sent to one of the Interblockchain input nodes. The latter transfers the requests to all of the Interblockchain network nodes. Some of these nodes are transaction processing nodes. Their role is to perform transactions on a destination network. The transaction in a destination network transfers funds into the users' wallet. A client user interface should provide a means, such as a QR code, to send a transaction to the source network reserve.

> Hence, transaction processors perform transactions solely on the destination networks.

Several transaction processors are involved in a transfer transaction process. A scheme of five processors will sign a transaction, and only one can perform the transfer of funds on the destination blockchain network. The transaction is executed only when the five (5) signatures are completed. Transaction processors are connected in different ways:

Model 1:

- A listener gets transactions from the Interblockchain network and writes them in a file stored on a NAS server. A transaction processor—located behind a NAT with no

incoming opened ports—reads the file from a NAS and performs blockchain transfers on the destination network. This type of processor is the last step of a transfer process.

Model 2:

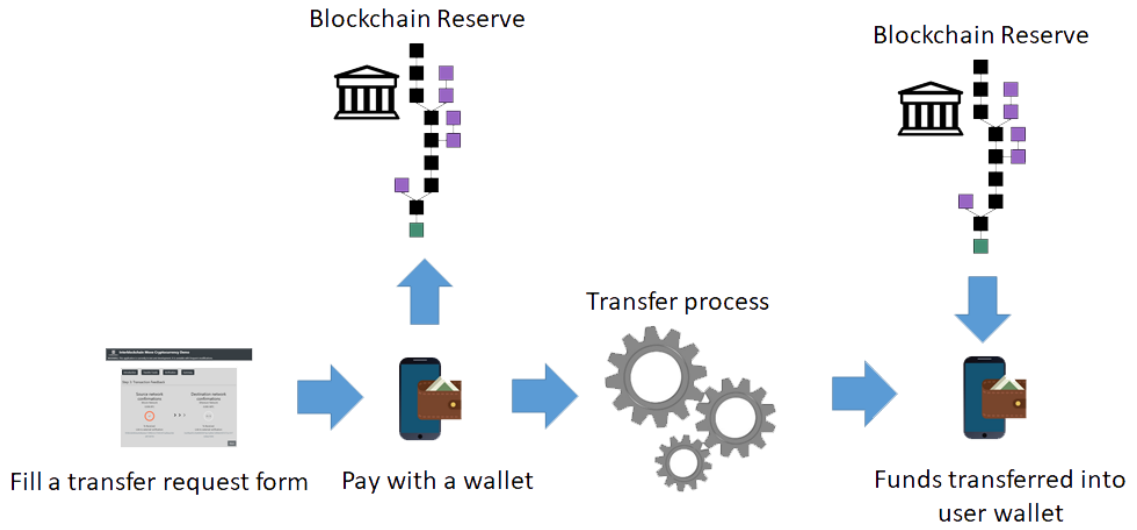
- A transaction processor is directly attached to the Interblockchain network and can only sign a transaction. When 5 signatures are completed, one of these nodes perform the transfer operation.

For more security, several nodes write into several NAS (model 1). A transaction processor reads several files, compares them, and performs the operation if all the data is identical. Otherwise it will suspend the operation. This is the type of structure we are currently implementing in the version 2 of the transaction processor.

Interblockchain transfer of funds

Since the actual Interblockchain network's first implementation is dedicated to financial transfers across blockchains, it is currently limited to the transfer of funds from one blockchain to another. Presently, the first implementation is used to move cryptocurrencies and cryptoassets across blockchain networks and later we will add the an exchange between pairs of different cryptoassets and cryptocurrencies across blockchains.

The transfer of funds process involves only a transfer between a reserve and user accounts on the source and destination networks. This enables the bidirectional movement of funds as a whole or as a fraction.



The transfer of funds process is similar to a bank's transfer of funds. Fiat money, like the USD, is independent of any technological substrate. A bank may store its ledger in an Oracle database while another bank may store it in a blockchain, and the USD transfer across these banks remains a USD. In the bank's ledger-to-ledger transfer of funds, there is no exchange rate because it is still the same currency. In a sense, fiat money, like the USD, is virtual and independent of any technology.

Until the appearance of the Interblockchain network technology, cryptocurrencies and cryptoassets were dependent on a single technology. The technology used to host the ledger (like Bitcoin) or the ledgers (like Ethereum) is the only host for all cryptoassets or cryptocurrencies hosted in these ledgers. The interblockchain.io network transforms any cryptoasset or cryptocurrencies into virtual entities, which is one essential characteristics of fiat money.

The transfer process starts with a transfer of funds from a user account to a source network reserve. This first step removes the funds from circulation in the source blockchain network but doesn't destroy them. The reserves are needed for any redemption of funds across blockchain networks. Reserves allow for the redemption of funds as a whole or as a fraction. A counterparty is always available since each reserve acts like a central bank on each blockchain network. Reserves are used to create and remove circulating funds.

In contrast to an exchange, where two active parties are involved, a single user can transfer funds from one blockchain to another without the need for any counterparty. Some reasons for why a user may transfer funds to another blockchain network would be, for example:

- Using the transferred funds in a distributed exchange. The destination network hosting the distributed exchange would be faster and less expensive than the source network. The users would do most of their trades in the destination network and settle through the redemption of funds in the original network. The latter is occurring less frequently.
- Using the transferred funds for e-commerce. The source network, like for instance Bitcoin, Bitcoin Cash, or Litecoin may be too slow for e-commerce. Users are accustomed to fast transaction confirmation times like the ones they get through Visa, MasterCard. Thus users would transfer their funds to faster and less expensive blockchain networks like EOS.