UNLOCK COINS FROM THEIR SILOS

WORK IN PROGRESS - VERSION 1.3

SEPTEMBER 30, 2019

Table of Contents

Introduction 2
Problems to be solved 3
First problem: A lack of liquidity for the distributed exchanges 3
Second problem: fees and transaction confirmation time 4
Third problem: high development costs to implement *blockchain applications* 5
Solutions 5
First Solution: Bringing liquidity to distributed exchanges 5
Second solution: faster and cheaper cryptoAsset e-commerce 6
Third solution: a common interface over the blockchain networks 7
Some Context: Three Financial Building Blocks 7
Transactions 8
Exchanges 8
Migration 9
Current State 9
The Fiat Currencies Realm 11
The Cryptocurrencies Realm 11
The Transledger Solution 15
The Interblockchain mechanism 15
How is the end user doing it? 17
Difference Between a Blockchain and an Interblockchain 18
The Transledger Architecture 21
The Interblockchain network 21
The Auditors 23
Transaction processing 26
Interblockchain transfer of funds 26
Roadmap 28
Stage 1 28
Stage 2 28

Introduction

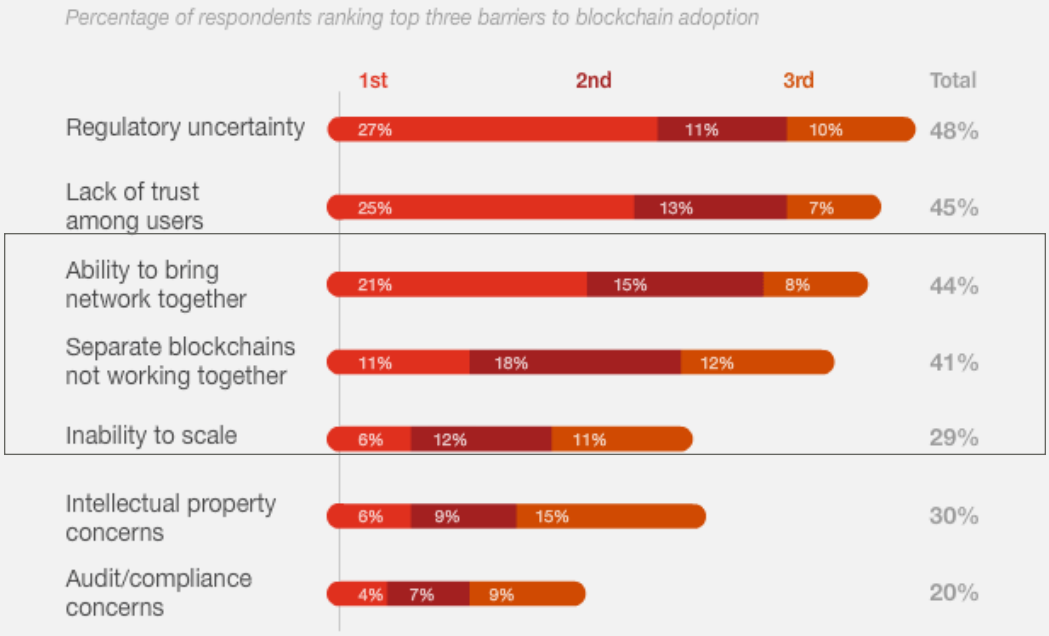
What Can we do With Transledger?

It all starts with the value stored in a major public blockchain. Let's say, one of these:

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

As of this writing, these blockchain networks are worth about 80% of total market capitalization for all tokens. Today, these cryptocurrencies are mainly used for storage of value and speculation.

According to Price Waterhouse (PwC), the ability to bring blockchain networks together and the fact that separate blockchains are not working together are major barriers to increase blockchain adoption. These factors are limiting the growth of the blockchain industry. More specifically, the dependence of cryptoAssets on a single blockchain network reduces competitiveness and limit technical progress and innovation.



Note: Base: 600.
Q: Which of the following will be the biggest barriers to blockchain adoption in your industry in the next three to five years?
Source: PwC Global Blockchain survey, 2018

National currencies are not dependent on any technology. A USD can be stored in a relational database in Bank A, and even in a blockchain network in bank B. In both cases, the USD remains the USD. Its value and location are independent of any particular technology. Unfortunately, this is not the case for cryptoAssets. CryptoAssets are totally dependent on a single technology.

The Transledger technology we propose frees cryptoAssets from any particular technology by allowing the free movement of them across the boundaries of blockchain networks. In other words, free them from any specific technology. This reintroduces competitiveness among the different technology proposition and reduces transaction costs, even make them free. It also allows high-value tokens, representing 80%, of the total capitalization to be freely moved to more efficient and less expensive public blockchain networks. And to retain their full value, the moved tokens can be redeemed back to their original network in total or in fraction.

Problems to be solved

The following section describes in more detail the problems solved and how the proposed solution works. But first, let's describe the problems Transledger resolves.

First problem: A lack of liquidity for the distributed exchanges

As of writing, wallet to wallet cryptoAsset trading is possible through three (3) kinds of services based on smart contracts on the Ethereum platform:

- Bancor
- Airswap
- About 20 exchanges based on the 0x protocol.

All share the same problem, they are restricted to offer asset pair trading only on, and solely on, the assets hosted on the Ethereum network. In other words, they can't exchange high-value assets such as Bitcoin, Bitcoin Cash, etc. These assets are hosted on different blockchain networks. They represent 80% of the total asset capitalization. Most of the tradable assets hosted on the Ethereum network are comparable to penny stocks. Imagine, for a moment, what if they could offer to their customers the capacity to trade high valued assets and no longer be restricted to penny assets? They suddenly would be able to compete with major players like Binance and other similar exchanges.

Centralized exchanges have some definitive advantages when compared to distributed exchanges such as those already present on the Ethereum blockchain network. For instance, not only they offer trading high-value cryptoAssets but also the important feature to exchange these assets with national currencies. Both benefits omitted in distributed exchanges. The absence of these features puts a serious limit on the profitability and growth of these distributed exchanges.

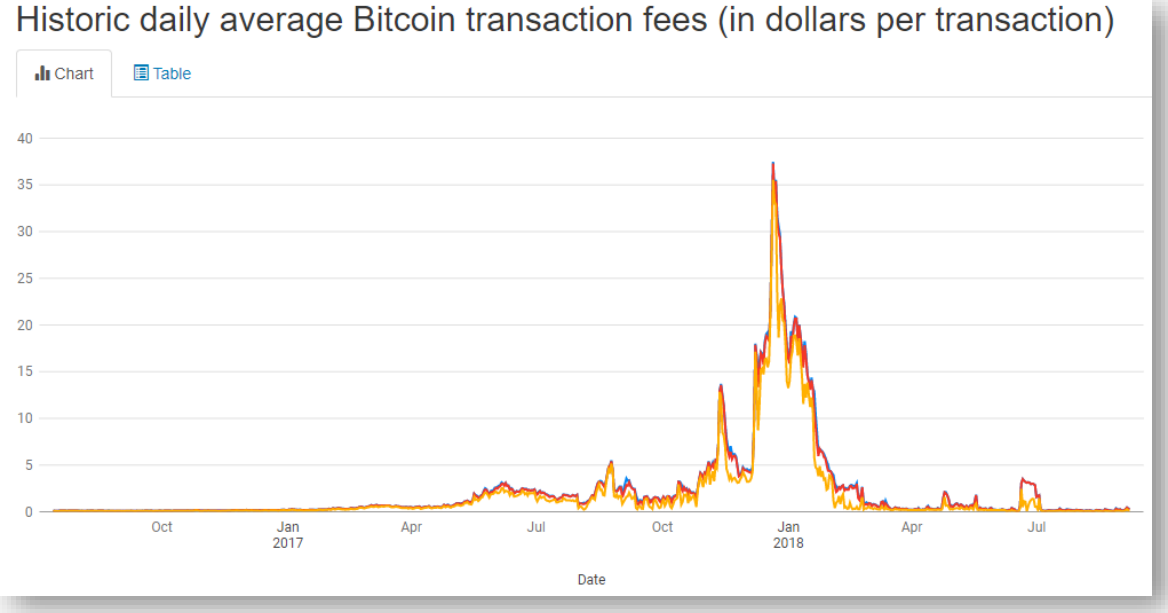
Moreover, the EOS network, may face the same challenges as Ethereum is facing today. EOS is a new challenger to the incumbent, the Ethereum network. It attracts new

investments and applications development with the promise of fast transaction confirmation time and no transaction fees for end users. This places EOS as a strong challenger to the Ethereum network. The same limitations encountered on the Ethereum network will also be present in any distributed exchange developed on the EOS network, more specifically when their implementation depends on the code executed on EOS.

In summary, all distributed exchanges, relying on smart contracts for wallet to wallet trading, are restricted to trade solely cryptoAssets hosted on the network where the code is executed. This prevents these applications to access most the capital already stored in other blockchain networks.

Second problem: fees and transaction confirmation time

Fees on UTXO blockchain networks such as Bitcoin are very variable, and sometimes, can be quite expensive



As the automatic reward for block production will decrease, these costs will increase. Moreover, most of the application wait for a certain amount of transaction confirmation to consider a transaction as officially confirmed. The delay for this final confirmation may reach up to 1 hour, a delay barely able to compete against the 3 or 4 seconds required for a Visa or Mastercard transaction confirmation.

Even if the networks such as Bitcoin and the others dependent on the proof of work can display good transparency and traceable history of the transactions, these transactions can be costly and slow to be confirmed.

Third problem: high development costs to implement *blockchain applications*

If you eliminate the cloned blockchain network from one of the major ones, there is a great diversity of application programming interface. For blockchain networks supporting smart contracts, the diversity of programming language has nothing to envy to the tower of Babel. As an example:

- Neo: the main smart contract language is C#
- EOS: the main smart contract language is C++
- Ethereum: the main smart contract language is Solidity
- Cardano: the main smart contract language is Plutus
- Lisks: the main smart contract language is Javascript.

Hence, developers wanting to port their application on several blockchain networks need to adapt to the plethora of interfaces and languages. This increases the development costs and adds delay to the delivery of the applications.

Solutions

The following section describes how Transledger develop software packages as an answer to these problems

First Solution: Bringing liquidity to distributed exchanges

DEX dependent on platform specific smart contracts like Bancor, Airswap or all the 0x protocol-based exchanges are limited to the tokens hosted on the platform hosting the smart contract. In other words, these DEX on Ethereum can only trade tokens on Ethereum. They can't offer high valued cryptoAssets like Bitcoin, bitcoin Cash, Ripple, etc. Among the top 10 cryptoAssets representing 80%, only Ether can be traded.

Now let's imagine a potential real-life scenario. Fred wants to exchange his bitcoins for some ERC20 coins and if possible, for some Litecoins. In 2017 and 2018, he lost quite a lot of money using centralized exchanges. They said the exchange was hacked and that he has no recourse. His money simply disappeared in an instant and no way to get it back. He heard about non-custodial exchanges and the fact that he could be back in charge of protecting his assets. This sounds easy to Fred. Fred has only to move his bitcoins to trading platform (i.e. a blockchain) by creating a proxy Bitcoin local to the blockchain used as a trading platform. If the trading platform is Ethereum, Fred heard that Radar, one of the distributed exchanges based on the 0x protocol could be used to

In a nutshell, Interblockchain allows Fred to move his Bitcoins a blockchain network allowing trades on distributed exchanges directly from his wallet. Moreover, Fred can now trade, from his wallet high value cryptoAssets representing 80% of the total capitalization.

trade directly from his wallet. At least, with real distributed exchanges, Fred can protect his private key. On radar or any of the other distributed exchange (DEX), Fred can trade his bitcoins for some ERC20 tokens or with a more valued token like Litecoin or Ripple. from this trading platform, the other party can redeem the proxy Bitcoins hosted on the Ethereum network back as Bitcoins hosted in the Bitcoin network. And so, it is for any high-value cryptoAsset representing 80% of the total market capitalization.

More recently, Transledger developed a peer to peer exchange on the EOSio technology. On any EOSio based platform, there is no costs and it is a lot faster than Ethereum. Ethereum can handle a maximum of approximatively 15 transactions per second, EOS can handle approximatively 4000 transactions per second. On Ethereum, any transaction has fees users should pay, on EOS, the service provider put at stake a certain value and the users do not pay transaction fees. So, Fred, in that case, would transfer the Bitcoins to one of the EOSio platform (EOS, Telos, Worbli), trade these bitcoins with a third party. Then, the other party can redeem back these proxy bitcoins as Bitcoins in their original network.

Second solution: faster and cheaper cryptoAsset e-commerce

What if any of the high-value cryptoAssets would be made available for transactions, to buy things? Not only Bitcoin or Bitcoin cash or Litecoin but also Ripple, Stellar even Ether.

So, let’s imagine Fred has a portfolio of Bitcoin, Bitcoin cash, and Ethereum. How can Fred use these funds for transactions?

Here is how Transledger proposes to help Fred and merchants exchange stored value for goods and services with these coins.

1. Fred uses Transledger to move some Bitcoins to a less expensive and faster blockchain, let’s say EOS.
2. On an EOSio platform, Transledger creates proxy bitcoins having the same value as bitcoins. Fred can now spend these funds and merchants can accept them with a less than five seconds (ideally, three seconds) transaction confirmation time.
3. The proxy bitcoins are spent on a myriad of commercial exchanges.
4. Let’s now introduce Bob, the merchant. Bob’s e-commerce site accepts several proxy coins including proxy bitcoins.
5. Bob’s e-commerce has accumulated a certain amount of proxy bitcoins, and now, Bob wants to redeem them back into bitcoins. After all, Bob received proxy bitcoins, didn’t he? So, Bob uses Transledger to redeem the proxy bitcoins back into bitcoins.

6. Now, Bob has bitcoins, an excellent store of value, easily traded into fiat money or with any other cryptocurrencies.

The whole story about Fred and Bob is centered on the fact that the coins previously locked as store of value or as speculative funds can now be used for transactions, and the fact that coins are redeemable back to their original blockchain. This keeps the value of bitcoins movements between blockchains intact.

Coins can be moved back and forth from one blockchain to another. It is the equivalent of a high-yield account (Bitcoin) to store value and an operation account (proxy Bitcoin) for daily transactions. Amounts can be freely moved back and forth between these two accounts like we already are accustomed to do with fiat money. But this time, with fewer intermediaries and under Fred and Bob's control.

Third solution: a common interface over the blockchain networks

The Transledger solution providing a single interface over blockchain networks consist of:

- A single event monitoring interface for confirmation events.
- A single interface to perform transactions
- A single transaction database allowing sophisticated queries

As of writing, the event monitoring interface is already developed and operational.

Some Context: Three Financial Building Blocks

If we pay attention to the basic building blocks of any financial system, we have:

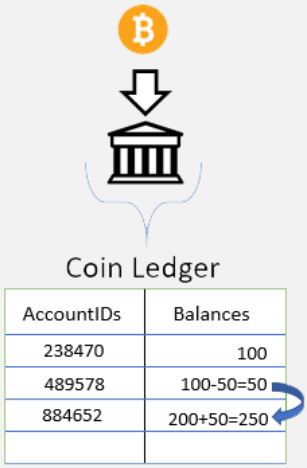
1. The capacity to **transfer** and receive value (funds) in the same reference system. In other words, to be able to pay or to be paid in the same currency, like the euro or dollar.
2. The capacity to **exchange** value between different reference systems. For example, to exchange dollars for euros or bitcoins for ethers. There is a certain arbitrage between the exchanged currencies because they have a difference in value expressed as a ratio. For example, the euro is valued more than the U.S. dollar with a ratio of 1.16 (1 euro = 1.16 USD).
3. The capacity to **move** a currency from one ledger to another. For instance, to move money from one bank to another or to move bitcoin from one blockchain to another.

Of course, we also have the whole universe of derivatives, but we can say that, at least, a monetary system stands on these three pillars:

1. Transaction
2. Exchange
3. Migration

Transactions

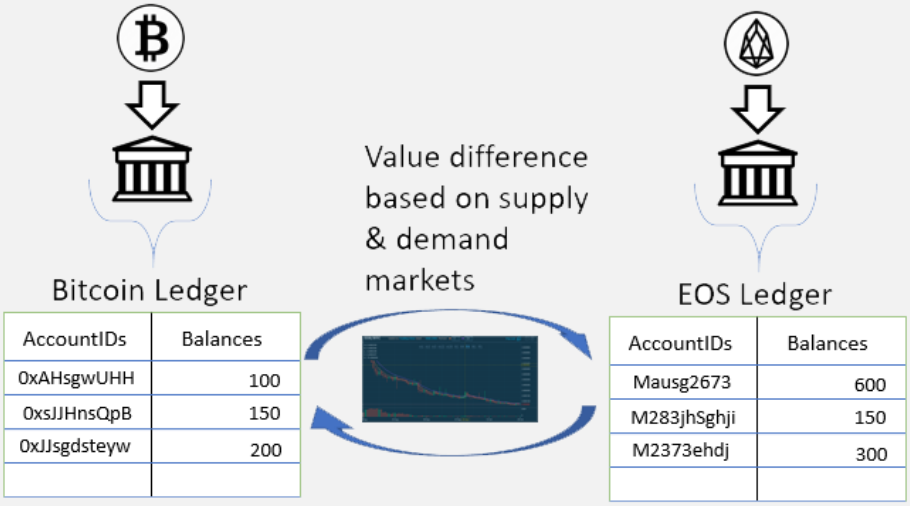
In the blockchain realm, we already can perform transactions within the same currency domain. In other words, within the same ledger. For example, we transfer bitcoins from one address to another. Or, in the realm of blockchains, like, for example, EOS or Ethereum, cryptocurrencies can be transferred only within the same blockchain ledger. Tokens can only be transferred from one account to another account. Multi-ledger blockchains can transfer custom tokens in addition to their system token. On multi-ledger platforms or account-based systems, a transaction is simply a writing in a ledger in both the source and destination accounts.



Exchanges

There is also the capacity to exchange tokens from one ledger to another ledger within the same blockchain network or across blockchains networks. This role is fulfilled by exchanges. Most of the time, these exchanges require funds to be moved to an exchange's custodial account. They let the market decide on the exchange ratio

between cryptocurrencies. The ratio will fluctuate along with the dynamics of supply and demand.



Migration

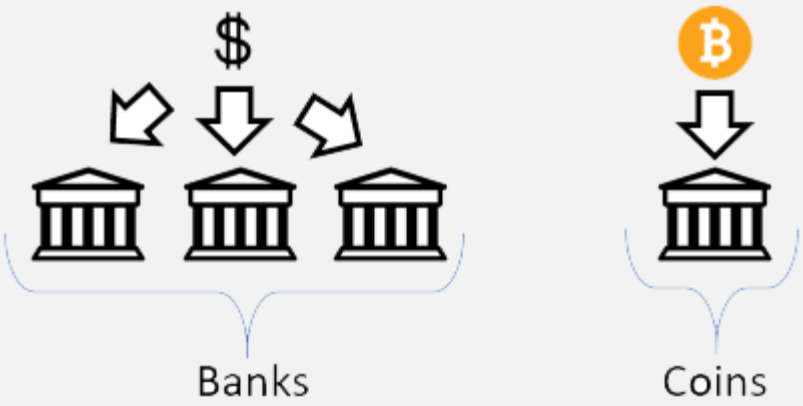
Actually, cryptocurrencies are tightly attached to a particular blockchain network technology. They cannot be moved easily to another ledger and keep their value. For example, the bitcoins reside solely in the Bitcoin blockchain network, the ether solely into the Ethereum blockchain network, and so on and so forth. In contrast to fiat money, which is increasingly more abstract, and can take several different forms, cryptocurrencies are restricted to a single technology where they are hosted. Fiat money can take the form of a metal coin, piece of paper, plastic card, or simply digits on a bank ledger and still represent the same value. On the one hand, in the case of fiat money, the same currency can easily move from one ledger (a bank ledger) to another one (a bank ledger). That can take place even if these two ledgers are implemented in different technologies. For example, one ledger could be implemented on a centralized database, and the other ledger could be on a blockchain network shared by all bank branches. On the other hand, cryptocurrencies cannot move from one ledger to another and keep their value and characteristics. They are simply attached to a single technology.

Current State

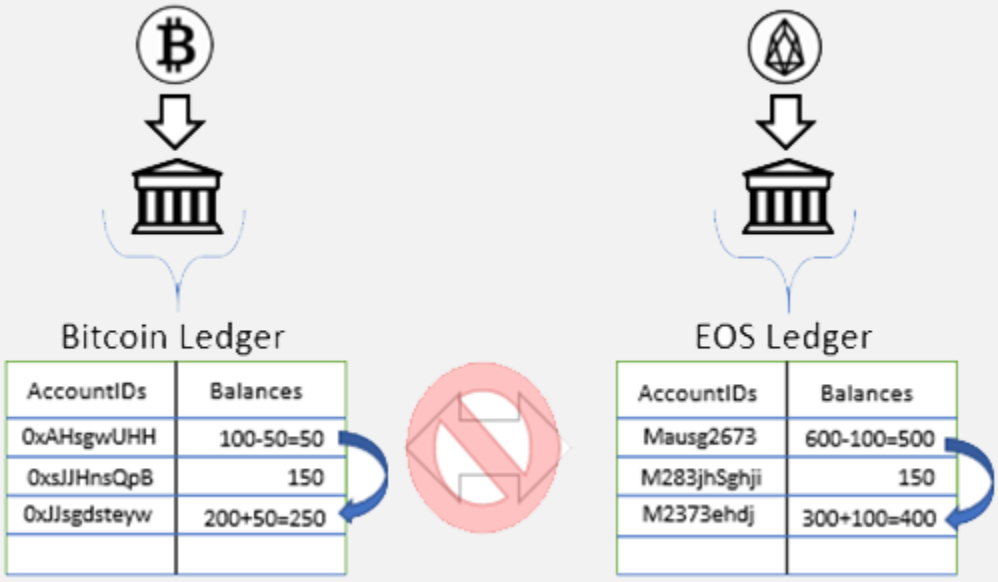
The ERC20 is an Ethereum standard that most new tokens created on this blockchain support. This common interface tremendously simplifies any application implementing a transfer of value, within the same ledger, from one account to another.

The exchange of cryptocurrencies occurs with their value constrained by the dynamics of a market or from constraints imposed by an algorithm.

Fiat currencies can easily move from one ledger to another or from one bank to another. Each bank can implement a different ledger technology.



Cryptocurrencies are limited by their ledger residing within one single blockchain network. Even, if this ledger is replicated in more than one location (more than one node), it remains that crypto-assets are limited to the single technology hosting them.



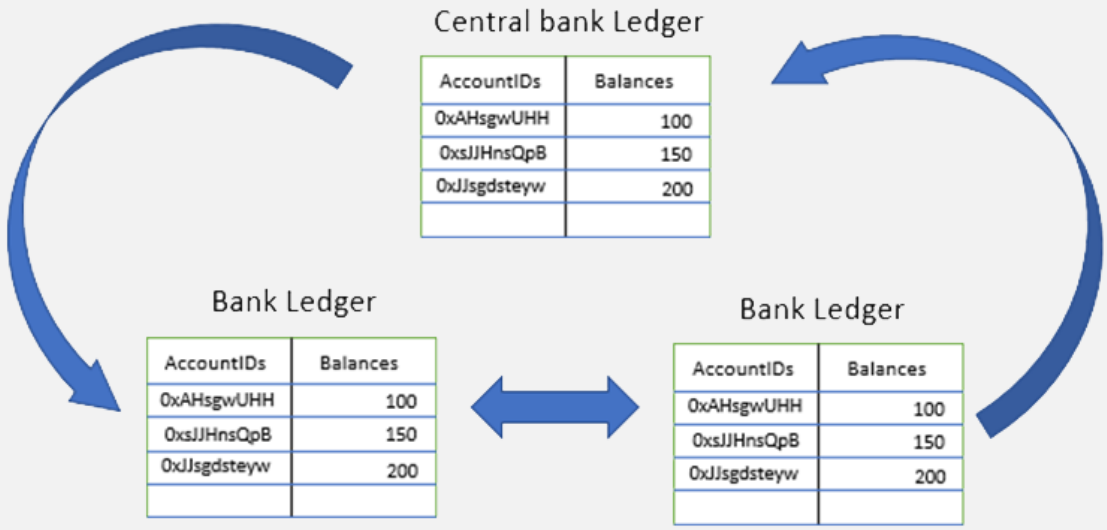
Improving the technology of these ledgers has proven to be a slow and arduous process. Even then, the progress is very limited compared to what improvements are technically possible. Moreover, there is no common way to freely move cryptocurrencies to different ledgers. It would be tremendously practical for e-commerce, for instance, to be able to move some cryptocurrencies like Bitcoin to a less expensive and faster blockchain for commercial transactions.

The Fiat Currencies Realm

In the actual fiat-based financial world, banks are used for transactions and loans. At its core, a bank is a ledger comprising a collection of records containing user account IDs and balances. Most of the time, they only manage local fiat currencies, sometimes they hold multi-currency accounts. Since fiat currency is the official currency of a country, this currency can be used by all competing banks within the geographical boundary of that country. In contrast, cryptocurrencies, even the ones contained in a single technology, for example, the Ethereum blockchain, have a different symbol and are currently traded like traded foreign fiat currencies through open market rules.

> There is a big difference between banks' ledgers and cryptocurrencies' ledgers. Fiat currencies can be stored in more than one type of ledger (bank), they can be transferred from one ledger (bank) to another and they can be exchanged with another fiat currency from another country.

In a nutshell, banks within the same country's monetary system use a Banker's Automated Clearing Service to transfer funds. This clearinghouse facilitates transfers between banks. If funds are missing for the transfer, the funds can be borrowed from a central bank, or from a loan offered by other banks. Funds transferred within the same bank are simple additions and subtractions applied to receiving and emitting accounts.

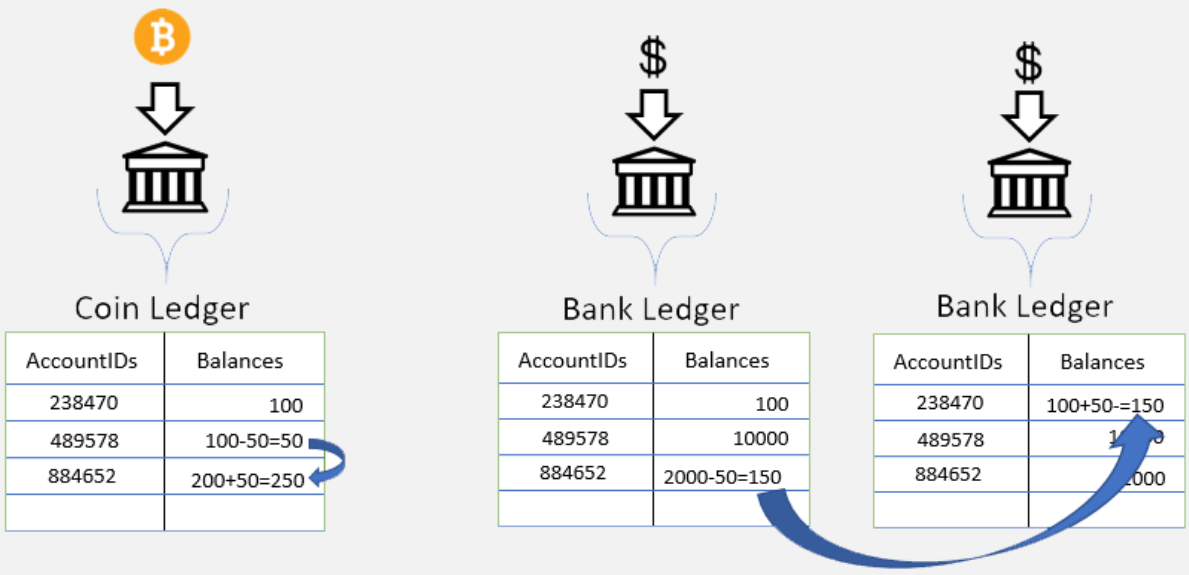


The Cryptocurrencies Realm

In the cryptocurrency world, a token (also nicknamed a coin), is by itself a bank. Associated with a token is a list of accounts identified by an ID (a key) and a balance. This is the case for most programmable blockchains like Ethereum, EOS or Neo.

Bitcoin-like blockchains are different. In several programmable blockchains, a single address is used to uniquely identify a user in different ledgers. This is the case for most ledgers based on the ERC20 interface. The same address can be used to identify an account owner in the plethora of ERC20 based ledgers that appeared in the landscape in the past months.

Blockchains like Bitcoin and programmable blockchains have a different approach. Blockchains like Bitcoin store bitcoins in addresses. A particular address can receive coins from more than one address in a transaction. In contrast, programmable blockchains like Ethereum are based on ledgers containing account-balance pairs. A value transfer is from account to account. Apart from ether, most of the newly created tokens on Ethereum are based on the ERC20 interface. Since most newly created coins conform to the ERC20 interface, a coin, uniquely identified by a symbol is attached to a ledger. Thus, a coin is a single ledger containing all accounts and their balances. Transfers can be performed within the same ledger.



In the current state of affairs, value transfer between different coins (between ledgers) is performed with a ratio adjusted to their respective value. This exchange between coins is happening on exchanges affected by the random walk of market sentiments.

Here is an analogy to understand the programmable blockchain ledger concept. Think of a coin as a kind of bank managing funds with a ledger composed of a collection of account-balance pairs, one for each customer.

Bank Ledger

AccountIDs	Balances
238470	100
489578	10000
884652	2000

Coin Ledger

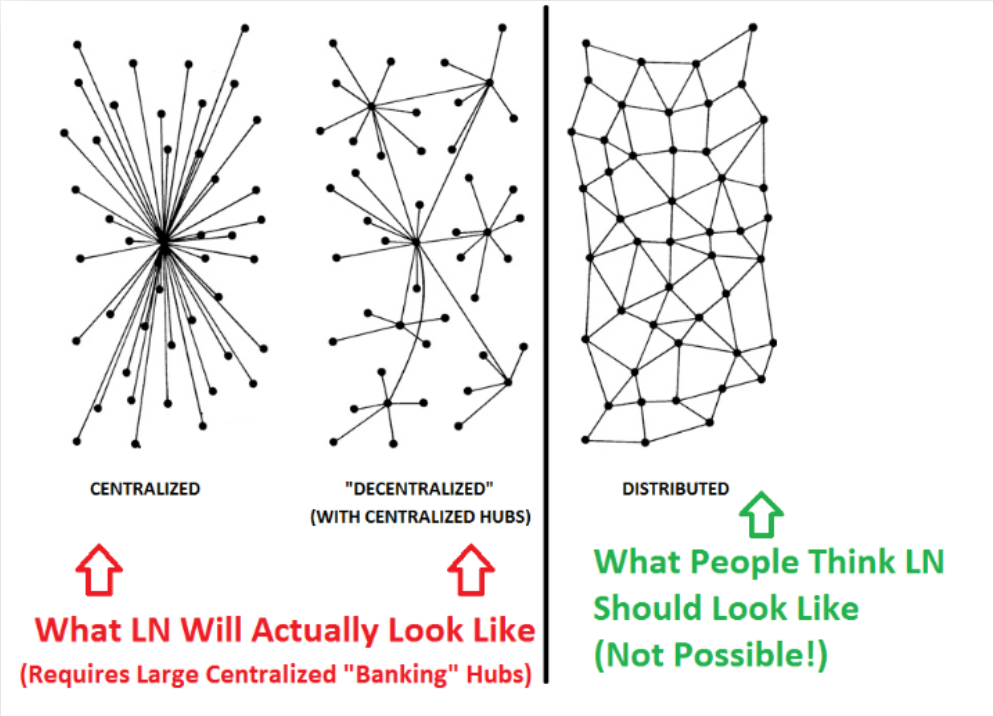
AccountIDs	Balances
0x29ShsmSkj	100
0x22HHweTe	10000
0x373hsdYSo	2000

Blockchains, either in a mono-currency system like Bitcoin or in multi-currency systems like Ethereum, do not allow other blockchains to host their coins, a particular coin is restricted to reside in a single blockchain network technology.

Blockchains like Bitcoin are getting slower and slower. As of writing, they had an average transaction rate of two transactions per seconds. This pales in comparison to Visa which can process an average of 1600 transactions per seconds. It is unlikely that Bitcoin speed will improve; social resistance and vested interests are in the way. Some solutions to improve processing speed like the one offered by the Lightning Network are not as versatile as they might at first seem.

> This solution (Lightning network) suppresses one major advantage of blockchains, a track record of transactions. The best solution would be to migrate back and forth these coins from one blockchain to another, from a slow blockchain to a fast blockchain. The fast blockchain keeps a log of the transactions in its blockchain. If the token can be moved on a blockchain with a processing as fast as Visa, then it becomes advantageous to use it for day-to-day payments. Moreover, as described by Jonald Fyookball in Medium, the social dynamics and technological constraints of the Lightning network will likely result in centralized off-chain systems[1].

[1] Mathematical proof that the lightning network cannot be a decentralized Bitcoin scaling solution



At this moment, a lot of action is happening in the blockchain world. New blockchains are under development with the promise of increased performance. Among them, EOS claiming a performance on par with Visa. So, on the one hand, we have Bitcoin and bitcoin-like blockchains trapped in a slow-motion world and, on the other hand, there is the emergence of a more agile system that provides fast action blockchains. The actual social and technological dynamics leads us to believe that Schumpeter's creative destruction is more efficient than a single-solution evolution. Sane competition drives innovation

So, to recap, in the blockchain world, transactions are permitted within a single crypto-asset realm (i.e. blockchain network). Inter crypto-asset transactions happen through exchanges' markets and are subject to an exchange ratio. This is because they are exchanged with a different crypto-asset (i.e. ledger). **Even if the ledger is replicated in several nodes, it remains that the whole is still acting like a single ledger**. Transactions occur only on the blockchain hosting the crypto-asset even if a better one would be faster and more scalable to host the coin. In the fiat currency realm, funds can freely move to another bank (i.e. ledger) and still be the same fiat money. Fiat money movement is independent of the underlying technology or ledger. In the cryptocurrency world, moving the coin to another blockchain also means it becomes another entity.

What if we could move bitcoins back and forth from the bitcoin network to, for instance, the EOS network?

The Transledger Solution

In a nutshell, the Transledger solution unlocks coins by allowing them to be moved back and forth from their original blockchains to other ones while always keeping their value independently of their location or the technological substrate.

Several constraints must be considered for the design of this type of infrastructure:

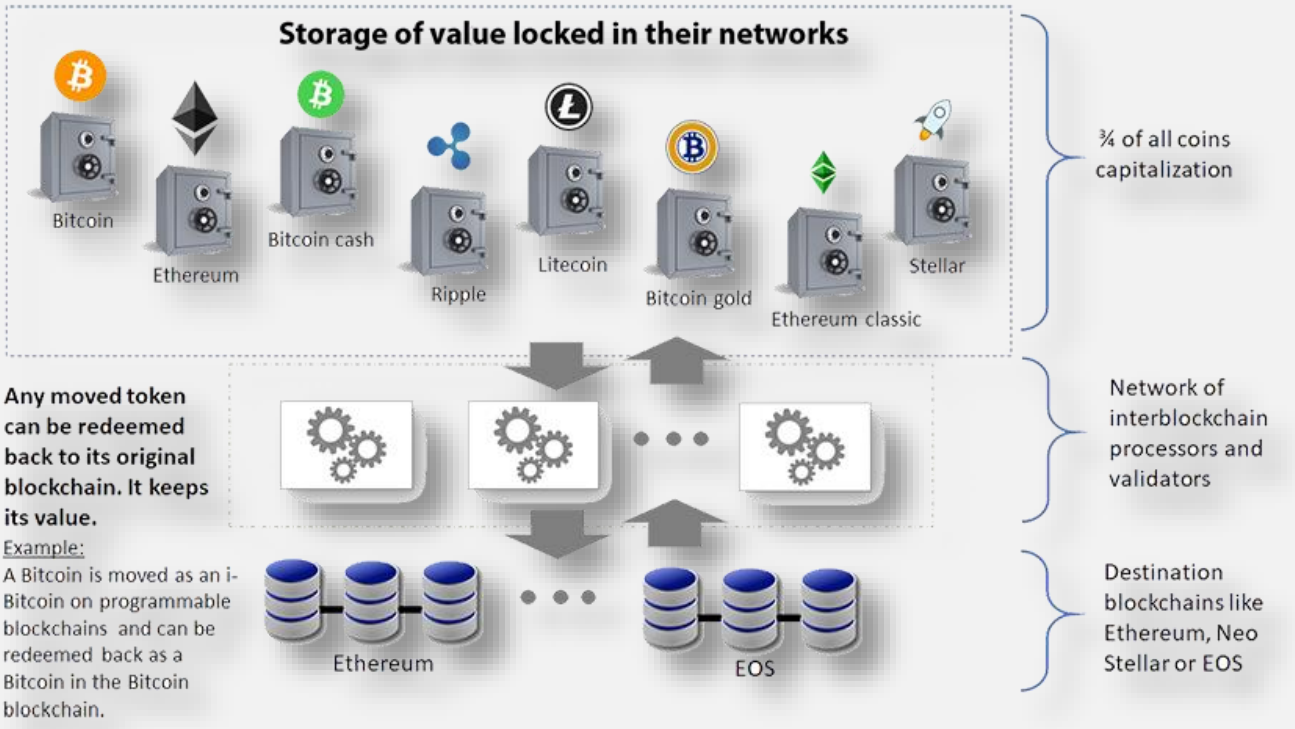
- **The code performing the transactions on both blockchains must be triggered only once**. This is a major difference with actual blockchain mechanisms in which the very same operation is performed on all nodes.
- **The node executing the code must be trusted and honest**. This is the same constraint like the one imposed on blockchains.
- **There should be several geographically distributed processors that can execute the code**. This is to prevent any dependency on a single location, legislation.
- **There should be a reward mechanism as an incentive to network node owners**. They should receive a reward for the work their node is performing.

The Interblockchain mechanism

Let's start with a scenario:

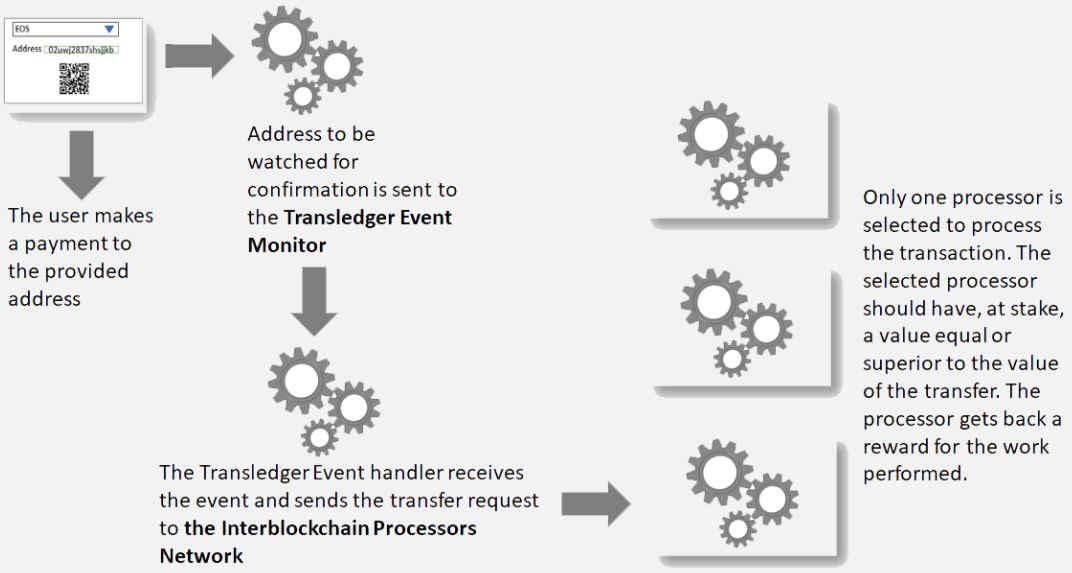
- We move a coin like a bitcoin to a more efficient and less expensive blockchain, like EOS.
- On EOS, we create a proxy version of the bitcoin. Let's say an i-bitcoin.
- The i-bitcoin can be traded or used to buy services and goods.
- Any iBitcoin owner should be able to be redeemed back to the Bitcoin network which allows this iBitcoin to retain its full Bitcoin value. Thus, while on the EOS network the i-bitcoin is to be considered as having the same value as it does on the Bitcoin network.

We actually support 9 networks, and we are currently working on the tenth. This concretely means that coins that originated from the following blockchains can be moved as proxies to other programmable blockchains such as Ethereum, Hedera or EOS and be redeemed back to their original blockchain while still keeping their full value.



A Transledger network is used to perform the required transactions on the origin blockchain and the destination one.

When moved to a multi-ledger blockchain, a bitcoin is converted into a proxy bitcoin named i-bitcoin. The latter keeps its full value because it can be redeemed back to its home blockchain. On a multi-ledger blockchain, it can be traded on a non-custodian exchange. For example, on the iBTC – iEOS pair: to exchange bitcoins to EOS with an ERC20 token on Ethereum or with a Transledger EOS contract. The recipient of the i-bitcoin can redeem it back to the Bitcoin blockchain with its full value.



How is the end user doing it?

With a web-based application, a person fills out a short form which includes an address to a destination account in a target blockchain. For our example, it is Ethereum. The application returns an address to which the amount can be sent. The person will then use his/her wallet to send some crypto-assets to a destination account. When funds are transferred (this is indicated by a confirmation from the blockchain), it triggers an event sent to an event handler. The latter sends a transfer operation to be performed by the interblochain network. In that case, the transfer is from the i-bitcoin reserve to an address in the previously filled-out form. That person has now an i-bitcoin that can be used to buy things with a reasonable confirmation delay better suited to e-commerce. Or that person can trade these crypto-assets through a non-custodian exchange.

It is important to note the main difference between the Interblockchain scheme and other popular ones advertised within the blockchain world.

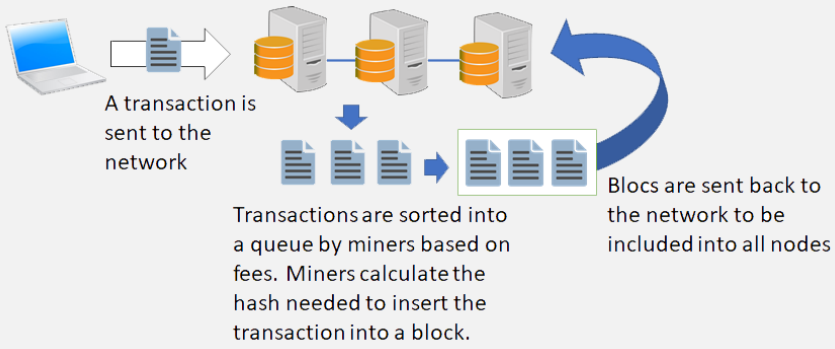
- i-bitcoins can be transferred from an original owner to third parties. Hence, the balance associated to the original owner account can be fragmented into several transactions. Each transaction is registered into the blockchain. Each transaction recipient of a transfer from the original owner or any other party owning i-bitcoins can redeem back the i-bitcoins as bitcoins. This is different from the channel concept. The i-bitcoin can even be moved to another blockchain and still be redeemable to its original home blockchain.
- Bitcoins are stored into a reserve fragmented by a hierarchical deterministic structure. Each address contains a limited amount equal to a transaction. Thus, the whole reserve is a fragmented poll of funds. This is limiting the risk exposure of the reserve. The reserve is used to redeem bitcoins to i-bitcoin owners

Difference Between a Blockchain and an Interblockchain

A blockchain is, basically a replicated database. Each node has a copy of the database.

> Hence, a blockchain is, in fact, under the current technology a **single database** replicated on each node of its network.

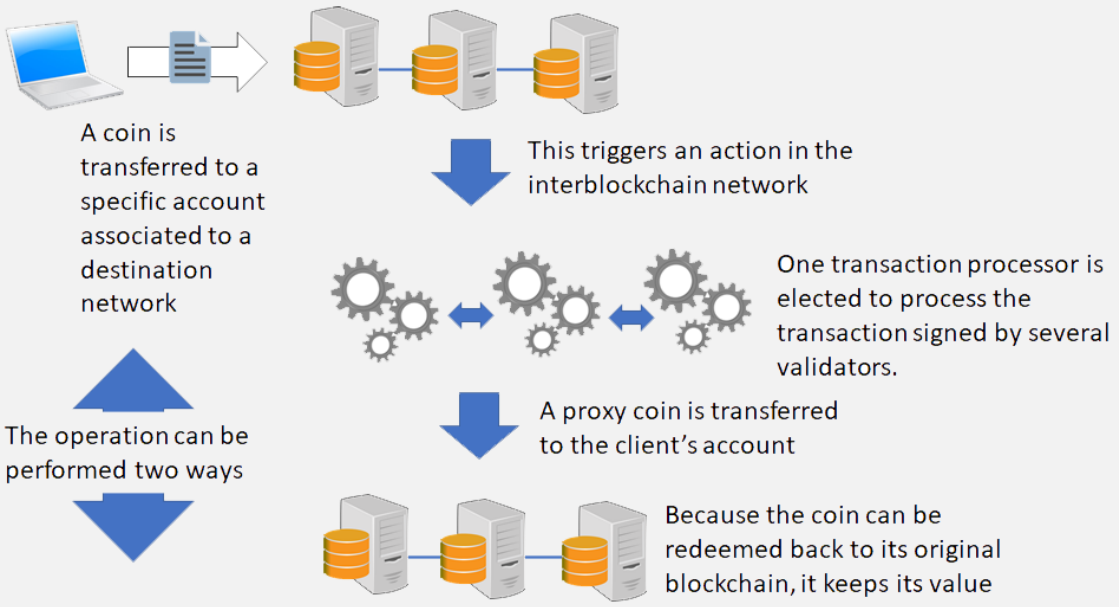
When a transaction is performed on a particular blockchain node, this transaction is replicated on all the nodes. A consensus mechanism is established to order and validate the transactions. On some blockchains, this order may be jeopardized by the miners in charge of validating and inserting transactions into blocks. For example, if a transaction A with a low fee is performed before a transaction B with a substantial fee, it may be treated and inserted after the transaction B. The miner's process prioritizes the transactions having the highest fees. They do not necessarily process transactions according to the strict order of published transactions.



An Transledger is very different because of the simple fact: a transaction must be performed only once. If a transaction is performed on all blockchain nodes, it will be interpreted as several transactions, one each time it is posted on the network. So, on a blockchain, a transaction is replicated on each node to update the node's local database.

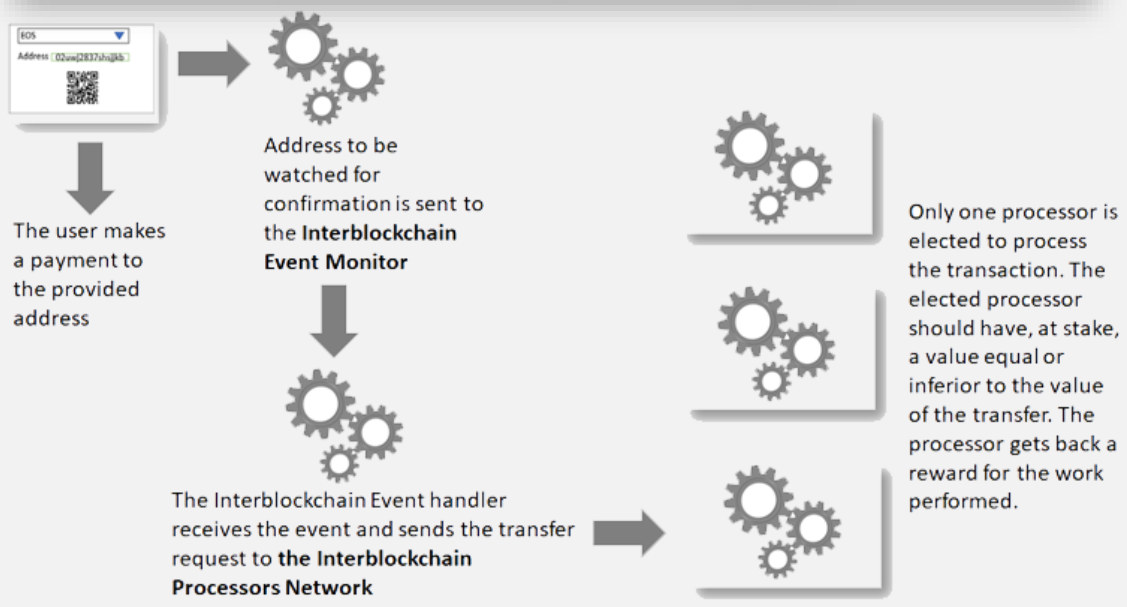
> In an interblockchain, **a transaction must be performed only once**.

For example, Fred sends a bitcoin on the Bitcoin network and an ether on the Ethereum network to Bob. Each node of the Bitcoin network and each node of the Ethereum network will replicate the transfer of the transaction, and they will update their local copy of the replicated database.



This time, Fred, sends a transaction to move a coin from the Bitcoin network to the Ethereum network. This operation must be performed only once. So, in an interblockchain network, only one node must perform the transfer operation.

> To recap, in a blockchain, all nodes perform the very same operation. in an interblockchain network, only one node performs the operation



.

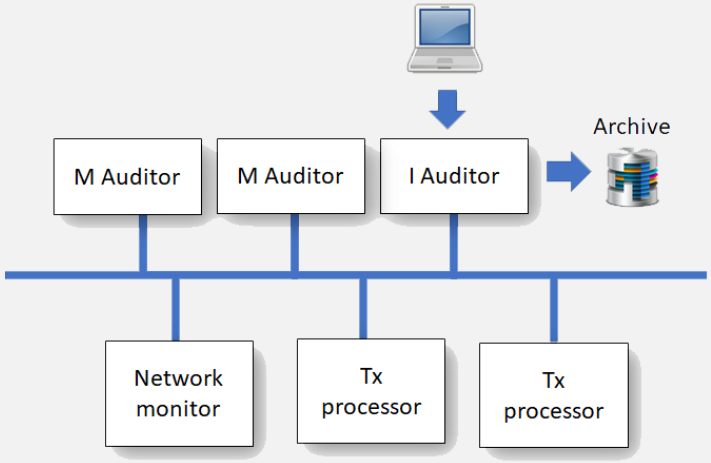
The Transledger Architecture

The interblockchain network is composed of these major elements:

- The interblockchain network
- Network monitor
- 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 Transledger 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 is not identical, to the RLPx protocol from Ethereum. The network supports several channels. Two channels are actually implemented:

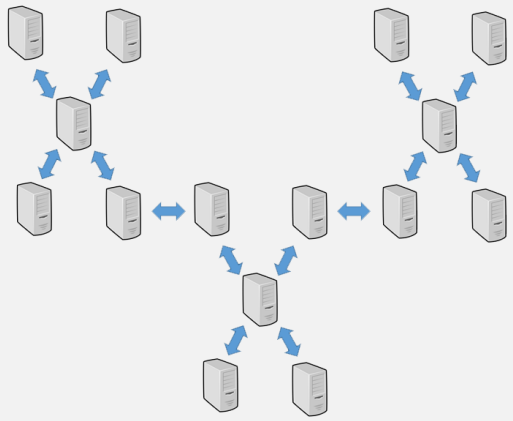
- A Production Channel
- A Test channel

The interblockchain network is composed of 3 payers:

- The Distributed Peer Table layer. The latter layer is responsible for peer discovery and maintaining a table of interblockchain peers.
- The messaging layer is responsible for validating and encrypting/decrypting messages.
- The application layer 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. A unique identifier identifies each channel.



As of writing, the Transledger 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 respectively in the source and the destination network. 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 action.

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

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

The Transledger network presents several input nodes for a truly distributed system starting from the entry points. This is in contrast to most actual blockchain system where their input node 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-auditors 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.

All auditors are used to audit all transactions 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 Transledger network can receive these messages. Network monitor databases records each transfer request and audit results. The messages sent by the auditors are cumulated 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 can either connect to the *Transledger Augmented Node service*, a service providing 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 can be standalone, not using the Transledger augmented node, and 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
    - 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 should also conform 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, and the server cannot execute code 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 *Transledger Augmented Node* (as a service client) and the interblockchain network.

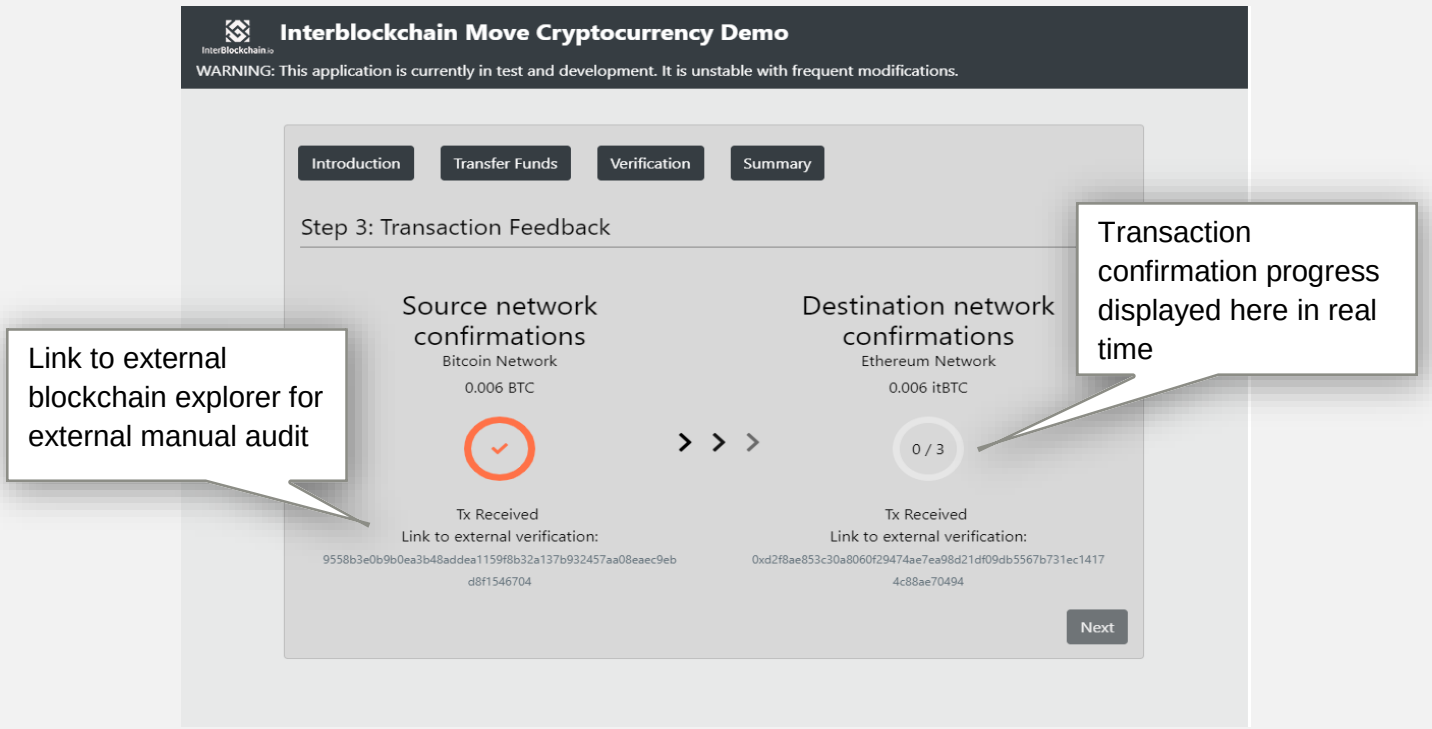
I-auditors are recording all transfer request records into a replicated database implemented over Tendermint. All transactions, validated or not, are stored in the archive blockchain. All transfer requests are stored as transactions in an interblockchain blockchain network; balance kept in each blockchain 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 Transledger client (as an embeddable library or standalone) or through a REST API, are received by one of the network I-auditor (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 later, wait for events to audit 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 transfers request records in the interblockchain archive network. The archive network is used solely to act as a distributed history audit trail and 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, provided by Transledger, includes a graphical interface displaying an accounting audit trail. Also, it displays 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 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 transfer funds in the users' wallet. A client user interface should provide a mean, 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 5 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 are completed. Transaction processors are connect in different ways:

Model 1:

- A listener gets transaction form the interblockchain network and write them in a file stored on a NAS server. A transaction processor, located behind a NAT with no incoming opened ports, read the file from a NAS and perform blockchain transfers on the destination network. This type of processor is the last step of a transfer process.

Model 2:

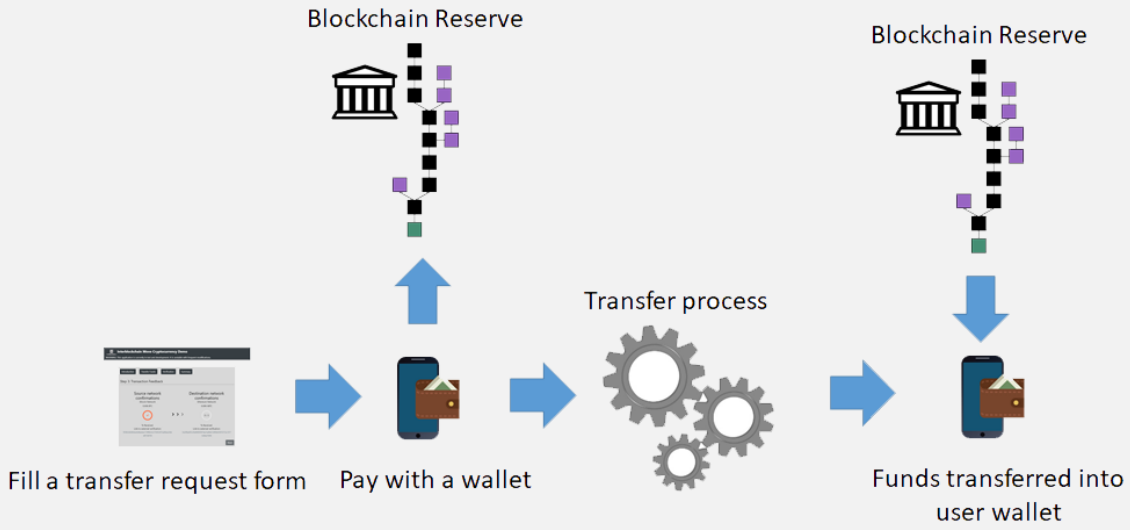
- A transaction processor is directly attached to the interblockchain network and can only sign a transaction.

For more security, several nodes write into several NAS. A transaction processor reads several files, compare them and perform the operation if all the data is identical, otherwise 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 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 crypto assets across blockchain networks and later by adding the exchange across blockchains.

The transfer of funds process involves only a transfer between a reserve and user accounts on the source and destination networks. The reasons behind this are to allow the bidirectional movement of funds as a whole or as a fraction.



The transfer of funds process is similar to banks transfer of funds. Fiat money, like the USD, is independent of any technological substrate. A bank may store its ledger in an Oracle database, another bank storing it in a blockchain, and the USD transfer across these banks remains a USD. In the bank's ledger to ledger transfer fo 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 crypto assets 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 crypto assets and cryptocurrencies hosted in these ledgers. The interledger network transforms any crypto asset or cryptocurrencies as virtual entities, similar to one of the 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 redemption of funds as a whole or as a fraction. A counterparty is always available since each reserve is acting 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 any need for any counterparty. The reasons why a user may transfer funds to another blockchain network would be, for example:

- Use 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.
- Use 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 from Visa, MasterCard or debit card. Thus users would transfer their funds to faster and less expensive blockchain networks like, for instance, EOS.

Roadmap

Stage 1

As of this writing, we already developed a good portion of the entire system. In particular:

- A blockchain monitor for the following blockchains:
  - Bitcoin
  - Bitcoin Cash
  - Bitcoin Gold
  - Litecoin
  - Ethereum,
  - Ethereum classic,
  - Ethereum ERC20 token
- A test event handler packaged as a Docker image. The latter can process a coin move from any previously mentioned blockchain to Ethereum. Each coin has its equivalent in Ethereum. For example, Bitcoin has its proxy as i-bitcoin, Bitcoin cash has its proxy as i-BCH, and so on and so forth. These proxy coins are based on the ERC20 smart contract.
- An implementation of the ERC20 (NEP5) smart contract on the Neo platform to enable coin transfer to this platform. The NEP5 contract is an improved version of the original contract and is written in C#. We are currently porting the same ERC20 contract on the EOS platform. In this case, it is written in C++.
- A test 0x relay order book. For the moment, the 0x protocol solely resides on the Ethereum platform, and therefore the order book, is active only on this platform, As the 0x protocol is ported on other platforms, the order book will be ported on other platforms.

Stage 2

For the next stage, the focus will be essentially on:

- Move from a single transaction-verification node to a network of nodes.
- A particular effort will be attributed to re-enforce the security level of the network