InterBlockchain.io

UNLOCK COINS FROM THEIR SILOS

WORK IN PROGRESS - VERSION 1.0.1

MAY 9, 2018

Table of Contents

What Can I do With Interblockchain?

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

- Bitcoin
- Bitcoin Cash
- Bitcoin Gold
- Litecoin
- Ripple
- Ethereum
- Ethereum classic

As of this writing, these blockchain networks are worth about 85% of total market capitalization for all tokens. Today, these cryptocurrencies are mainly used for storage of value and speculation. What if they could be made available for transactions, to buy things?

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 Interblockchain proposes to help Fred and merchants exchange stored value for goods and services with these coins.

1. Fred uses Interblockchain to move some Bitcoins to a less expensive and faster blockchain, let's say EOS.
2. On EOS, Interblockchain 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 Interblockchain 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.

Now let's imagine another story. This time, Fred wants to exchange his bitcoins for ERC20 coins. In 2017, he lost quite a lot of money using centralized exchanges. They said the exchange was hacked and that he has no recourse. 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 the Ethereum blockchain by creating a proxy Bitcoin local to Ethereum and, from there, exchange it with other ERC20 coins. The other party of this exchange can then redeem the proxy bitcoins back as bitcoins on the Bitcoin blockchain. So, even if the exchange occurred in a distributed exchange on Ethereum, the two parties can exchange their tokens directly from their personal accounts and addresses. To exchange two ERC20 coins with a 0x order book is usual now, but exchange a bitcoin for ERC20 coins directly from users' account is not.

In a nutshell, Interblockchain allows Fred to move his Bitcoins to a fast blockchain like EOS for expenses and to blockchains like Ethereum to exchange his bitcoins for ERC20 coins directly from his account.

In other words, most of the actual capitalization is stored in slow and inefficient blockchain networks. These crypto-assets are digitalized in faster and more efficient networks to be transacted and exchanged. They can be redeemed back to their original networks. Throughout this whole process, the crypto-assets keep their value.

Some Context: Three Financial Building Blocks

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

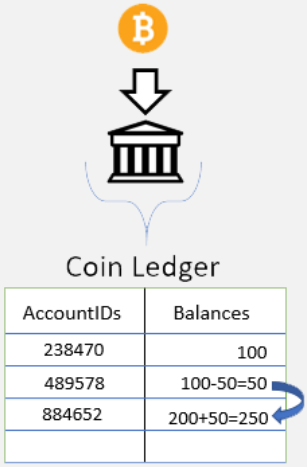
1. The capacity to transfer and receive value (funds) in the same reference system. In other words, to be able to pay or to be paid in the same currency, like the euro or dollar.
2. The capacity to exchange value between different reference systems. For example, to exchange dollars for euros or bitcoins 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

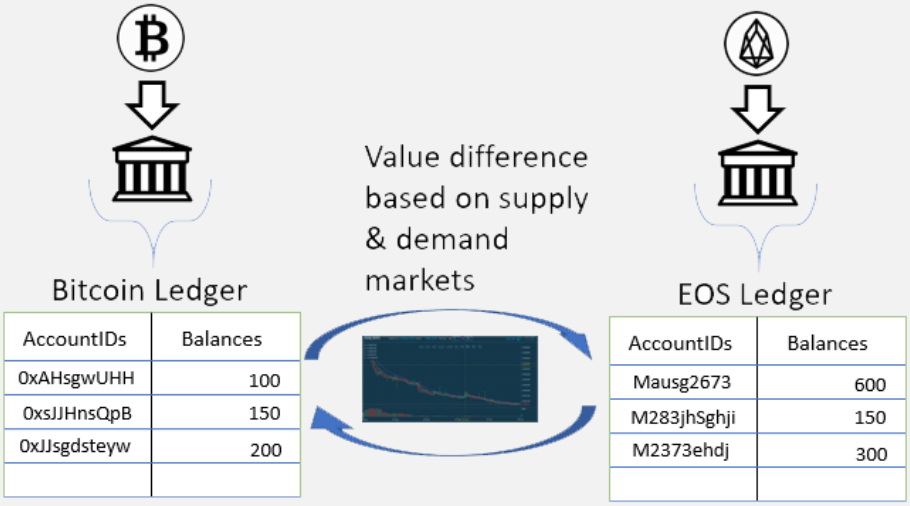
In the blockchain realm, we already can perform transactions within the same currency domain. In other words, within the same ledger. For example, we transfer bitcoins from one address to another. Or, in the realm of programmable blockchains, like, for example, Ethereum, *Qtum* tokens can be transferred only within the same *Qtum* ledger. EOS tokens can only be transferred from one EOS account to another EOS account.



Exchanges

There is also the capacity to exchange coins 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

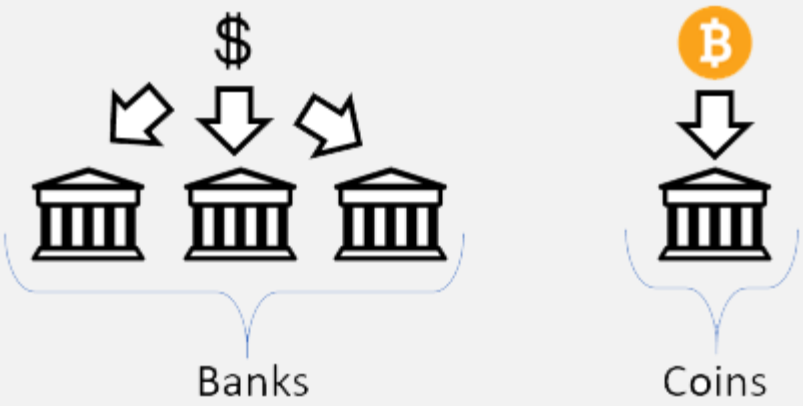
Actually, cryptocurrencies are tightly attached to a particular blockchain network technology. They cannot be moved easily to another ledger and keep their value. For example, the bitcoins reside solely in the Bitcoin blockchain network, the ether solely into the Ethereum blockchain network, and so on 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. On the one hand, 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

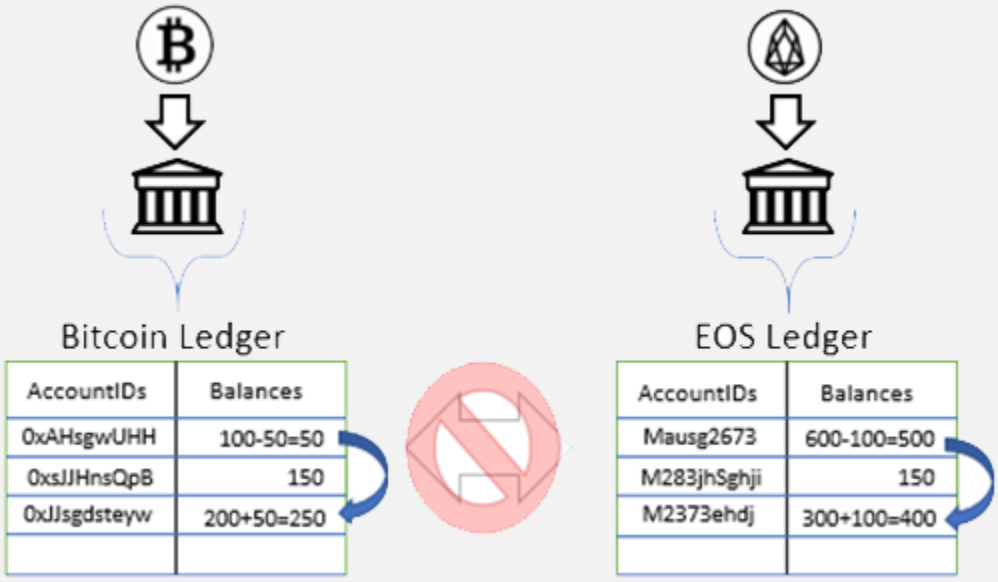
The ERC20 is an Ethereum standard that most new tokens created on this blockchain support. This common interface tremendously simplifies any application implementing a transfer of value, within the same ledger, from one account to another.

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.



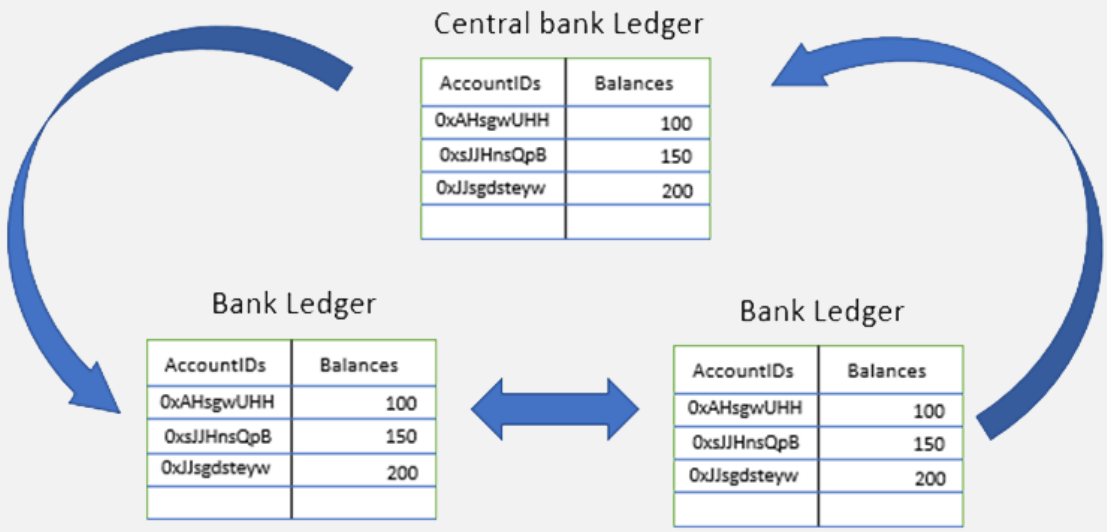
Improving the technology of these ledgers has proven to be a slow and arduous process. Even then, the progress is very limited compared to what improvements are technically possible. Moreover, there is no common way to freely move cryptocurrencies to different ledgers. It would be tremendously practical 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 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 exchange funds. This clearinghouse adds all transfers amounts between banks, and the difference is then transferred to the destination bank through a central bank. 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.

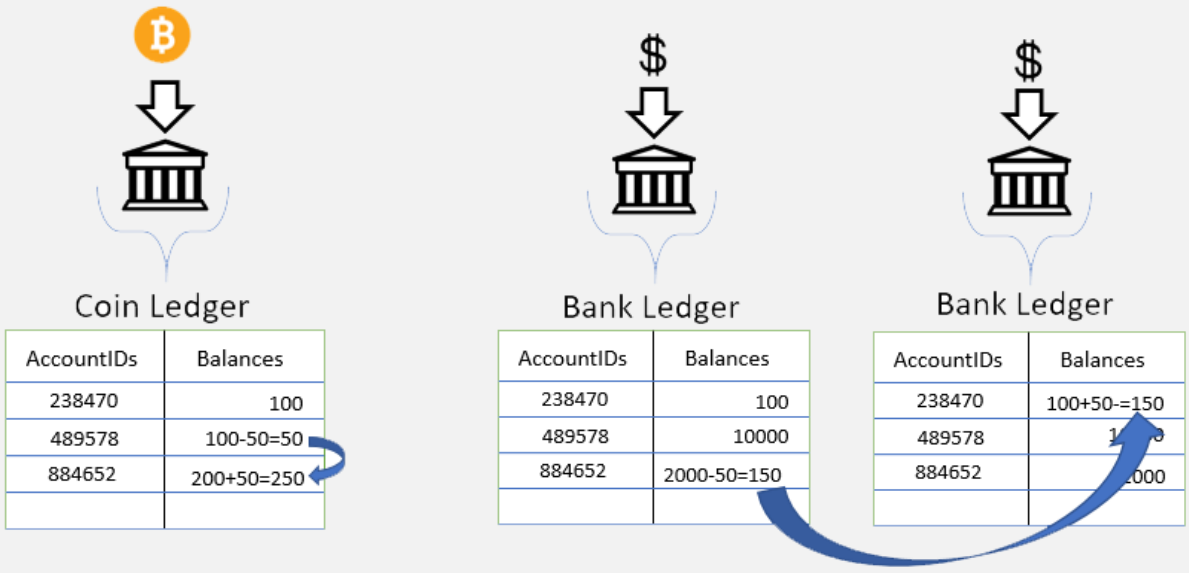


The Cryptocurrencies Realm

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

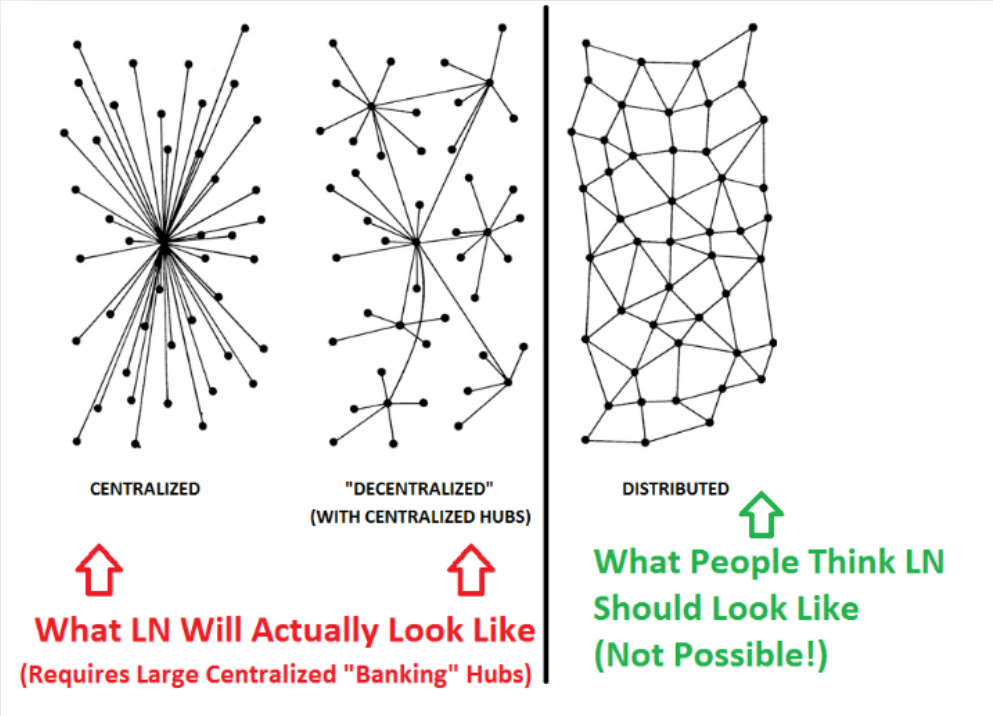
AccountIDs	Balances
0x29ShsmSkj	100
0x22HHweTe	10000
0x373hsdYSo	2000

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 Interblockchain Solution

In a nutshell, the Interblockchain 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:

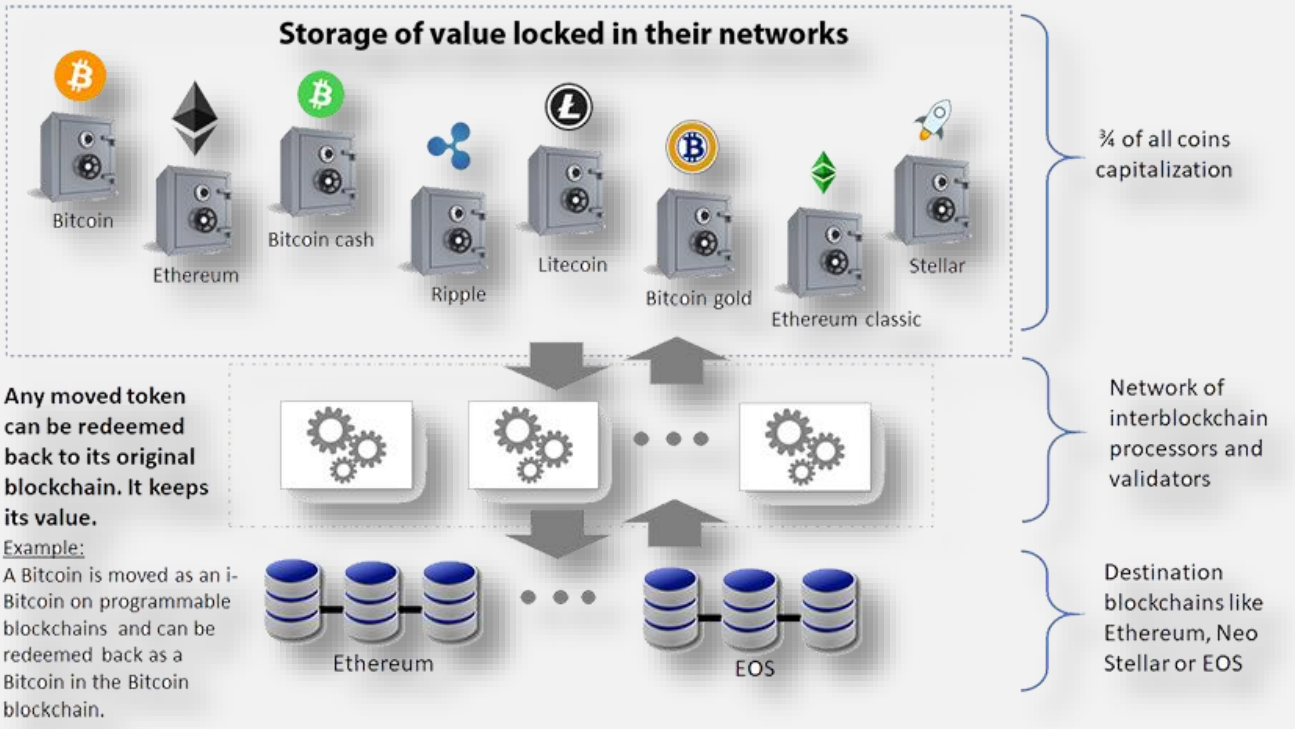
- **The code performing the transactions on both blockchains must be triggered only once**. This is a major difference with actual blockchain mechanisms in which the very same operation is performed on all nodes.
- **The node executing the code must be trusted and honest**. This is the same constraint 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:

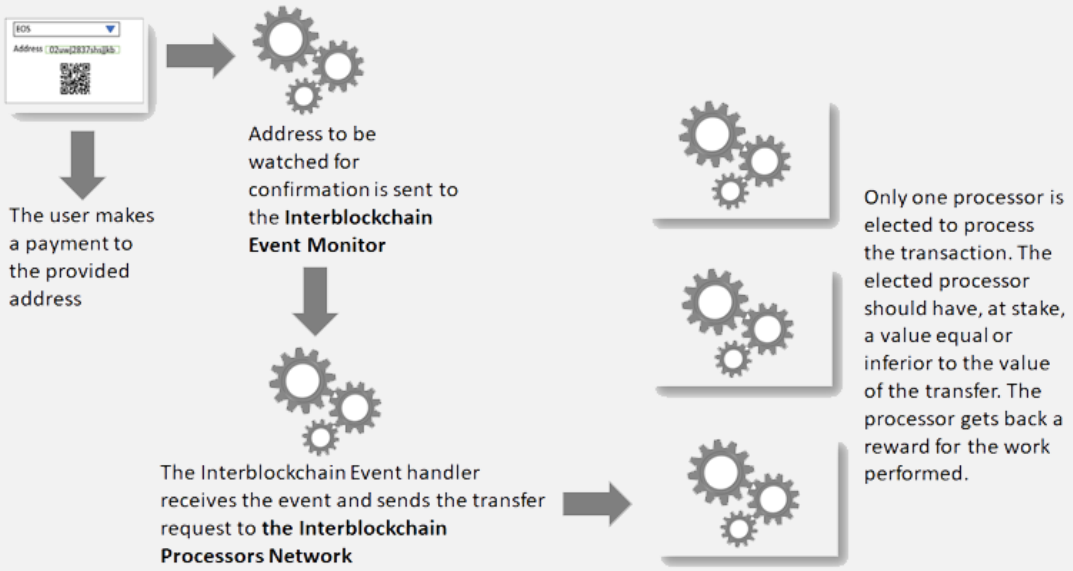
- We move a coin like a bitcoin to a more efficient and less expensive blockchain, like EOS.
- On EOS, we create a proxy version of the bitcoin. Let's say an i-bitcoin.
- The i-bitcoin can be redeemed back to the Bitcoin network hence retaining its full value. Thus, while on the EOS network the i-bitcoin is to be considered as having the same value as it does on the Bitcoin network.

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



An Interblockchain network is used to perform the required transactions on the origin blockchain and the destination one.

When moved to Ethereum, 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 Ethereum, EOS, Neo or other blockchain networks, 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 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 Interblockchain 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.

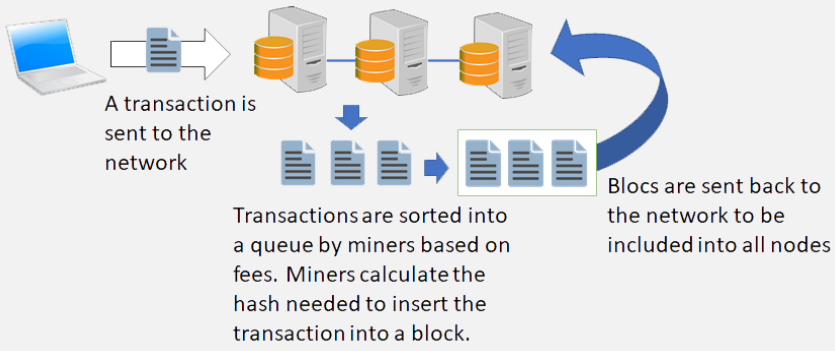
- i-bitcoins can be transferred from an original owner to third parties. Hence, the balance associated to the original owner account can be fragmented into several transactions. Each transaction is registered into the blockchain. Each transaction recipient of a transfer from the original owner or any 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.

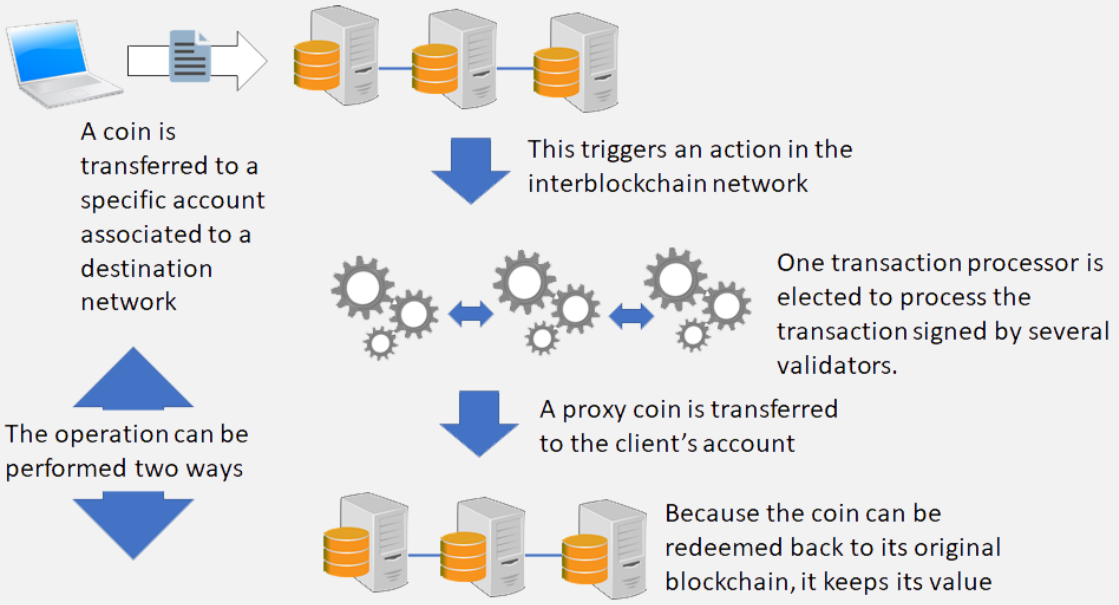


An interblockchain is very different because of the simple fact: a transaction must be performed only once. If a transaction is performed on all blockchain nodes, it will be interpreted as several transactions, one each time it is posted on the network. So, on a blockchain, a transaction is replicated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

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

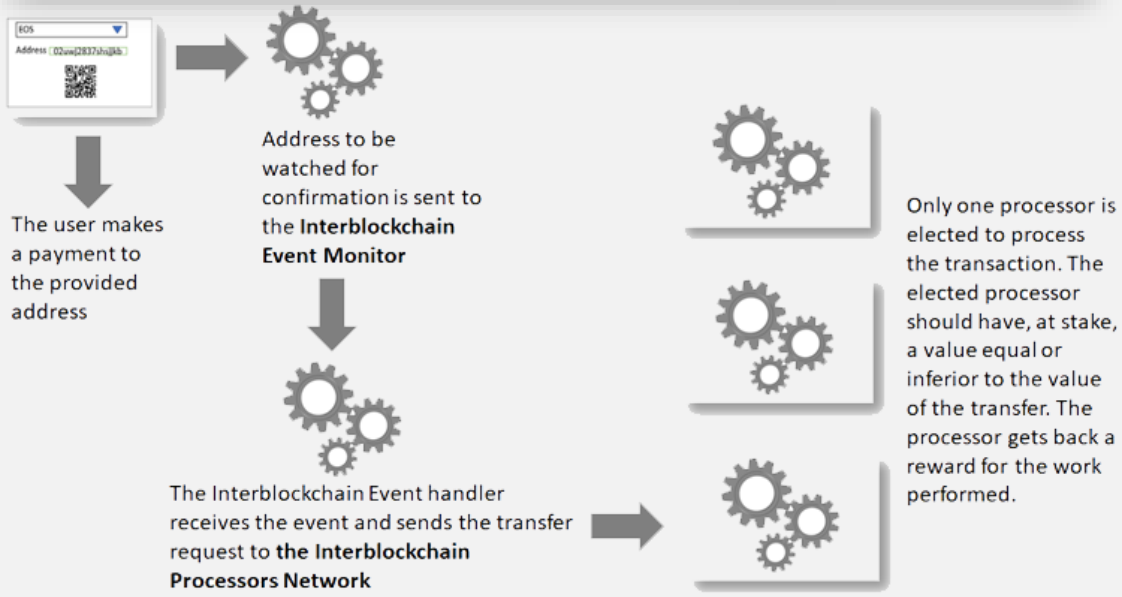
For example, Fred sends a bitcoin on the Bitcoin network and an ether on the Ethereum network to Bob. Each node of the Bitcoin network and each node of the Ethereum

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 Interblockchain Architecture

The Interblockchain is composed of these major actors:

- The processors
- The validators
- The blockchains

As its name indicates, the processors are the ones executing the transaction or the piece of code that needs to be executed only once. The validators obviously validate the actions of the processors. The validators use a Shamir secret sharing algorithm[2] to validate a transaction. Several key parts are required to validate a transaction. A full Interblockchain node must include the full data of several blockchains as follow:

- Bitcoin
- Bitcoin Cash
- Bitcoin Gold
- Ethereum
- Ethereum classic
- Litecoin

Several others will be added to the list in the future.

In addition to these blockchains, a node should include:

- A blockchain event monitor for each blockchain
- An event handler which can be used for multiple blockchains. The event handler collects from the reference blockchain the value at stake. Several event handlers should determine which transaction server will do the operation based on the value at stake. The decision is determined by a group of event handlers.
- A transaction server. The server which will perform the transaction on the destination blockchain. The transaction server can perform a transaction only when several keys are transmitted by the validator and the transaction signed by several validators. The code to be executed is located inside a Docker image decrypted by the keys provided by the validators (multiple keys).
- A validator server. This server communicates a message to unlock the image with a fragment key and communicates through a port to code inside the container to get the hash of the code to be executed. We still need to evaluate an alternative algorithm where a key is dynamically generated and matched against the hash of the image to be decrypted and run with a docker run command.

[2] Shamir Secret Sharing algorithm: https://en.wikipedia.org/wiki/Shamir%27s_Secret_Sharing

Transaction processing

In our previous example, Fred transfers a bitcoin to an i-bitcoin on Ethereum. The whole process starts with a form Fred must fill out. The only thing Fred must provide is the destination Ethereum address. In return, a Bitcoin address is displayed. This is the address where Fred should transfer his Bitcoins. It is uniquely created for this particular transaction. When the bitcoin is received at the provided address, this triggers an event in the *Interblockchain Bitcoin Network Monitor,* and the *Transaction Event Handler* performs a series of operations:

- It records the transaction in the reference blockchain.
- It triggers the process to vote for the elected server which will perform the transaction on the Ethereum network and to verifiers
- Each verifier signs the transaction through a unique secured port of the container encapsulating the transaction process. The container is a black box having only a secured port to sign.
- When all verifiers have signed the transaction, the transaction is performed. It transfers an i-bitcoin to the account of Fred. Fred can now either use it to trade it with another ERC20 token on a 0x-based relay (order book). So, Fred exchanged a bitcoin for several EOS tokens. Bob has now a Bitcoin and Fred several EOS tokens.

Now let's see how Bob redeems his i-bitcoin back to a bitcoin on the Bitcoin network.

We envision that the first use of transferring any of the following crypto-assets to Ethereum will be to add value to 0x-based exchanges. This will bring new liquidity and the capacity to trade ether- and ERC20-based coins with:

- Bitcoin
- Bitcoin Cash
- Bitcoin Gold
- Ethereum classic
- Litecoin

We are considering adding Ripple to this collection. Supporting Ripple, as of writing, would allow 85% of the total market capitalization to the Ethereum platform to be traded on non-custodian 0x-based exchanges.

Transaction verification by third parties

Transactions can easily be verified by end users through tools provided by Interblockchain or through third party explorers. When a transaction is successfully realized, the transaction information on both blockchains (source and destination) is provided. The number of coins should match. For example, a bitcoin moved to the Ethereum network should be listed as an i-bitcoin. The reverse operation is symmetrical.

Transfer from non-programmable blockchain to another programmable blockchain:

If we take, for example, a coin movement from Bitcoin to Ethereum, this transfer will appear on any bitcoin explorer like, for instance, blockchain.info. It will document the transfer of funds executed by a user with his/her wallet. On the other hand, the transfer from the i-Bitcoin from the reserve to the user's account will appear on an Ethereum explorer such as Etherscan. The very same verification is possible also for the other blockchains supported as follow at the moment:

- Bitcoin
- Bitcoin Cash
- Bitcoin gold
- Litecoin,
- Ethereum classic

Transfer from programmable blockchain to non-programmable blockchains:

To take another example, a movement from Ethereum to Bitcoin is triggered by a transfer of funds from a user transfer to the i-bitcoin reserve. This transaction is documented in an explorer such as Etherscan. Then the movement of funds will appear on an explorer like blockchain.info documenting the transfer of funds from the Bitcoin reserve to the user's account.

Transaction and validation processors rewards

For each coin movement, a reward is given to validators and transaction nodes. Each node should have the capacity to be both a validator and a transaction execution server. A full node supports all blockchains which, for the moment are:

- Bitcoin
- Bitcoin Cash
- Bitcoin gold
- Litecoin
- Ethereum
- Ethereum classic

Other blockchains will be added in the future.

Processing priorities are attributed to nodes having more value at stake and supporting more blockchains. For example, this entails supporting all blockchains instead of only a few. Supporting more blockchains is considered to be a form of the stake to be added to the value at stake in the form of an asset like Bitcoin or any other valued coins.

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