LQDEX

Decentralized, Trustless, Cross-Chain Exchange

Sergey Nikitin
sergey@lqdex.com

Yogesh Srihari
yogesh@lqdex.com

Whitepaper

June 12, 2018
Version 1.0

Table of Contents

Abstract

In the last few months, the blockchain community has seen a rapid proliferation of DEX, decentralized digital asset exchanges. The advantages of DEX over their centralized counterparts are:

1. Substantially higher security
2. No (or fewer) restrictions on the types of assets that can be traded and who can trade them

But, the modern DEX have major shortcomings. Typically:

- Only single blockchain assets can be traded
- High cost due to miner fees
- Trade execution is slow

As a result, most DEX suffer from low liquidity. Professional traders still, for the most part, prefer using centralized exchanges with larger trading volumes and lower fees, even though it means exposing themselves to the risk of losing funds. [Appendix A]

In contrast, LQDEX is a decentralized trustless **cross-chain** digital asset exchange. It has all of the advantages of DEX without the typical shortcomings. The main features of LQDEX are:

- Cross-chain trading
- Low cost, no miner fees
- Trade execution speed comparable to centralized exchanges

LQDEX supports trading of digital tokens across multiple blockchains without counterparty risk. For example, Bitcoin can be traded for Ether. It does not use Atomic Swaps and does not require modifications to the existing blockchains. The system accomplishes these goals by using the following technologies:

1. Proxy token trading with smart contracts
2. Economically bonded collators providing cross-chain interoperability
3. A purposely built blockchain without miner fees and high execution speed

By solving the challenges of decentralized trading, LQDEX plans to attract institutional traders, which will bring high liquidity to the network.

Digital asset trading is a huge market. At the moment of this writing, the combined **daily** trading volume of all cryptocurrency exchanges is **$10 Billion**.

The Challenge

Users of modern cryptocurrency exchanges demand risk-free trading, a wide range of tradable assets, liquidity, and transparency. Market research (see Appendix A) indicates that the ideal exchange should have the following characteristics:

1. Is counterparty risk-free
2. Allows trading of assets on multiple blockchains
3. Has substantial liquidity
4. Is inexpensive to use
5. Has fast order execution
6. Is transparent and publicly auditable

Let us consider some of these requirements in more detail and the technology that can be used to implement them.

Counterparty Risk

The main concern of using centralized cryptocurrency exchanges is the risk of losing funds. There have been multiple instances of centralized exchanges losing all or part of user funds. For example, in 2014, Mt. Gox, a Japanese-based exchange, lost almost half a billion US dollars of user funds. [1] The reason centralized exchanges are vulnerable is because they have a single point of failure. If the server hosting the exchange is compromised or shut down, users lose their funds.

The risk of losing funds when trusting a third party, such as a centralized exchange, with holding user assets is called “counterparty risk.”

But, counterparty risk is not just an exchange specific issue. In fact, it is an age-old problem humans had to deal with since the advent of trading.

If two people traded with each other, they traditionally had to deal with counterparty risk. Let us say human A wants to trade chickens for lambs, and human B wants to trade lambs for chickens. Both are happy with the price the other person is offering. However, one of the two traders has to give his or her product to the other first. Whoever gives it first risks losing everything if the other party runs away with both chickens and lambs!

While the risk may be acceptable for smaller transactions, for larger deals, a “trusted third party” has emerged. The trusted third party is a person or company that both transaction participants trust. In this situation, both participants relinquish their goods to the third party. When both exchanged items are received, the third party makes the exchange and presents the goods to the corresponding clients. This scenario has the risk of the trusted third party going bankrupt or running away with both chickens and lambs.

Exchanges, in particular, are more vulnerable to the counterparty risk issues. If an exchange is to have substantial liquidity, it needs market makers to deposit large amounts of funds on the exchange.

In addition, exchanges typically take a long time and require a payment of fees to move funds in and out of an exchange, so even regular users usually keep some amount of funds on an exchange to quickly take advantage of favorable prices.

As a result, if a centralized exchange is compromised, the loss of user funds can be substantial.

Benefits of Decentralization

For the first time in human history, blockchain technology has solved the age-old problem of counterparty risk. Theoretically, if done correctly, one person should be able to exchange digital assets with another without any amount of trust involved.

What makes this possible is the design of the blockchain itself. Instead of entrusting funds to a single entity, the asset ledger is held by a large number of blockchain nodes. Even if one node is attacked by a hacker, or decides to run away with user's assets, it would not make a difference, as consensus of the majority nodes is needed to modify the asset ledger. The only way to compromise a blockchain is to attack the majority of its nodes. But, the nodes are hosted on many different servers, often in different parts of the world. Attacking the majority of the nodes is typically very expensive and impractical.

So, the solution to the trustless exchange problem is a decentralized exchange hosted on multiple servers without a single point of failure. If one server is hacked, the entire system continues functioning and, theoretically, users do not lose their funds.

The Technological Challenge

So, why has a proper cross-chain decentralized exchange not yet been built? There is one more technological challenge that has not been solved.

The problem is that it is easy to exchange digital tokens within the same blockchain. However, to exchange tokens generated by one blockchain for tokens generated by another blockchain, the two blockchains need to be able to somehow communicate and send commands to each other. But, a universal counterparty risk-free cross-chain protocol does not yet exist.

Smart Contracts

Within the same blockchain, users can trade digital tokens risk-free by using "smart contracts." A smart contract is a computer program that executes certain predefined instructions on the blockchain. The benefit of a smart contract is that users do not have to trust each other when performing a trade or another operation.

For example, a simple smart contract can perform the following instructions:

1. Wait until token X is received from user A and token Y is received from user B.
2. If both received, send token X to user B and token Y to user A (do the exchange).
3. If condition 1 is not met, give the tokens back to the users (void transaction).

Cross-Chain Interoperability

Smart contracts require the manipulation of tokens, thus limiting trade to tokens within the same blockchain as the smart contract. For example, users can easily trade ERC20 tokens on the Ethereum blockchain with smart contracts.

But, what if someone wants to trade Bitcoin for Ether with a smart contact? If there was an algorithm that could accomplish this counterparty risk-free, it would be called a "cross-chain smart contract."

The difficulty with implementing cross-chain smart contracts has to do with how blockchains work.

The Private Key Dilemma

First, to execute a transaction, one must sign with a "private key." If a blockchain instruction does not get signed, the transaction will not execute. If you have sole access to the private key of your Bitcoin wallet, there is no way in the world that any person, computer, or thing can generate a transaction that takes your bitcoin out of your wallet. If there were, it would null the value in holding Bitcoin or any other cryptocurrency.

Second, blockchains cannot conceal information. Anything that gets put on any blockchain is instantly public knowledge. Can a blockchain be developed that can store private information? No! It will not be a blockchain then. Blockchains work by allowing independent and unknown parties to host the blockchain ledger on their computers. Anyone can install the Bitcoin core (or any other blockchain core) on their computer and obtain a copy of all Bitcoin data from the genesis of Bitcoin.

Now, it is clear why connecting two blockchains is difficult. To initiate a transaction on Blockchain A, Blockchain B requires access to the private key of Blockchain A to sign the transaction with the private key before the transaction can be written on

Blockchain B after miner verification. However, blockchains are public and thus cannot be trusted with private keys.

Cross-Chain Trading

Let us see what solutions have been proposed for accomplishing cross-chain trading.

Trusted Third Party

We will codename this solution "Mt. Gox." It is a privately held server holding private keys for all blockchains it works with. When users send tokens to the server, computations are performed and sent out to the appropriate blockchains. This is how all centralized exchanges work. This solution is not counterparty risk-free. Even the most secure server can be compromised or taken down.

Trading within One Blockchain

The word 'DEX' means trading with just one blockchain which is mostly referring to decentralized exchanges on Ethereum. Examples include EtherDelta and 0X which we will discuss later in more detail. Their solutions do not work across multiple blockchains, and thus fail to offer one of the most desirable features of the ideal exchange: the ability to trade a wide range of assets on multiple blockchains.

Proxy Tokens with Trusted Third Parties

Some exchanges have developed a concept of "proxy tokens." Proxy tokens are tokens on one blockchain that represent tokens on another blockchain. They operate similarly to plastic chips in a casino. Each chip corresponds to an amount of money, but it is not real money. They cannot be used outside of the casino that issued them.

Proxy tokens are useful because they can be exchanged risk-free with smart contracts within one blockchain even though they represent real tokens on other blockchains.

However, trusted third parties are still required to convert these proxy tokens into real tokens once the user finishes trading and wants to cash out. The exchange that pioneered this model is BitShares. This solution is not counterparty risk-free because trusted third parties can be compromised.

Atomic Swaps

Atomic Swap technology allows some limited cross-chain interoperability. To execute a "swap" (an exchange), two users must manually sign their transactions with their private keys. A technology layer acts as an escrow, which either performs the swap or returns funds backs to the users. Because each user holds the corresponding private key, a swap can only be executed when both users are online and sign within a specified time window. It does not allow automated order execution if one of the users is offline.

The inability to execute orders automatically means that users cannot place any type of conditional orders such as limit orders on the exchange. The lack of limit orders means the absence of market makers. The absence of market makers means lack of liquidity on the exchange. In other words, a user would have to come to the exchange and wait for another user who is willing to trade to appear in real time. As a result, a traditional exchange with liquidity and automated order execution cannot be built using Atomic Swap technology.

Another drawback of the technology is that it is limited to only Bitcoin clone blockchains or requires modifications to the blockchain core software (a hard fork) in order to work. While this solution comes closest to accomplishing cross-chain

trading functionality, it is not universal and not suitable for an exchange in the traditional sense of the word.

Summary

To summarize, there are only three possibilities of what type of entity can hold the private key. Each has its own pros and cons.

Entity Type	Pros	Cons
The private key is stored on the blockchain.	Cross-chain transactions are possible.	Everyone will see the key and can steal user funds. This is not a viable solution.
The private key is stored on the private server (the "trusted third party").	Cross-chain transactions are possible.	The "trusted third party" can steal or inadvertently lose user funds (the Mt. Gox scenario).
The user (a human) has the private key.	Some cross-chain risk-free transactions are possible.	The user must be online to sign each transaction. Not suitable for frequent trading or conditional orders. Requires modifications (hard forks) to blockchain cores.

Each solution proposing any type of cross-chain functionality must be evaluated based on which entity holds the private key. It must fall in one of the three categories above. Depending on which category it falls in, it will have its advantages and potential vulnerabilities.

Other Decentralized Exchange Projects

A trustless decentralized cryptocurrency exchange with zero counterparty risk is the holy grail of digital asset trading. The first company to successfully implement this is likely to achieve a high degree of commercial success. As a result, many startups have attempted to tackle this problem. Some have called their system a "decentralized exchange," but as with anything else, the devil is in the details.

BitShares

BitShares is a decentralized exchange. It uses proxy tokens for counterparty risk-free trading. It also uses gateways that issue IOUs for trading on their platform [2]. However, the IOUs are not backed by collateral. If the gateway is hacked or shutdown, users lose their funds. The zero counterparty risk extends only to trading of proxy tokens. A user holding a proxy token IOU is not guaranteed to be able to convert it into an actual asset.

In addition to gateway IOUs, BitShares also has Market Pegged Assets (MPA), backed by a collateral in BitShares core currency, BTS [2]. However, they are not backed by real assets. The user cannot convert an MPA directly to the corresponding real asset. The user can either convert it to BTS and then convert BTS to the correct asset at a different exchange, or convert it to an IOU proxy token, and convert that IOU to the asset at one of the gateways. Neither of these options are counterparty risk-free.

In short, BitShares cannot execute counterparty risk-free trades. BitShares can only offer counterparty risk-free trading of various types of native proxy tokens within its network.

EtherDelta and RadarRelay

EtherDelta and RadarRelay are exchanges that allow counterparty risk-free trading of ERC20 tokens on the Ethereum blockchain [3, 4]. Since trading is performed with tokens issued by only one blockchain, it can be performed with smart contracts without counterparty risk.

The primary limitation of these two platforms is that they only work with Ethereum tokens. They do not support Bitcoin, for example. The secondary limitation is that trading on the Ethereum network is slow and relatively expensive, as new blocks are produced only every 14 seconds [5], and Ether must be paid for each transaction.

ARK

ARK is a blockchain with the ability to execute transactions on other blockchains using proprietary SmartBridge technology. It uses "Encoded Listeners" to scan for SmartBridge data and execute cross-chain transactions. According to ARK's website:

"The Encoded listener node is a hub for listening to SmartBridge transactions. This transaction hub can be setup and run by anyone, Shapeshift, Changelly or even Coinbase. Anyone that wants to act as a medium to help the network can. And in exchange for providing this service they will be collecting transaction fees for passing data or exchanging currencies via SmartBridge." [6]

To execute a transaction on a blockchain, one must sign with a private key that has to be stored on the Encoded listener node. This makes the system vulnerable to hacking of the Encoded Listeners. This is not in any way a counterparty risk-free transaction due to a single point of failure.

In addition, if "anyone that wants to act as a medium" can set up an Encoded Listener node and send and receive cryptocurrency on behalf of ARK, there will likely be many incidences of Encoded Listeners disappearing after receiving substantial amounts of user funds.

Atomic Swaps

Atomic Swaps is a promising technology that can allow counterparty risk-free transactions across certain blockchains [7]. It can work on Bitcoin clone blockchains such as Litecoin or Decred by using their script language. Atomic Swaps can also be performed with the Lightning Network. However, the support for Atomic Swaps with scripting is not universal across different blockchains. It is also not clear which blockchains will support the Lightning Network, as it requires a hard fork.

The limitation of this technology is that it only allows funds to be exchanged when both users are online to sign the transactions with their private keys. It is more suitable for large OTC trades. It is not as convenient for frequent trading common on cryptocurrency exchanges. It also does not allow execution of any automated orders, such as limit or stop-loss orders.

LQDEX Blockchain

The LQDEX Blockchain (LB) is a proof-of-stake public blockchain. It features fast block creation, and it does not have miner fees. The network can issue native tokens, similar to Ethereum tokens.

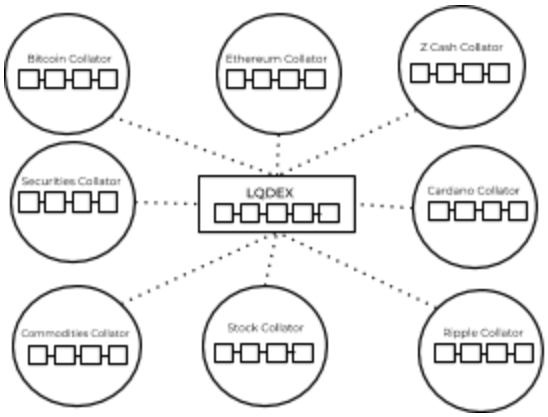


Figure 1: High-level LQDEX blockchain architecture

LQD Token

The main currency of LB is called LQDEX (LQD), similar to Ether in Ethereum. LQD is traded on cryptocurrency exchanges and can be purchased for Bitcoin, Ether, USD, or other currency.

The LQD token pays a reward. The LQDEX Network generates profits by charging commissions for trades and withdrawal fees. It distributes profits to LQD token holders as rewards.

Proxy Tokens

LQDEX also issues proxy tokens, such as lq-BTC or lq-ETH. These correspond to digital tokens on external blockchains. There are always as many outstanding proxy tokens as assets on the balances of the Collators. When assets are deposited, the corresponding proxy tokens are created. When assets are withdrawn, the corresponding proxy tokens are destroyed. For example, if LB has 1,000 lq-BTC tokens issued, there are exactly 1,000 BTC on the balances of all of its Collators.

Trustless Cross-Chain Trading

LB can natively execute smart contracts with its native tokens, LQD or proxy tokens. All trades are performed as smart contracts using proxy tokens with zero counterparty risk.

Collators extend this functionality further and enable the LQDEX Network to execute counterparty risk-free trades across multiple blockchains.

Collators

A Collator is a server hosting an LB core and a core of another blockchain, such as Bitcoin core or Ethereum core ("external blockchain"). The server keeps the private key for accessing the external blockchain. A Collator performs the following functions:

1. Executes commands it receives from LB.
2. Provides information about external blockchain transactions to LB.

A Collator receives the share of profits from the exchange operations proportional to its LQD collateral deposit amount with LB. Collators are analogous to “miners” in a proof-of-work or proof-of-stake blockchain.

Here are examples of commands that can be executed by Collators running the Bitcoin core:

1. Deposit X amount of BTC.
2. Withdraw Y amount of BTC to an address.
3. Provide information about a Bitcoin transaction or wallet.

When a Collator receives tokens, such as BTC, it stores them in its wallet. Upon detecting the transaction, LB creates new proxy tokens, such as lq-BTC, for the amount of external blockchain tokens received by the Collator.

Likewise, when LB instructs the Collator to send tokens, such as BTC, the Collator sends tokens from its wallet to the address specified by LB. LQDEX then destroys proxy tokens, such as lq-BTC, for the amount of external blockchain tokens sent by the Collator.

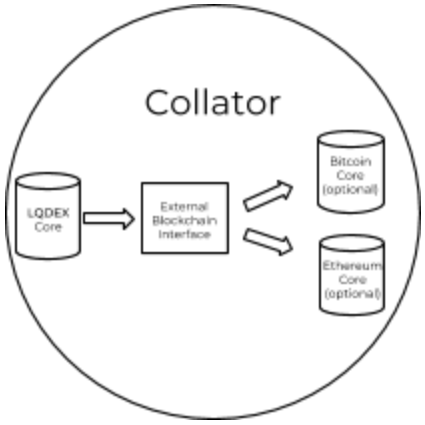


Figure 2: Collator software architecture

The LB software combines the LB Core, which records LB transactions, and the Collator functionality into one package. A participant of the network may install the core and only use it for recording transactions, or use it for both recording transactions and providing the external blockchain connectivity. In both cases, the participant would need to deposit an amount of LQD tokens, which serves simultaneously as the voting stake and the Collator's Collateral.

The Collateral

A Collator must maintain a deposit with LB in LQD in the amount of 200% or more of its token balance. For example, if a Collator has a balance of 100 BTC, it must maintain a deposit of 200 BTC or more in LQD with LB. This deposit is used as collateral. The collateral makes it unprofitable for a Collator to "walk away" with user funds.

One way to think about a Collateral is as a stake in a proof-of-stake blockchain. See Proof-of-Stake vs. Proof-of-Work section for a more detailed explanation of what the stake is used for. To participate in block creation on any kind of blockchain whether it is PoW or PoS, the participant has to make a capital expenditure, which is substantial.

In the case of Bitcoin, a miner has to invest in expensive mining equipment and electricity lines, the cost of which can run millions of dollars. In the case of a PoW blockchain, such as Ethereum Casper, a miner needs to invest in the stake. In either case, an investment has to be made and participation is not free.

Since miners inevitably have to invest funds, this investment can also be used as a Collateral to entrust miners with holding a limited amount of user funds, not to exceed half of their stake in the system. In addition to voting power, the use of the stake as Collateral to hold user funds is a natural extension of the PoW blockchain concept.

Collator Transactions

Deposit Transactions

There is no counterparty risk for deposit transactions, as the funds have already been

deposited to LB as collateral. If a Collator's balance reaches 200% of the collateral or higher, LB stops sending deposit requests to that Collator and informs the Collator to increase its collateral to resume processing deposits.

Withdrawal Transactions

If a Collator fails to perform a withdrawal transaction, LB will first attempt to execute the command with a different Collator, supporting the same external currency. If all Collators fail to perform the transaction, LB will liquidate a part of the Collator's collateral proportional to the amount of the withdrawal. It will send that amount in LQD to the user instead of the external currency. The user will receive an amount of LQD larger than the amount of withdrawal requested. He or she can then convert that amount of LQD to the currency that the Collators failed to send at a different exchange.

External Blockchain Reporting

Collators report information about transactions on external blockchains to LB. If LB needs information on a specific transaction, it broadcasts this query to all Collators that are known to hold a given external asset, such as Bitcoin.

For example, LB can request information about whether or not a deposit was made to a specific Bitcoin address. After the query is made, the corresponding Collators submit their votes on whether or not they think the deposit was made. Once a certain time period passes, LB determines that the deposit was made if the supermajority of Bitcoin Collators reported the deposit.

Transaction Examples

Let us consider some example transactions on the LQDEX Network in more detail.

Scenario 1: Account Funding

A user wants to start trading on the LQDEX Network. He or she first must deposit funds to LB. At the moment, the user wishes to deposit 1 BTC. To process the deposit, the network will perform the following steps:

1. LB creates a wallet for the user on its blockchain.
2. LB finds the Collator, which supports Bitcoin and has the highest collateral ratio.
3. LB instructs the Collator to commence a deposit transaction for 1 BTC.
4. Collator provides a Bitcoin address to LB, to which the user needs to send his or her deposit.
5. LB informs the user to send 1 BTC to the Bitcoin address provided by Collator. LB also sets a time window, during which the user needs to perform the deposit.
6. LB keeps querying the provided Bitcoin address to see if a deposit of 1 BTC appears in it.

If the deposit appears:

1. LB creates lq-BTC tokens for 1 BTC. It places the lq-BTC tokens for 1 BTC in the user's wallet.

If the deposit does not appear:

1. If the deposit does not appear during the time window, the received transaction is cancelled.

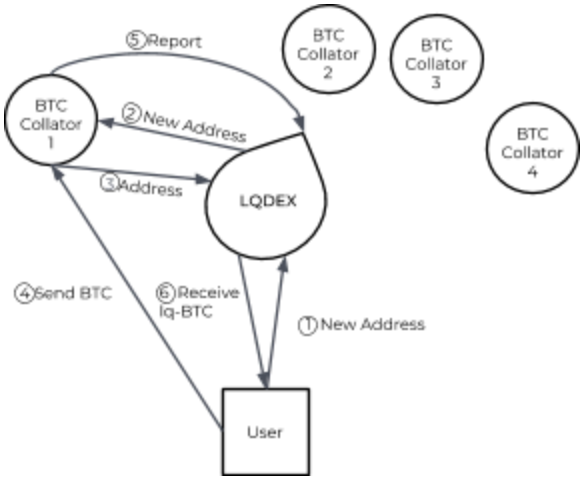


Figure 3: Deposit transaction flow

Scenario 2: Trading

The user wants to exchange his or her lq-BTC tokens for lq-ETH tokens. LB can natively trade its tokens with smart contracts. Users can trade any internal tokens on LB without counterparty risk.

Figure 4: Trade transaction flow

Scenario 3: Withdrawal

The user finishes trading and now wants to withdraw his or her Ether. At the moment, he or she has 10 ETH.

1. The user provides an Ethereum address where he wishes to withdraw the funds to.
2. LB finds the Collator, that supports Ethereum with the sufficient balance and the lowest collateral ratio.
3. LB instructs that Collator to send 10 ETH to the address provided by the user (the transaction can be broken up among multiple RBGs).
4. The Collator executes the transaction and returns the blockchain transaction number to LB.
5. LB confirms that the transaction number is valid and the transaction has been executed.

If the transaction has been executed:

1. LB destroys 10 lq-ETH tokens and removes them from the user's wallet.

If the transaction has not been executed:

1. LB finds another Collator, that supports Ethereum and has the sufficient balance and continues with Step 3.

If no suitable Collators are found:

1. LB calculates an amount of LQD held on deposit by all Collators proportional to 10 ETH. Let us say it is 20 ETH equivalent in LQD.
2. LB takes an amount of LQD worth 20 ETH from the Collator's collaterals and sends it to the user.
3. The user can optionally convert LQD to at least 10 ETH at a different exchange.

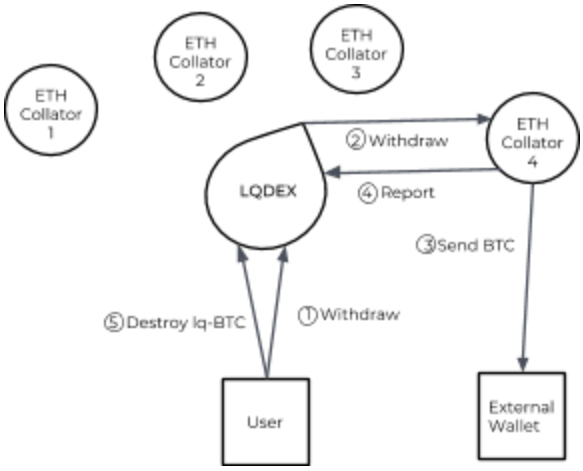


Figure 5: Withdraw transaction flow

Collateral Management

Collators must maintain sufficient collateral in order to perform certain operations including accepting deposits from users. As the value of the external asset fluctuates, the ratio of the amount of the collateral to the value of the external asset held by a Collator changes.

A Collator may also withdraw all or part of its collateral, but only if that the remaining amount is at least 200% of the value of the external asset held by the Collator.

LB keeps balance information of all assets, for which it issued proxy tokens, of all Collators. It computes the value of each asset held by a Collator and the value of its collateral. If the ratio of the value of the collateral and value of the asset held by a Collator becomes low, LB can increase that ratio by sending withdrawal requests only to that Collator until the ratio becomes at least 200%.

There may be situations when all Collators do not maintain sufficient ratios for a particular asset. In this case, LB can perform the following actions:

Collateral Ratio	Action
> 200%	The Collator can process withdrawals. The Collator can process deposits for amounts that would not bring the collateral amount below 200% of the Collator's balance.
<= 200%	The Collator can process withdrawals only. LB sends a notice to the Collator to increase the collateral.
<=175%	LB sends notices to all users holding the corresponding proxy tokens informing them that support for the external asset will be soon discontinued. Users may optionally withdraw or exchange the external asset.
<=150%	LB liquidates the Collator's collateral. LB cancels proxy tokens of the asset held by the users. LB sends LQD tokens in the amount of ~150% of the value of the cancelled tokens to the users.

Collator Loss Recovery

So far, we have discussed what happens when everything is running smoothly, also known as the "happy path." Let us consider a scenario when a Collator is compromised.

While it is unprofitable for a Collator to walk away with user funds, it is still possible for a Collator to be compromised due to hacker attacks, mismanagement, hardware malfunction, or other events. Since each individual Collator is a centralized server holding a private key to its assets, a hacking attack on a Collator can potentially lead to a complete loss of funds held by that Collator.

The LQDEX Blockchain must be designed so that a loss of any Collator does not lead to a loss of user funds. In fact, LB counts on the fact that some Collators will be compromised periodically, as is the case with all centralized entities holding private keys.

Withdrawal Recovery

So how does that work? One misconception is that if a Collator (let's say for Bitcoin) goes down, LB blockchain distributes its Collateral to the users, whose Bitcoin was held in custody of that Collator. But, this is not how it usually works. Instead, users would typically be unaffected and unaware of a Bitcoin Collator going offline.

When a Collator becomes unavailable for any reason, the following steps occur:

1. LB sends a command to the Collator to perform another withdrawal.
2. The Collator does not respond within a given time period.
3. LB sends the withdrawal command to the next Bitcoin Collator.

In most cases, the user withdrawal is performed either way. In this scenario, the user does not notice or care if one Bitcoin Collator goes offline. The system continues to function as if nothing happened.

Hypothetically, what if there is no available Collator to process the withdrawal command for the requested amount in Step 3? This scenario is possible if the user requests to withdraw a relatively rare asset held by a limited number of Collators. Only in this case, LB would have to liquidate the unavailable Collator's Collateral and distribute it to the users affected by the loss of that Collator.

Asset Recovery

In Step 3 of the algorithm, LB simply sends the command to the next Collator able to process the withdrawal. This allows completing the withdrawal operation without any user friction. However, now there is a situation that the total amount of assets (in our example it was Bitcoin) held by all Collators is smaller than the amount of the corresponding proxy tokens in the system.

If the asset deficit is left uncorrected, a situation may arise where a user will request to withdraw Bitcoin, and no Collator will be able to process the request as the total amount of Bitcoin held by all Collators is smaller than the amount of the corresponding proxy token. However, in the future, the system may no longer be able to compensate users for the loss of Bitcoin with the lost Collator's Collateral. Imagine, if the Collator went down a year ago, but the situation, when the withdrawal could not be processed, occurred just now. The exchange rate of the LQD token against BTC may have changed substantially, and the Collateral may no longer be enough to compensate users for the loss of Bitcoin.

To prevent this situation from occurring, LB attempts to recover the lost asset and restore the one-to-one correspondence of the actual asset and the corresponding proxy token in the system.

The asset recovery works as follows; when a Collator becomes unavailable and does not respond within a specified period of time, LB assumes that the Collator is now permanently offline. LB now offers the Collateral of that Collator to other Collators in exchange for the asset held by the lost Collator.

The Collateral-asset exchange is structured as an auction. LB broadcasts the intent to acquire the exact amount of the lost asset to all Collators known to hold that asset. The Collators submit bids with the LQD token to provide the asset. For example, let us say LB must acquire 100 BTC. Collators bid how much LQD they would like to receive for providing 100 BTC to LB. These amounts can be calculated as the current market rate of BTC vs. LQD, plus a premium for providing the service.

This is an opportunity for Collators to acquire more LQD tokens at a discount. How much of a discount? The lost Collator's Collateral was at least double the amount of the asset held, so LB has a lot of room to offer a discount for selling its Collateral in exchange for the lost asset.

After the bids are submitted, LB simply selects the lowest bid and executes the exchange of LQD for the real asset.

The mechanics of the exchange are very simple, as no real assets such as BTC or LQD are moved anywhere. LB simply increases the amount of Bitcoin held by that Collator and its Collateral by the amount of LQD it received from the exchange in the Collator ledger. It will now count on that Collator to process Bitcoin withdrawals up to the new amount of Bitcoin.

Blockchain Architecture

In order to satisfy Requirements 4 (low fees) and 5 (fast order execution) of the ideal exchange, the LQDEX Blockchain must have high transaction throughput and zero miner fees. These requirements are accomplished by the proof-of-stake (PoS) blockchain architecture.

Proof-of-Stake vs. Proof-of-Work

In a PoS blockchain, nodes generate blocks based on how many tokens they have, not on their computational power. This is different from a proof-of-work (PoW) blockchain, where nodes need to solve a computation puzzle to produce new blocks. The primary disadvantage of a PoW blockchain is the substantial time and energy required to produce a block. So, the recording of the transactions is slow and requires miner fees to pay for the expense of the nodes (also called "miners"), which produce blocks.

For example, Ethereum, at the moment, uses the PoW block creation mechanism. As a result Ethereum-based decentralized exchanges, such as EtherDelta and 0X, suffer from slow speeds and miner fees for each transaction. They do not generate profit for the exchanges.

Another drawback of the PoW system is the higher potential vulnerability to the 51% attack discussed later in more detail. Some coins, such as Bitcoin, have limited supply. At some point in the future, when all coins are mined, miners will no longer receive rewards for mining new coins. They will only be rewarded with transaction miner fees. It is possible that fewer miners will operate at that time since the reward will be lower. With fewer miners, a situation is possible where someone compromises 51% or more of the nodes, thus launching the 51% attack. If someone gains control of 51% or more of the nodes, he or she can send fraudulent transactions to the network and steal other users' funds.

PoS blockchain implementations also have the advantage of being able to reach consensus on block finality (discussed later), an important feature for an exchange.

LQDEX blockchain is a PoS blockchain. The PoS blockchain model was selected because of the benefits outlined above. This implementation of the PoS blockchain prioritizes consistency over availability.

The Stake

LB uses its LQD token as a stake to record transactions or to supply external blockchain information. Each node must deposit an amount of LQD tokens in order to produce blocks on LB blockchain. When a new transaction occurs on the network, all nodes record it when they receive it. The recording of new transactions occur instantly (with the speed of the network), as solving of a computational puzzle is not required.

The Reward

Recording a transaction on LB requires zero miner fees. Instead, the nodes get rewarded with payment from the LQD token. The more LQD tokens a node deposits on to the network, the higher its stake and the larger share of the total network reward it receives.

The reward comes from commissions charged for trades and withdrawal of funds. It is fundamentally

different from miner fees. An Ethereum dapp, such as EtherDelta, pays miner fees to third parties—the miners. In turn, they spend the miner fees on their electricity bills. These miner fees do not contribute to EtherDelta's profit. In contrast, commissions and fees paid on LB are distributed to the prospective stakeholders as rewards, so they contribute to the participants' profits.

Functional Requirements

Because this blockchain application is an exchange, it has a set of unique requirements that other blockchains, such as Bitcoin or Ethereum, may not implement.

Fast Execution

Users expect trades to be executed quickly. Execution time of one or two seconds, or even less, is ideal. In contrast, on the Bitcoin blockchain, blocks are mined an average of once every ten minutes. When a block is mined, the transaction is not confirmed. Users will not wait this long to execute an operation.

High Transaction Volume

High transaction volume is essential for an exchange. If the volume is low, spreads become larger and trading becomes less attractive for most users.

Finality

Commonly used blockchains have not solved the finality problem. In other words, users never receive a 100% guarantee that the acceptance of their transaction by the blockchain is final. For example, on Bitcoin or Ethereum (the current version), there is still a chance that a transaction can be rejected by the blockchain even after multiple confirmations. However, this likelihood decreases as time transpires.

The absence of finality is unacceptable for any type of exchange application. If there is no finality, it is possible that a user will have already withdrawn all funds from the exchange by the time the transaction is found invalid — therefore the blockchain state cannot be reversed to be corrected.

Fairness

Trade execution order is important to an exchange. Bitcoin or Ethereum blockchains group several transactions in one block. After the transactions are arranged in a block their order is not saved. The exchange blockchain needs to keep track of the trade timestamps and reach consensus on that order.

High Security

The exchange blockchain must have an efficient mechanism in place to reward and penalize the nodes for recording transactions. It must be Byzantine fault tolerant, resilient to DDOS attacks, long range attacks, and other possible attacks, as long as the number of malicious blockchain nodes is no higher than one third of all nodes (the theoretical limit of proof-of-stake blockchain resilience).

Simple Implementation

Simple implementation is an important requirement. Complex algorithms and systems take longer to implement and they are more difficult to test and audit. The probability of a vulnerability or an error substantially increases with implementation complexity. In addition, the exchange blockchain needs to be predictable and

publicly auditable. If the inner workings are overly complex, the public may not trust the exchange.

Low Equipment Cost

It is important to incorporate low barriers to entry for businesses that wish to run blockchain nodes. If business are required to spend substantial amounts on equipment alone, running a node will be less desirable. Thus, the number of nodes will be smaller and the network will be less stable.

Byzantine Fault Tolerance

Byzantine fault tolerance (BFT) was named after the Byzantine Generals' Problem. Imagine that you are a member of a group of generals in the ancient Byzantine Empire. Each of you commands a portion of the army. You must reach an agreement on whether to attack an ancient city or retreat. You can be certain that whatever decision is made, if it is not a coordinated attack or a retreat, in the worst case scenario, the entire army can be defeated.

Imagine now, that some generals are traitors and may cast malicious votes for a suboptimal strategy, but you cannot identify which ones.

Imagine that all generals are located far away from one another and send messages via couriers. These couriers may forge the message or even fail to deliver the message.

In blockchain architecture, each node can be thought of as a Byzantine general. The nodes need to come to consensus on whether or not to keep or discard a block of data.

Byzantine fault tolerant systems are networks that function in an environment, where it is unknown whether or not each node is malicious.

Byzantine fault tolerance typically refers to a measure of what fraction of nodes in the network can be malicious before the network seizes to properly function. For example, a 33% BFT system means that the network can function correctly, if up to 33% of its nodes are compromised.

General Assumptions

The LQDEX network is first and foremost a PoS blockchain.

However, it also has the disadvantages inherent in all blockchains. When we discuss LB architecture and how it functions in different usage scenarios, it is important to understand the limitations of blockchain technology.

For example, Bitcoin would function poorly if the entire network consisted of just one node, controlled by one person. It could function, but it would not be trustless. The users would have to trust the sole owner of the Bitcoin node to correctly record transactions. That node operator could double spend his payments to users. (Although, it is debatable whether or not the owner would benefit from defrauding its users. Various adversarial scenarios are discussed later in this paper.)

It is a known fact that blockchains become more vulnerable as the number of nodes decrease.

Both PoW and PoS blockchains are also vulnerable to 51% attacks. In other words, a malicious actor has the ability to takeover the majority number of nodes or stake in the network.

Furthermore, it can be shown that PoS blockchains remain Byzantine fault tolerant if no more than 1/3 of total stake involved in malicious voting in the

network environment with bounded, but unknown network latency. [17]

For the purpose of this whitepaper, unless stated otherwise, the following assumptions apply:

1. There is a very large number of nodes, all operated by different entities.
2. There is a very substantial amount of total stake in the system.
3. For each asset there is a very large number of Collators that work with that asset.

In this context, "very large" means a number that would make it impractical to mount a coordinated attack, where a substantial number of nodes collude with each other.

A "substantial amount" means a large enough amount that makes it prohibitively expensive for any malicious actor to invest in a stake equal to 1/3 of that amount in order to attempt an attack on the network.

We understand that these assumptions will not always be true in the real world, and we will go over possible attack scenarios later in this paper.

However, if 51% of all nodes (or total stake) become malicious or all Bitcoin Collators collude with each other and decide to misbehave, we have to say that LB is by design unequipped to handle these types of attack scenarios. But, neither does Bitcoin nor Ethereum. This is a limitation of all blockchains, not just LQDEX.

Block Content

Each block contains the following types of data:

1. Funding requests (deposit and withdrawals)
2. Trade orders
3. Trade executions
4. Trade settlements (asset account balance changes)
5. Available Nodes table
6. Submitted votes
7. Finalization decision on a prior block
8. Node ID, which proposed the block

LQDEX Block
Header
Funding requests
Trade orders
Trade executions
Trade settlements
Submitted votes
Available nodes
Finalization or previous block
Node ID

Figure 6: LQDEX block contents

Only the changes to the data need to be stored in each block. For example, if only one new trade order came in during block generation, only that information is stored in the block. In order to fetch the entire order book, the client must collect data from multiple blocks.

LB Performance

As we saw earlier, execution speed is one of the top requirements for a successful exchange. LB is designed to accomplish the highest possible execution speed. In fact, as we will see below, the order processing speed of LQDEX is comparable to the speed of a centralized exchange.

Most POS blockchains utilize node voting in one form or another to reach consensus. As a result, their processing speed is limited by the internet

round-trip delay time also known as network latency. The speed in which block consensus is reached depends on the speed in which nodes could cast their votes over the network.

In addition, if a particular application requires computation-intensive calculations, the nodes are typically not rewarded for computing the tasks faster than the other nodes. Even if one node completes the computation quickly, it still needs to wait for the other nodes to reach consensus on the results. Although most PoS systems are a step up from PoW blockchains, PoS systems remain inherently slow.

In contrast, LB has the following features:

1. Performs as many operations as possible without a voting consensus.
2. Rewards and takes advantages of the nodes with higher computing power.

Lead Node

To accomplish these objectives, LB introduces a concept of a Lead Node. The Lead Node is the most powerful node among all nodes in the network, capable of executing the highest number of transactions per second. The Lead Node receives the highest reward out of all LB nodes, so LB encourages the competition on computation power among its nodes.

This concept is somewhat similar to a PoW blockchain such as Bitcoin, where a more powerful node would mine more blocks and receive more reward. However, the difference is that in the case of Bitcoin, the nodes compute hashes of no useful intrinsic value. In LB, the nodes compute the actual exchange application payload such as trade matching and settlements.

The Lead Node is selected by voting. All nodes in the system compute new blocks. When a block is computed, the time of the computation is recorded as part of the block. The node that computes all blocks faster than the current Lead Node for a period of time (let us say 100 blocks in a row) is voted to become the new Lead Node.

Finality

The trading within LB is implemented with the use of proxy tokens. As discussed earlier, a user can convert proxy tokens into a real underlying asset at their discretion. In order to make this possible, we need to introduce a concept of finality.

Consider blockchains similar to Bitcoin or the current version of Ethereum. On these blockchains, the user does not know when a transaction is finalized, and the transaction cannot be reversed. Instead, the user is given the number of confirmations or a “block height” of the transaction. The number of confirmations indirectly indicates the likelihood of the transactions ever being reversed. The more confirmations, the lower the probability.

If LB were like Bitcoin or Ethereum, and a user obtained a particular proxy token as a result of trade to convert his or her proxy token into a real asset, there would be a small probability that the trade would be found invalid, and the proxy tokens received would be cancelled. But, the user has already received the real asset, and LB cannot cancel or reverse withdrawal!

It becomes clear that LB needs to implement a concept of finality. If a block is considered final, the transactions contained in that block and the resulting proxy tokens can never be cancelled. The user can safely convert these “finalized” proxy

tokens into the corresponding real asset without any risk to the network.

While the above conclusion is fairly obvious, the reverse is slightly less intuitive. Specifically, the finality is only required for the conversion of proxy tokens into real assets. In other words, a user can potentially perform any number of operations by only using proxy tokens. As long as nothing is withdrawn, it is not important whether these transaction are finalized or not. At worst, the proxy token transactions can be reversed and executed again at a slightly different price or order, but no real assets or money will be lost. (We will also see later that since Collators get their stake slashed for performing incorrect operations, it is highly unlikely that even the unfinalized proxy token transactions would be reversed.)

To summarize, finality is required, but it is irrelevant to users until they decide to withdraw their funds.

Trade Execution

With finality in mind, LB is structured in way that allows it to perform proxy token trades at the same speed as a centralized exchange. The consensus is only required prior to performing withdrawal operations.

It functions as follows:

The Lead Node receives trade orders from clients. It executes all orders with maximum speed. The Lead Node does not wait for any other nodes. Therefore, the internet round-trip delay time is no longer a factor in trade execution speed.

The Lead Node arranges transactions in blocks and makes them immediately available to clients and other nodes. End users see their trades executed almost instantly.

The only limitation is that users cannot withdraw their funds until consensus is reached.

Consensus, however, is not a major drawback. Sending Bitcoin, Ether, or other assets is a lengthy process, much longer than internet network latency time. The additional minor delay required for consensus will not significantly affect the user experience. (Even though centralized exchanges do not wait for consensus, they often implement various time consuming security checks prior to fund withdrawal.)

Block Arrangement

Transactions are arranged in blocks based on the time they were received by a node. One block can have any number of transactions in it. However, if there were no transactions received during the block time period, no block is created. For example, a block time interval can be precisely ten seconds.

Because of network latency and unequal transaction propagation paths, all nodes receive transactions at slightly different times. In borderline cases, two nodes may decide to put the same transaction in two different blocks.

Block Validation

While the Lead Node executes all trades on its own, all other nodes perform validation of its work. They iterate over the following steps:

1. Fetch the blocks produced by the Lead Node, that have not been finalized.
2. Out of these nodes, select a random block that has not been yet validated by the current node.

3. Compute the block based on the prior state of accounts and new orders received by the current node.
4. Vote yes on the block, if the result matches. Vote no otherwise.
5. Continue with Step 1.

When comparing a computed block result with the block generated by the Lead Node, the nodes need to take into account that transaction timestamps may be slightly different. As a result, some transactions may not be included in the block or an extra transaction may be included. The node must verify the order of the transactions and consider the borderline inclusion or exclusion cases.

Consensus

Each block has a timestamp of when it was generated by the Lead Node. After a certain time period called "Voting Time Threshold," the Lead Node tallies up all votes for a particular block.

If the node supermajority voted "yes," the validation is deemed successful. The Lead Node records the validation result in the current block.

However, if the supermajority did not vote yes, the block, and all blocks generated after this block, is discarded. The Lead Node starts computing blocks, beginning with the discarded block.

When the current block is successfully validated by the other nodes, it is ready to be finalized. As soon as all blocks are finalized prior to this block, it also becomes finalized.

Collator Deficit

LQDEX is a great solution for a fast blockchain that allows nodes to generate blocks quickly and reach consensus even if they have different computational power. The system relies on a large number of nodes to be able to function. The availability of a large number of nodes is a typical requirement for all types of blockchains.

However, it is possible that the LB may operate with significantly fewer number of nodes than would be ideal for a typical PoS blockchain. Imagine now a situation, when a Lead Node generates so quickly, that a few other nodes struggle to keep up with block validation. Only a small number, let us say two or three nodes, are able to submit votes for each block. In this situation, we would not be able to reliably conclude that a particular block is a valid block.

To avoid the situation of nodes being "spread too thin" over a high number of blocks requiring validation, LB requires a minimum number of "yes" votes to be submitted before a block is considered valid. This minimum number has to be a statistically significant sample, let us say a minimum of 31 nodes.

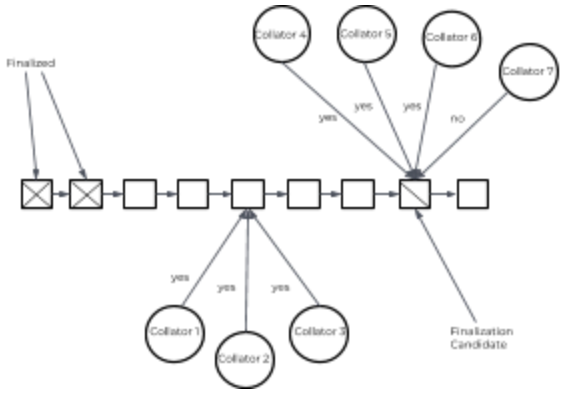


Figure 7: LQDEX blockchain consensus

When newly generated blocks accumulate too quickly, and the nodes cannot keep up with the minimum validation rules, the Lead Node must slow down to match the speed of the remaining nodes.

However, this situation should not occur if there are a sufficient amount of available Collators.

Gossip Protocol

To further increase the network speed, LB uses a modified version of a gossip protocol between its nodes and client connectivity.

In a typical blockchain, each node connects to a number of other random nodes. Let us say that this number is eight nodes. Likewise, end user client applications transmit their transactions to eight random blockchain nodes.

In LB, the node connectivity protocol is similar. But, a node or client app always attempts to secure at least one connection directly to the Lead Node. The remaining connections are to the seven random other nodes. If the Lead Node refuses a connection, the node or client app seeks a connection to another node closely connected to the Lead Node.

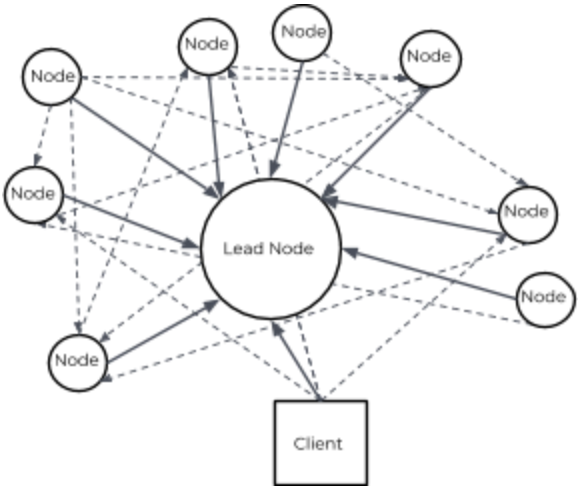


Figure 8: LQDEX modified gossip protocol

This modified gossip protocol shortens the signal travel time between the Lead Node and the other nodes and client applications.

Reward and Penalty

The reward is paid to each node for a generated block or for a block the node voted on. The amount of the reward is computed with the formula:

$$R = K \cdot S$$

K - is the reward coefficient determined by LB
S - is the amount of collateral or stake deposited by the node

As discussed in the monetary policy section, the reward coefficient depends on the network profits, the size of the stabilization fund, and the overall collateral ratios.

The reward is paid to the node in two cases:

1. A block generated by the Lead Node is successfully validated.
2. A node voted correctly on a block.

On the other hand, if the Lead Node generates an incorrect block or a regular node votes incorrectly on a block, the amount equal to a reward is taken out of the node's stake on LB as a penalty.

Cryptographic Primitives

LQDEX uses standard cryptographic primitives that are proven to be scalable with networks like Ethereum. The following are two important choices with respect to cryptographic primitives in a design of any blockchain:

1. Hashing Algorithm.
2. Digital Signature Algorithm.

Hashing Algorithm

Ethereum uses a variation of SHA3 called KECCAK-256, which differs in the padding as described below.

SHA3-256(M) = KECCAK [512] (M || 01, 256)

We will be using KECCAK-256 as an Ethereum standard implementation for our block hashing and computation of merkle hashes.

Digital Signatures

Cryptographic signatures have been instrumental in the success of blockchain and verification of the fact that the message was actually sent by the claimed sender.

Ethereum uses the ECDSA of the SECP-256k1 curve and hash of the datum to sign.

We will be using exactly the same implementation as Ethereum for signing trade and voting transactions on the LQDEX blockchain.

Governance

LQDEX is governed by Collator Users (stakeholders). Collator Users can submit various proposals on how the LQDEX system can be modified. The issues for modification include:

1. Commission and withdrawal fees
2. Collator reward
3. Stabilization fund amount

When a proposal for modification is submitted, other Collator Users can optionally vote on the proposal. The voting is weighted with Collateral. If supermajority approves the proposal, the modifications of the system take effect.

More substantial system modifications are also possible. The Collator Users can also collaborate offline to agree on greater modifications of the system that require programming changes in the LQDEX core software.

Price Volatility of LQD Token

The LQD token is used as a collateral by Collators. In the Collateral Management section, we discussed what actions the network will take if the collateral ratio of a given Collator decreases. However, if the price of the LQD token drops rapidly, it may still be possible for Collators to become under-collateralized.

To prevent the price of the LQD token from fluctuating significantly against the value of other assets traded on the LQDEX exchange, the network implements the token monetary policy. Similar to the monetary policy of the Federal Reserve, this policy is designed to keep the price of the LQD token as stable as possible.

Token Value Model

Collators holding LQD tokens receive rewards for performing operations on the network, such as block confirmations. The present value of this token can be calculated with the formula:

$$PV = \frac{R}{(1+i)^1} + \frac{R}{(1+i)^2} + \frac{R}{(1+i)^3} + \dots + \frac{F}{(1+i)^n}$$

R - reward payment
F - price at the time of sale
i - inflation rate or opportunity cost
n - the number of time periods the tokens are held for

Example: suppose a Collator plans to hold tokens for one year. It estimates opportunity cost to be 15% on an annual basis and the future sale price to be the same as the buy price. The reward paid by the network is currently set at 15% on an annual basis. The current price of tokens is 1,000 USD.

In this case, the present value of the token to the Collator is exactly 1,000 USD. In other words, the Collator is indifferent on whether to sell tokens or buy more tokens.

Let us consider another case; the reward is set at 30%. With everything else staying the same, the price of the tokens is now 1,130 USD. The Collator has an incentive to purchase tokens at the current price of 1,000 USD to make a profit of 130 USD.

If the reward decreases to only 10%, the present value of the tokens decreases to 957 USD. The Collator has an incentive to sell the tokens to avoid losses.

If all market participants are rational, they buy assets when they can generate profit and sell assets when holding them becomes unprofitable. When demand for the asset increases, the price goes up to point where it becomes indifferent for the market players to buy more or sell that asset. Likewise, when the demand drops, the price of the asset decreases to the point of equilibrium. While in practice these price movements can take some time, we will assume for simplicity that the market for cryptocurrency assets is very efficient and any changes to the reward are instantly reflected in the price of the token.

Reward and Inflation

LB generates profits by charging users trade commissions and withdrawal fees. These profits are used for payments of the reward to the Collators. For a given time period a Collator receives a reward, which is proportional to the Collators stake (the collateral amount) and the number of operations

performed by that Collator on the network, such as block creation, etc. As we saw earlier, if the network could increase the amount of the reward, it could increase the price of its token.

Another way for LB to affect the price of its token is to create new tokens (print money). When new tokens are created, a "token inflation" occurs. If the demand for tokens stays constant, the price of one token decreases due to inflation. You can see in the formula above, if R (reward) stays the same, but F (future value) decreases, then P (current price) also decreases.

In the following sections, we will show how both controlling the reward amount and issuing more tokens can be effectively used to control the price of the token.

A "Black Swan" Event

A "black swan" event is an event when an unexpected and unusual financial calamity occurs. In regards to our application, this could only occur if the price of LQD tokens fell so rapidly that most, if not all Collators would become undercollateralized quicker than the network could perform collateral liquidations at the rate of 100% or higher of the asset value held by the Collators. If this event were to occur, network users could potentially lose their funds.

We also have to take into account that if such event were to occur, the profit generated by the network would potentially not be enough to increase the reward sufficiently to increase the price of the LQD token. Creating new tokens, as we saw earlier, would also be ineffective.

Stabilization Fund

To address the potential black swan event problem, the network maintains a Stabilization Fund. The Stabilization Fund is simply an amount of LQD tokens held by the network. The fund is used to quickly stabilize the price of the token if it starts declining unexpectedly and the risk of under-collateralization increases. Just like anything else, the Stabilization Fund is managed by a smart contract (a predetermined formula). The algorithm is as follows:

Each reward payment period, the network performs the following steps:

1. The network analyzes the collateral ratios of all Collators.

IF ratios are too high (LQD appreciated):

2. The network decreases the reward to Collators.

3. If the reward is already near zero, and the price of LQD keeps increasing, it signals a spike in the demand for LQD tokens due to more users or Collators joining the network. In this case, the network creates more tokens (prints money) to increase the supply.

4. The surplus tokens (all that are not paid to Collators) are added to the Stabilization Fund.

IF ratios are too low (LQD depreciated):

2. The network increases the reward to Collators. The reward is taken from the network profits and from the Stabilization Fund.

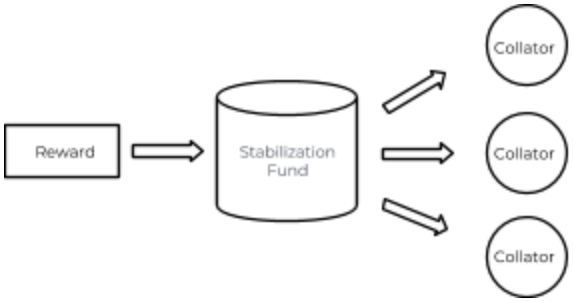


Figure 9: Reward payment flow

How large should the Stabilization Fund be? It is easy to compute the size of the Stabilization Fund that is required to prevent the price of token falling by a given number of percentage points.

For simplicity of calculation, let us assume that Collators plan to hold the token for an indefinitely long time. In this case, the token becomes an annuity. Its pricing is now determined by a simpler formula:

$$PV = \frac{R}{(1+i)^1} + \frac{R}{(1+i)^2} + \frac{R}{(1+i)^3} + \dots = \frac{R}{i}$$

R - reward payment
i - current inflation rate or opportunity cost

In order to increase the price of the token by a factor of two, we must increase the reward by a factor of two.

Let us also assume that currently all Collators are well collateralized, meaning that each Collator has a collateral ratio of 200% or higher. In order for the users to be at risk of losing their funds, the collateral ratio must fall by a factor of two or more to 100% or lower.

Let us say that the current reward rate is 15% on an annual basis. If the total amount of all tokens held as collateral is 1 million, the network pays out 150,000 as rewards per year to all Collators.

If the token price decreases by a factor of two, how many tokens should be kept in the Stabilization Fund to prevent Collators to become undercollateralized, if the price of token decreases by a factor of two?

To keep the price of the token constant, we will need to double the reward. Instead of 150,000, the network will need to pay out 300,000 in rewards per year to keep the price of the token on the same level. The network will need an additional 150,000 to pay a total of 300,000. That extra 150,000 will need to come from the Stabilization Fund. In this scenario, the size of the Stabilization Fund should be 150,000 or about 15% of the total collateral amounts held by all Collators.

A good rule of thumb is to keep the size of the Stabilization Fund equal to the amount of the current reward that must be paid to all Collators for the period of one year. This way, if the price of the LQD token drops by up to 50% (factor of two), it can be quickly brought up to the original level by doubling the reward and sustaining the larger reward payments for at least one year.

If the low demand for LQD tokens and the sale pressure persist for longer than one year, the Stabilization Fund will be depleted, the reward payment will drop, and as a result, the price of LQD will drop as well.

However, one year is usually plenty of time for the effects of the financial calamity to subside or to address any fundamental problems within the network, if any. In the worst case scenario, if nothing can be done, one year is enough time to liquidate the Collator collaterals and reimburse all users of the network, so no one loses their funds.

Adversarial Models

Nothing at Stake

The nothing at stake problem occurs when a node is incentivized to vote "yes" for a block, but is not penalized in any way for incorrect voting. The lack of penalty is referred to as "nothing at stake."

In this situation, the optimal strategy of each network participant is to vote "yes" regardless of the actual block content. If a fork is created accidentally or maliciously on the network, the nodes will always vote "yes" for both versions. This creates a possibility when funds can be double spent, or other conflicting type of transactions can exist on the blockchain.

To address this problem, LB has a penalty in the amount equal to the reward for incorrect block generation or voting.

If a node votes "yes" on two conflicting blocks, it will receive the reward for the correct block and lose exactly the same amount for the incorrect block. The total gain in this case is zero.

Similarly, if a node votes "yes" for three (or more) conflicting blocks, the total gain becomes negative, as only one block will be correct.

As a result, in any situation, the node has zero incentive to vote "yes" on more than one block.

Sybil Attack

In a Sybil attack, the attacker creates a large number of malicious nodes controlled by the attacker. The nodes then cast incorrect votes in the system. If the voting power of misbehaving nodes is higher than the voting power of "honest" nodes, the attacker can potentially perform incorrect transactions, such as steal funds from other users.

This attack method is named after the subject of the book Sybil, a case study of a woman diagnosed with dissociative identity disorder. [16]

Some PoW blockchains can be vulnerable to Sybil attacks. PoS blockchains are typically not susceptible to attacks of this type.

Specifically, LB is not vulnerable to a Sybil attack, because the node's voting power is proportional to its stake in the network. In other words, it is not enough to create malicious nodes in the system. The attacker would also have to make a substantial investment in the staking token to have voting power in the network.

In fact, the actual number of voting nodes does not make a difference. To launch a Sybil-style attack, the attacker would need only one node with a stake amount sufficient to provide a supermajority vote in the system. In this case, the attack becomes the 51% attack, discussed below.

51% Attack

A 51% attack occurs when a malicious actor takes over a substantial portion of the network. In the case of PoW blockchains, this usually means the number of nodes or the amount of hashing power. In the case of PoS blockchains, it controls the majority of voting stake.

All blockchains are vulnerable to 51% attacks. Specifically, PoW blockchains can tolerate up to 1/3 of malicious actors in an environment with bounded, but unknown network latency.

Since LB is a PoS blockchain, the same limitations apply to LQDEX.

If a malicious actor takes over 34% of the stake in the system, it can prevent new blocks from being finalized. Since the supermajority vote is required for block finalization, the misbehaving node(s) can prevent the network from finalizing blocks. While the trades would continue to perform, the users would not be able to withdraw funds.

If a misbehaving actor takes over 67% of the stake, it can effectively generate malicious blocks and defraude other users.

The same scenario can occur on smaller scale if a malicious actor takes over a subset of Collators that processes transactions for a given asset, such as Bitcoin. It can then either prevent Bitcoin withdrawals with 34% stake or perform fraudulent withdrawals with 67% stake.

The only way to protect against the 51% attack is to have the total stake in the system large enough and spread over a large number of Collator Users.

The total stake should be large enough to make it prohibitively expensive for any single entity to acquire a stake equal to 34% of the total stake on the network.

Similarly, the number of Nodes and Collators for any particular asset should be large enough to make it impractical to launch a coordinated attack on all nodes.

The 51% attack vulnerability is inherent to all blockchains. That said, we should also note that even if one actor takes over the substantial part of the network, it may not be necessarily motivated to defraud the users. Satoshi made an interesting point in the Bitcoin Whitepaper:

> *If a greedy attacker is able to assemble more CPU power than all the honest nodes, he would have to choose between using it to defraud people by stealing back his payments, or using it to generate new coins. He ought to find it more profitable to play by the rules, such rules that favour him with more new coins than everyone else combined, than to undermine the system and the validity of his own wealth.* [18]

Intuitively, the rationale is clear. Let us say you were able to acquire 51% of your neighborhood Walmart. You now have full control to do what you want with it. You have a choice to make. You can:

a) Steal everyone's wallet now and disappear with the money.
b) Continue operating the store and receive profits on a continuous basis.

Chances are if someone has enough money to acquire a substantial portion of the stake in the network, he or she might be more motivated to play by the rules and make continuous profits as opposed to defrauding the users.

However, predicting human behaviour is beyond the scope of this whitepaper. So, technically, we have to say that LB is, in fact, vulnerable to the 51% attack, as are all other blockchains.

Non-Best Price Execution

Centralized exchanges may have algorithms in place that do not offer the best price execution. For example, an exchange may engage in practices that trade against its users. When a new order is received, the exchange may attempt to match this order with its own and trade against the user, as

opposed to matching the order with the best price order available in the system. When a trade against the user is made, the exchange benefits not only from the trade commission, but also from the spread. This practice is commonly used by "Dark Pools."

Can a Collator receive an order and attempt to match it with its own order at a price that is not the best for the user?

This situation is not possible on LQDEX. The Collator software is programmed to always execute the order with the best price. If a Collator modifies its software to match an order with another order that does not have the best price, no matter its own or not, the remaining "honest" nodes will not validate this trade.

Front-Running

Front-running is a practice of exploiting information about an order before it enters the exchange order book.

For example, a trader places an order to buy 100 BTC with USD at market price i.e. a market order. Currently, there is a limit order in the order book that offers 100 BTC for sale at 10,000 BTC/USD. There is also another limit order to sell another 100 BTC at 10,100 BTC/USD.

The "front-runner" has somehow obtained information that the market order to buy 100 BTC and is about to enter the exchange. This front-runner now has an informational advantage. He or she can quickly purchase 100 BTC for 10,000 BTC/USD and offer it for sale at a higher price, but not higher than the next limit order of 10,100 BTC/USD.

The front-runner now buys 100 BTC at 10,000 BTC/USD and places a limit order to sell 100 BTC for 10,099 BTC/USD.

When the market order for 100 BTC enters the order book, it gets matched at the best price with the front-runner's order. The trader pays 10,099 USD for each BTC.

The front-runner earns 99 x 100 = 9,900 USD from the transaction with no risk! The trader, however, loses 9,900 USD, as he or she could have bought at 10,000 BTC/USD, if there was no front-runner.

Can one engage in front-running on LQDEX? It is theoretically possible, but given the large number of Collators, the infrastructure investment required to gain an informational advantage is cost prohibitive.

Each trade order is submitted simultaneously to multiple Collators. They, in turn, transmit the order via gossip protocol to other Collators and so forth. The order propagates through the LQDEX network. When an order is received by a Collator, it records the order time stamp. Collators would then have to reach the supermajority voting consensus on the sequence of which the orders were received.

If an aspiring front-runner sets itself up on the same network as the Collators, it sees the orders at approximately the same time as the other Collators. Therefore, it has no informational advantage.

But, what if a front-runner finds a way to connect to one Collator, let us say the Lead Node, with a very fast network connection? The same front-runner also finds a way to connect to two thirds of all other nodes with very fast connections. He or she can now receive new order

information from the Lead Node and send its own orders to the two thirds of the other nodes faster than the trader's order propagates through the network.

While this scenario is theoretically possible, given a large number of Collators, the infrastructure investment to perform this type of front-running will likely be cost prohibitive. In addition, new Collators periodically enter the network in various geographical locations. Being able to build and maintain fast network connections to two thirds of all Collators is unrealistic.

Next Steps

So far, we have seen two major applications of the blockchain technology:

- Store and transfer of value
- Fundraising via ICOs

Many other useful applications have also been proposed, but have not yet entered mainstream adoption.

What will be the next major use case for blockchain?

Asset Tokenization

To an extent, the real-world asset tokenization has already began. Some Initial Coin Offering (ICO) tokens may represent a share of the company that issued them. In that case, they represent an asset in the real world. It is expected, however, that many other real-world asset classes will be "tokenized" in the nearest future.

So, what is tokenization? Simply speaking, tokenization is a process of issuing a digital token that represents ownership of an asset in the real world. [21] It can be a tangible asset such as an ounce of gold or an intangible asset such as a trademark ownership or a share of a company.

Imagine, you would like to allocate a portion of our investment portfolio to gold, but you do not want to go through the expense of moving or storing physical gold. Or, you want to obtain a fractional ownership of a commercial building in Shanghai. Tokenization will make it possible to purchase tokens. They will ultimately become digital asset exchanges. We will observe a convergence of tokens that represent ownership in both of these asset classes.

Tokenization makes assets that could not be previously traded easily very liquid. It is expected that tokenization will unlock trillions of dollars in world asset liquidity. The "early adopter" assets that will be tokenized first will probably be:

- Company shares
- Financial instruments
- Real estate
- Commodities

According to *Fortune.com*, the world's real estate alone is currently valued at $217 trillion. [22]

Exchange Convergence

Of course, the holders of these tokens will need a place where they can buy, sell, and trade them. And, the users will definitely want to do so in a secure and trustless manner.

It is unknown yet which blockchain will be used for creating these tokens. Maybe, it will be Ethereum. But, most likely, new blockchains will be developed with features targeted at specific underlying asset properties. A trustless cross-chain exchange will play a key role in the world's asset liquidity.

As stocks and financial instruments become tokenized, the existing stock exchanges such as NYSE and NASDAQ will also start trading digital existing stock exchanges and "crypto" exchanges. It

will be somewhat similar to the convergence of TV and the internet a few years back.

Users of these exchanges will be able to take advantage of trading a wide range of asset pairs, such as buying Google stock with Bitcoin.

LQDEX is a public trading platform that anyone can use. A Collator for any external blockchain can be connected to it. The system provides blockchain interoperability and supports trading of asset pairs across multiple blockchains. Regardless of what the underlying asset is, or what blockchain its token is issued on, LQDEX can trade it. Trading GOOG for BTC will be a reality.

It is our goal to make LQDEX the standard platform, on which all of the world's assets are traded.

Glossary

LQDEX Blockchain	(Or "LB" for short), a blockchain consisting of LQDEX Nodes.
External Blockchain	(Or "EB"), any blockchain, except LB, such as Bitcoin or Ethereum.
LQD Token	The main token on the LQDEX blockchain, similar to ETH on Ethereum.
Proxy Token	A token on LQDEX Blockchain, corresponding to another asset such as Bitcoin or Ether. It is similar to an ERC20 token on Ethereum.
LQDEX Core	Software, which performs and records operations of the LQDEX blockchain, similar to Bitcoin Core or Ethereum Core.
EB Core	Software, which performs and records operations on an External Blockchain such as Bitcoin Core or Ethereum Core.
EBI	(Stands for "External Blockchain Interface"), a software that relays commands from LQDEX Core to an EB Core and relays information from an EB Core to LQDEX Core.
Collator	(A.k.a. "LQDEX Node" or simply "Node"), a device, hardware and software, running a LQDEX Core and optionally an EBI and one or more of EB Cores.
Collateral	(A.k.a. a "Stake"), a sum of LQD Token a Collator needs to deposit to LB in order to perform operations and optionally accept deposits of other assets such as Bitcoin or Ether.
Reward	A sum of LQD Token paid to a Collator for performing operations on LB.
Node Supermajority	2/3 of all Collators which submitted a vote, or 2/3 of all Collators running a specific EB which submitted a vote.
End User	(Or a "User" or "Trader"), a person or an organization using LQDEX services such as trading of digital assets.
Collator User	A person or an organization operating a Collator.
Client Application	(Or a "Client"), a software providing access to LB running on the End User's device such as a personal computer or a smartphone.

Market Order	A trade order without any price conditions.
Limit Order	A trade order with a condition to execute only at (or better than) a specified price, called “limit price.”
Market Maker	A trader, which placed one or more limit order.
Market Taker	A trader, which placed a market order.
Liquidity	The total amount of all limit orders (converted to the same currency, such us US dollar) at a given moment.
Exchange Facility	(Or a “Exchange”), a device, hardware and software, that performs trade order execution, including execution of automated orders such as limit orders.
Best Price Execution	Matching of a specific order with other orders to accomplish a trade in a way that yields the most favorable price.
Dark Pool	(For our purposes), an Exchange, which does not guarantee Best Price Execution.

References

[1] *Wikipedia.org*, Mt. Gox (https://en.wikipedia.org/wiki/Mt._Gox)

[2] *Bitshares.org*, BitShares 2.0: Financial Smart Contract Platform, Fabian Schuh, Daniel Larimer, 11/12/2015 (http://docs.bitshares.org/_downloads/bitshares-financial-platform.pdf)

[3] *Bitcointalk.org*, EtherDelta - Decentralized Token Exchange (https://bitcointalk.org/index.php?topic=2018051.0)

[4] *0xproject.com*, (https://0xproject.com)

[5] *Medium.com*, Ethereum Block Production Continues to Slide, Thomas Jay Rush (https://medium.com/@tjayrush/ethereum-block-production-continues-to-slide-1b74a2123e3f)

[6] A*rk.io*, What is the ARK SmartBridge, and How Does it Work?, Travis W. (https://blog.ark.io/what-is-the-ark-smartbridge-and-how-does-it-work-1dd7fb1e17a0)

[7] *Bitcointechtalk.com*, Atomic Swaps, Jimmy Song (https://bitcointechtalk.com/atomic-swaps-d6ca26b680fe)

[8] The Dai Stable Coin System Whitepaper (https://makerdao.com/whitepaper/DaiDec17WP.pdf)

[9] Atomic Swaps (https://en.bitcoin.it/wiki/Atomic_cross-chain_trading)

[10] PolkaDot Whitepaper (https://github.com/w3f/polkadot-white-paper/blob/master/PolkaDotPaper.pdf)

[11] Ethereum Whitepaper (https://github.com/ethereum/wiki/wiki/White-Paper)

[12] BaseCoin Whitepaper (http://www.getbasecoin.com/basecoin_whitepaper_0_99.pdf)

[13] Omega One Whitepaper (https://omega.one/static/media/whitepaper-eng-1.25.f65dc5a4.pdf)

[14] Decentralized Token Exchange (https://bitcointalk.org/index.php?topic=2018051.0)

[15] CDO, Vitalik Buterin (https://ethresear.ch/t/collateralized-debt-obligations-for-issuer-backed-tokens/525)

[16] *Wikipedia.org,* Sybil Attack (https://en.wikipedia.org/wiki/Sybil_attack)

[17] Consensus in the Presence of Partial Synchrony, Cyntyha Dwork, Nancy Lynch, Larry Stockmeyer (http://groups.csail.mit.edu/tds/papers/Lynch/jacm88.pdf)

[18] Bitcoin Whitepaper, Satoshi Nakamoto (https://bitcoin.org/bitcoin.pdf)

[19] NIST SHA3, (https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf)

[20] Ethereum Yellow Paper, Dr. Gavin Wood (http://gavwood.com/paper.pdf)

[21] *Nasdaq.com*, How Tokenization Is Putting Real-World Assets on Blockchains (https://www.nasdaq.com/article/how-tokenization-is-putting-real-world-assets-on-blockchains-cm767952)

[22] *Fortune.com*, How Critical Real Estate Is to the Global Economy -- In One Chart (http://fortune.com/2016/01/26/rea-estate-global-economy/)

Appendix A: UCLA Market Research

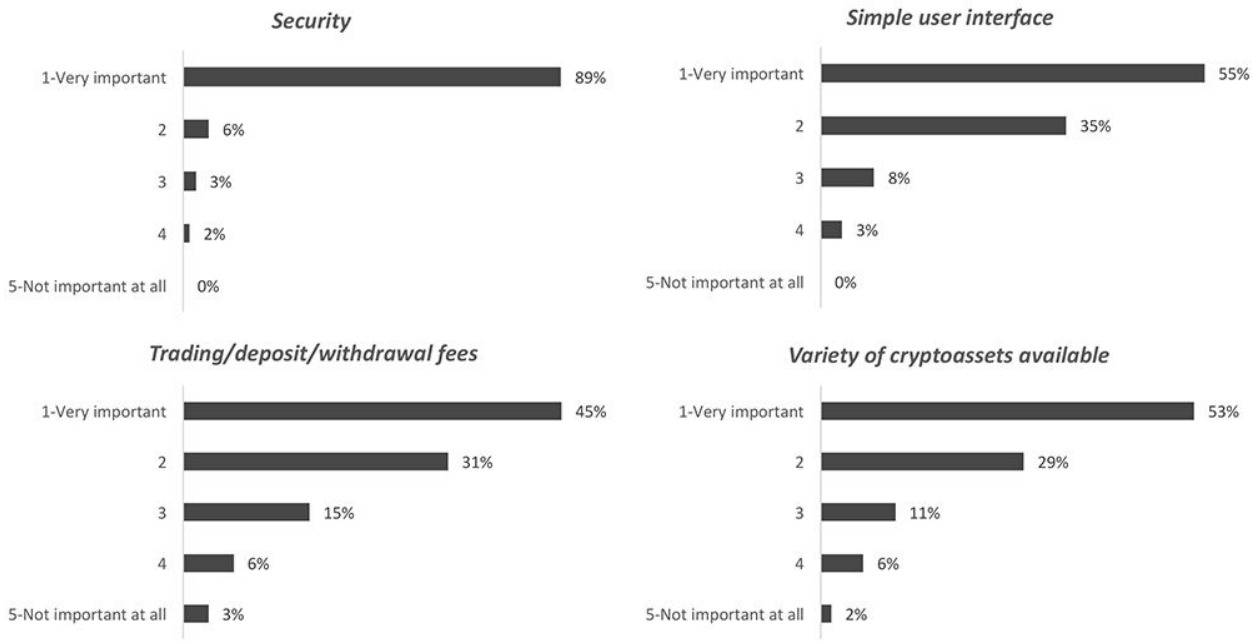
The company has engaged MBA students to perform primary and secondary market research on the digital asset exchange industry as part of the Applied Management Research program at UCLA Anderson School of Management. This appendix contains the summary of their findings.

Primary Research Details

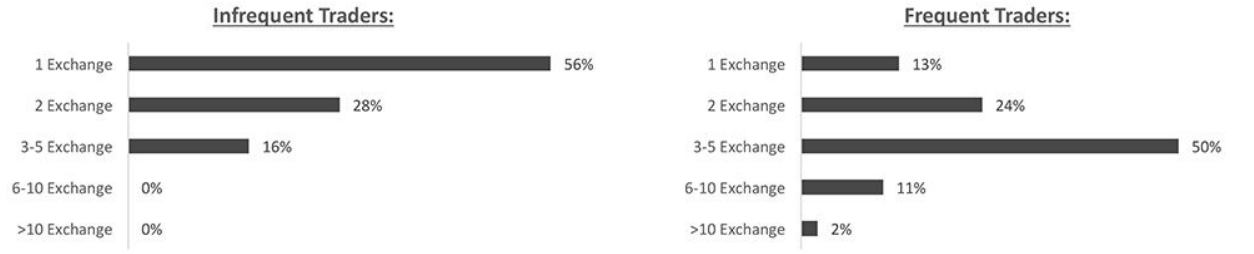
- Period: November 20, 2017 to January 07, 2018.
- Seeking only respondents who have purchased crypto assets.
- The 95% confidence interval for the frequent traders population proportion is 0.561 to 0.919.
- The 95% confidence interval for the infrequent traders population proportion is 0.218 to 0.513.

Responses Summary

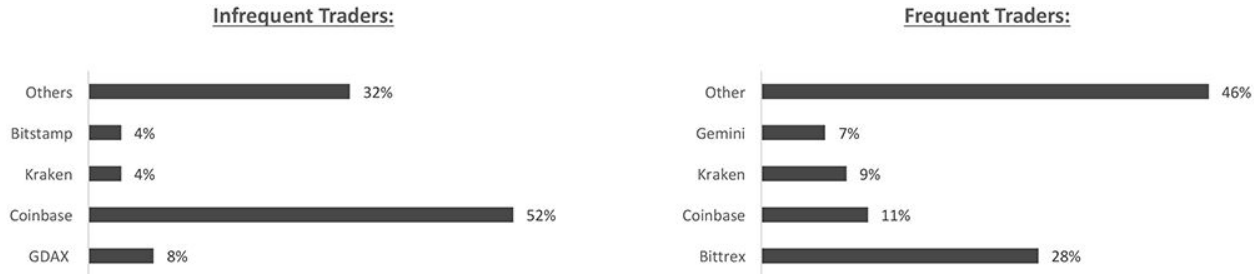
How important is a feature listed below to selecting an exchange you predominantly use?



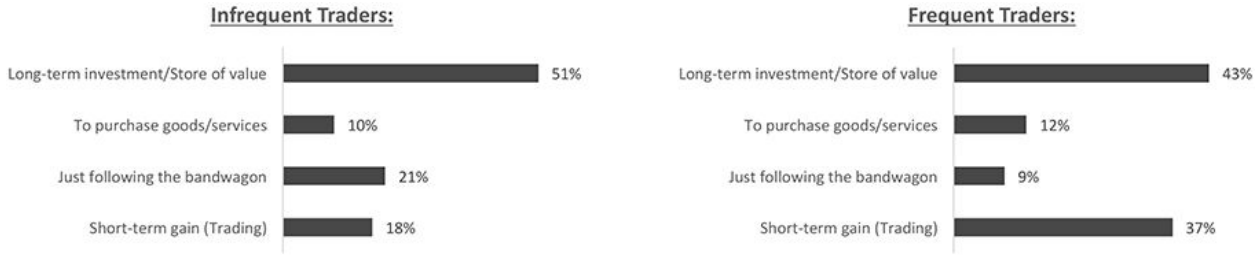
How many exchange platforms do you have an account with?



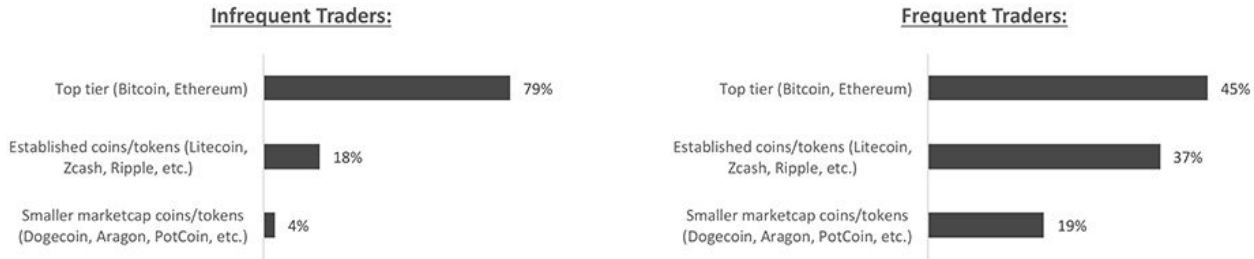
What is your favorite exchange?



For what purposes do you purchase crypto assets? (check all that apply)



Which types of coins/tokens do you usually invest/trade? (check all that apply)



Secondary Research Findings

Competitor Analysis

Platform	Trade Fee		Deposit Crypto	Withdrawal Crypto	Deposit Fiat			Withdrawal Fiat				Margin Trading		
	Maker Fee	Taker Fee			ACH	Wire	Credit Card	ACH	Wire	Paypal	Debit Card	Maker	Taker	Lending
Coinbase	1.49%	1.49%	free	only pay network fee	free	$10	3.99%	free	$25	3.99%	N/A	1.49%	1.49%	N/A
Bithumb	0.15%	0.15%	free	only pay network fee	N/A	free	N/A	N/A	1,000 KRW	N/A	N/A	N/A	N/A	N/A
Bitfinex	<= 0.1% Free if >$7.5M	<= 0.2%	free if>$1K	only pay network fee	N/A	0.1%	N/A	N/A	0.1% (1%for24hrs)	N/A	N/A	N/A	N/A	N/A
Bittrex	0.25%	0.25%	free	only pay network fee	N/A	free >$100k	N/A	N/A	free >$100k	N/A	N/A	N/A	N/A	N/A
Poloniex	<= 0.15% Free if >24K BTC	<= 0.25%	free	only pay network fee	N/A	N/A	N/A	N/A	N/A	N/A	N/A	<= 0.15% Free if >24K BTC	<= 0.25%	N/A
Coinone	<= 0.1% Free if >30T KRW	<= 0.1%	free	only pay network fee	N/A	N/A	N/A	N/A	N/A	N/A	N/A	0.15%	0.15%	15% of earned interest
HitBTC	0.1%	0.1%	free	only pay network fee	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
GDAX	<= 0.25% BTC, <=0.3% ETH	0%	free	free	free	$10	N/A	free	$25	N/A	N/A	<= 0.25% BTC, <=0.3% ETH	0%	N/A
Binance	0.1%	0.1%	free	only pay network fee	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
Korbit	<= 0.08% Free if >10T KRW	<=0.2%	free	only pay network fee	free	N/A	N/A	free	N/A	N/A	N/A	N/A	N/A	N/A
Kraken	<= 0.16% Free if >$10M	<=0.26%	free	only pay network fee	N/A	$5	N/A	N/A	$5	N/A	N/A	N/A	N/A	N/A
Bitstamp	<= 0.25%	<= 0.25%	free	only pay network fee 0.1% for bitgo instant	N/A	free	5%	N/A	0.9 EUR	N/A	2% or $10 if <$1000	N/A	N/A	N/A
bitFlyer	<= 0.15%	<= 0.15%	free	only pay network fee	756 JPY	$10	free	756 JPY	$10	N/A	N/A	<= 0.15%	<= 0.15%	N/A
Huobi	0.2%	0.2%	free	only pay network fee	free	1%	N/A	free	1%	N/A	N/A	0.1% for 24 hours		N/A
BTCC	0.1%	0.1%	free	only pay network fee	0.1%	N/A	5%	0.3%	N/A	N/A	N/A	N/A	N/A	N/A
Cryptopia	0.2%	0.2%										N/A	N/A	N/A
Gemini	<= 0.25%	<= 0.25%	free	only pay network fee	free	free	N/A	free	free	N/A	N/A	N/A	N/A	N/A
Bit-Z	0.1%	0.1%	free	0.5%	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A	N/A
BitBay	<=0.43%	<=0.3%	free	0.5%	N/A	free	N/A	N/A	0.35% (min$5.2 max$45)	N/A	N/A	N/A	N/A	N/A

Trading Fees (Top 20 Exchanges)

Volume Traded at Notable Crypto Exchanges

Name	24h trading volume[13]	Fiat-to-Crypto	Crypto-to-Crypto	Cryptoassets available	Centralized or Decentralized
Coinbase/GDAX	$1.4B	Yes	Yes	4	Centralized
Bitstamp	$1.0B	Yes	Yes	5	Centralized
Kraken	$1.3B	Yes	Yes	17	Centralized
Poloniex	$0.5B	No	Yes	68	Centralized
Gemini	$0.3B	Yes	Yes	2	Centralized
Bittrex	$0.8B	No	Yes	> 100	Centralized
Binance	$2.8B	No	Yes	> 100	Centralized
Bithumb	$2.7B	Yes	Yes	12	Centralized
Cryptopia	$0.04B	Yes	Yes	> 100	Centralized
Bitfinex	$2.6B	Yes	Yes	> 100	Centralized
Huobi	$1.1B	Yes	Yes	> 100	Centralized
EtherDelta	$0.008B	No	Yes	> 100	Decentralized