



# Liquid Technical Overview

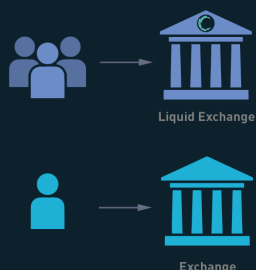
## Liquid Network

Liquid is an interexchange settlement network linking together cryptocurrency exchanges, brokers, and institutions around the world.

Liquid enables rapid, confidential, and secure transfer of funds between members of the network by innovating on top of Bitcoin and extending its features to securely, and privately transfer Bitcoin and other Issued Assets with no single point of failure. It consists of a federation of members which form the backbone of a global financial network powered by digital assets.

## Liquid Benefits

Liquid can be used by exchanges and financial institutions for a wide variety of applications. These applications can bring additional business and solve problems you may be facing.

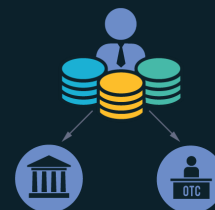


### 1. Increase Trading Volume

Exchanges who are part of the Liquid Network will increase trade volume and attract more customers by offering competitive spreads, greater liquidity, and low friction options for deposit and withdrawal.

### 2. Improve Liquidity

Brokers and OTC trading desks who are members of the Liquid Network can quickly source liquidity around the clock to fulfill customer demand and reduce volatility risk.





### 3. Expand Your Markets

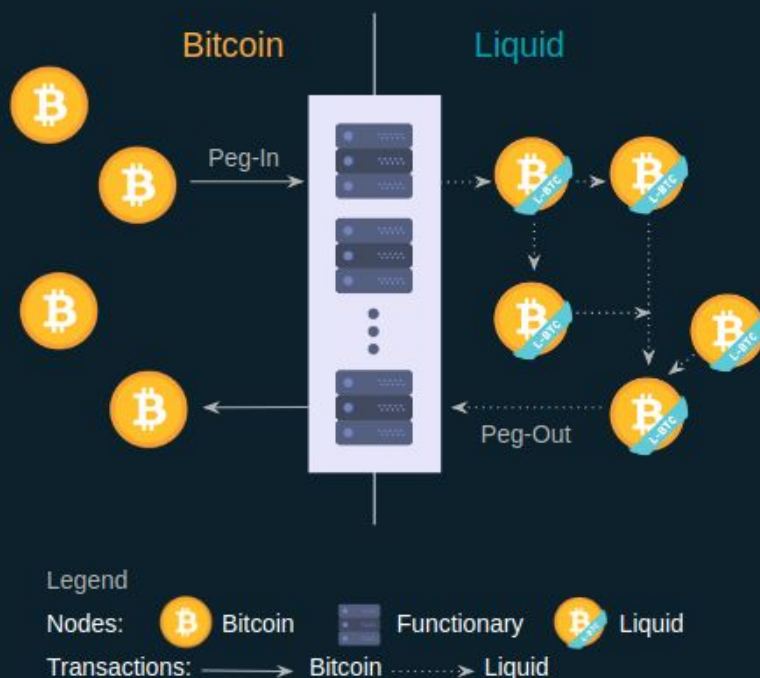
Exchanges can expand their markets by easily adding more cryptocurrency pairs to their order book via Liquid's Issued Assets functionality without needing to interact with other blockchains and incur the associated software development costs. This enables greater scalability without compromising security.

## Liquid Architecture

Liquid is a sidechain of Bitcoin that allows users of the Liquid Network to move Bitcoin between the two networks with a two-way peg. Bitcoin used in the Liquid Network is referred to as L-BTC, and each L-BTC has a verifiably equivalent amount of BTC secured by the Liquid members called functionaries.

### 1. Sidechain Basics

A sidechain is a mechanism that allows tokens from one blockchain to be used securely in an independent blockchain which runs in parallel and uses a different set of rules, performance requirements, and security mechanisms. On a sidechain, one can move tokens back to the original chain through a two-way peg. Sidechains enable new functionality that may have security trade-offs or as a way to test new features that may not be ready for use on the parent blockchain.



## 2. Functionary Roles

The Liquid Network is operated by its members - large exchanges and financial institutions that benefit from its use. Blockstream has no control of the network and serves only as a technology provider. With no single entity in control, there is no longer any single point of failure.

Liquid uses an approach to consensus called Strong Federations. A Strong Federation removes the need for costly Proof of Work mechanisms and replaces it with the collective actions of a group of mutually distrusting participants called functionaries.

These functionaries each serve two roles on the network - as **block signers** they operate the Liquid sidechain, and as **watchmen** they secure Bitcoins held by the Network.

## 3. Block Signers

Liquid's block generation occurs every minute. This means that Liquid's block generation is more consistent than Bitcoin's (which has probabilistic generation). Block signers keep track of the block height they have signed along with its parent and refuse to sign blocks that would result in a reorganization of more than one block. Once a block has been created, its parent block will never be reorganized from the longest chain, which is why Liquid transactions can be considered final once they receive two confirmations. Liquid transactions will settle between two and three minutes when the network is functioning normally.

Liquid's federated model requires blocks to be signed by at least two-thirds of all block signers. Block signers take turns proposing a new block every minute in a round-robin fashion, and other functionaries sign that block after validating its contents. Blocks will be created every minute when the network is functioning normally. However, it is possible that network instability or missing functionaries can result in some block rounds being missed. When fewer than one-third functionaries are offline, the network can continue. When the offline functionary becomes the block proposer of a round, that round will fail, which will result in no block being created during that interval.





If one-third or more of the functionaries are no longer operating, blocks will no longer be signed and the Liquid blockchain will be frozen until at least two-thirds of the functionaries come back online. Once a quorum of functionaries are communicating, block creation will resume.

## 4. Watchmen

One of the two duties of a functionary is to serve as a watchman. In this role, the functionary is responsible for managing and securing the Bitcoin held by the federation.

## 5. Peg-in Transactions (Bitcoin to Liquid)

Moving funds from Bitcoin to Liquid is called a peg-in; a member of Liquid sends Bitcoin to an address generated by the Liquid client software and then creates a peg-in transaction on the Liquid Network to claim its equivalent Liquid Bitcoin (L-BTC) from the Liquid Network. A peg-in transaction requires 102 confirmations on the Bitcoin network before the funds can be claimed on the Liquid Network. This high level of security is



- 1 Liquid User sends BTC over Bitcoin Network to peg-in address.
- 2 Liquid User waits for 102 confirmations and then requests L-BTC from the Liquid Network.
- 3 Liquid User claims L-BTC and it appears in their Liquid Wallet.

required to protect all participants' funds in the event of a large block reorganization of the Bitcoin blockchain.

## 6. Peg-out Transactions (Liquid to Bitcoin)

The peg-out process moves funds from Liquid back to the Bitcoin blockchain. These transactions are processed by the watchmen in batches every fifteen minutes.

For added security, the watchmen will only send Bitcoin to an address under the control of an authorized user. This is done through the use of a Peg-out Authorization Key (PAK). Functionaries control a list a of PAKs that can be updated throughout the network operation to determine which users are authorized to make a peg-out transaction. In order to protect Liquid from unauthorized withdrawals, it takes three days to update the PAK list. This allows the

network to detect an attacker that is able to compromise a set of functionaries before the attacker is able to make a withdrawal to their own wallet. PAK entries are linked to a BIP32 (Hierarchical Deterministic) Wallet owned by the user. Liquid users create a peg-out transaction proving that their address is derived from one of the PAK entries without revealing any additional identifying information.



- 1 Liquid User creates a peg-out transaction to request release of BTC.
- 2 Liquid Network releases BTC after 2 Liquid confirmations.
- 3 Liquid User receives BTC into Bitcoin wallet.

## 7. Emergency Recovery Procedure

The watchmen require a greater than two-thirds threshold to spend funds in Liquid which provides sufficient security for byzantine fault tolerance. If one-third or more of the network is ever unable to continue operating, the network would stall and the funds held would be locked up forever. To avoid this, all funds held by the Liquid Network are also accessible by a set of three emergency keys when the network has been non-functional for thirty consecutive days. These keys cannot be used to spend any funds when the

network is operating correctly. Two of the three emergency keys can then be used to access funds held by the Liquid Network so that they can be distributed back to their owners' authorized wallets. These keys are held in separate, secure locations to avoid a single point of failure.

## 8. Functionary Hardware Overview

The functionary server itself consists of two components - the host server and a key storage module. The host is a standard server that is used to run a full Bitcoin and Liquid node and communicates with the other functionaries over Tor. Tor is used by the functionaries to ensure that all communications between the functionaries do not contain IP addresses which could lead to members of the network being subject to denial of service attack, and to avoid disclosing the physical location of the servers. The host is responsible for proposing blocks and staying in sync with each of the other functionaries. Attached to each host is a key storage module that is connected via a limited interface. No block signing or watchman key material is ever stored on the host to limit the ability of a remote attacker compromising the network. The host is configured to only allow incoming SSH connections when a button is pressed which allows for authorized users to connect and perform updates to the software or PAK list. This protection means that physical access to the functionary server is required to perform any changes.

The key module does additional validation before signing blocks or creating Bitcoin transactions. The key module also ensures that Bitcoin spent from the network only is spent to a set of authorized users.

It is recommended to have physical access restricted to the functionary server in order to avoid tampering. The functionary server must be installed on a private network with unrestricted outgoing connections. Liquid wallets and transactions are managed through separate Liquid node software that will connect directly to your functionary.

## 9. Participating Without a Functionary Server

The Liquid Network consists of a fixed group of functionary members that is defined at launch. Other Participants will connect to the Liquid Network by using pseudo-functionary nodes that connects to all the functionaries in the network. Participant members will then have the ability to perform transactions, peg-in, peg-out and fully validate the Liquid blockchain, but without being responsible of securing the network

	Functionaries	Participants
Secure the Network	✓	✗
Peg-In (BTC to Liquid)	✓	✓
Peg-Out (Liquid to BTC)	✓	✓
Perform Transactions	✓	✓

## Using Liquid

### 1. Confidential Transactions

Liquid uses Confidential Transactions, which hides the amounts and asset types within transactions from all third parties. This information is only known by the parties involved in the transaction and other third parties they designate. Liquid transactions use confidential addresses that include a public blinding key and a base address. Only the receiver alone can decrypt the amount sent in a transaction. The receiver can share the private blinding key with any third party in order for that party to be able to validate the amount and asset type.

`ee6bb46e4aa6f2dd684a8858c81e46a0d9107208a3e9deaad1ec6b7e8c7df912`

ADVANCED DETAILS +

2dkvfKccem5bEVHyLribzXpRjGPGzct1umF

2dkBre95QZ4HPV7fTmy59QPRp1LoPFBWfRe

→

2dkXebd7Z8SCyrqQcRi34Q43wwG1zumoCEK  
Confidential

2dk8kPaiGuDHtXVZgizC4b8XN8HHEQMAjQT  
Confidential

Fee0.00038882 BTC

TRANSACTION TIME  
PDT

Tue, 26 Jun 2018 11:42:10

316 CONFIRMATIONS

CONFIDENTIAL



Liquid transactions include a transaction fee that is used as a denial of service protection mechanism. Transaction fees are a minimum value of 1 satoshi/vbyte, but can rise if network congestion increases. Liquid transactions are larger than similar Bitcoin transactions due to “range proofs” that must be included in Confidential Transactions and are used to prove that no outputs are negative values.

## 2. Issued Assets

Liquid allows for users to create and transfer other assets using a feature called Issued Assets (IA). These assets can enable applications such as tokenized fiat, tokenized non-BTC cryptocurrency, digital collectibles, reward points and attested assets (e.g. gold coins). The obligations under an IA belong to the issuer and Liquid does not verify whether the underlying asset exists or is properly maintained (in contrast to the BTC peg-in procedures).

Issued Assets in Liquid are given a unique identifier (64 hexadecimal characters) when created. For example, an asset created in Liquid might be created with the id “243dcf927316a91f01dfd4672337ee1d5cd947417bdc9aacd29b3b529c633d3d”. There is no global human readable naming scheme for assets. Users who wish to label this asset can do so in their wallets. Each asset type can optionally be configured to allow reissuance by generating reissuance tokens when it is created. Assets in Liquid can also be also be verifiably destroyed by their owner to reduce the supply.

The reissuance tokens are used to prove authority and reissue more of the newly created asset at a later date. These tokens can be set up with a multisignature scheme generally described as being “m of n”. That means that the reissuance transaction requires a group of “m” keys in order to create new tokens.

## 3. Common Scenarios

Issued Assets can be used for many different purposes, but some of the most commonly requested ones include tokenized fiat, tokenized equities, and tokenized cryptocurrencies.

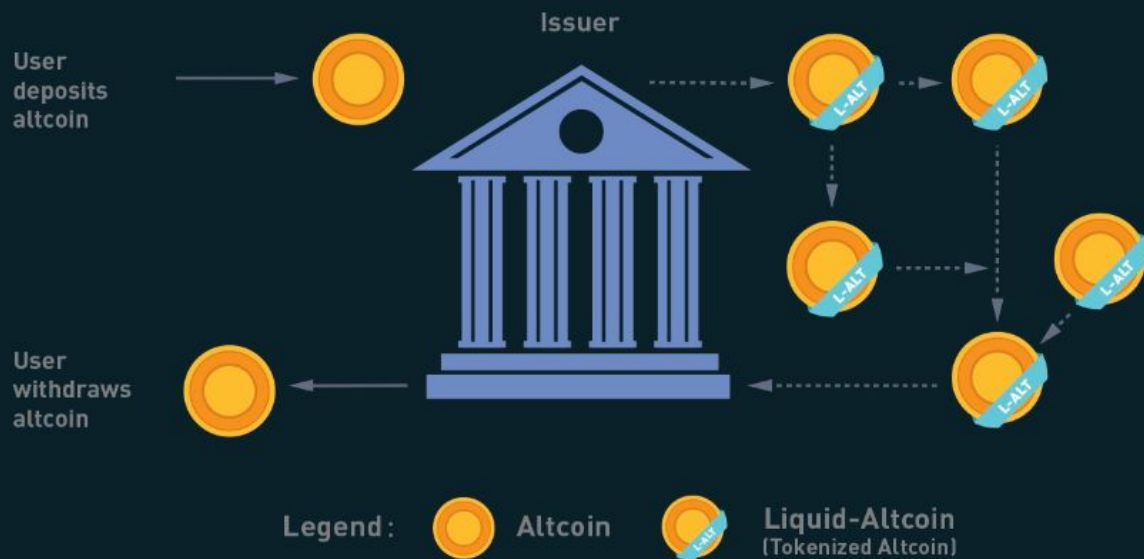
## 4. Tokenized Fiat

In this scenario, fiat currency is deposited in a bank account and held in trust of an issuer. The issuer generates tokens in Liquid representing the amount of money in that account and distributes the tokens to the depositors of the account. If the owner of one of these

tokens wishes to receive fiat currency in return for it, he may redeem through the issuer. The issuer can then destroy the token and maintain an equal supply of fiat currency and outstanding tokens. As more fiat currency is deposited into the account, additional tokens can also be issued by the issuer. The issuer can prove to any auditor or regulator that the amount of outstanding tokens always matches the balance of the bank account. Issuers can also choose to use the scripting feature of Liquid to comply with different regulations around the world without adding any artificial requirements to the functionaries.

## 5. Tokenized Cryptocurrencies

While Liquid supports Bitcoin through its Federation, other cryptocurrencies are not natively supported. Very few cryptocurrencies have the track record for stability and security as Bitcoin and it would be risky to include them as part of the consensus rules of the system. Instead, Liquid members can create a token that represents a collateralized cryptocurrency. These tokens can now be traded and settled between Liquid users with the same speed and privacy as Bitcoin and other Issued Assets. This approach also allows exchanges and traders to safely handle these assets without ever needing to support the underlying asset. This removes the amount of work needed to support extra blockchains and clients when supporting other assets. Owners of these tokens could then take the issued token and redeem it from the issuer. This opt-in model allows for users who wish to benefit to work with parties they trust to issue and secure the assets without requiring the entire federation to know about the asset.



## 6. Unique Tokens and Digital Collectables

Liquid can be used to track unique items such as ordered prints by an artist or digital collectables like a set of CryptoLions. You can track unique assets using Issued Assets by issuing a single individual token for each individual asset. The issuer would then keep track of the asset ids that are created and provide a registry to help identify which asset is associated with which digital collectable. There is no way to natively categorize or group assets in Liquid, although wallet software could support this use case.

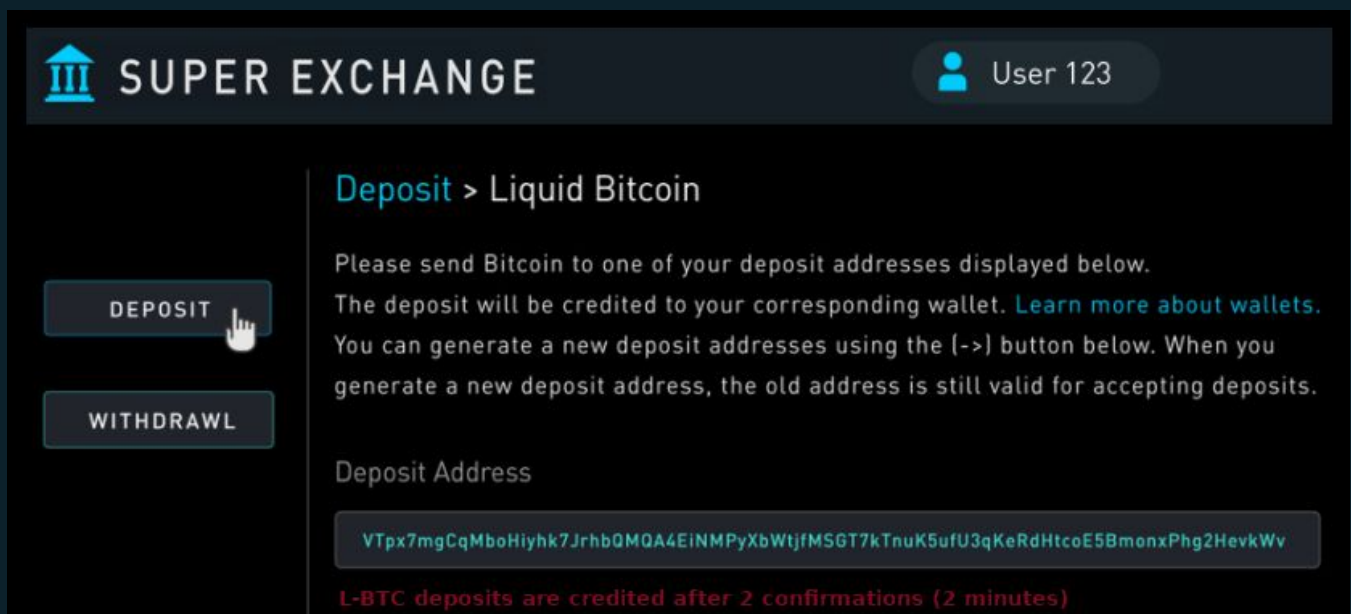
## 7. Integration Overview

Liquid extends the existing Bitcoin codebase. Users who are already familiar with using the Bitcoin RPC API will be able to easily integrate Liquid into their existing business systems. There are many wrappers for the RPC API in many languages such as Python, Go, Javascript, and others can work out-of-the-box with Liquid's API.

## 8. Allowing Rapid User Deposits and Withdrawals

Using Liquid, exchanges may offer the ability for their users to quickly and privately deposit and withdraw funds. To do this, exchanges will hold a portion of funds on the Liquid Network. When a user wishes to deposit on an exchange, they will request a Liquid

deposit address to be generated on their behalf by the exchange. The exchange will then generate a unique Liquid deposit address for this customer. The customer will then take this address to another exchange and request a Liquid withdrawal. The sending exchange will deduct the balance of the customer and send the funds through Liquid to the receiving exchange. When the transaction receives two confirmations, the receiving exchange can credit the user's account without the risk of having a double-spend, typically in less than three minutes from when the original transaction was sent.



The screenshot shows the 'SUPER EXCHANGE' interface for 'User 123'. On the left, there are two buttons: 'DEPOSIT' (highlighted with a hand cursor) and 'WITHDRAWAL'. The main content area is titled 'Deposit > Liquid Bitcoin'. It contains the following text: 'Please send Bitcoin to one of your deposit addresses displayed below. The deposit will be credited to your corresponding wallet. [Learn more about wallets.](#) You can generate a new deposit addresses using the [->] button below. When you generate a new deposit address, the old address is still valid for accepting deposits.' Below this text, there is a section labeled 'Deposit Address' with a text box containing the address: 'VTpx7mgCqMboHiyhk7JrhbQMQA4EiNMPyXbWtjfMSGT7kTnuK5ufU3qKeRdHtcoE5BmonxPhg2HevkWv'. At the bottom, a red message states: 'L-BTC deposits are credited after 2 confirmations (2 minutes)'.

## 9. Institutional Traders Using Liquid Wallets

Without Liquid, traders must split their funds allocated on different exchanges in order to take advantage of advantageous situations that may emerge within markets. This leaves the trader open to the risk of losing funds on a compromised exchange, and limits the amount that can be traded due to the elongated process of moving funds to another exchange. Moving funds between an exchange can take over an hour, letting trade opportunities potentially slip away.



With Liquid, traders can hold their funds in their own wallet within Liquid and send very quickly to any exchange that supports Liquid deposits to trade within minutes. In this scenario, an exchange sees a trading opportunity at Exchange A and can quickly deposit in around 2 minutes onto an exchange. Once trading is complete, the trader can now move the funds back to their own Liquid wallet or to another exchange. Custodial risk is now moved from a single exchange to the entire Liquid federation.



## 10. Balance Management and Securing Funds of Liquid Members

Liquid members should maintain an appropriate balance of L-BTC based on their needs. If their balance rises too high compared to their needs, L-BTC can be pegged-out into their Bitcoin wallet. If their Liquid balance get too low, they can peg-in Bitcoin to maintain an adequate balance.

Like Bitcoin, Liquid supports multi-signature transactions. You can use your existing infrastructure to secure and transact with L-BTC and Issued Assets. Like Bitcoin, Liquid



allows users to use hot and cold storage to reduce the risk of attack on L-BTC and Issued Assets. Using combinations of multi-signature transactions and hot and cold storage helps you manage your risk appropriately.

## Summary

Liquid is the first production sidechain to solve problems experienced by exchanges, brokers, and traders when dealing with the transfer of large quantities of Bitcoin without introducing a single point of failure. The innovations of Confidential Transactions and Issued Assets enable large institutional investors to meet their business needs without compromising privacy and take advantage of rapidly changing trading conditions. Exchanges now can offer their customers a faster deposit experience to allow faster trading. Financial institutions can take advantage of the most private and secure blockchain to allow settlement at speeds that were not previously possible. Liquid is redefining the possibilities available to exchanges and financial institutions in speed, privacy, and security.

## Additional Information

Visit our website <http://www.blockstream.com/liquid> or contact us at [liquid@blockstream.com](mailto:liquid@blockstream.com) for more information on how to participate in the liquid Network

## Further Reading

[Strong Federations](#)

[Confidential Assets](#)