Liquid

by Blockstream

Blockstream

Contents

What is Elements?

Free software project

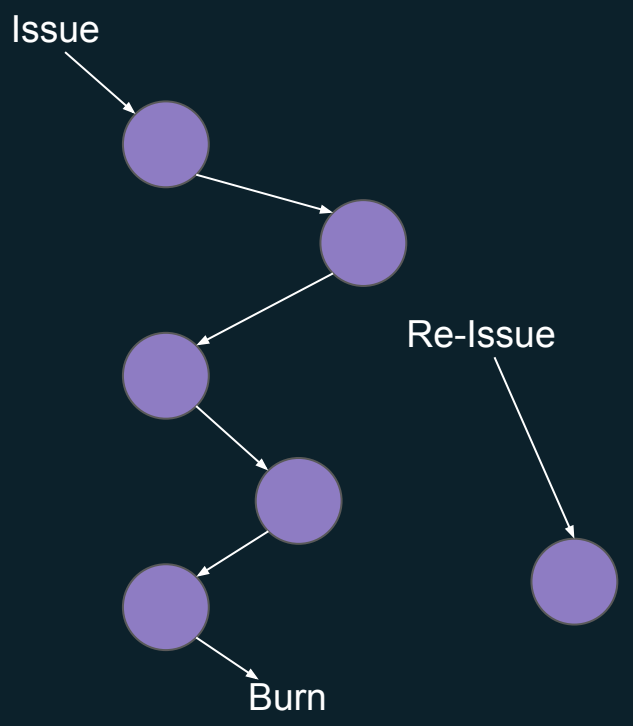
- Software Fork of Bitcoin Core https://github.com/ElementsProject/elements
- Enables creation of chains and sidechains (like Liquid)
- Proof of Work (PoW) is replaced with Signed blocks:

  More centralization, less resilience, less costs, better scalability and latency
- Federated two-way peg (for now, parent chain must use pow [SHA256])
- Confidential Transactions: amounts hidden to third parties
- Confidential Assets: asset ids are hidden to third parties

Elements: Features

Confidential Assets

- Users can issue, reissue, and destroy assets
- Asset type is optionally not visible to third parties
- Use Cases:
  - Tokenized fiat
  - Tokenized real asset
  - Other IOUs, vouchers...
  - Pegged alternative cryptocurrencies**



What is Liquid?

An Interexchange Settlement Network

- Faster trading and settlement times
- Enhanced privacy using Confidential Transactions
- Operated and controlled by the Liquid Federation, supported by Blockstream
- Custodial risk reduction through user wallets (currently liquid core's wallet, later GreenAddress)
- Issue and transact multiple assets*

Hardware + Software

- Functionary server that secures and operates the Liquid Network
- Wallet software to transact with other members

*Feature Under Development

Why Liquid?

Enable Faster User Deposits Between Exchanges

- Add additional liquidity to an exchange through rapid transfers
- Reduce volatility risk through rapid settlement
- Enhance privacy for transfers between exchanges

  (Outside parties can still validate that inputs and outputs contain same amount of each asset)

Remove Single Point of Failure for Custodians

- User wallets allow rapid transfers, eliminating need for storing bitcoin on exchanges for long

Future: Why Liquid?

Simplify Managing Multiple Assets

- Support rapid transfer of fiat currencies*
- Easily add new trading pairs and currencies included in Liquid*

On-chain trades and contracts

- Custodian-free trades between users using tokenized fiat*
- Multi-asset and multi-chain lightning*

*Feature Under Development

Liquid: Costs

Monthly Subscription Fees for functionaries and participants

- Includes support, software upgrades, hardware replacement

Network Fees

- Liquid uses transaction fees as DoS protection (1 satoshi/vbyte minimum)
- Bitcoin network fees when entering the network
- Used to fund peg-out transactions

User vs Participant vs Functionary

	User	Participant	Functionary
Able to Transfer L-BTC	✓	✓	✓
Able to Peg-In	✓	✓	✓
Able to Peg-Out	⛔	✓	✓
Signs blocks	⛔	⛔	✓

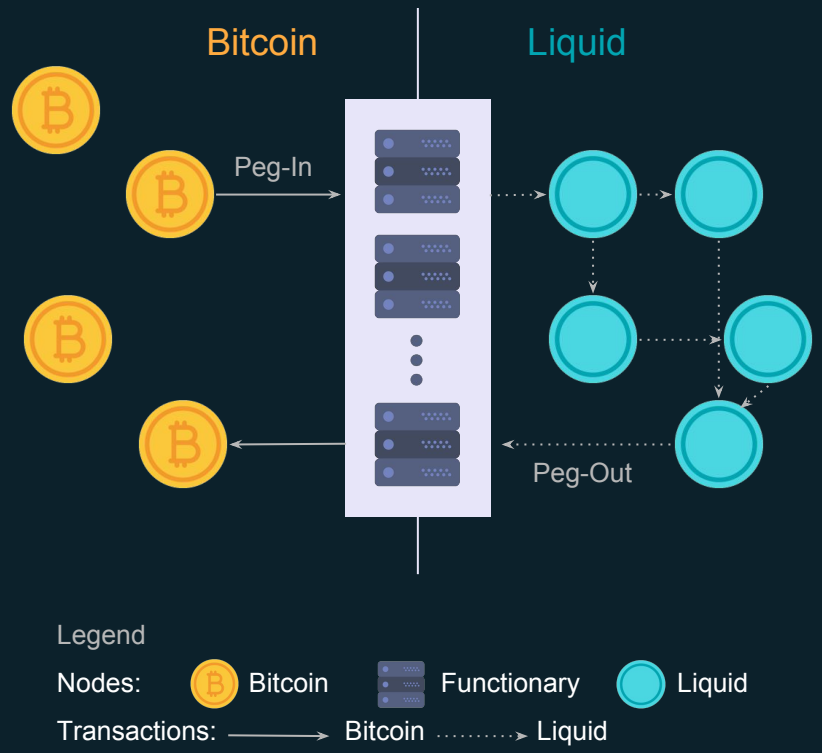
Functionary Duties

- Limited to 15 Members at launch, future versions will add more
- Secures Bitcoin in Liquid Network
- Signs Liquid Blocks
- Enforce Peg-Out Whitelist

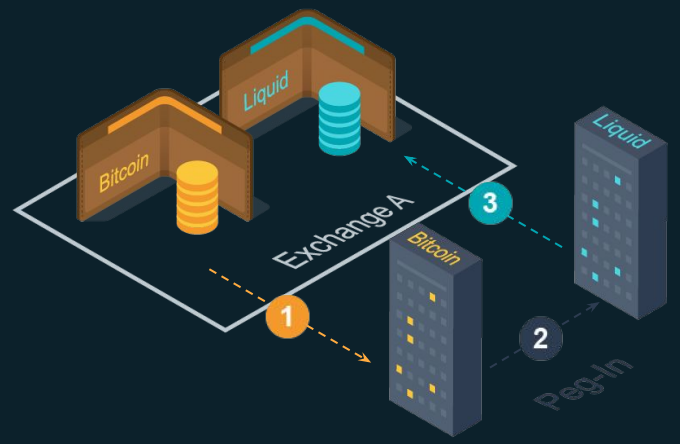
How It Works

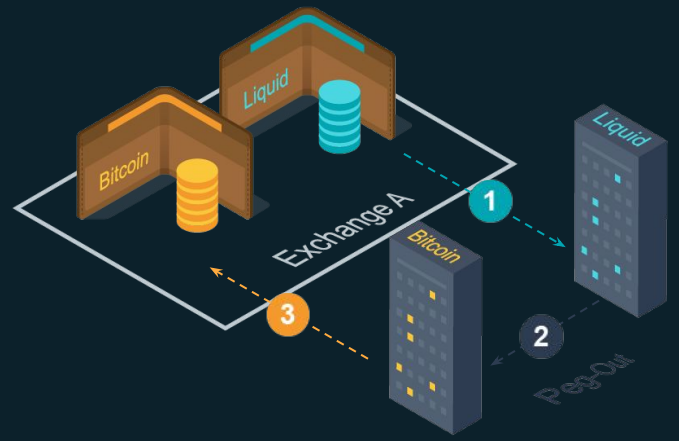
Liquid Federated Sidechain

- Parallel blockchain operated by Functionaries
- Blocks are signed by members instead of mined
- 1 minute blocks
- Requires >⅔ of functionaries to be online for blocks to be created
- Bitcoins can be moved between chains
- Confidential Transactions
- Confidential Assets



How It Works: Peg-In and Peg-Out

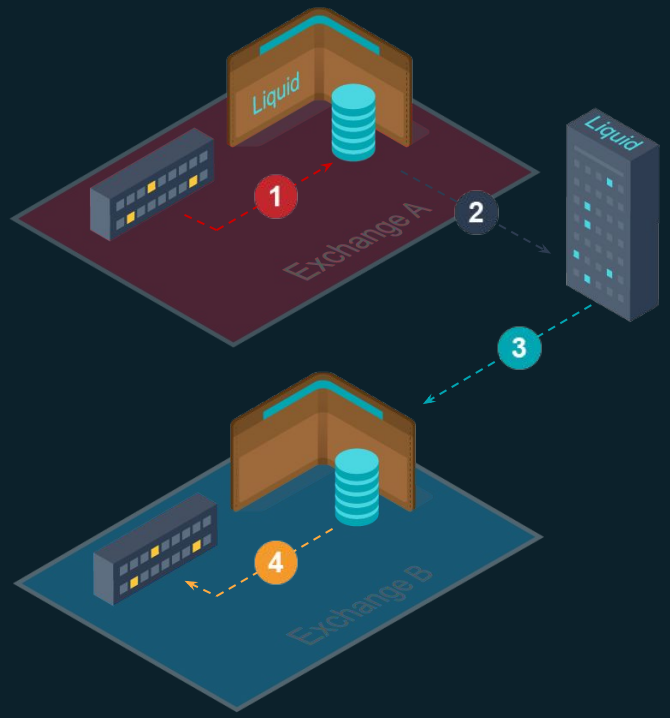




1. Liquid User Sends BTC over Bitcoin Network to peg-in address.
2. Liquid User waits for 102 Confirmations. Watchmen in Liquid Network now accept this freezing of bitcoin and allow access to L-BTC.
3. Liquid User claims L-BTC and it appears in their Liquid Wallet.

1. Liquid User creates a Peg-out transaction to unfreeze BTC.
2. Watchmen unfreeze BTC after 2 confirmations.
3. Liquid User receives BTC.

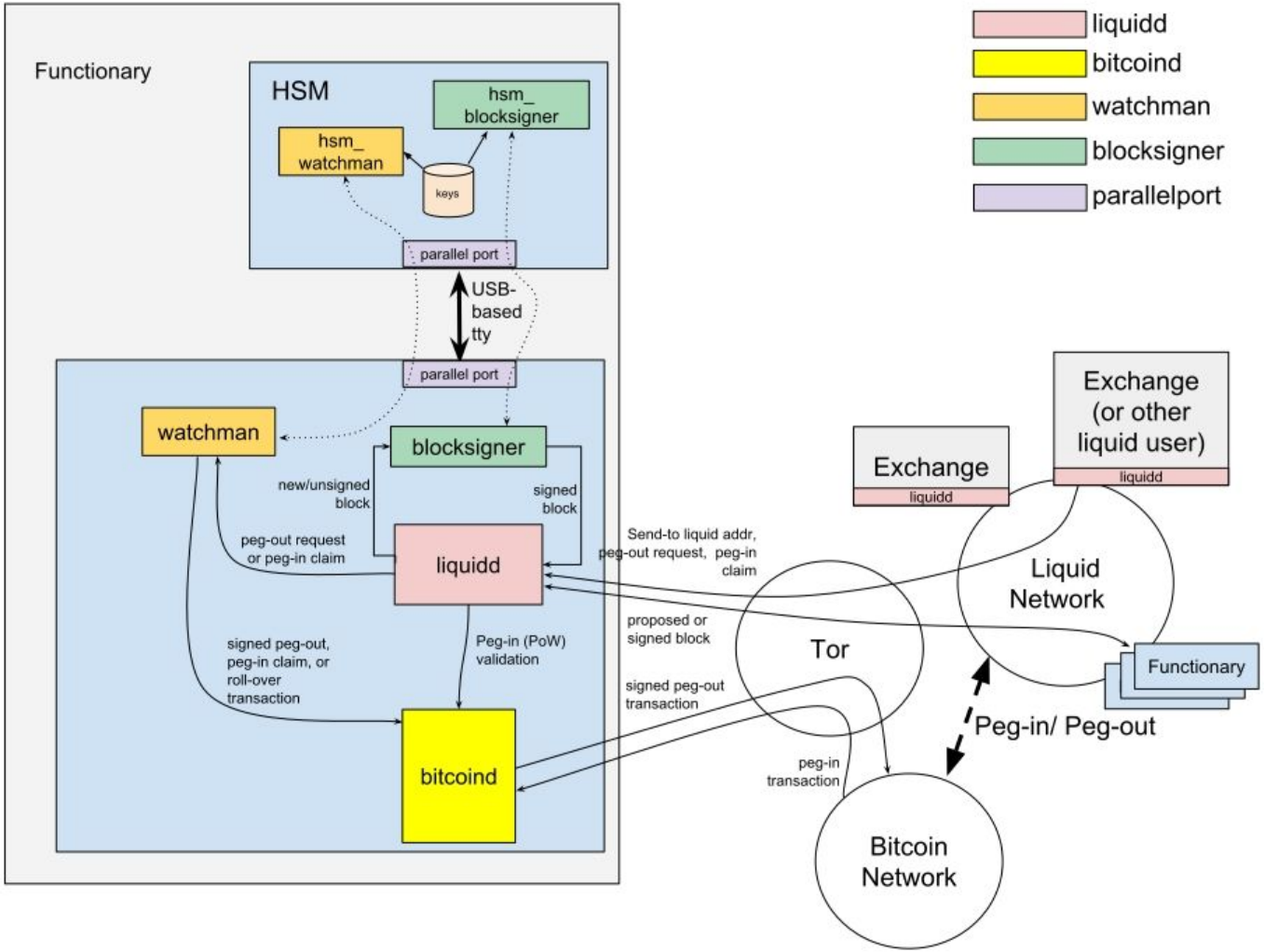
How It Works: Customer Interexchange Transfer



Simplest Liquid Exchange Integration

- Exchanges can have liquid hot wallets
- With a hot wallet, exchanges can allow L-BTC withdrawals
- Exchanges can allow users to have L-BTC balances explicitly
- “Move X BTC from exchange A to B”

1. Exchange A deducts customer BTC Balance in database.
2. Exchange A sends L-BTC from Liquid Wallet over Liquid Network.
3. Exchange B receives L-BTC over Liquid Network.
4. Exchange B credits BTC to customer in database.


liquidd
bitcoind
watchman
blocksigner
parallelport
Functionary
HSM
hsm_ blocksigner
hsm_ watchman
keys
parallel port
USB-based tty
parallel port
watchman
blocksigner
new/unsigned block
signed block
peg-out request or peg-in claim
liquidd
signed peg-out, peg-in claim, or roll-over transaction
Peg-in (PoW) validation
bitcoind
Send-to liquid addr, peg-out request, peg-in claim
proposed or signed block
signed peg-out transaction
peg-in transaction
Tor
Exchange
liquidd
Exchange (or other liquid user)
liquidd
Liquid Network
Functionary
Peg-in/ Peg-out
Bitcoin Network

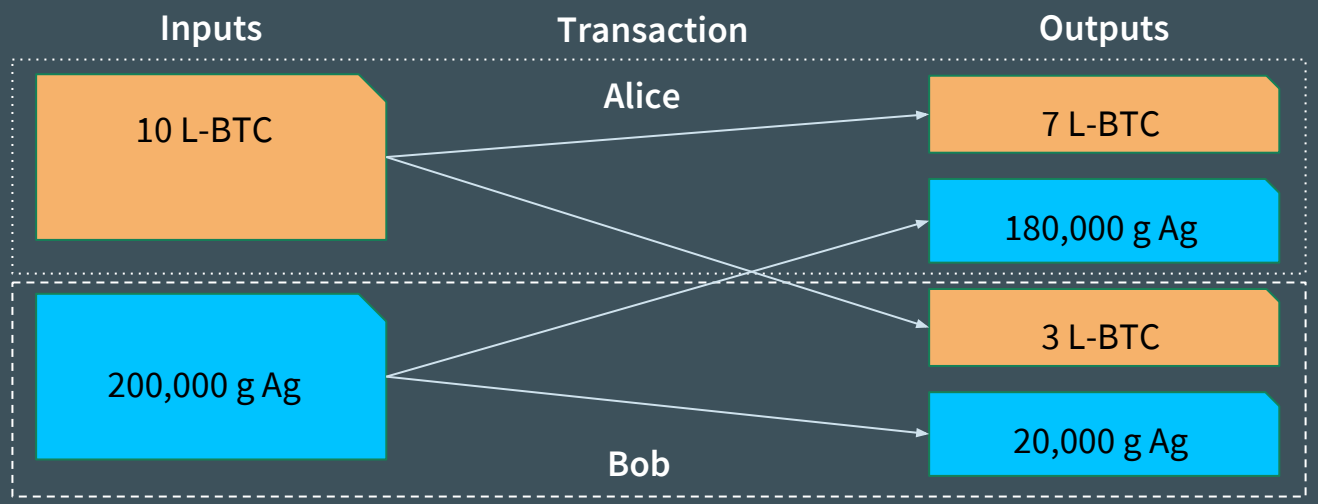
Questions?

liquid@blockstream.com

Appendix: Non-Custodial Trades Example

Atomic Swap

- Alice and Bob can create a trade where no escrow is required and neither party ever holds both assets until trade is complete



Appendix: Liquid vs. Lightning

Liquid Chain

- Lightning on Liquid is possible
- Suitable for larger transactions
- Confidential Transactions
- 1-minute confirmation times
- Transact any amount to any participant
- Fast settlement to Bitcoin dependent on functionaries
- Allows for hot and cold wallets

Lightning Network of payment channels

- Lightning on Liquid is possible
- Suitable for smaller transactions
- Onion routing
- Near-instant payments
- Transactions amounts and destinations limited by routing topology
- Fast settlement to Bitcoin dependent on cooperation of channel partner
- Requires hot wallet