Liquid

by Blockstream

Cryptocurrency Market Dynamics
Sessions, Oct 2019

Jonas Nick - jonas@blockstream.com

Blockstream

- **The Times 03/Jan/2009** Chancellor on brink of second bailout for banks

- **The Times 03/Jan/2009** Chancellor on brink of second bailout for banks
- ...
- **The Financial Times 23/Jul/2018** Trade dispute teeters on verge of currency war as Trump weighs in
- **The Global Times 05/Sep/2018** Social credit system China’s answer to credit crisis
- **The New York Times 05/Nov/2018** Important European Financial Firm Bows to Trump’s Iran Sanctions
- **The New York Times 28/Nov/2018** Two Words From Fed Chairman Jerome Powell Sent Markets Soaring

Bitcoin

Trust minimized
Nobody in control

Fixed Supply
Auditable

Censorship resistant
Inclusive and Global

Private
More so than fiat

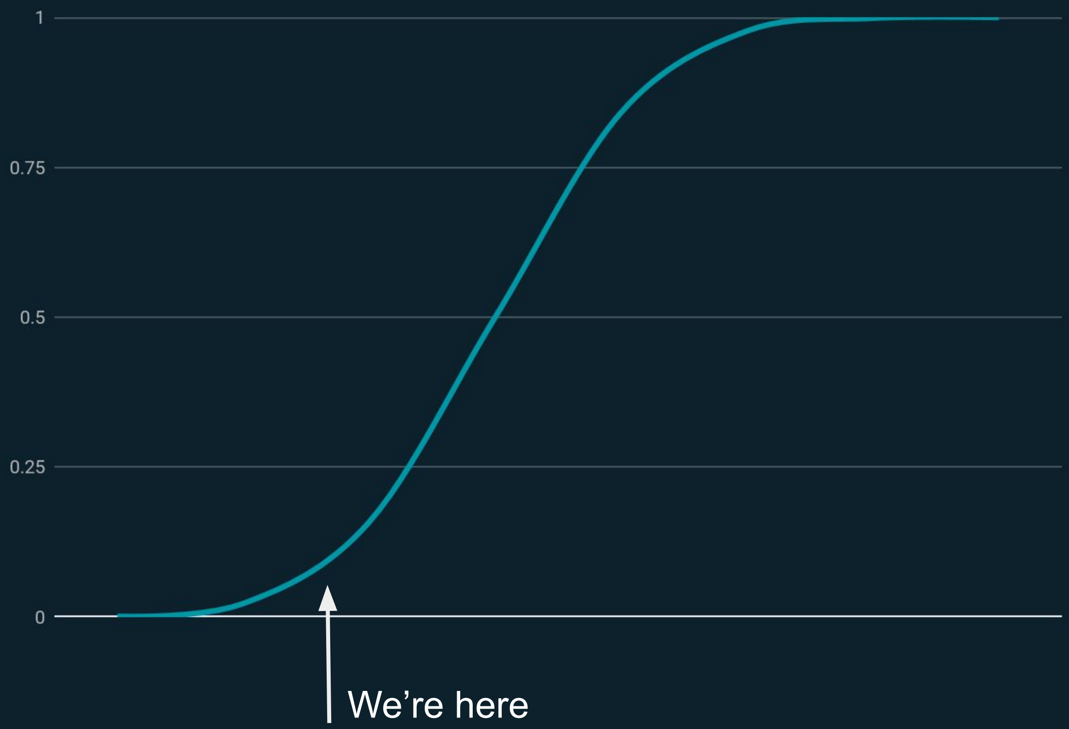
“But Bitcoin can’t work because X!”

FUD dice

“But Bitcoin can’t work because X!”

- Slow
- Expensive
- Not anonymous
- Programmability insufficient
- Volatile
- Custodial exchanges
- ...

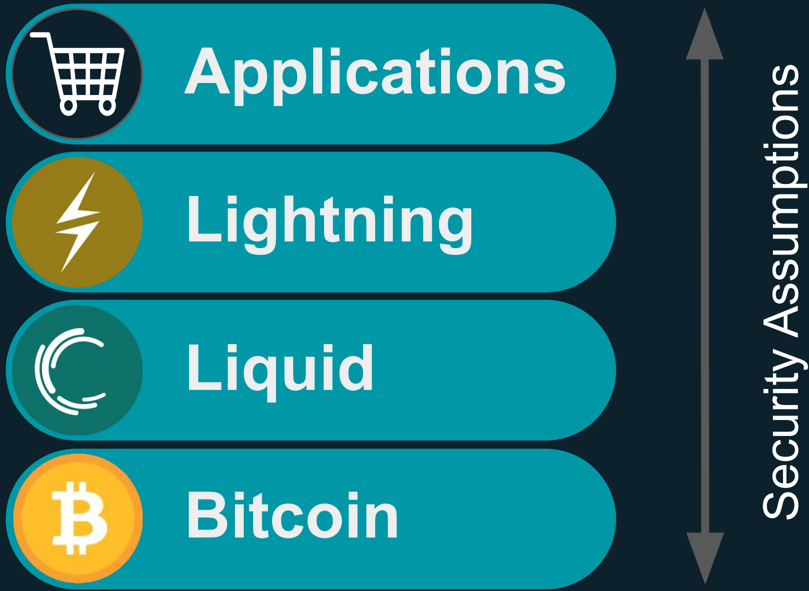
It does work! But it’s still early.



Why does it take so long?

Because above all, Bitcoin MUST remain decentralized, secure and resistant to change.

How to innovate on Bitcoin? In Layers



Applications

Lightning

Liquid

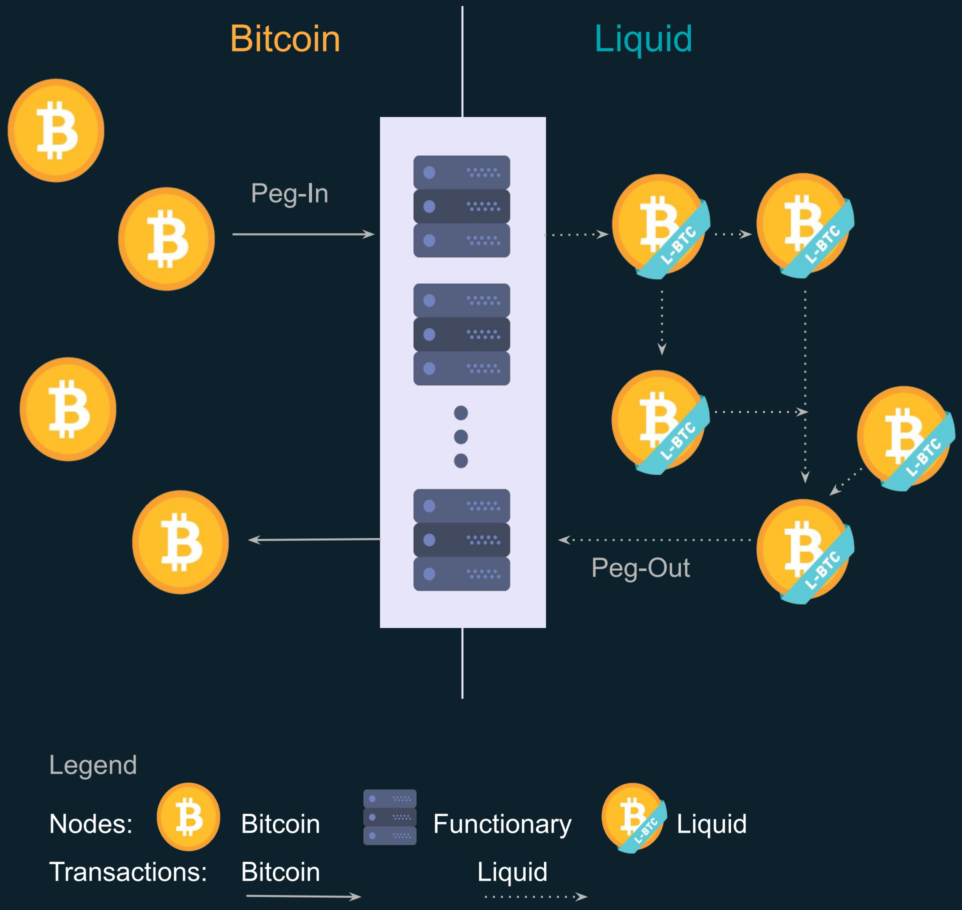
Bitcoin

Security Assumptions

How Liquid Works

Sidechain Basics

- Parallel blockchain operated by *Functionaries* without affecting the main chain
- Bitcoins can be moved between chains
- Different rules can exist on a sidechain



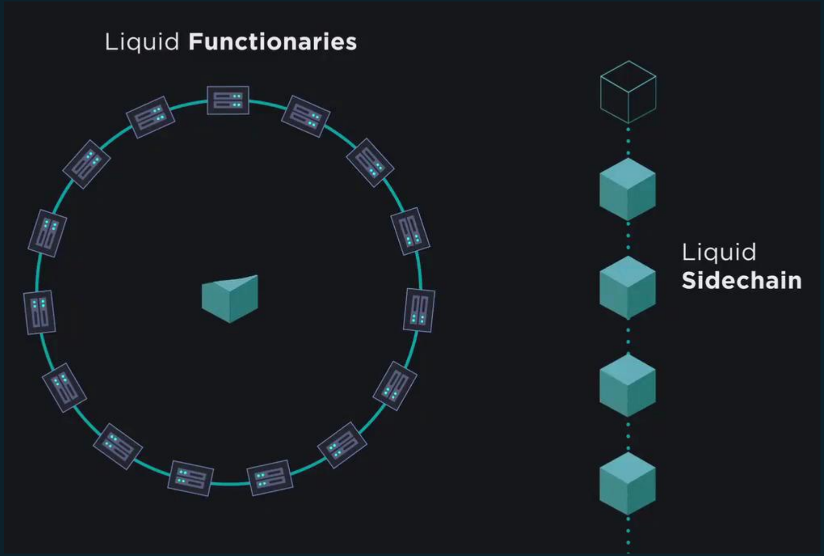
What is Liquid?

An Interexchange Settlement Network

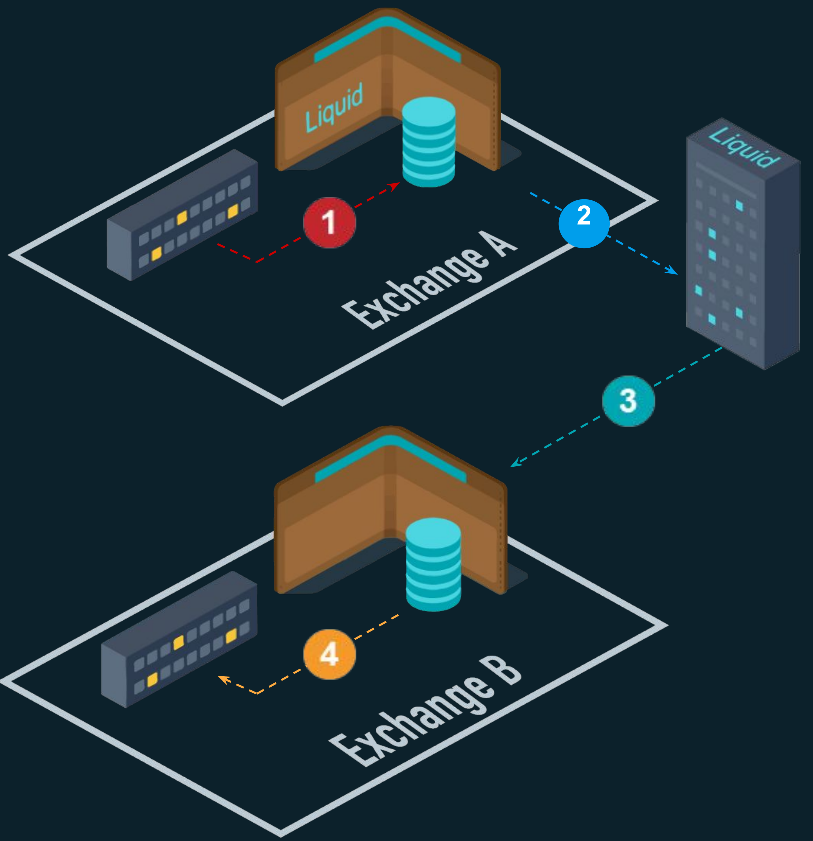
- addresses the needs of traders who use exchanges

1-Minute Block Times

- Blocks are signed by members instead of mined
- Creates predictable block times
- 2 minute settlement
- Reduced counterparty risk
- Improved capital efficiency



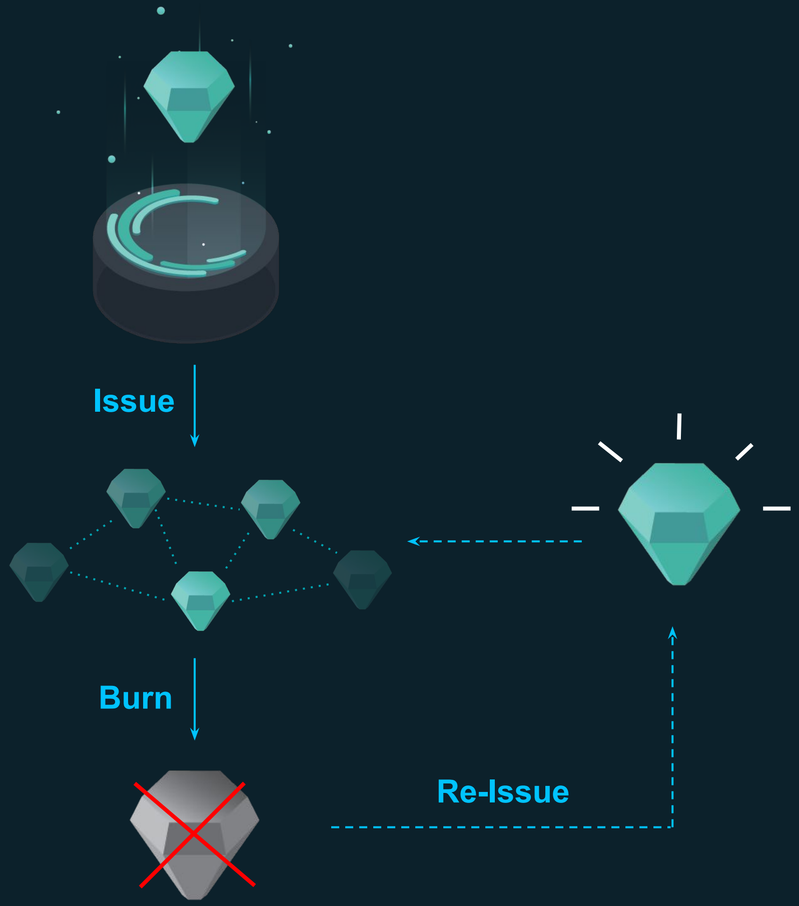
Customer Interexchange Transfer



Liquid Features

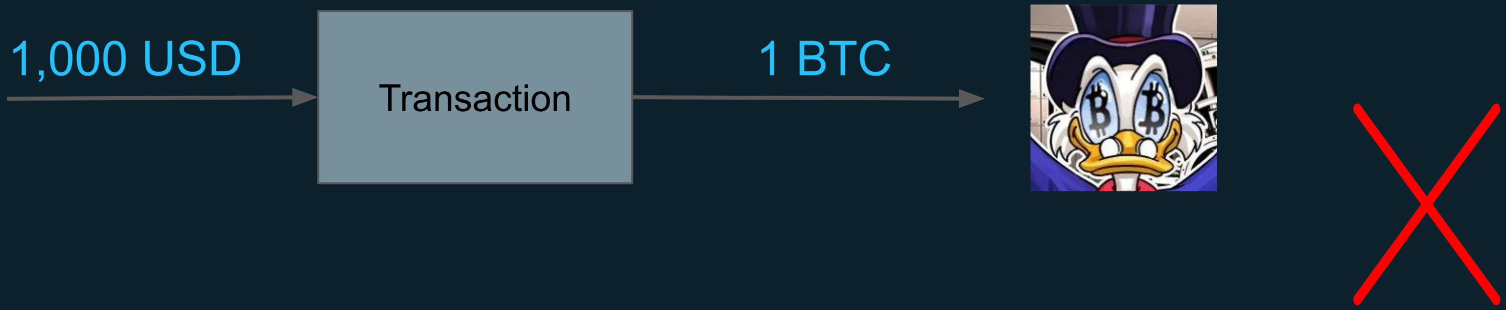
Issued Assets (IA)

- Users can create arbitrary assets
- Use Cases:
  - Tokenized fiat
  - Tokenized altcoins
  - Digital collectables
  - Attested assets
  - Utility tokens
  - Security tokens
- Users can issue, reissue, and destroy assets



Non-Custodial Trades Example

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



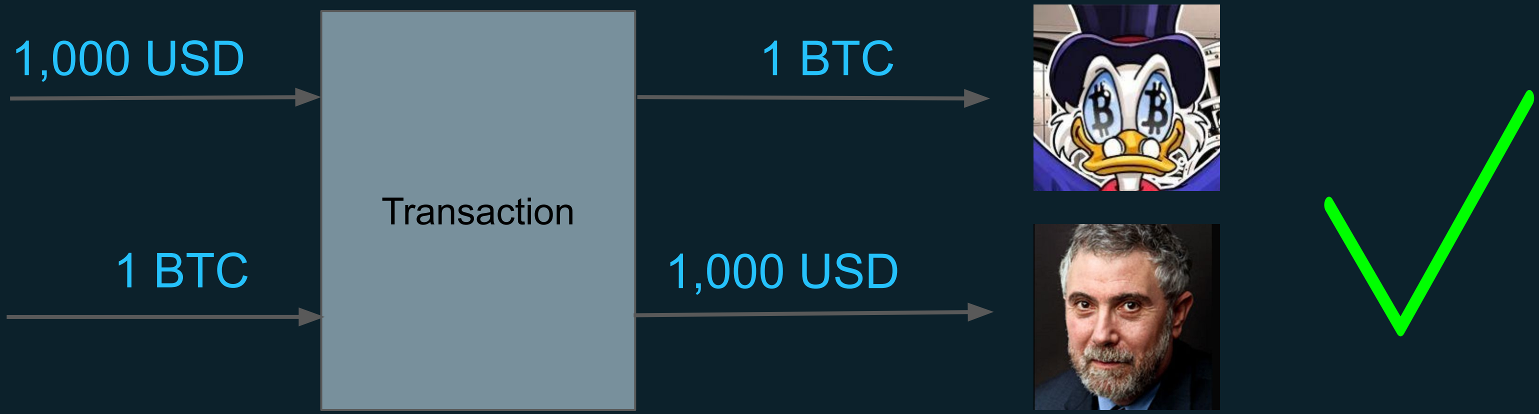
1,000 USD

Transaction

1 BTC

Non-Custodial Trades Example

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



1,000 USD

1 BTC

Transaction

1 BTC

1,000 USD

Issued Assets Comparison

Meta-Protocol Layers (ColoredCoins, Counterparty,etc…)

- x Requires processing entire blockchain
- x High fees during Bitcoin congestion

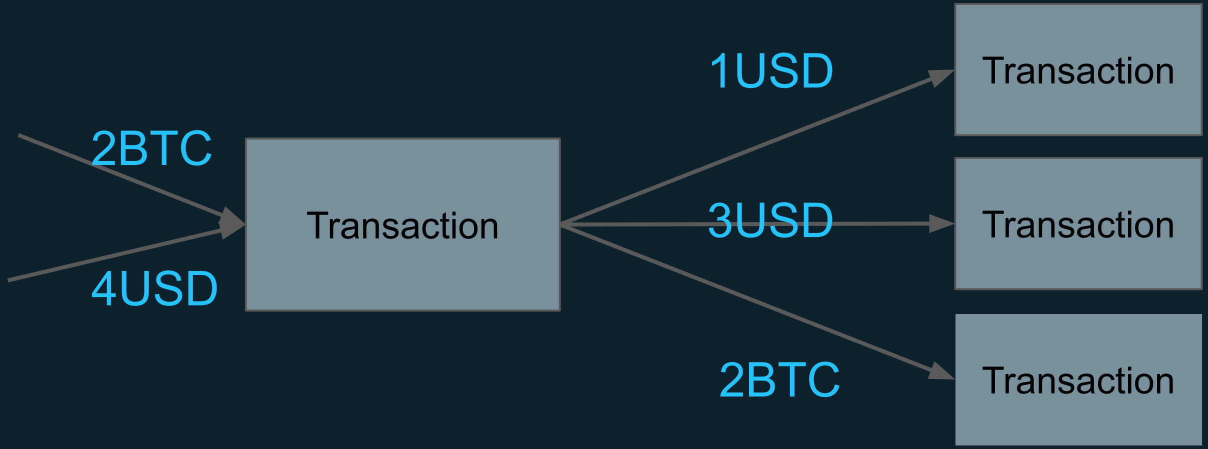
Tokens on Altcoins (Ethereum, …)

- x High fees during congestion
- x Insecure infrastructure
- x Centralized

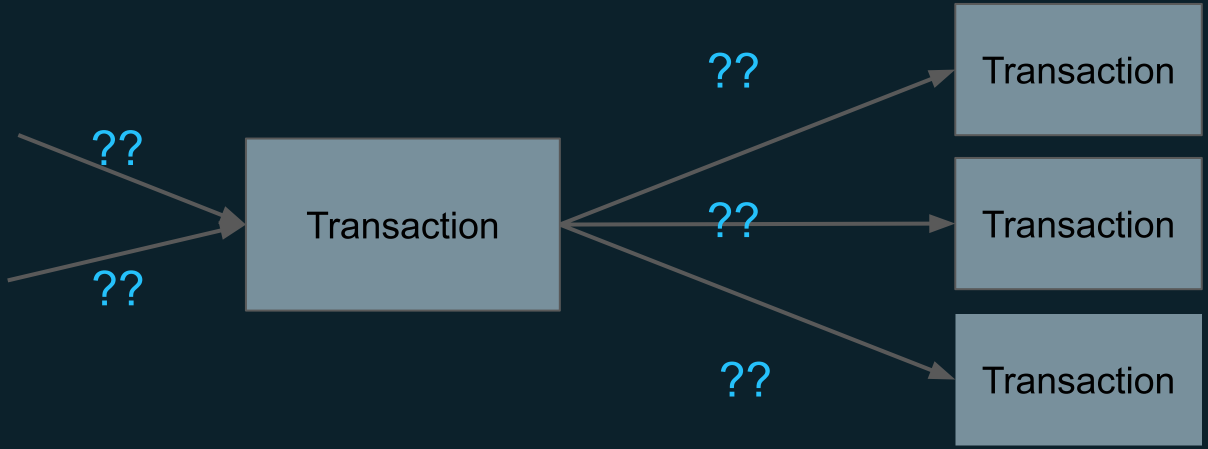
Liquid

- ✓ Secured by Liquid Strong Federation
- ✓ Built on Bitcoin
- ✓ L-BTC as native currency
- ✓ Allows non-custodial exchange
- ✓ Confidential Transactions

Non-Confidential Transactions



Confidential Transactions



Liquid Features

Confidential Transactions

- Transaction amounts and asset type are hidden to third parties
- Outside parties can still validate that inputs and outputs contain same amount of each asset
- Protects from exposure and front-running
- Auditable
- Simplifies classic Bitcoin mixing techniques such as coinjoin

Liquid Features

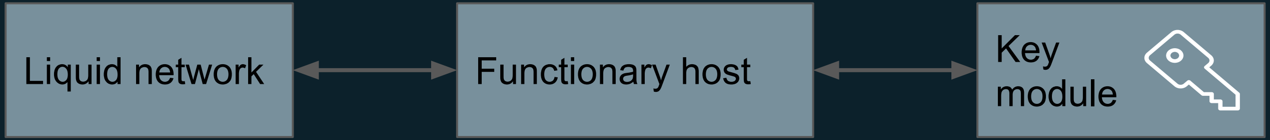
Elements
by Blockstream

Built on Elements which is built on Bitcoin

- Built on open source sidechain platform Elements
- Uses familiar Bitcoin API, easy to use tools from the Bitcoin world
- More powerful script language than Bitcoin, allowing covenants and key trees
- Quick adoption of new Bitcoin features

Trust Model

- Sidechain can be validated by every user. It's a public blockchain.
- BUT: functionaries can in principle reorganize chain
- BUT: functionaries can in principle steal bitcoins on the chain
  - Can't happen without detection
  - More than a third of functionaries have to be malicious
- Use separate hardware to store cryptographic keys
  - Validates: no reorg, peg-outs only to authorized addresses



Trust Model

- Emergency Condition
  - Bitcoin Script: `<11-of-15 multisig> OR <after 2 weeks> <2-of-3 multisig>`
- Liquid relies on a distributed strong federation with skin in the game

Liquid Members

ALTONOMY

bitbank

BITFINEX

Bitmax

BitMEX

BTCBOX

DGROUP

Buull EXCHANGE

CRYPTO GARAGE

coinone

ATLANTIC FINANCIAL
Since 1994

GOPAX

KORBIT

OKCoin

THE ROCK TRADING

SIX
Swiss Exchange

BTSE

Zaif

xapo

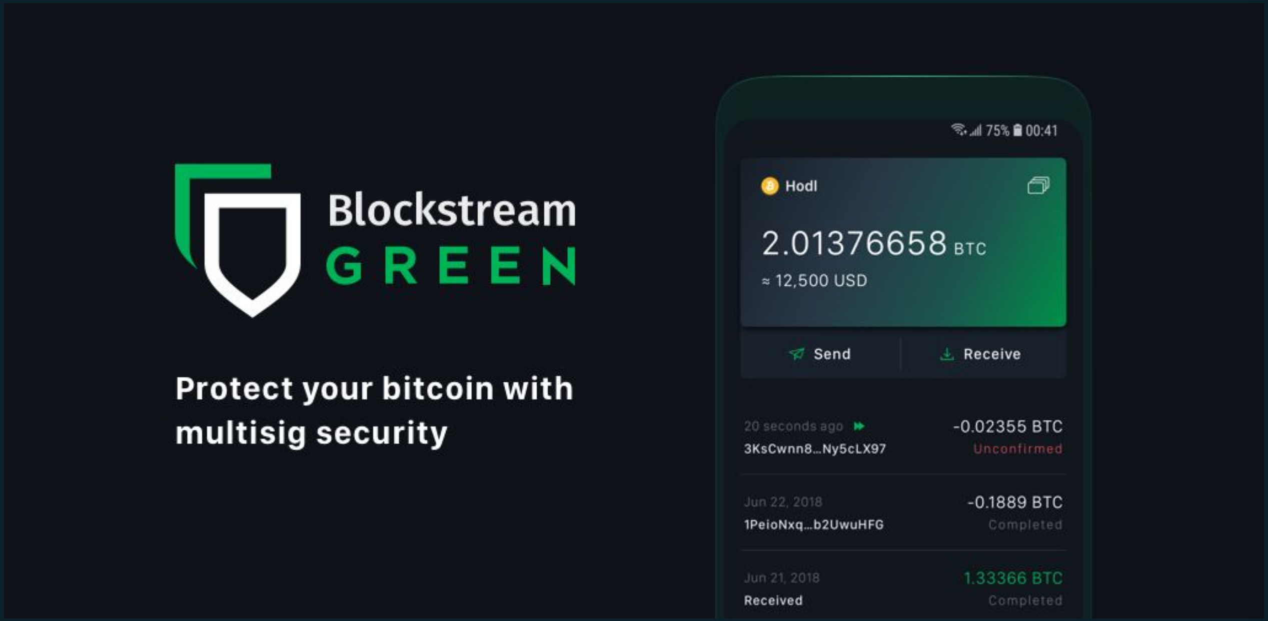
BITSO

XBTO

UNOCOIN

L2B GLOBAL

Using Liquid



00:41 75%

Hodl

2.01376658 BTC

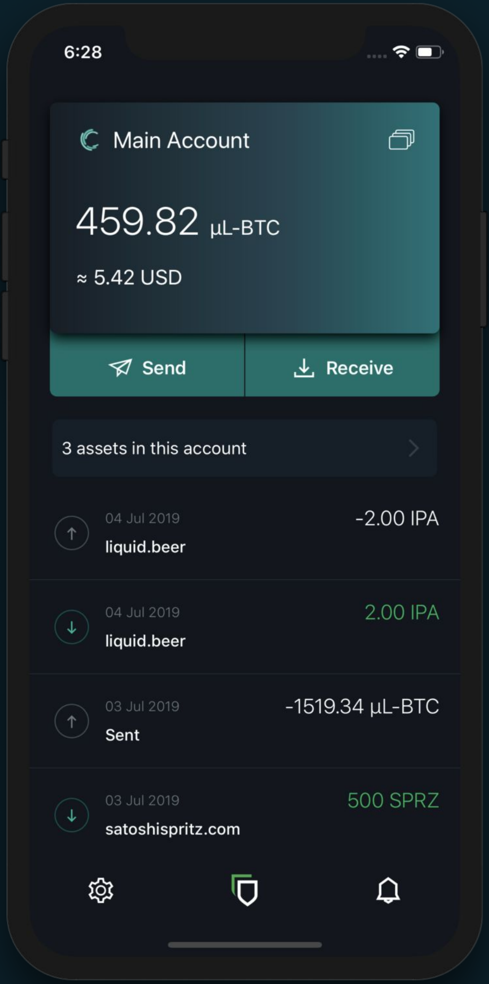
≈ 12,500 USD

Send | Receive

20 seconds ago — 3KsCwnn8...Ny5cLX97 — -0.02355 BTC — Unconfirmed

Jun 22, 2018 — 1PeioNxq...b2UwuHFG — -0.1889 BTC — Completed

Jun 21, 2018 — Received — 1.33366 BTC — Completed



6:28

Main Account

459.82 µL-BTC

≈ 5.42 USD

Send | Receive

3 assets in this account

04 Jul 2019 — liquid.beer — -2.00 IPA

04 Jul 2019 — liquid.beer — 2.00 IPA

03 Jul 2019 — Sent — -1519.34 µL-BTC

03 Jul 2019 — satoshispritz.com — 500 SPRZ

Using Liquid

- Open Source full node `elementsd` available
- Peg-in to the sidechain
  - Generate Liquid address
  - Send Bitcoin to address (“peg-in”)
  - Wait 102 Bitcoin confirmations
- Liquid requires transaction fees as denial-of-service (DoS) protection (1 satoshi/vbyte minimum)
- **Peg-out: only through members**
  - In the future: Lightning & atomic swaps

Resources

- https://blockstream.com/liquid/
- Liquid documentation: https://docs.blockstream.com (incl. issued assets tutorial)
    - webinars: https://www.youtube.com/playlist?list=PLseHpvCI1BjAfUx8zjJXadlBh_eKV9zJi
- Elements daemon: https://github.com/ElementsProject/elements
- Block explorer: https://blockstream.info/liquid/
- Updates: @blockstream twitter, https://blockstream.com/blog/

Conclusion

- Bitcoin is highly relevant in 2019 and in the years to come
- Bitcoin scales through different trust models
- Liquid is a sidechain for an interexchange settlement network built on Bitcoin
- It provides fast transaction confirmations, issued assets and confidential transactions
- Lots of updates in the coming months
- Anyone can use Liquid today

Questions?

Appendix: Liquid by Blockstream vs. Lightning

Liquid by Blockstream

- 1-minute block times
- Confidential Transactions
- Multiple assets
- Transact any amount to any participant
- Automatic fast settlement to Bitcoin
- For large transactions
- Allows for hot and cold wallets
- Lightning on Liquid is possible

Lightning

- Near-instant payments
- Transactions amounts and destinations limited by routing topology
- Fast settlement to Bitcoin dependent on cooperation of channel partner
- For microtransactions
- Requires hot wallet