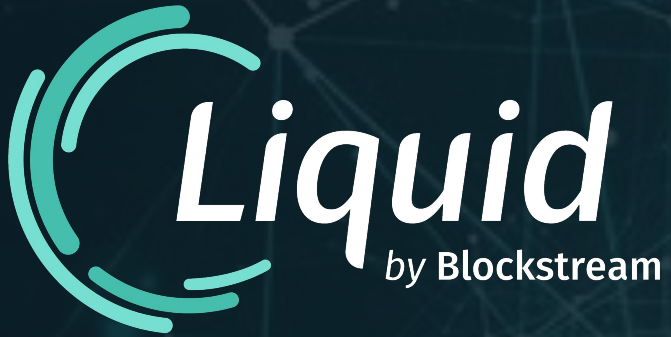


Bitcoin Meetup Switzerland, Dec 2018

Jonas Nick - jonas@blockstream.com



- **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



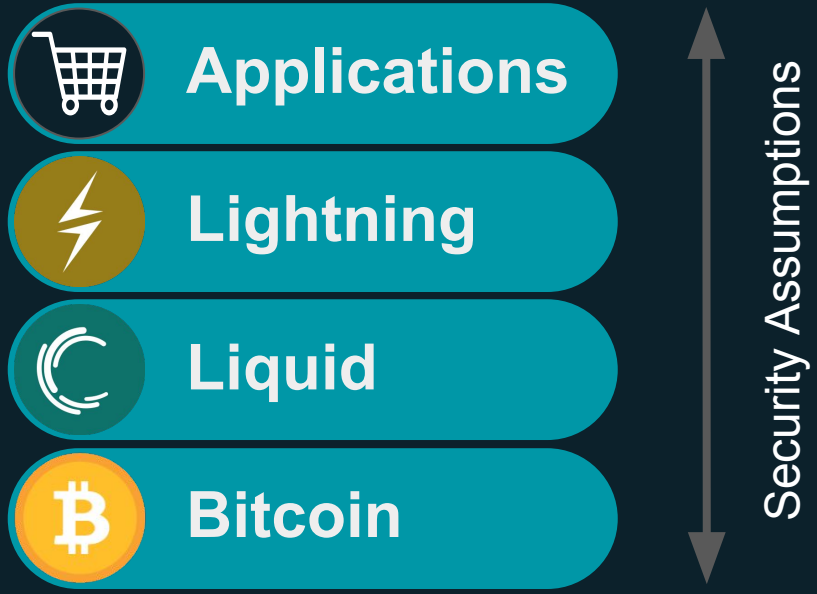
Private
More so than fiat

State of Bitcoin



Slow
Expensive
Not anonymous
Volatile
Custodial exchanges

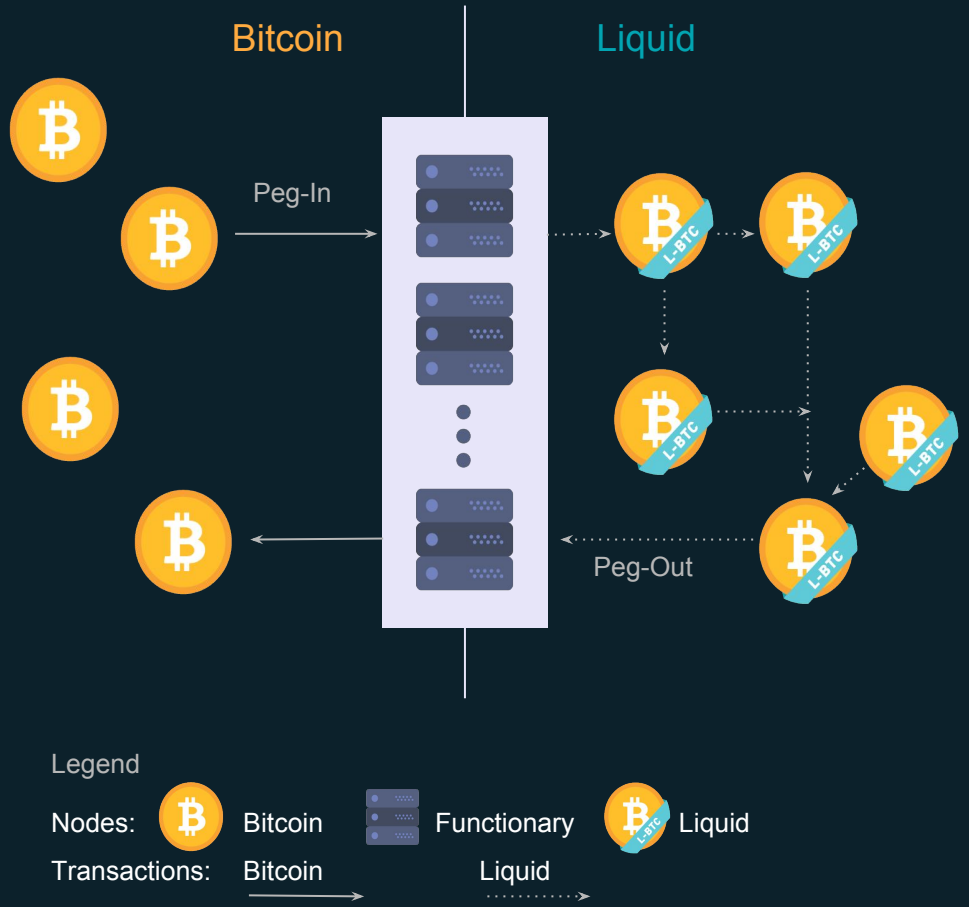
Layering on Bitcoin



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



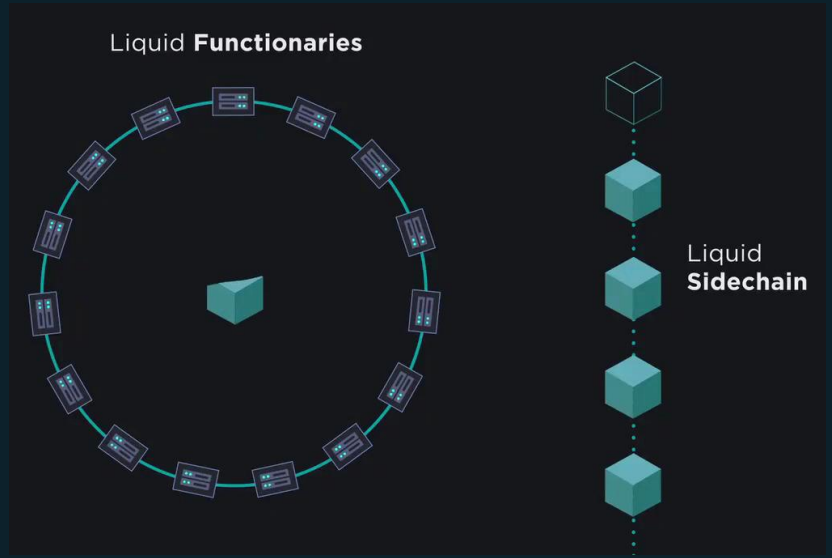
What is Liquid?

An Interexchange Settlement Network

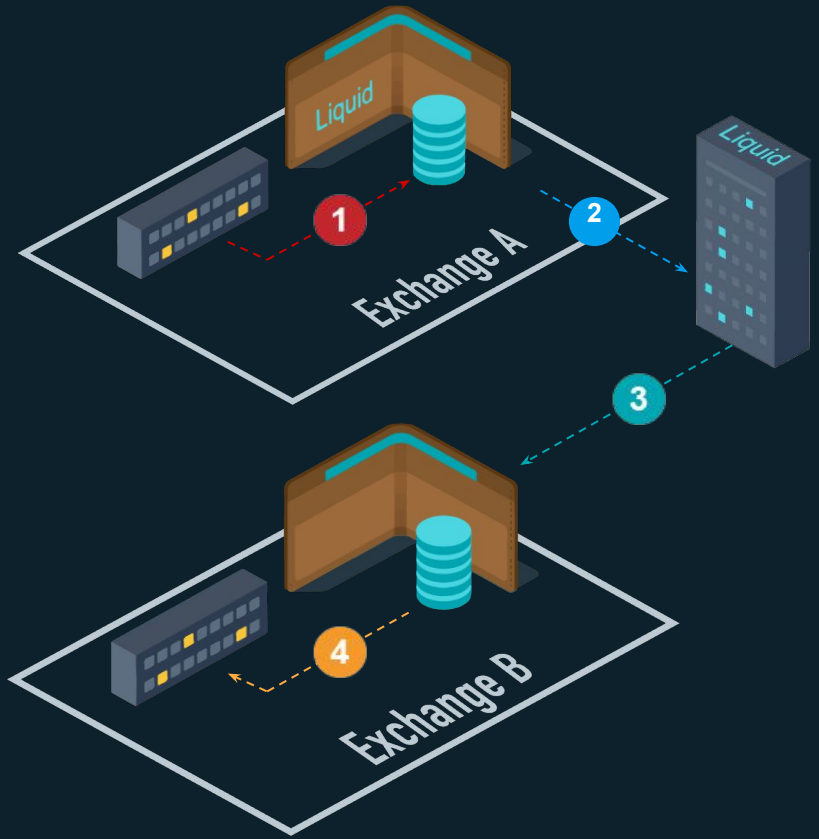
- addresses the needs of traders who use exchanges

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



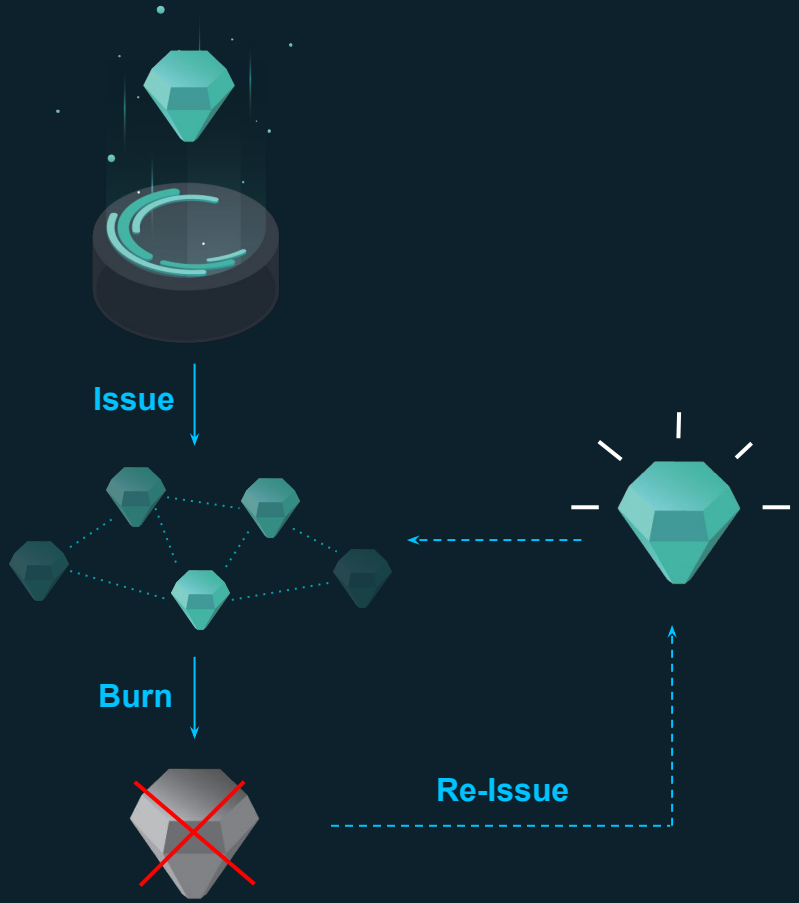
Customer Interexchange Transfer



Liquid Features

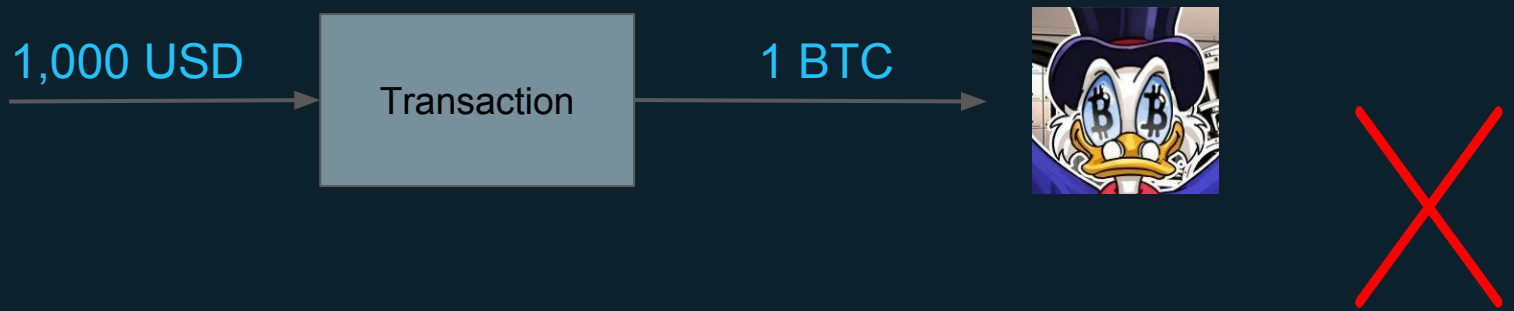
Issued Assets (IA)

- 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



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



Issued Assets Comparison

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

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

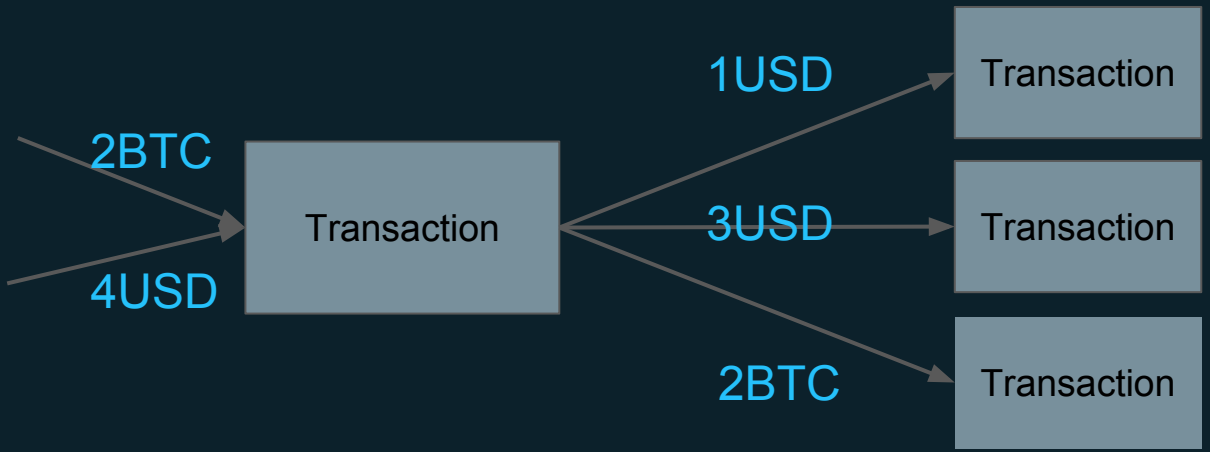
Tokens on Altcoins (Ethereum, …)

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

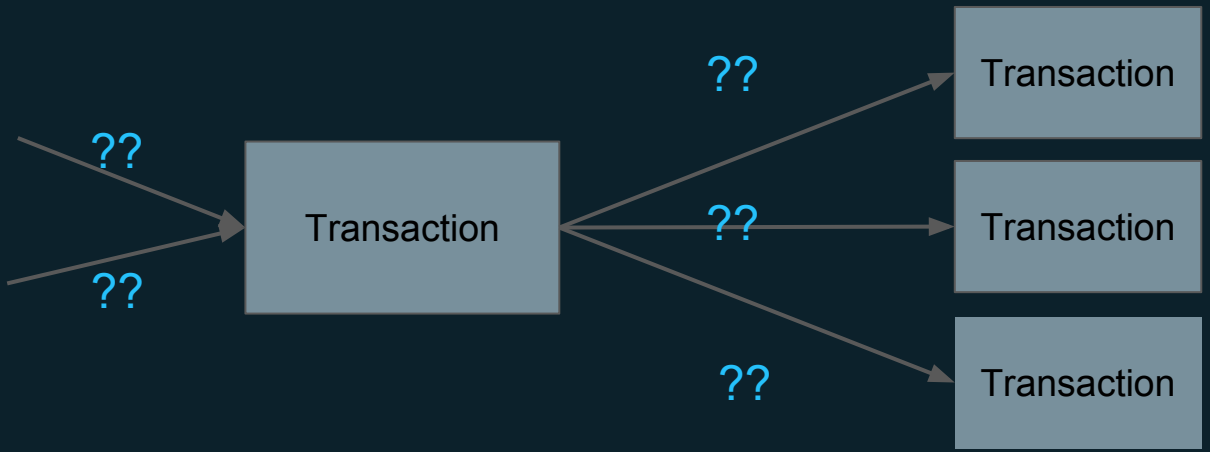
Liquid

- ✓ 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



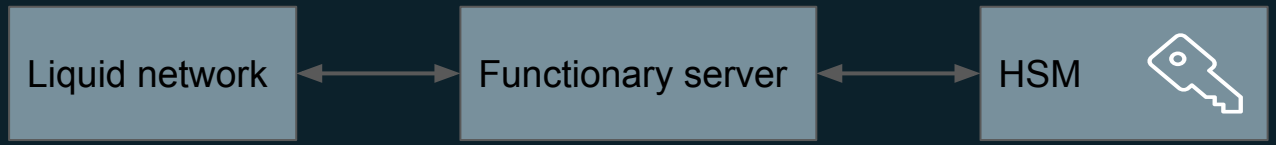
Elements
by Blockstream

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
- BUT: functionaries can in principle reorganize chain
- BUT: functionaries can in principle steal bitcoins on the chain
  - Can’t happen without detection
  - Without global network adversary more than ⅔ of functionaries have to be malicious
- Use Hardware Security Module (HSM) to make it difficult for attackers
  - 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



Using Liquid

- Liquid is a public blockchain
- Open Source command line full node `liquidd` available
- Peg-in
  - 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/2018/11/06/liquid-full-node-and-wallet-release/
- Liquid-daemon: https://github.com/blockstream/liquid-daemon
- Elements: https://elementsproject.org, issued assets tutorial
- Block explorer: https://blockstream.info/liquid/
- Updates: @blockstream twitter, https://blockstream.com/blog/

Conclusion

- Bitcoin is relevant in 2018
- 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
- 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