Blockchain analysis and Liquid

A guide to understanding privacy

SideSwap

Blockchain analysis...

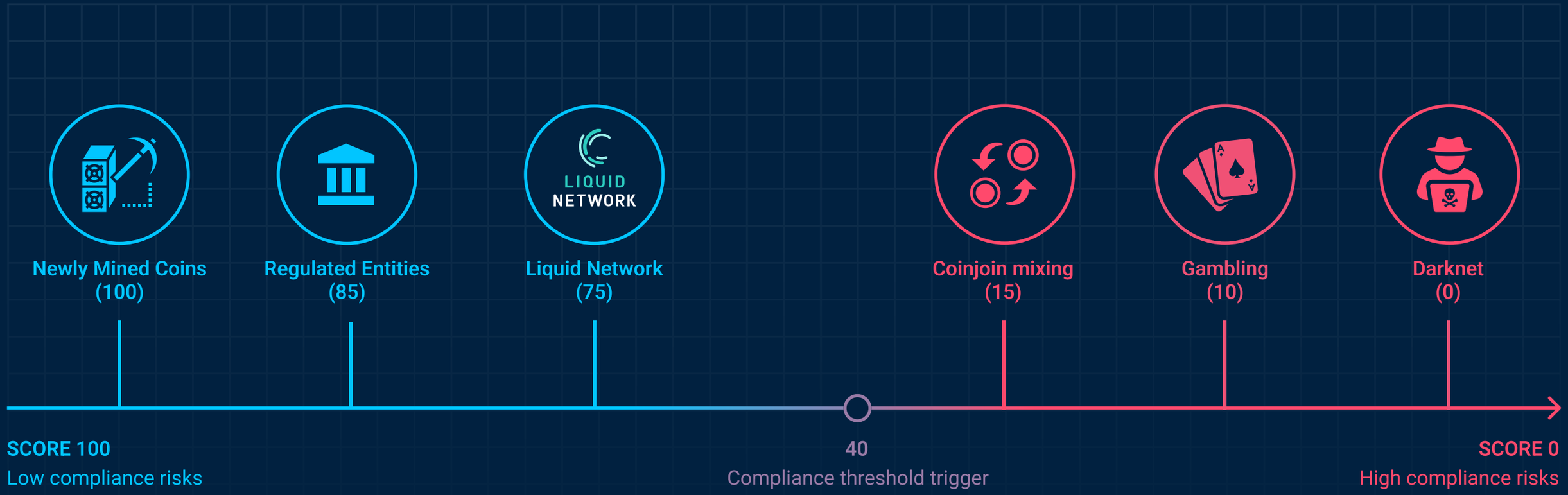
- Attempts to discover useful information about different actors transacting in cryptocurrency

- Clusters entities and assigns scores based on their activity

- Relies on publicly visible asset and amounts for common-input-ownership and change address detection

SideSwap

Assigns “cleanliness” scores to entities



*Scores are approximations

SideSwap

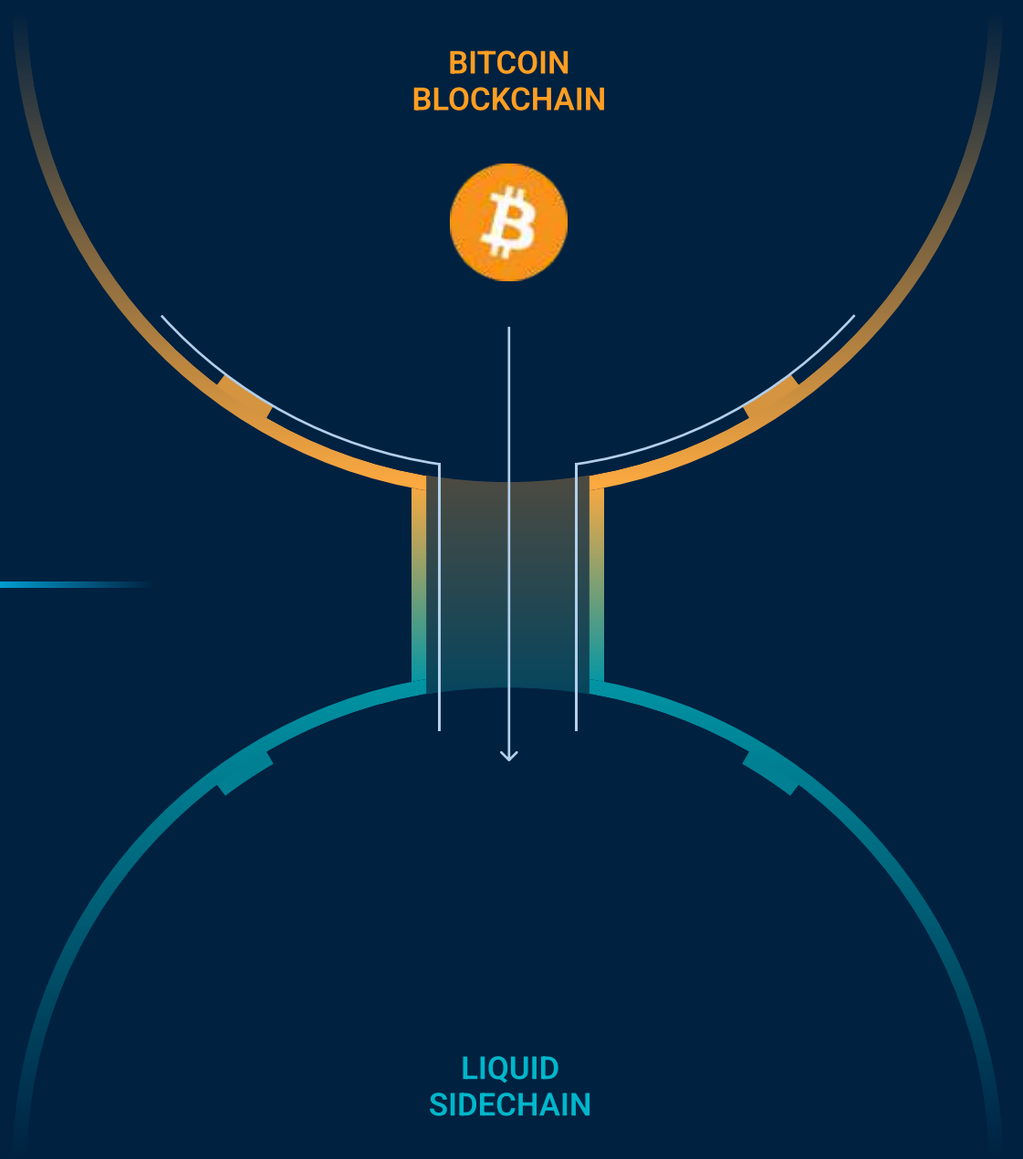
Liquid and privacy

- Bitcoin as its native currency
- Permissionless issuance of assets and securities
- Confidential Transactions publicly conceal assets and amounts
  - User may unblind transaction for regular assets
  - User and issuer may unblind transaction for AMP assets

SideSwap

Peg-in transactions...

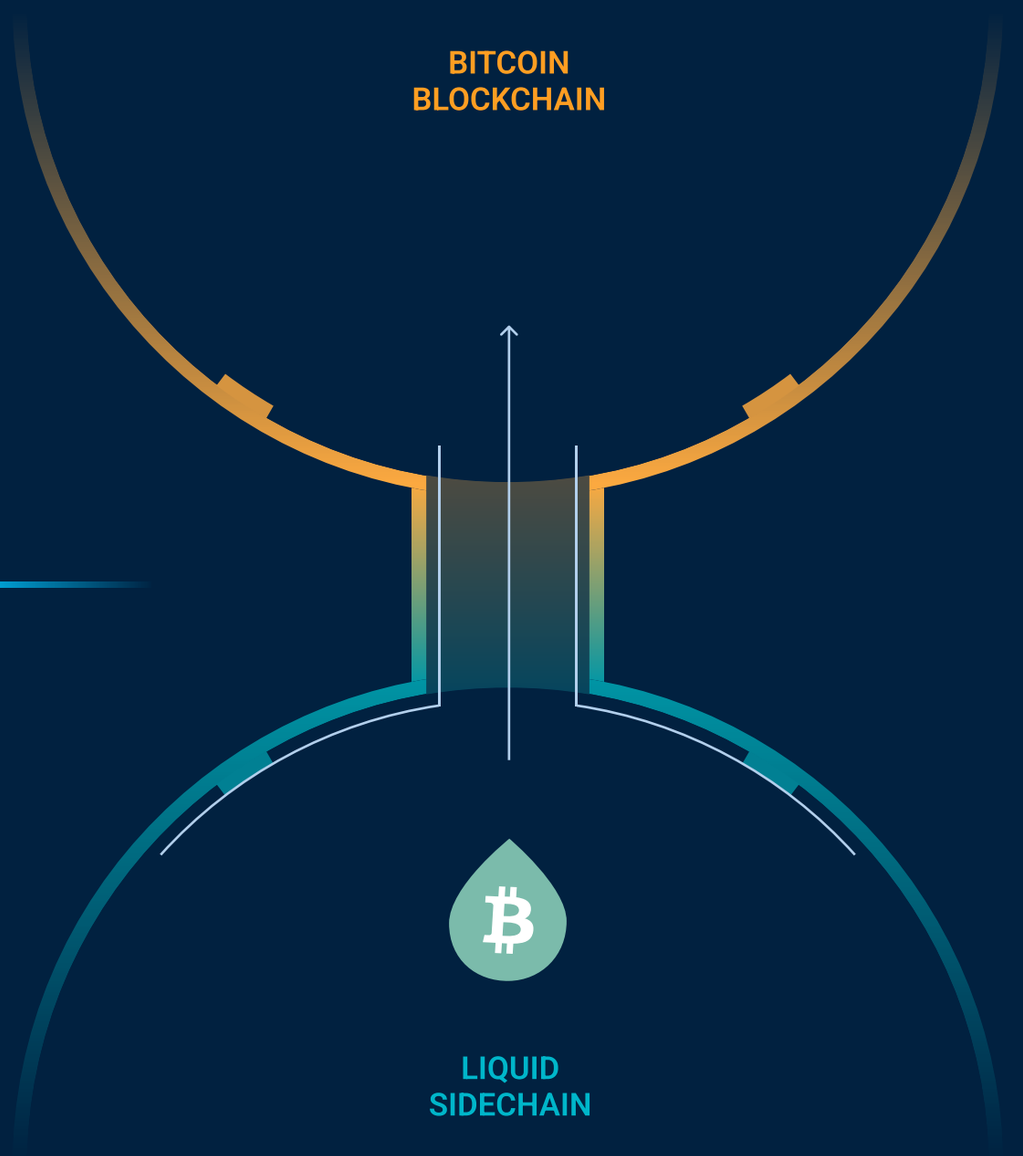
- Bind BTC to a Federation multi-sig address
- Issues L-BTC on the Liquid Network
- Are executed as non-confidential to ensure circulating amount integrity
- Treats all BTC as fungible



SideSwap

Peg-out transactions...

- Removes L-BTC from circulation
- Releases BTC from Federation multi-sig addresses
- Conducted by Liquid Federation members
- Are executed as non-confidential to ensure circulating amount integrity
- Have auto-selected UTXOs without relation to peg-in transactions



SideSwap

Confidential Transactions

- Blinds assets and amounts
- Protects financial privacy
- Optional user unblinding

3b0887a72f91fdfc925c894b3560faadda7aab225a4b0c6ec8905e20e63bdb2f

DETAILS +

#0	2a40eb8d10c830d741a062e6cd1ed70030a8679005a99efc038c4aa71e12b8bf:1	Confidential
#1	bc78a0364d5516ff9d0176f6ddaa5ef7ea7132dce925341eb9fb178d3da14074:0	Confidential

#0	GxVvaF53yBZPtg2gn2HrzJ8Vkcxg5dZyWA	Confidential
#1	GiAYmPSVUybcspEd9r54aHvPJ1c96JdzLx	Confidential
#2	Transaction fees	0.00000264 L-BTC

4 CONFIRMATIONS Confidential

SideSwap

Swaps

- Allows two users to exchange assets without counterparty risks
- Invalidates common-input-ownership assumptions

SideSwap

AMP Assets

- Require a server to co-sign the movement of assets
- Permit the issuer to whitelist who may hold the asset
- Reveals transaction details to the issuer
- Prevents outside analysis by using confidential transaction

SideSwap

In summary

- No restrictions on moving BTC between Bitcoin mainchain and Liquid sidechain
- No relationship between pegged BTC and released L-BTC
- Confidential Transactions permit user driven transaction disclosure
- Swaps are trustless and obfuscate input and output ownership
- AMP asset transactions are visible to issuers

SideSwap

Thank You!

SideSwap