Lightning <> Liquid Swaps

by Boltz

What is Boltz?

Non-Custodial Bitcoin Exchange or “Bitcoin Layer 2 Bridge”

- Swap ⚡-BTC/BTC, ⚡-BTC/L-BTC
- Differentiation: atomic swaps - non-custodial
- Differentiation: web app, public API

What is Boltz?

Privacy first

- All services, including API exposed via Tor
- No accounts, no user-identifying data logged or stored

Stability

- Operating since 2019
- One of the oldest & largest lightning nodes
- Move slow, try hard not to break things
- Major uptime improvements with e.g. additional CLN

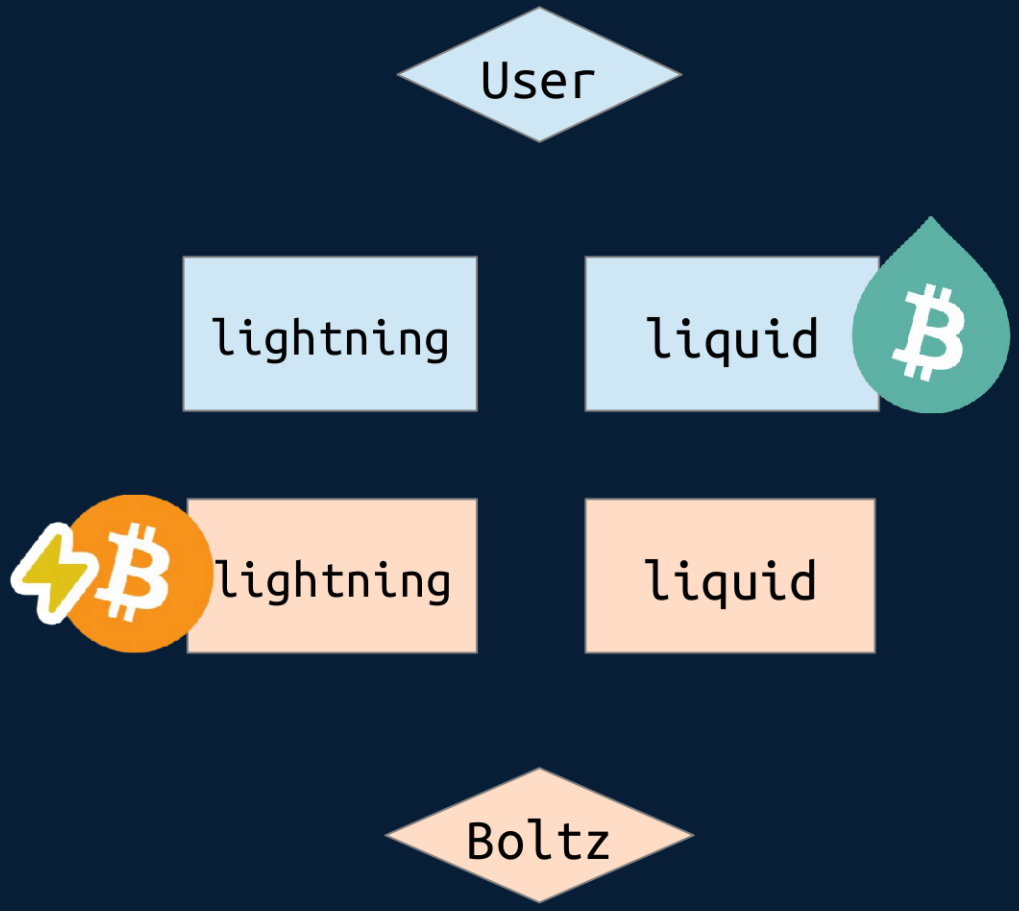
Who uses Boltz?

- Lightning Node operators
  - Rebalance channels (focus of Liquid Swaps)
  - Get a new channel (currently disabled, relaunch soon)
- Lightning-Only Wallets: receive from/pay to on-chain
- Chain-Only Wallets: receive from/pay to lightning
- Multilayer Wallets like Green, Wallby
  - receive from/pay to lightning & mainchain
  - Move between layers
- Do more with your Bitcoin
  - Use advanced financial products like fuji.money

What are Atomic Swaps?

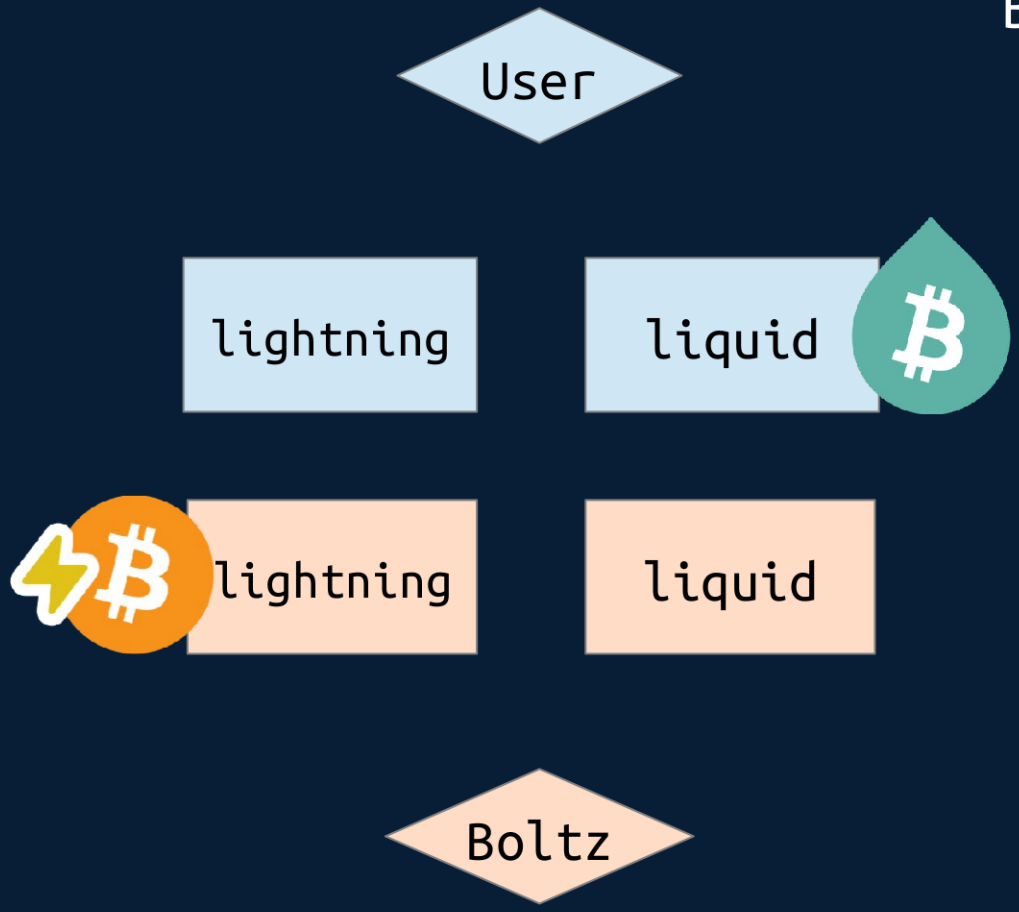
- A way to swap two coins secured by cryptography so that no party can cheat the other.
- The swap only executes if both transactions execute. If 1 out of the 2 does *not* execute, the swap gets refunded.
- Both Transactions in a swap use same hash
- In contrast to many definitions found online, they don’t have to be between two different chains or P2P.
- Very important for us as a swap provider: this means we are never control customer funds, not even for a split-second

Atomic Swaps - Submarine Swaps

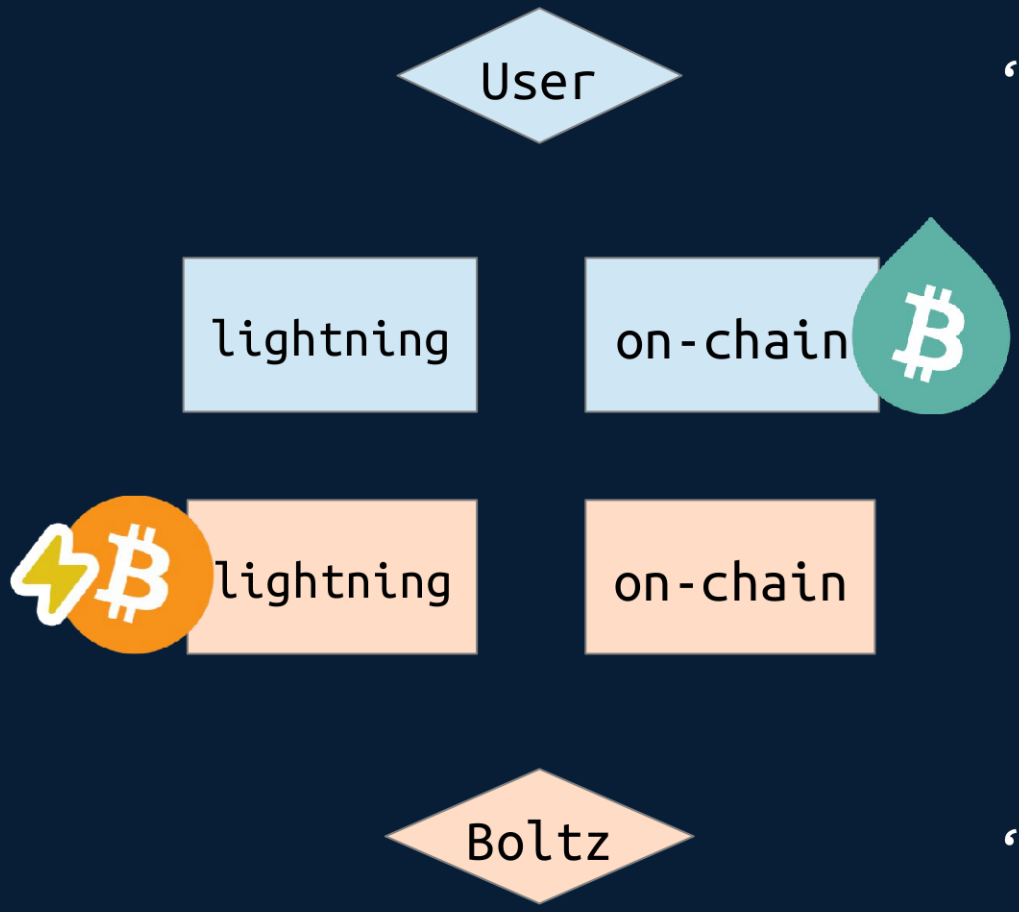


Normal Submarine Swaps (L-BTC -> ⚡-BTC)

Boltz Swap Protocol (simplified):



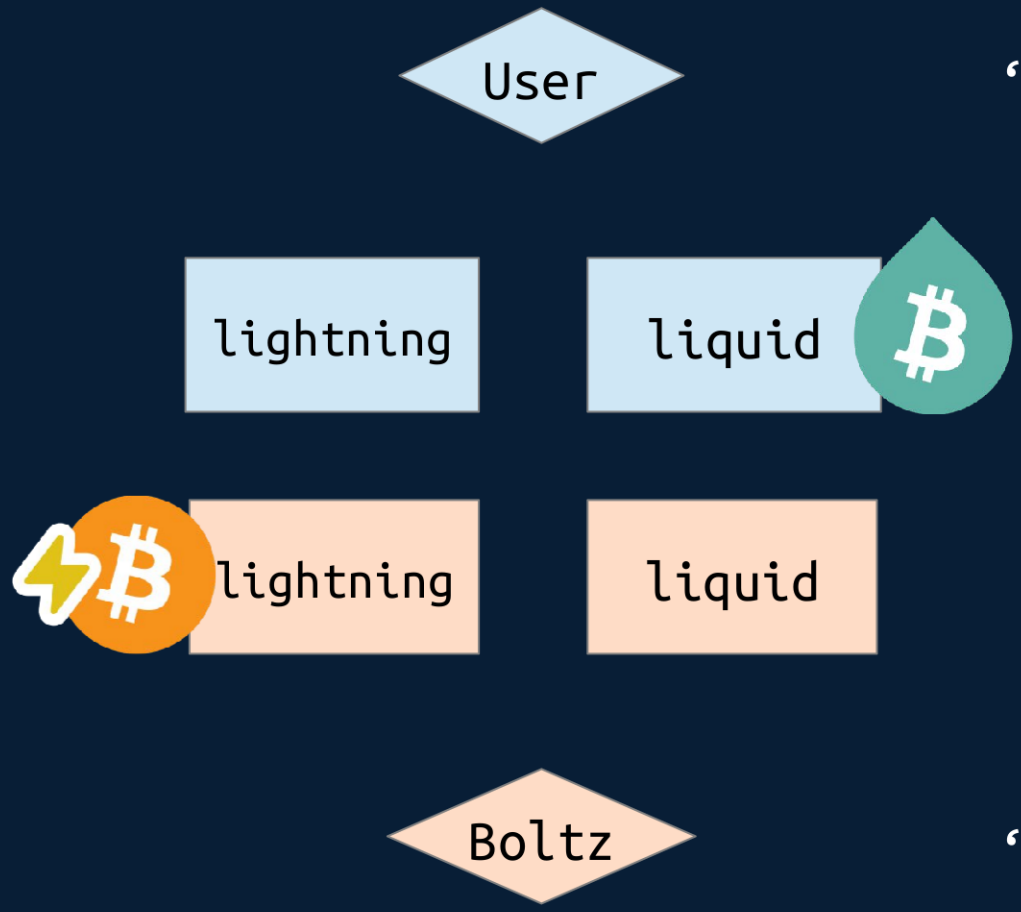
Normal Submarine Swaps (L-BTC -> ⚡-BTC)



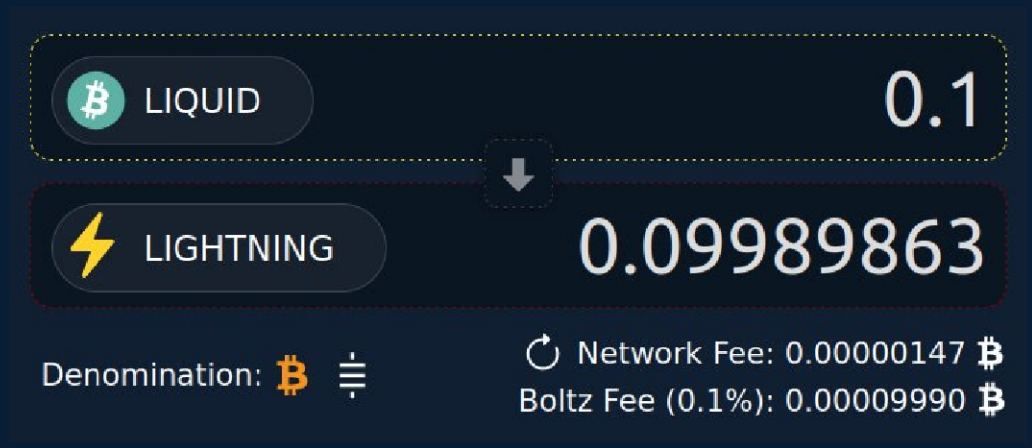
“Send: 0.1 L-BTC”

“Receive: 0.099 ⚡-BTC”

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



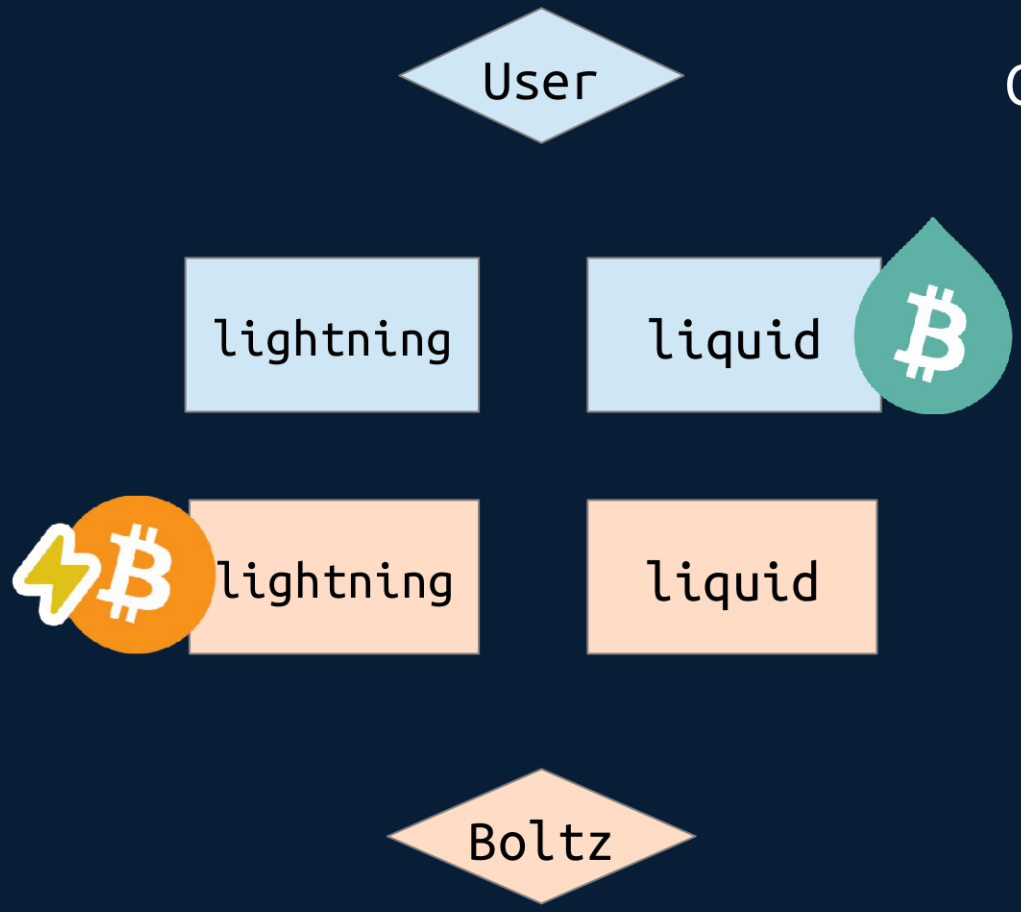
“Send: 0.1 L-BTC”



liquid.boltz.exchange

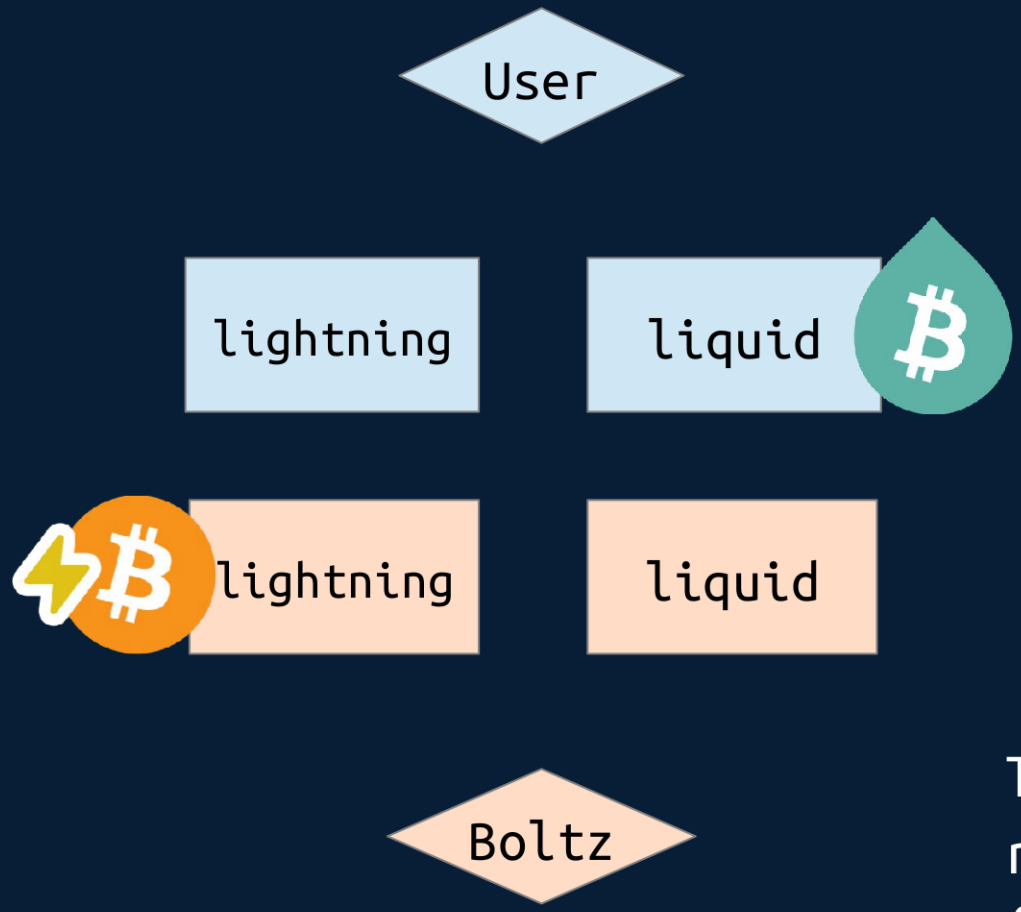
“Receive: 0.099 ⚡-BTC”

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



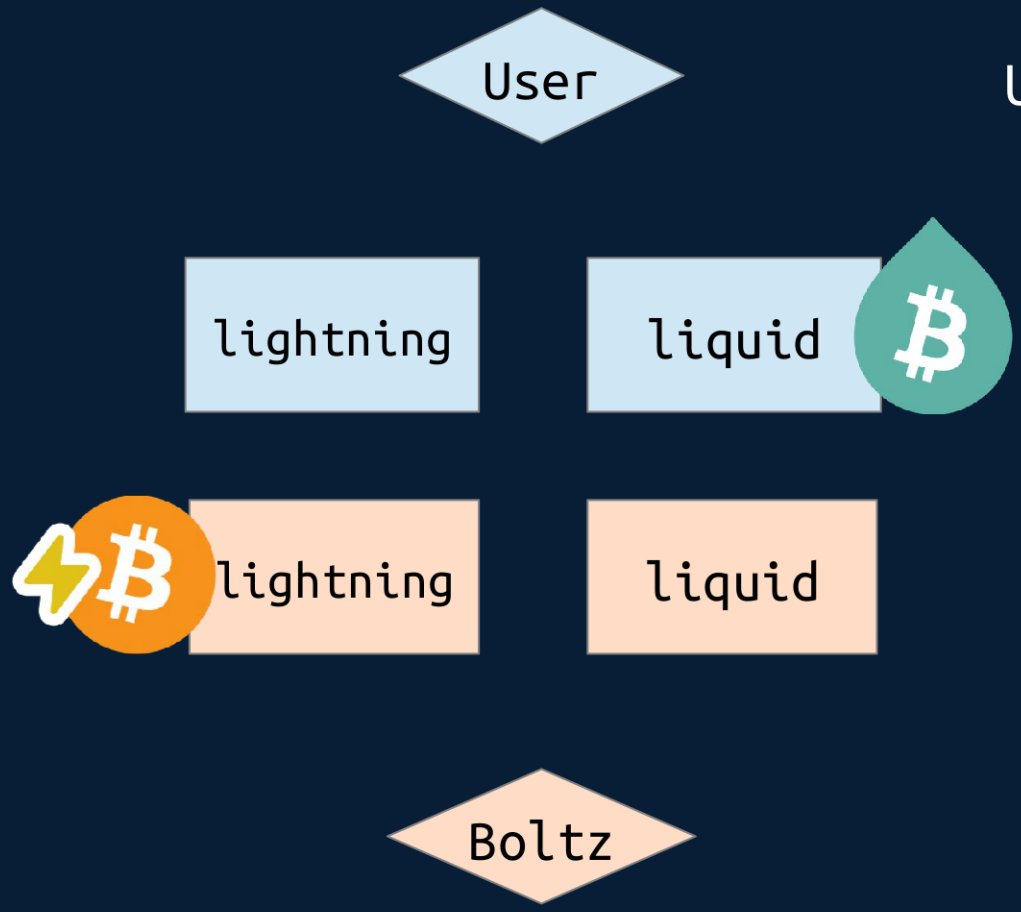
Create ⚡-invoice for 0.099 ⚡-BTC

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



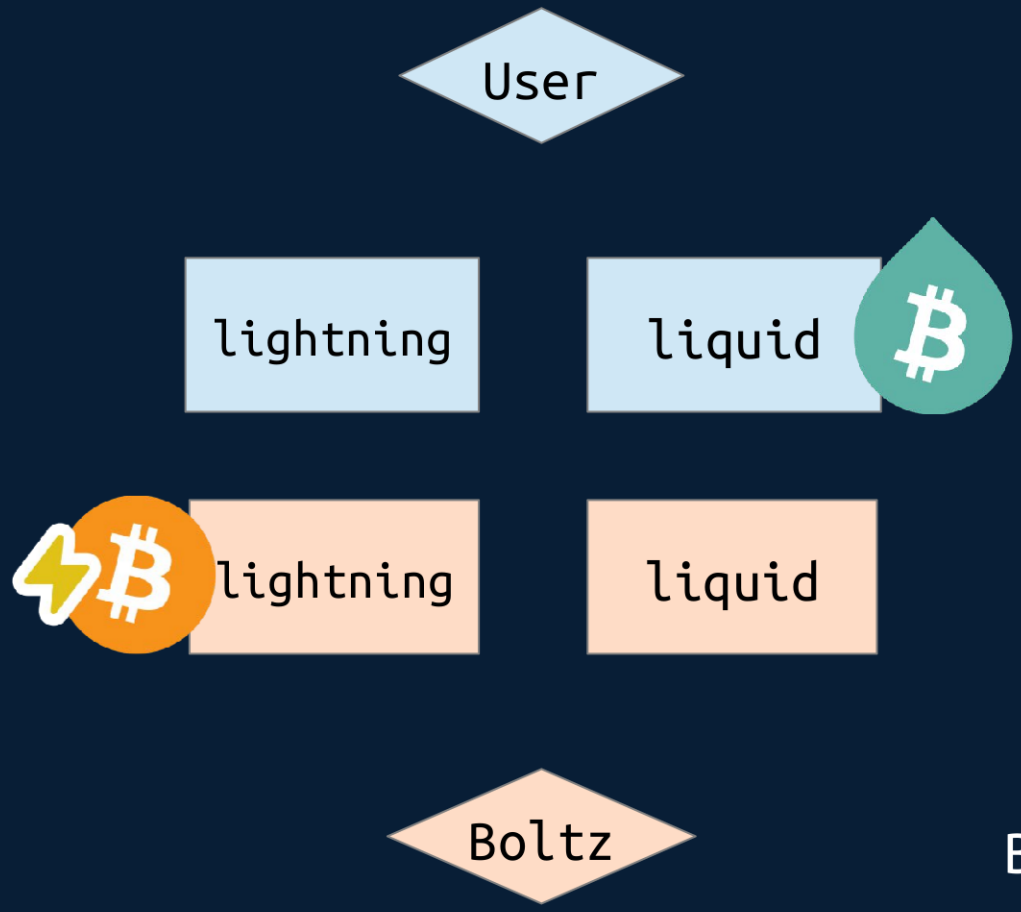
Take invoice preimage hash and create redeem script to generate liquid address for user to send 0.1 L-BTC to

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



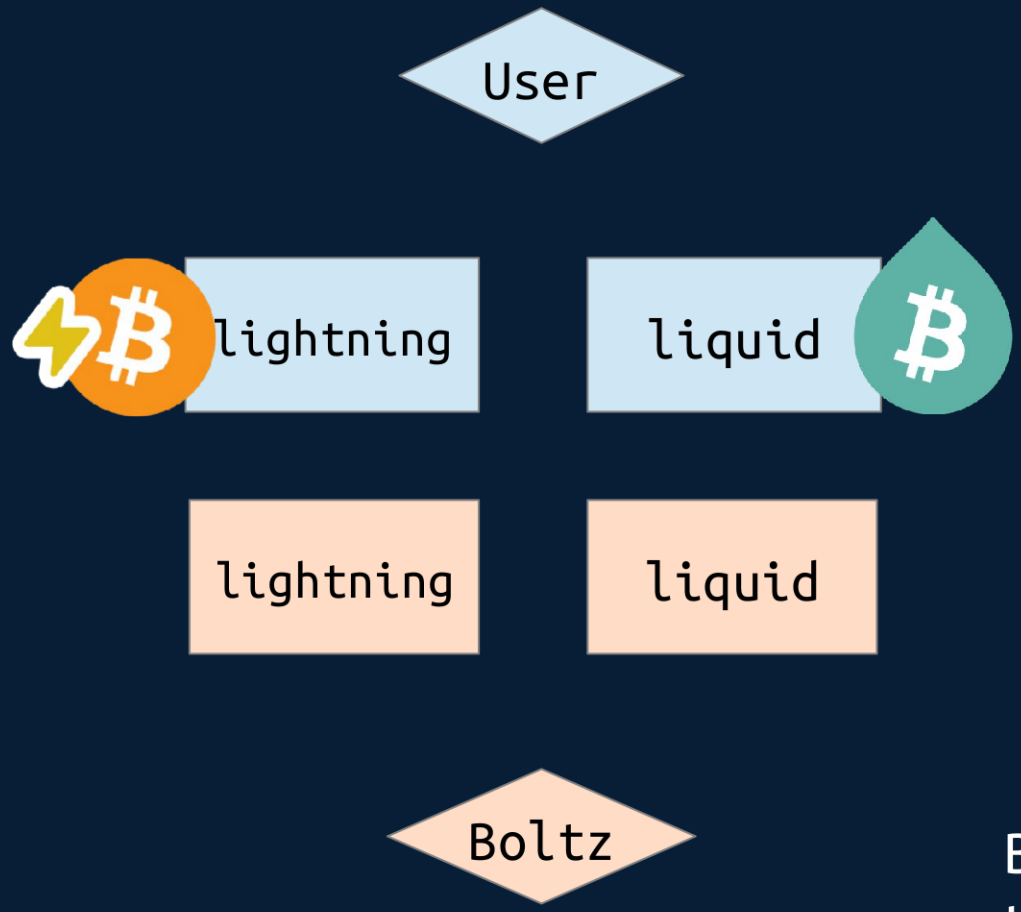
User sends 0.1 L-BTC to this address

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



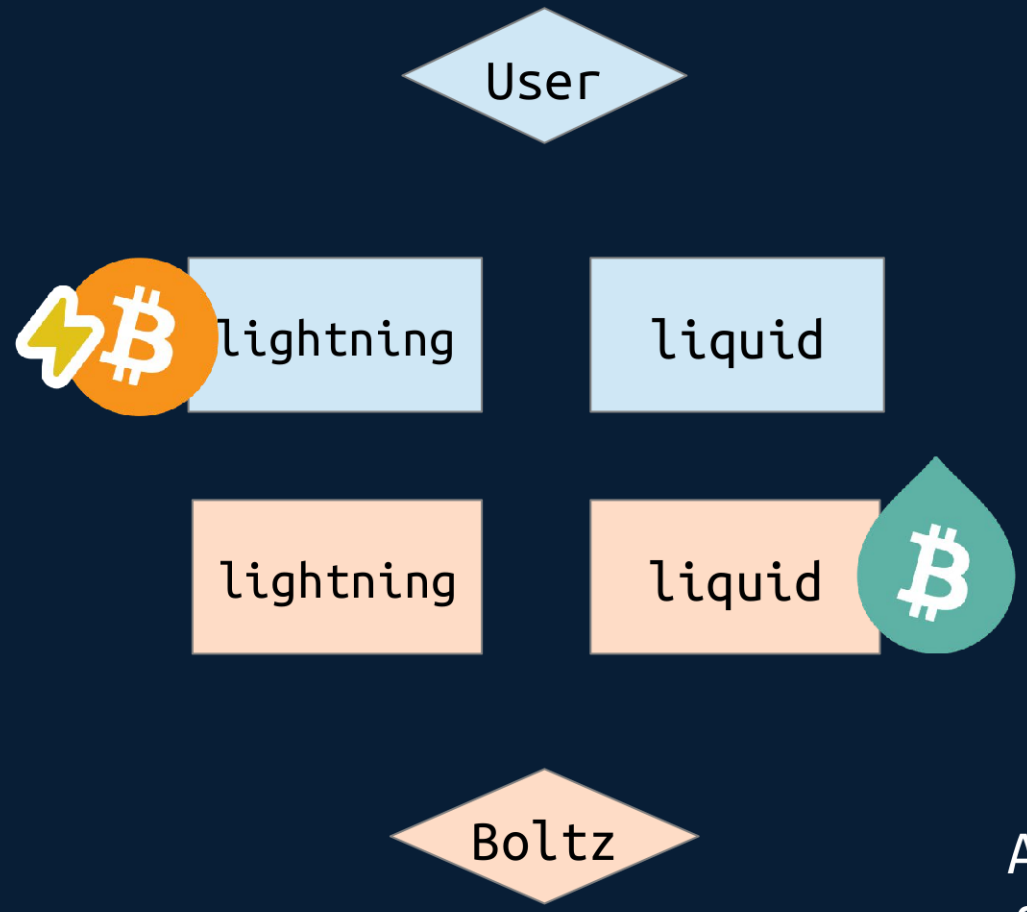
Boltz waits for one confirmation

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



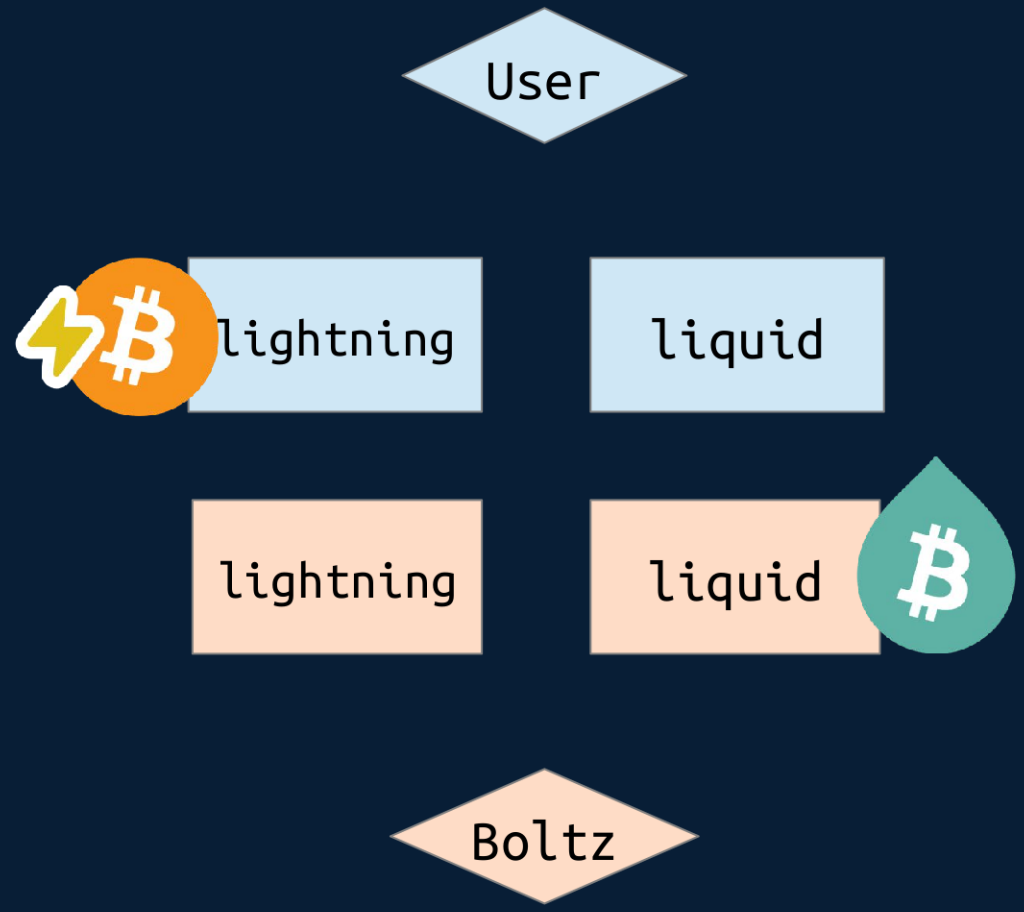
Boltz pays 0.099 lightning invoice,
because of this, preimage gets revealed

Normal Submarine Swaps (L-BTC -> ⚡-BTC)



And Boltz can claim 0.1 L-BTC on Liquid from redeem script

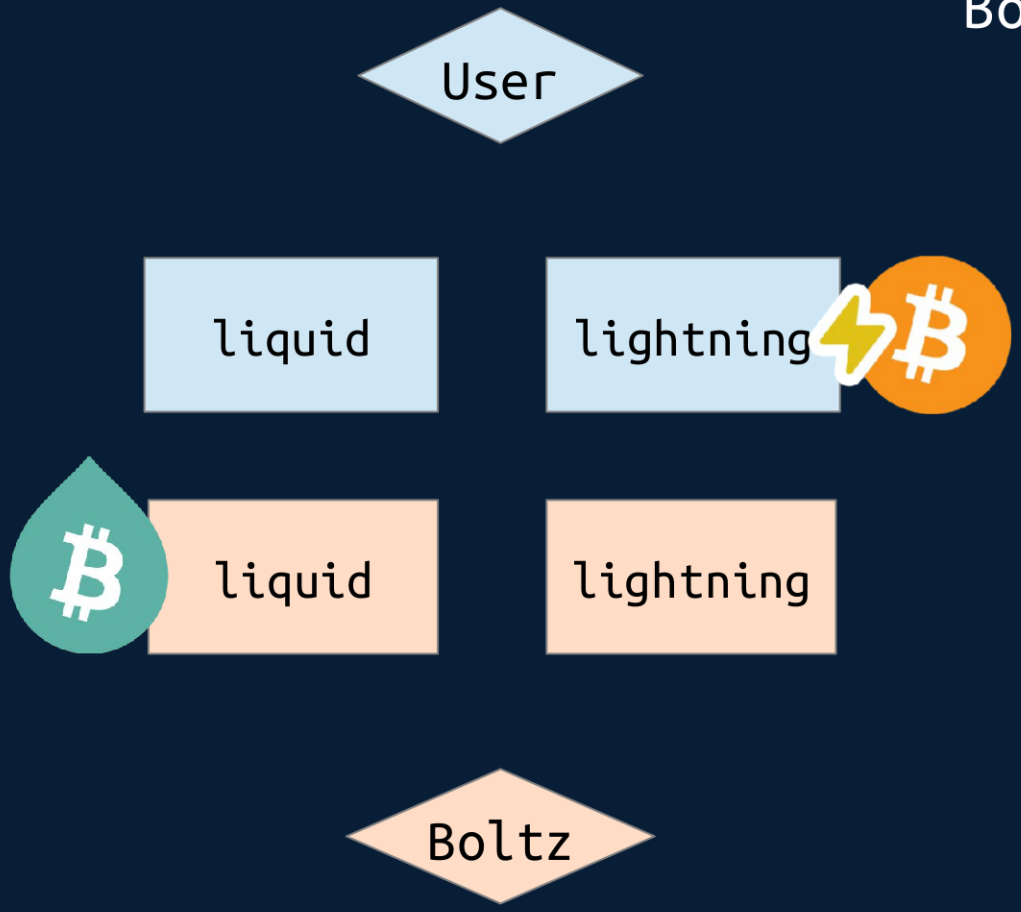
Normal Submarine Swaps (L-BTC -> ⚡-BTC)



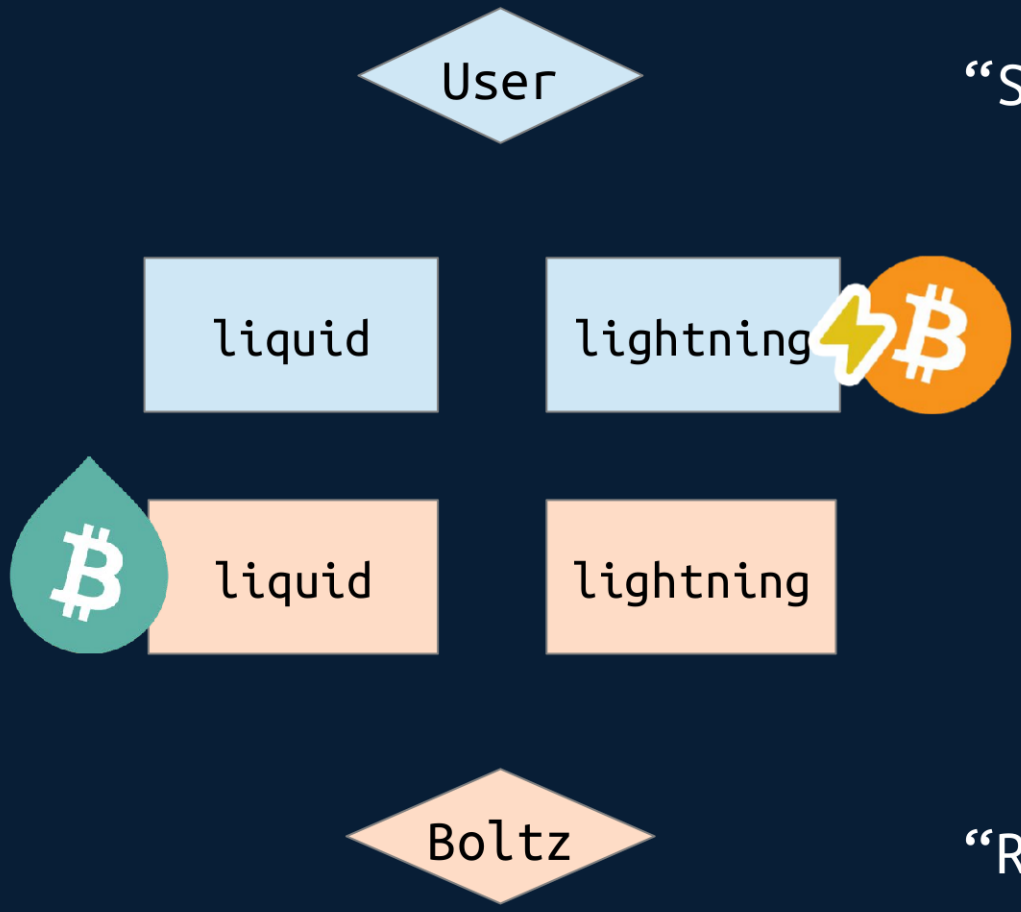
SWAP COMPLETED

Reverse Submarine Swaps (⚡-BTC -> L-BTC)

Boltz Swap Protocol (simplified):



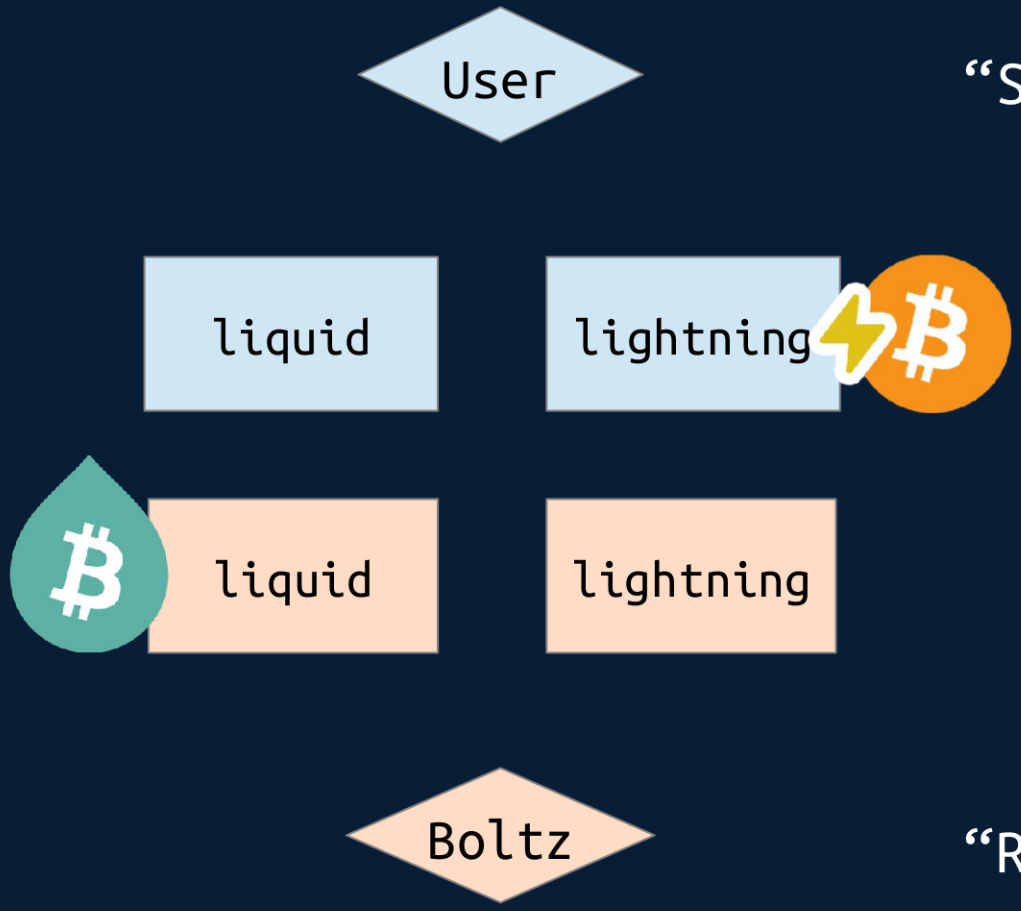
Reverse Submarine Swaps (⚡-BTC -> L-BTC)



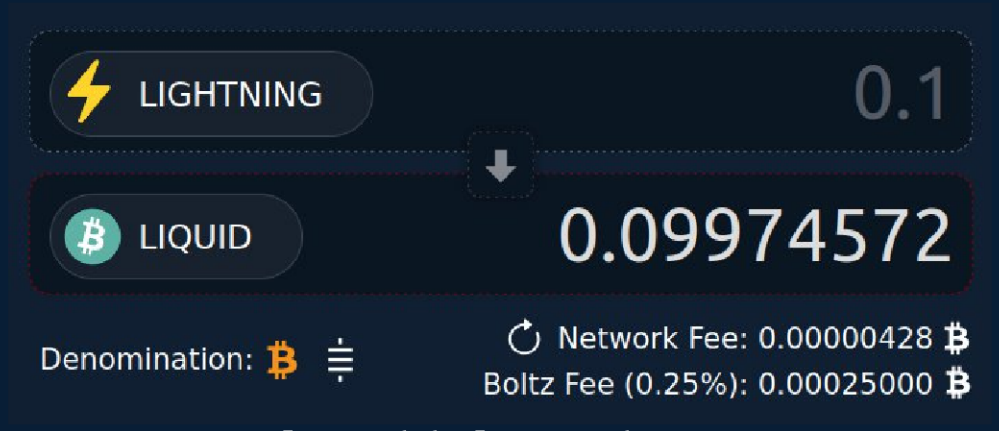
“Send: 0.1 ⚡-BTC”

“Receive: 0.099 L-BTC”

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



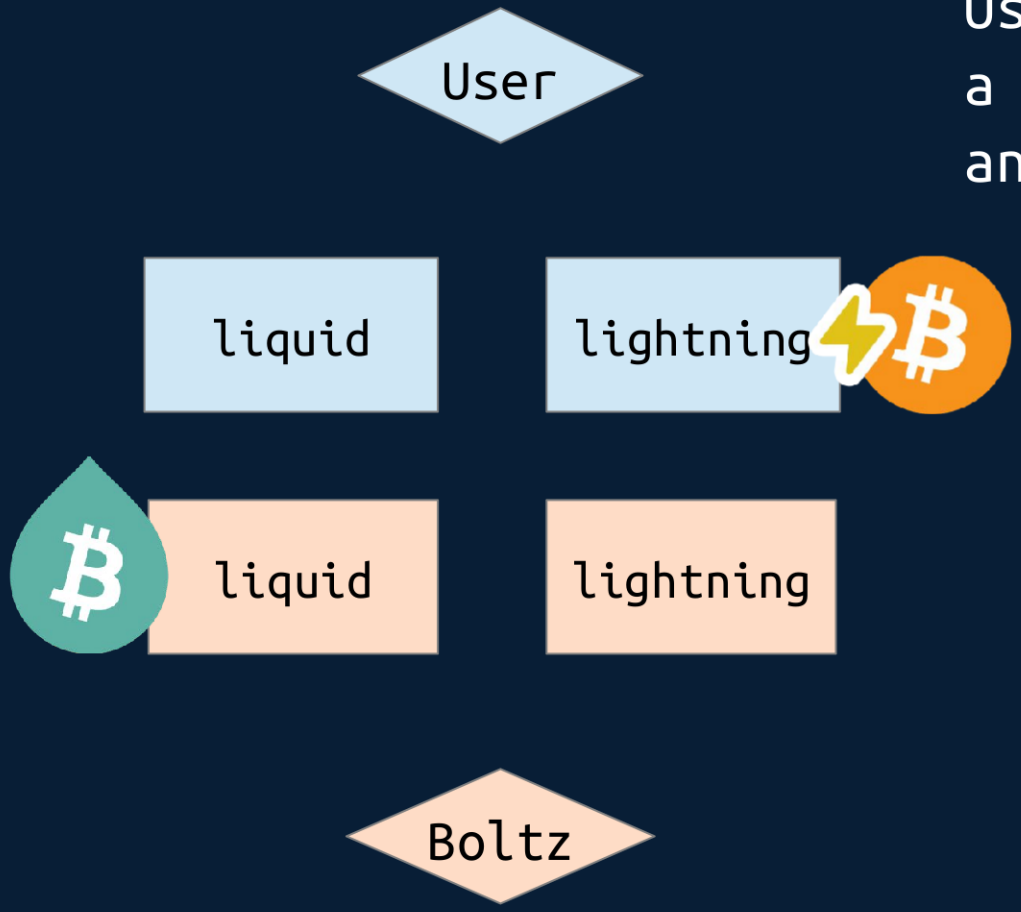
“Send: 0.1 ⚡-BTC”



liquid.boltz.exchange

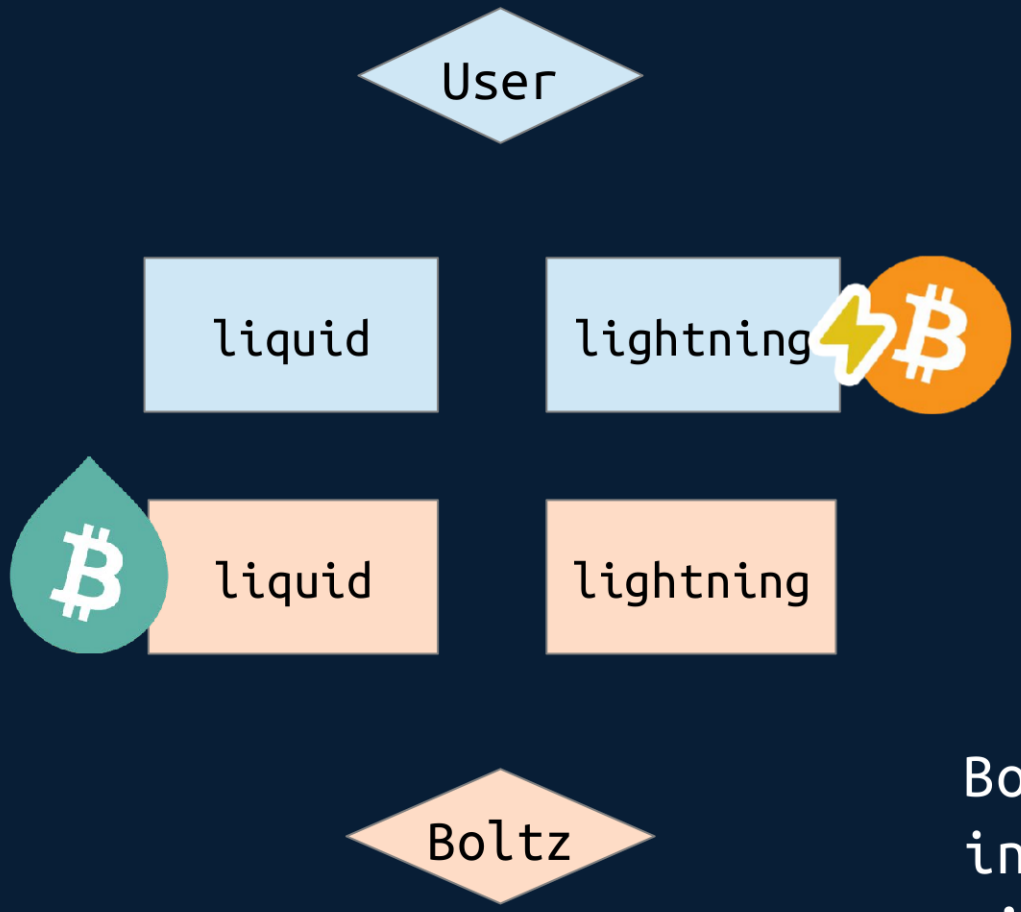
“Receive: 0.099 L-BTC”

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



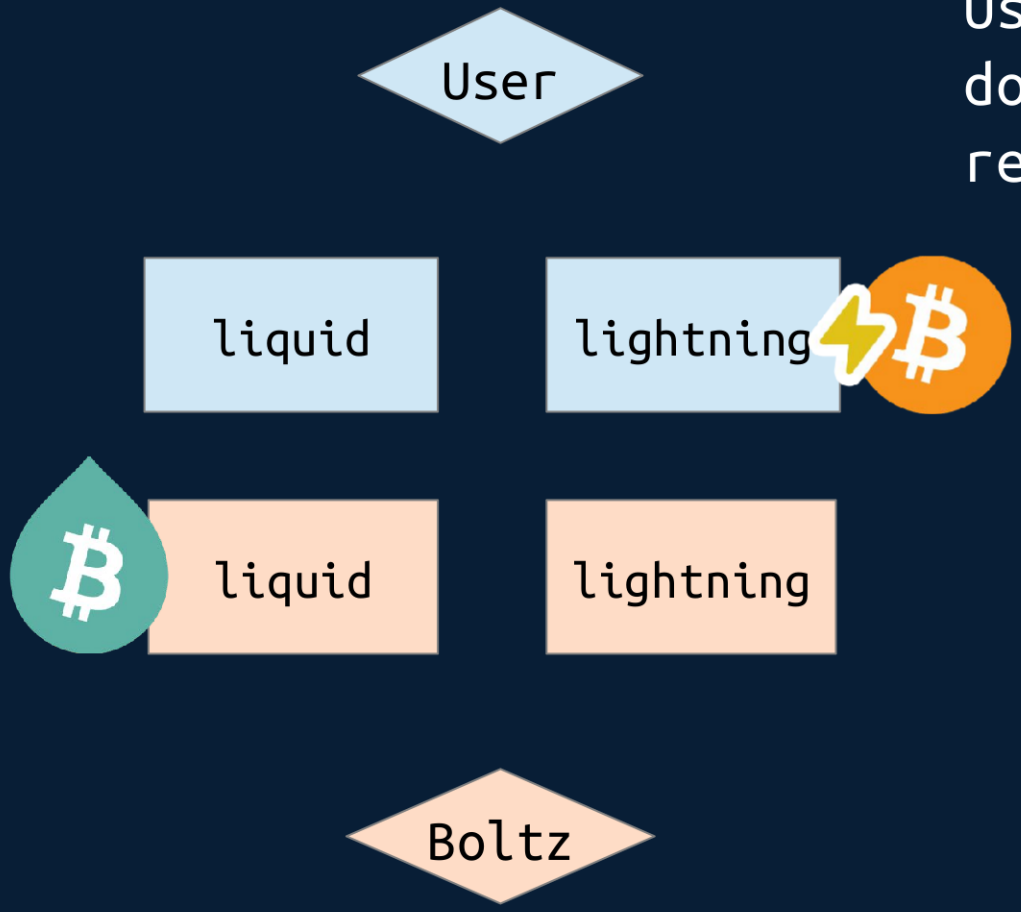
User's app (boltz.exchange) generates a preimage, creates SHA256 hash of it and sends hash to Boltz

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



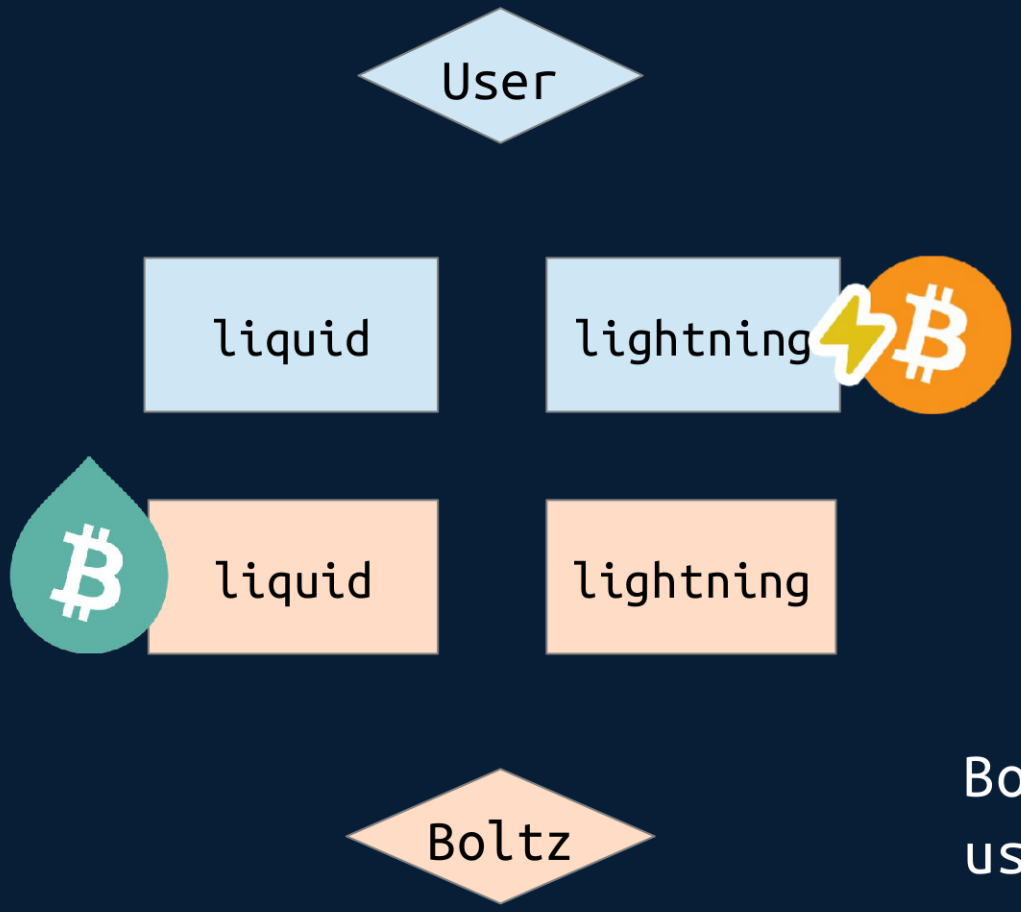
Boltz creates a so-called “hold invoice” about 0.1 ⚡-BTC
with hash received from user

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



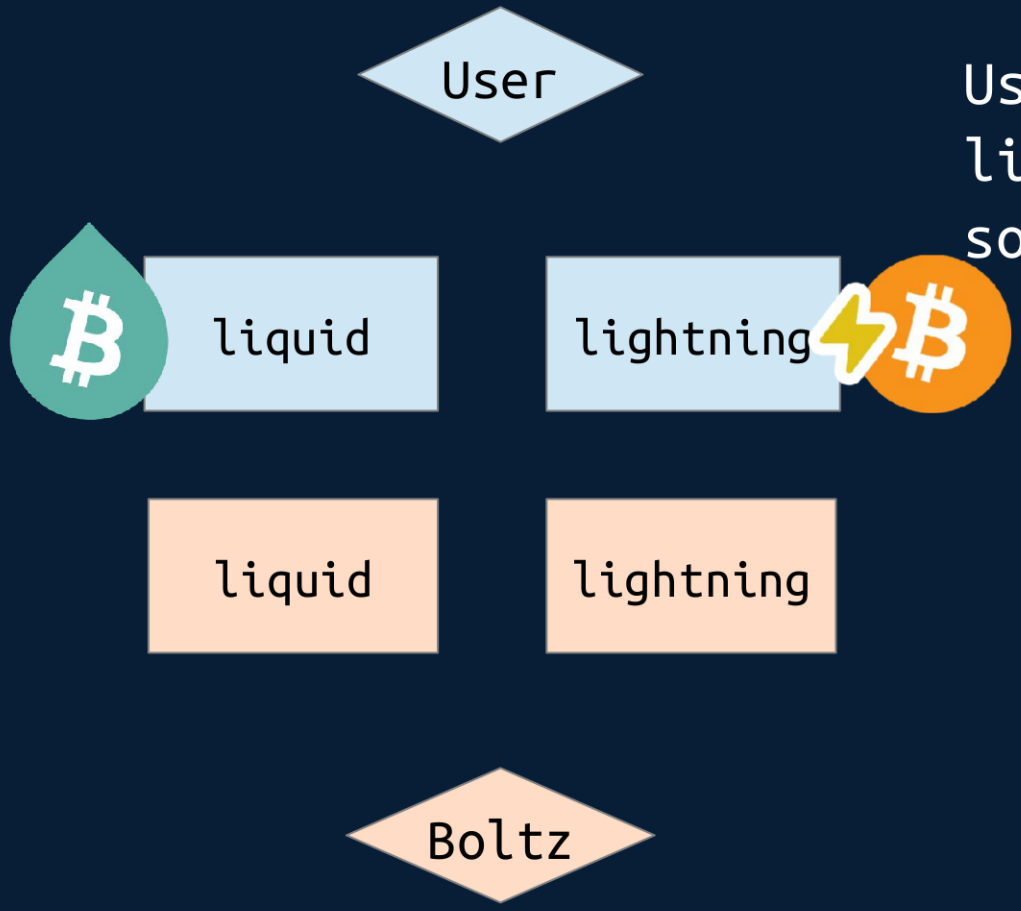
User pays Boltz's invoice, but invoice does not settle because user doesn't reveal preimage to Boltz **yet**

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



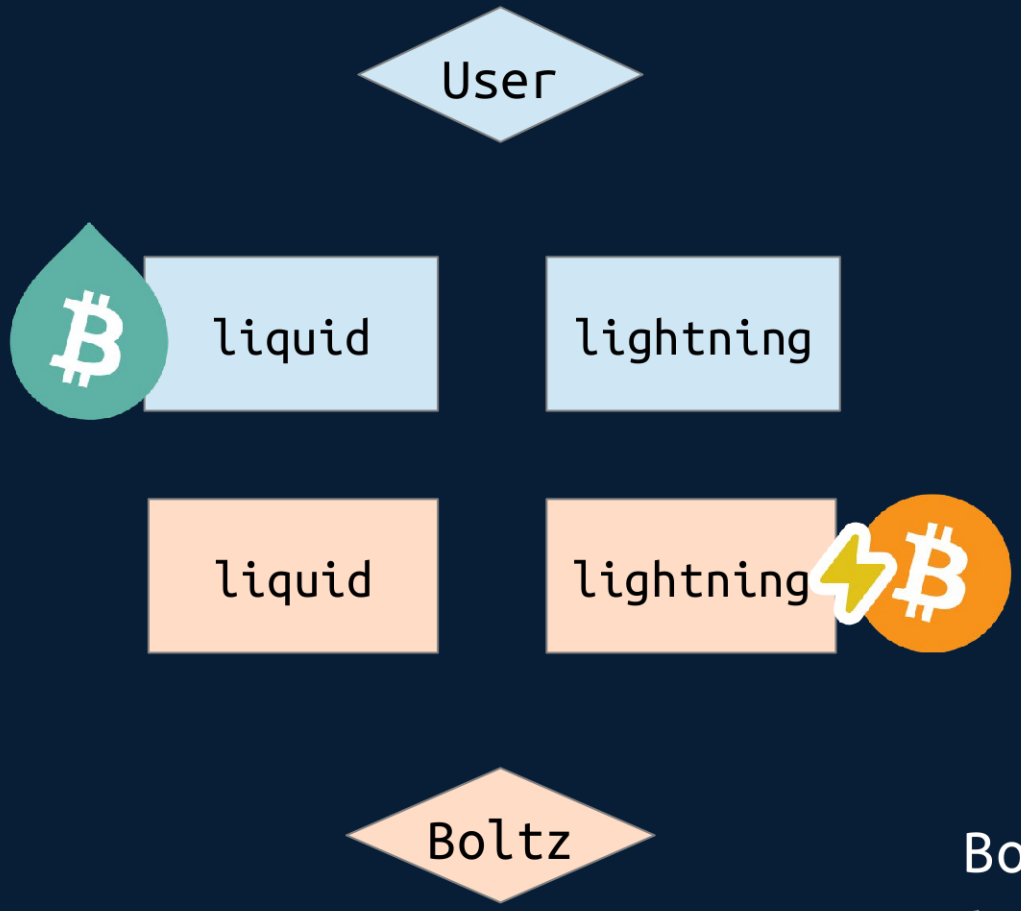
Boltz locks up 0.099 L-BTC on Liquid using **same hash from user**

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



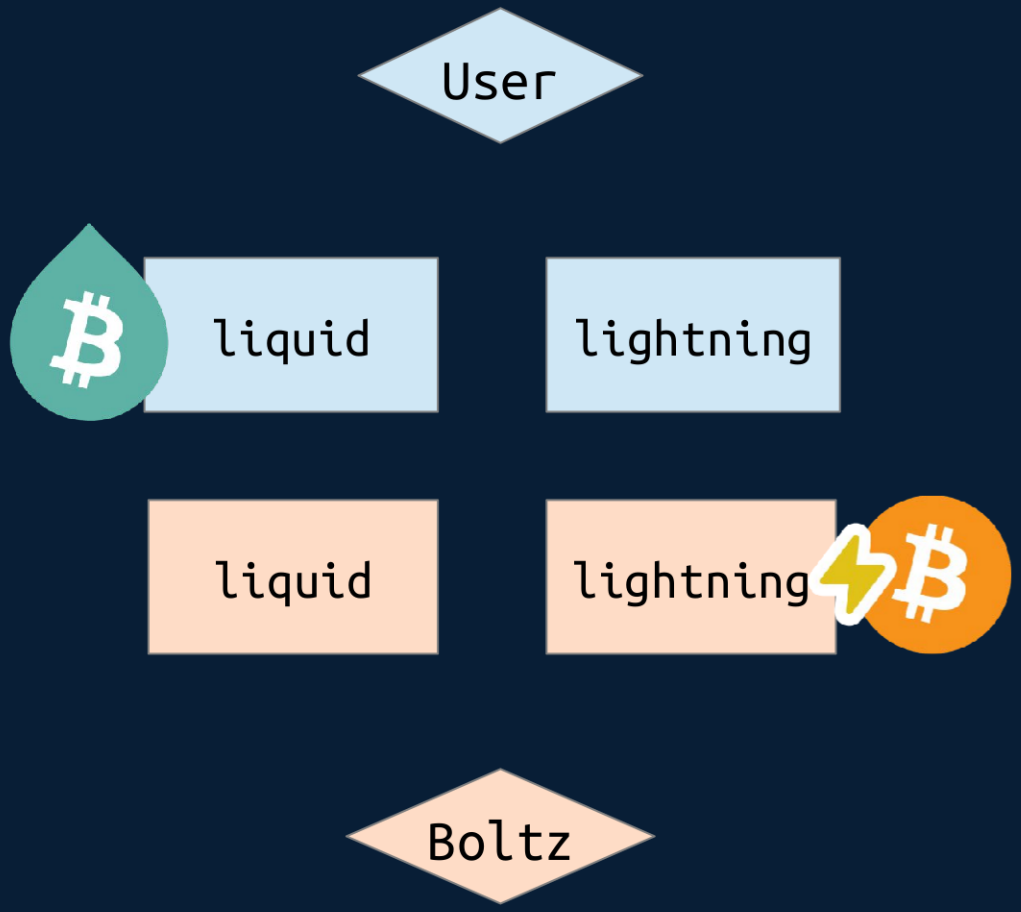
User broadcasts claim transaction on liquid because it has preimage to do so and receives 0.099 L-BTC

Reverse Submarine Swaps (⚡-BTC -> L-BTC)



Boltz detects preimage in users claim transaction and uses it to settle 0.1 BTC lightning invoice

Reverse Submarine Swaps (⚡-BTC -> L-BTC)

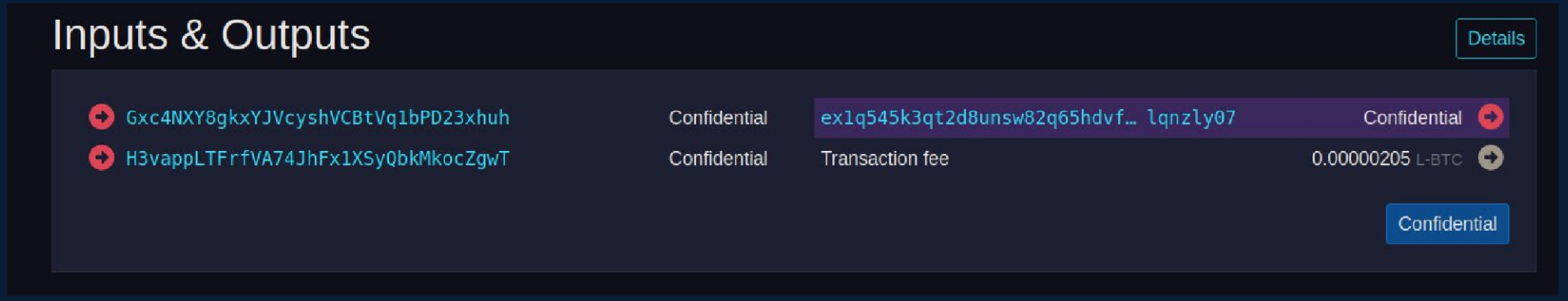


SWAP COMPLETED

That’s it!

The best part

- Reliably cheap (we broadcast with 0.11 sat/vbyte as long as liquid blocks are not full)
- Delinking from mainchain UTXO
- All liquid transactions are confidential




bol.tz