Atomic Swaps

by Boltz

What is Boltz?

Bitcoin & Lightning Service provider (LSP)

- Swap ⚡-BTC/BTC
- Channel creation
- Differentiation: atomic swaps
- Differentiation: web interface, usable via API, open-source

What is Boltz?

Privacy first

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

Stability:

- Operating since 2019
- One of the oldest & largest lightning nodes

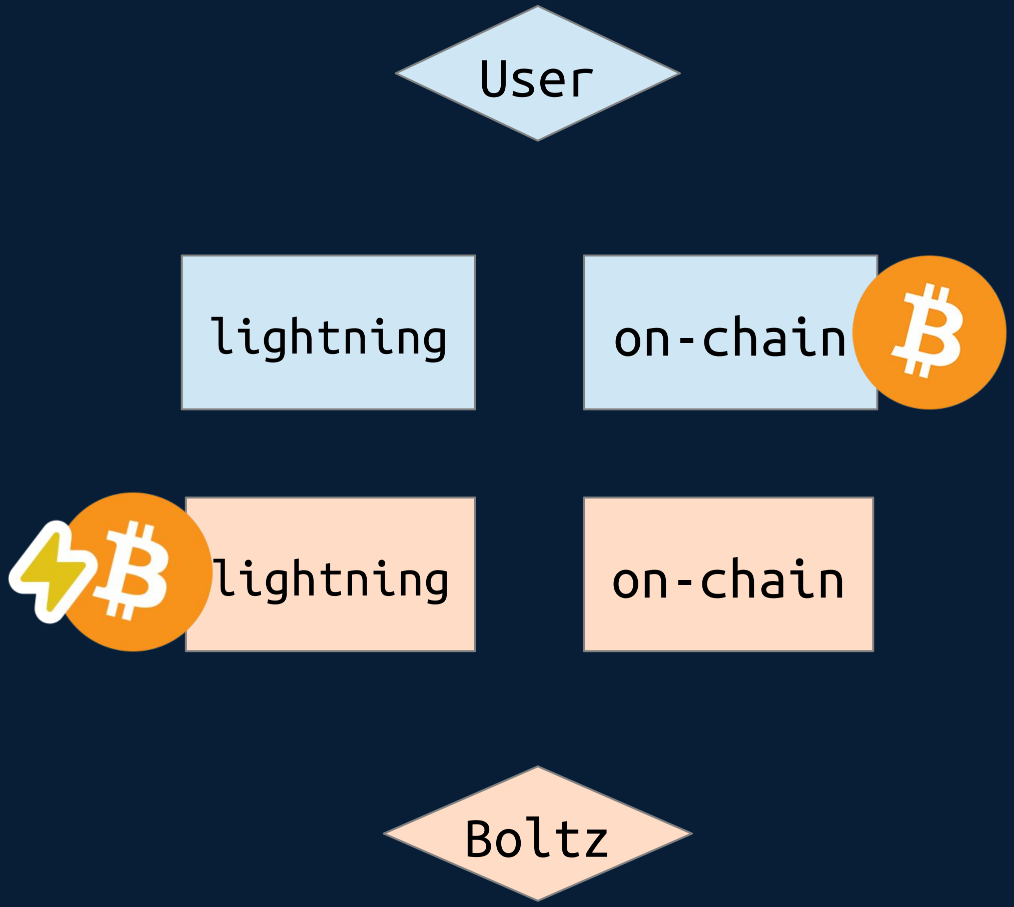
What are Atomic Swaps?

- 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.
- In contrast to many definitions found online, they don’t have to be between two different chains or even P2P.
- Very important for us as a swap provider: this means we are never holding customer funds, not even for a split-second

Who uses Boltz?

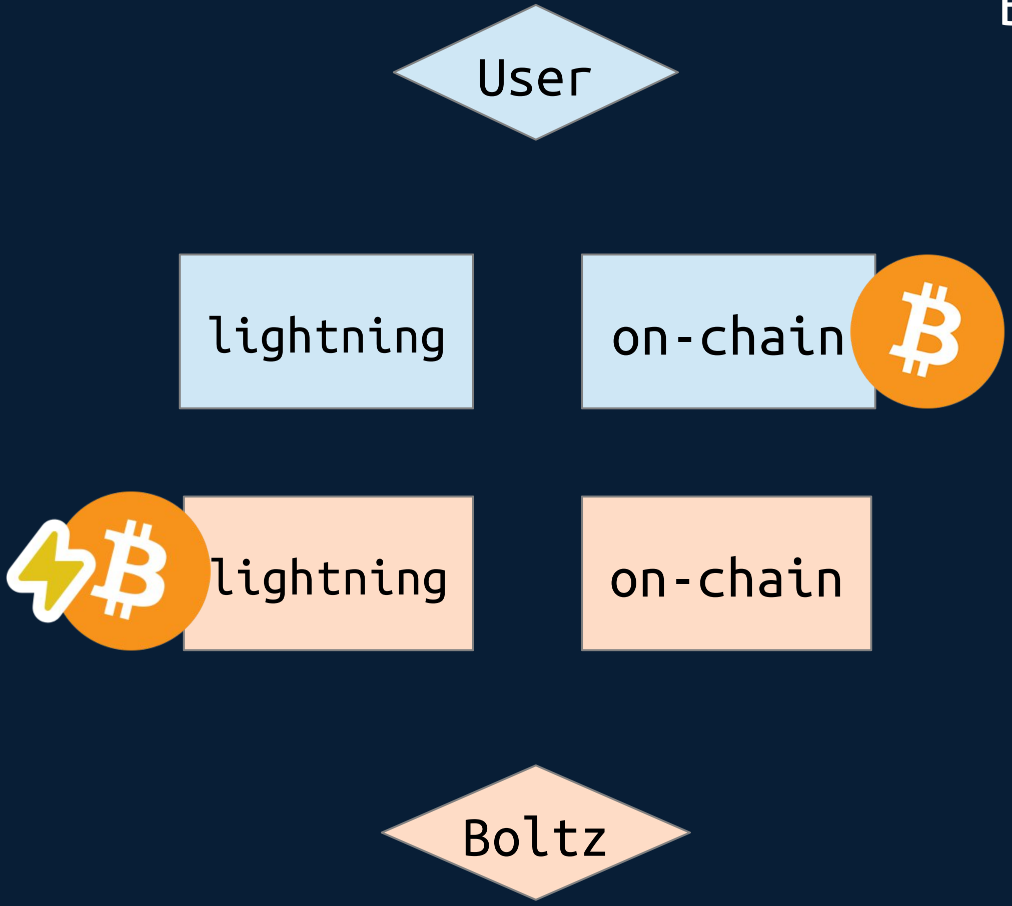
- Lightning Node operators
  - Rebalance channels
  - Get a new channel
- Lightning Wallets
  - receive from/pay to on-chain
- On-chain Wallets
  - receive from/pay to lightning
- Do more with your Bitcoin
  - Convert them to L-BTC to use financial products on the Liquid sidechain

Atomic Swaps

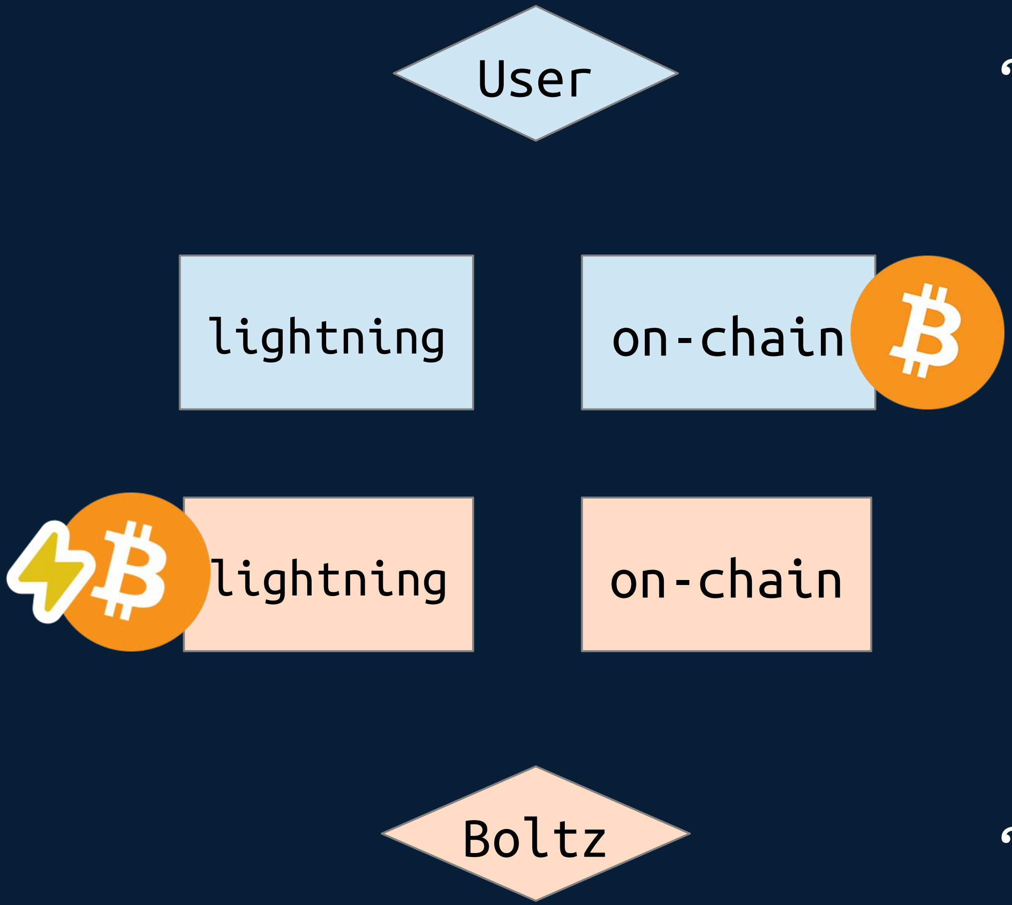


Normal Submarine Swaps (BTC -> ⚡-BTC)

Boltz Swap Protocol (simplified):



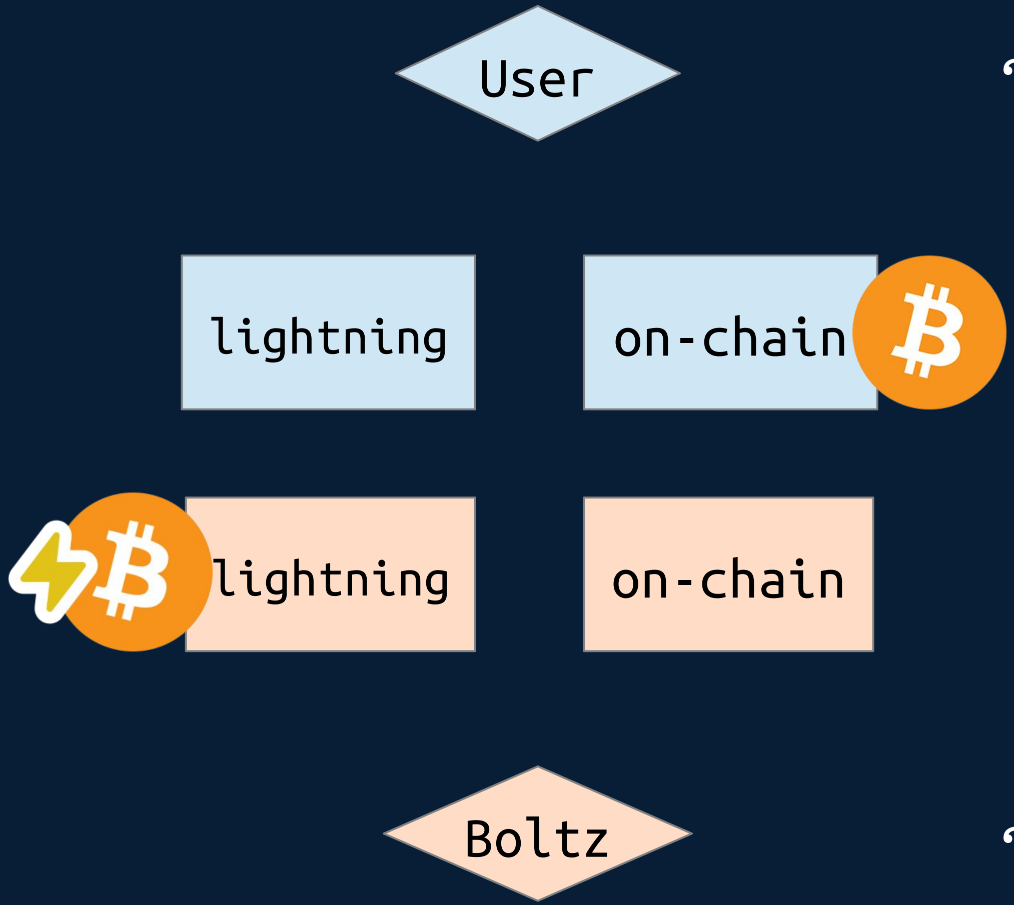
Normal Submarine Swaps (BTC -> ⚡-BTC)



“Send: 0.1 BTC”

“Receive: 0.09 BTC”

Normal Submarine Swaps (BTC -> ⚡-BTC)



User

lightning

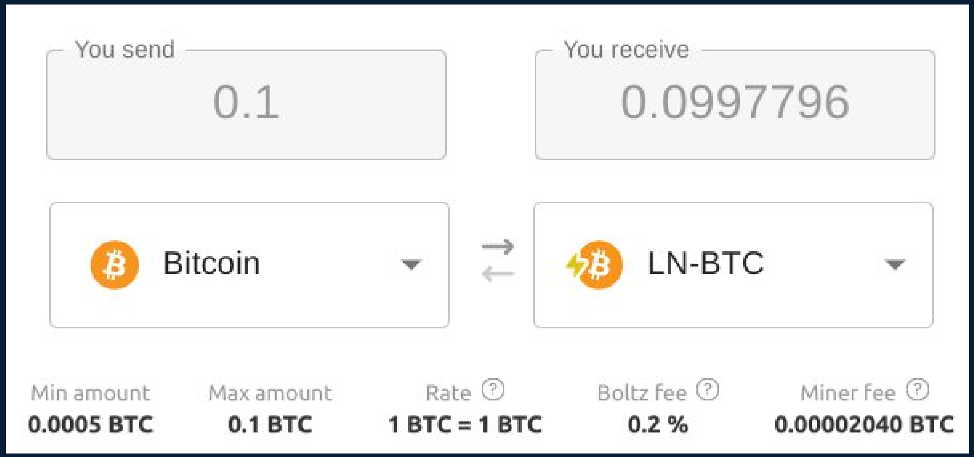
on-chain

lightning

on-chain

Boltz

“Send: 0.1 BTC”



You send: 0.1

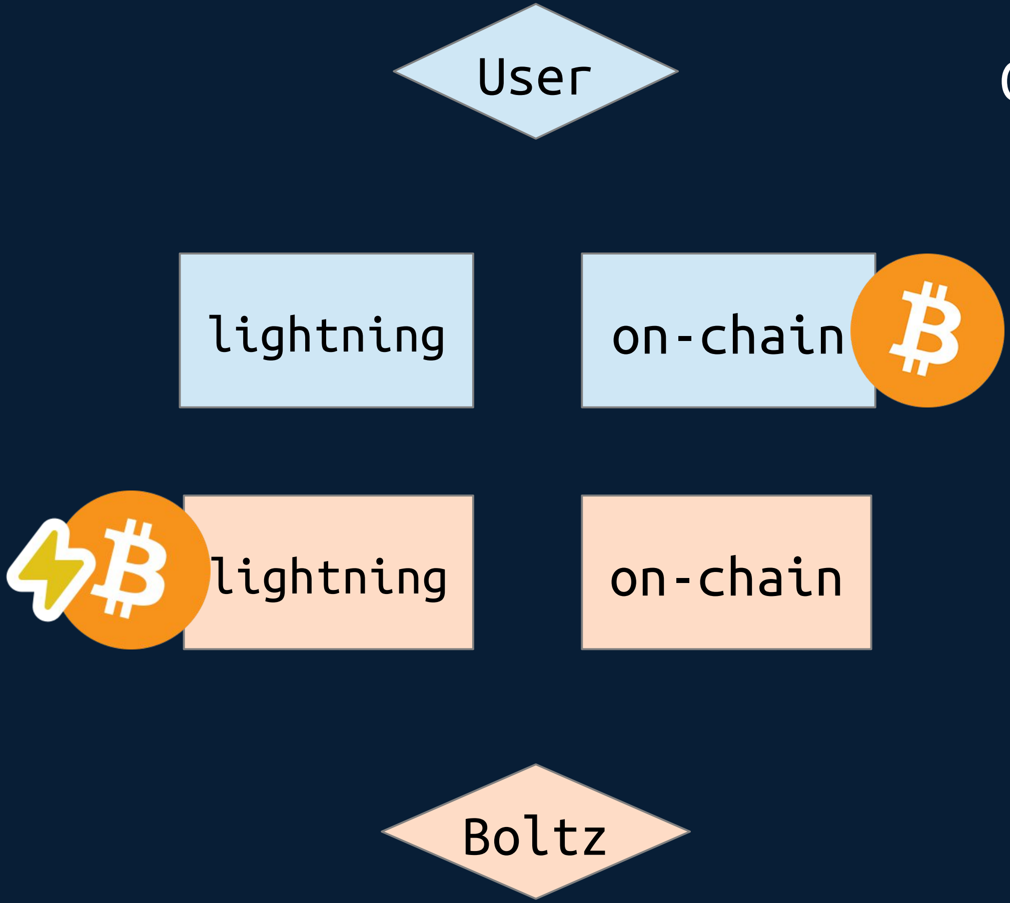
You receive: 0.0997796

Bitcoin ⇄ LN-BTC

Min amount	Max amount	Rate	Boltz fee	Miner fee
0.0005 BTC	0.1 BTC	1 BTC = 1 BTC	0.2 %	0.00002040 BTC

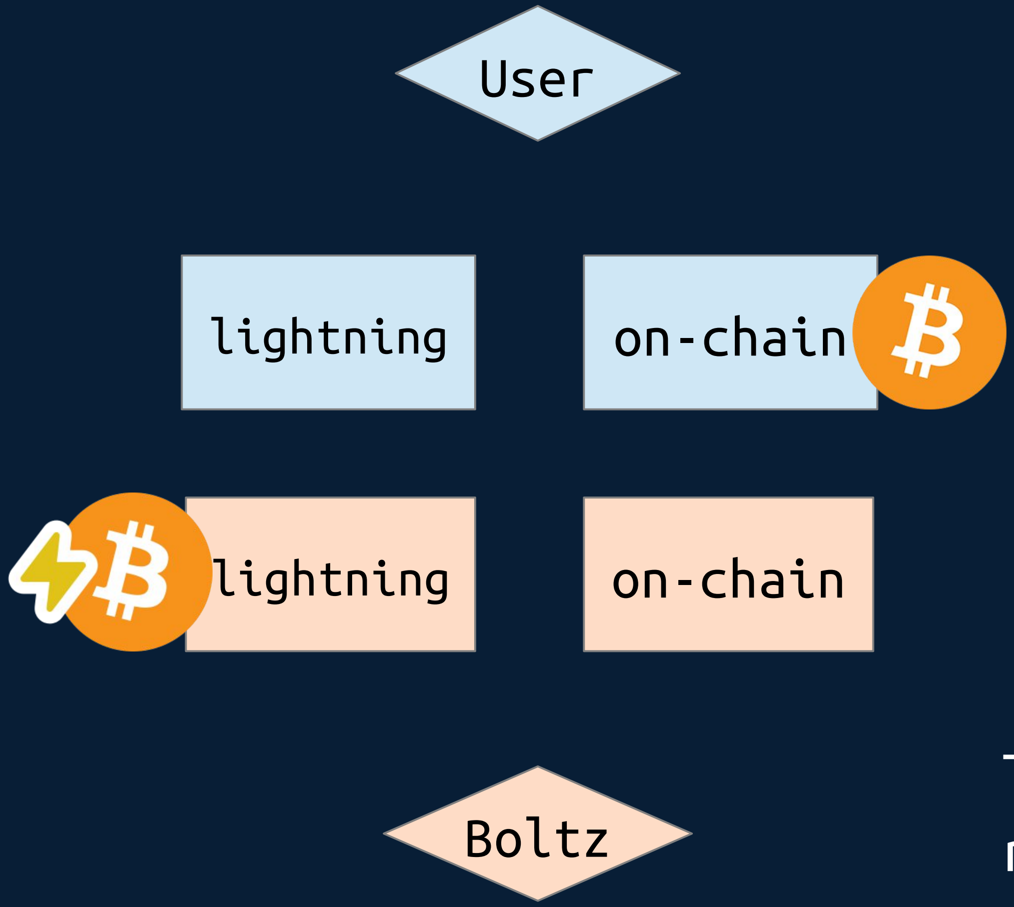
“Receive: 0.09 BTC”

Normal Submarine Swaps (BTC -> ⚡-BTC)



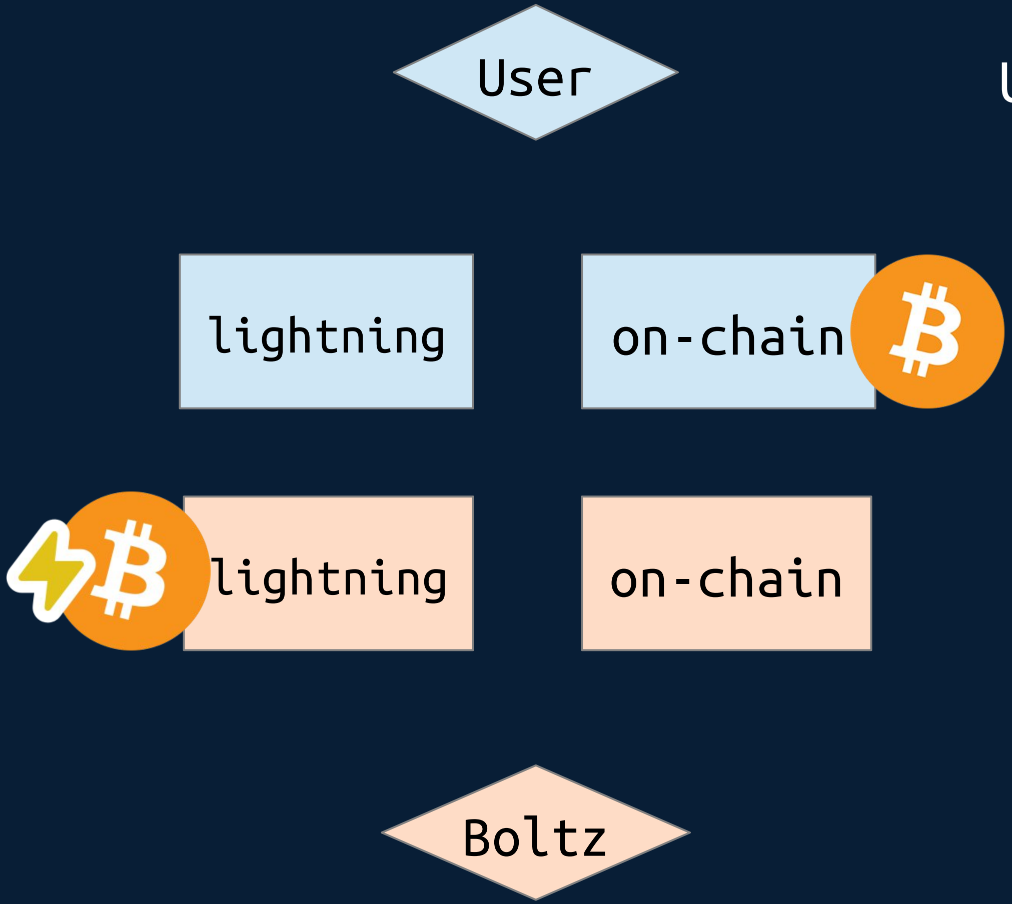
Create ⚡-invoice for 0.09 BTC

Normal Submarine Swaps (BTC -> ⚡-BTC)



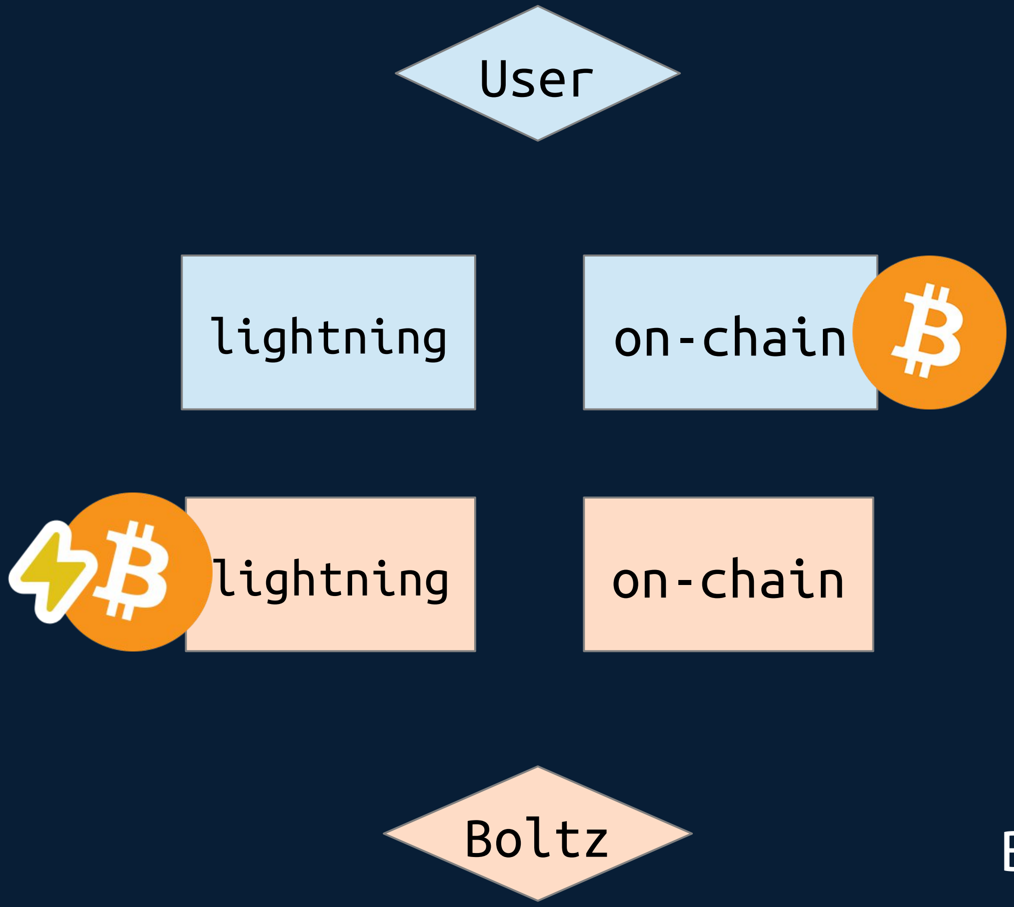
Take invoice preimage hash and create redeem script to generate on-chain btc address for user to send 0.1 BTC to

Normal Submarine Swaps (BTC -> ⚡-BTC)



User sends 0.1 BTC to this address

Normal Submarine Swaps (BTC -> ⚡-BTC)



User

lightning

on-chain

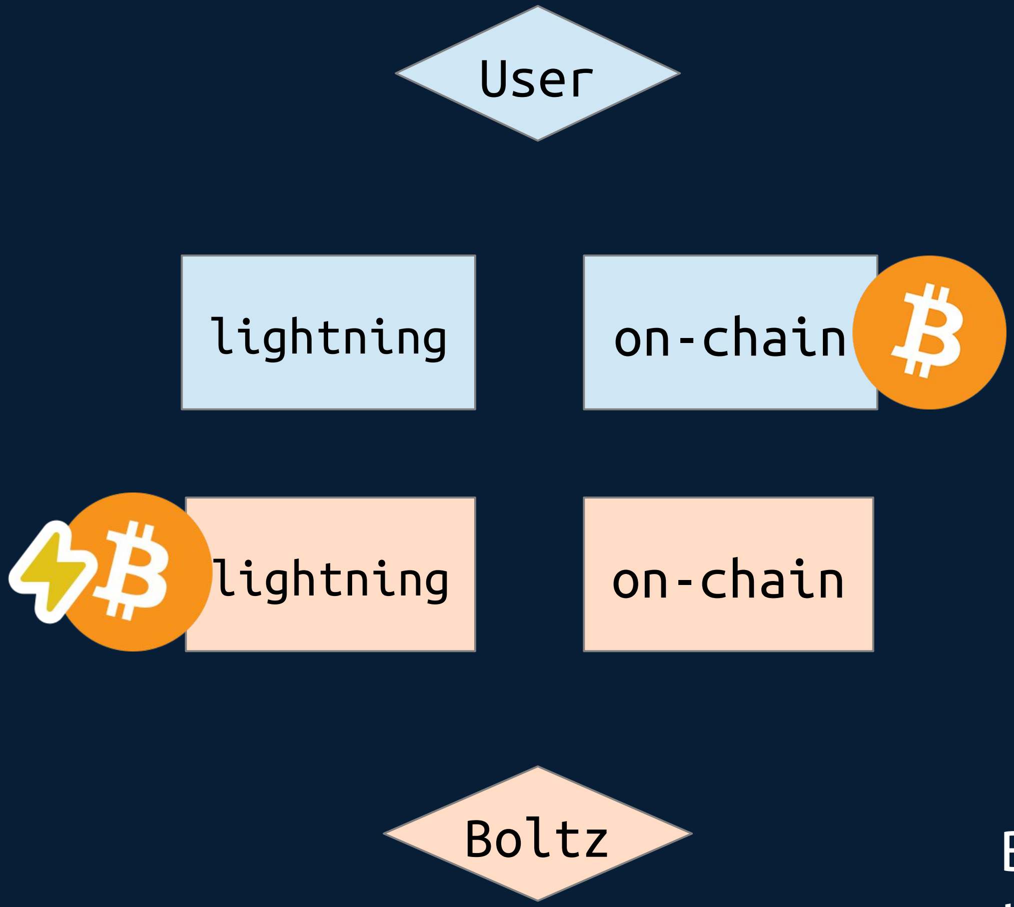
lightning

on-chain

Boltz

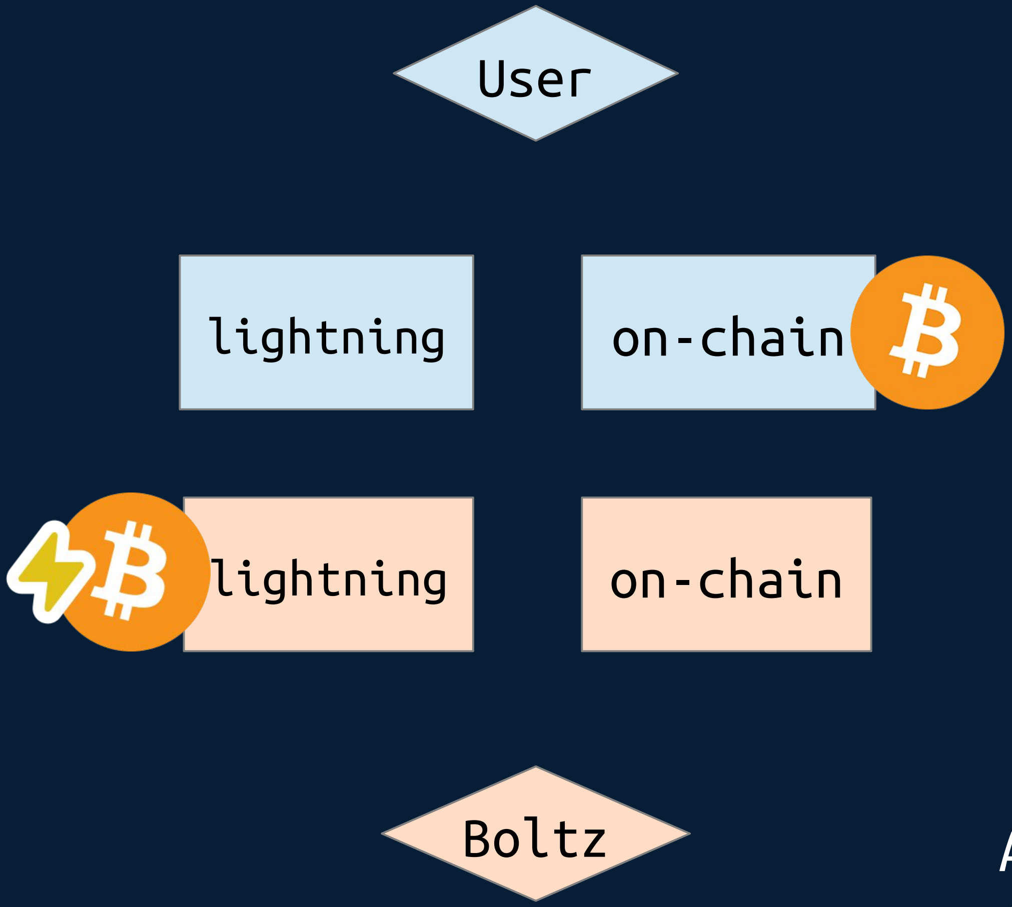
Boltz waits for one confirmation

Normal Submarine Swaps (BTC -> ⚡-BTC)



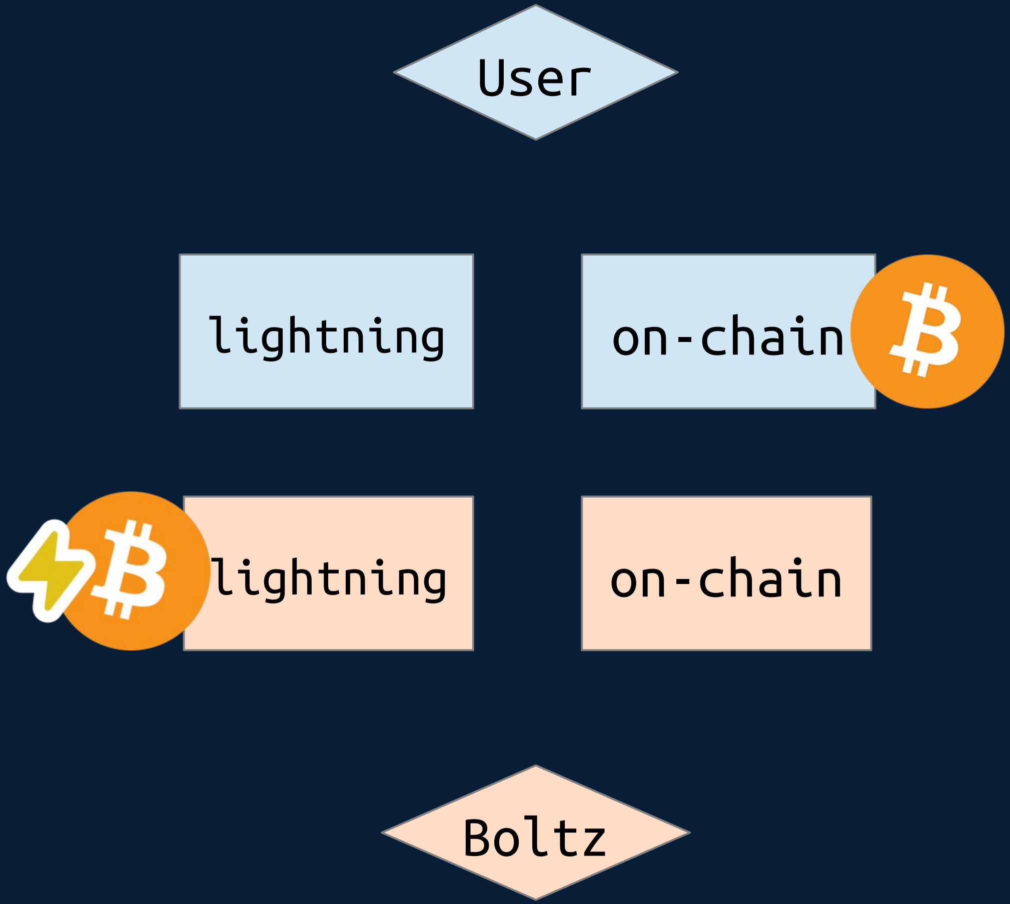
Boltz pays 0.09 BTC lightning invoice,
because of this preimage gets revealed

Normal Submarine Swaps (BTC -> ⚡-BTC)



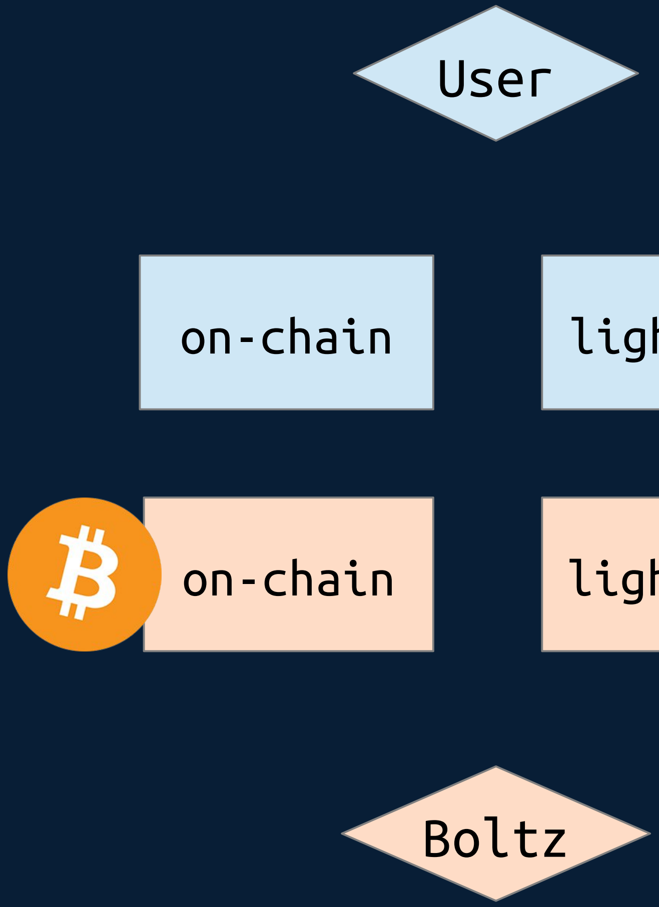
And Boltz can claim 0.1 BTC on-chain from redeem script

Normal Submarine Swaps (BTC -> ⚡-BTC)



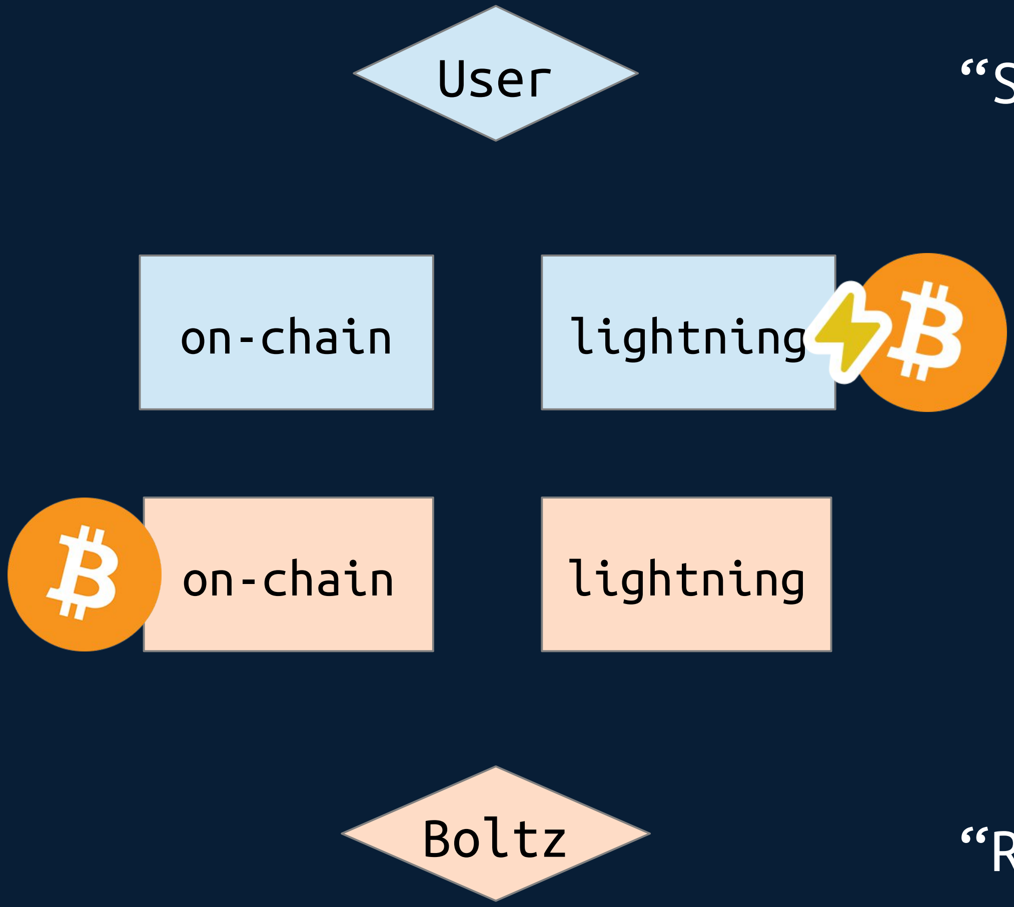
SWAP COMPLETED

Reverse Submarine Swaps (⚡-BTC -> BTC)



Boltz Swap Protocol (simplified):

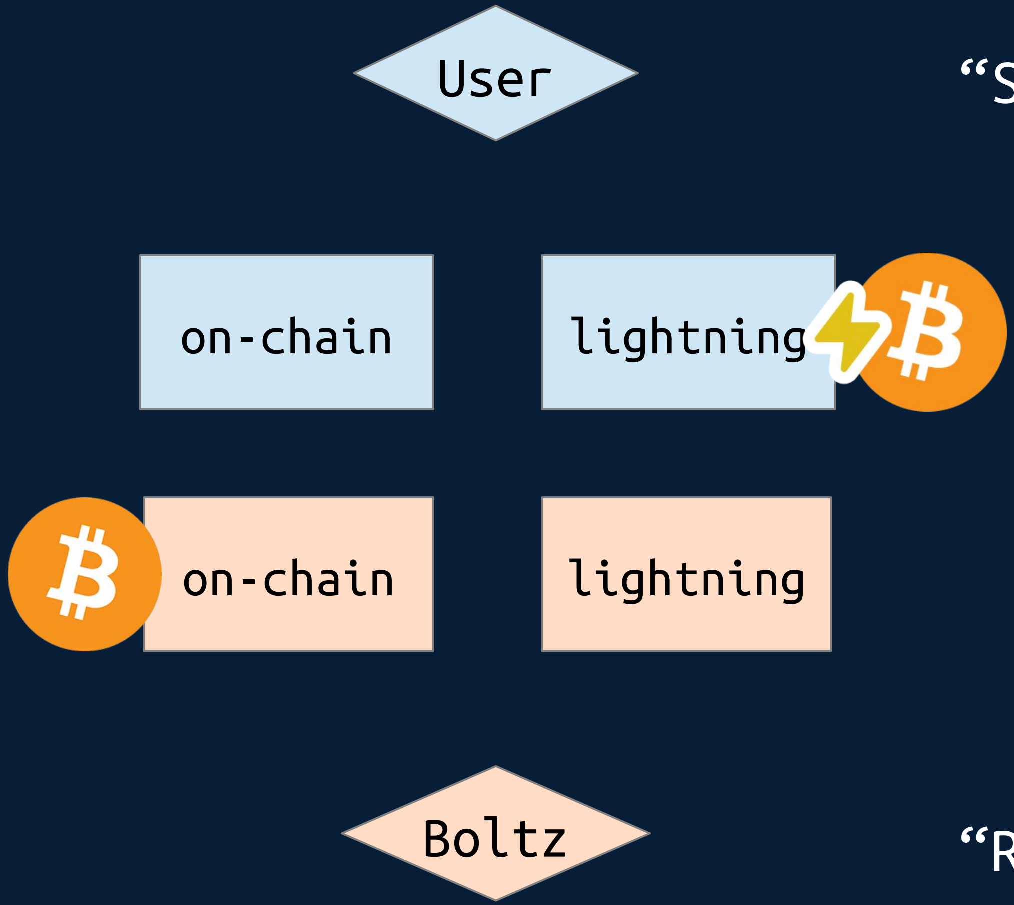
Reverse Submarine Swaps (⚡-BTC -> BTC)



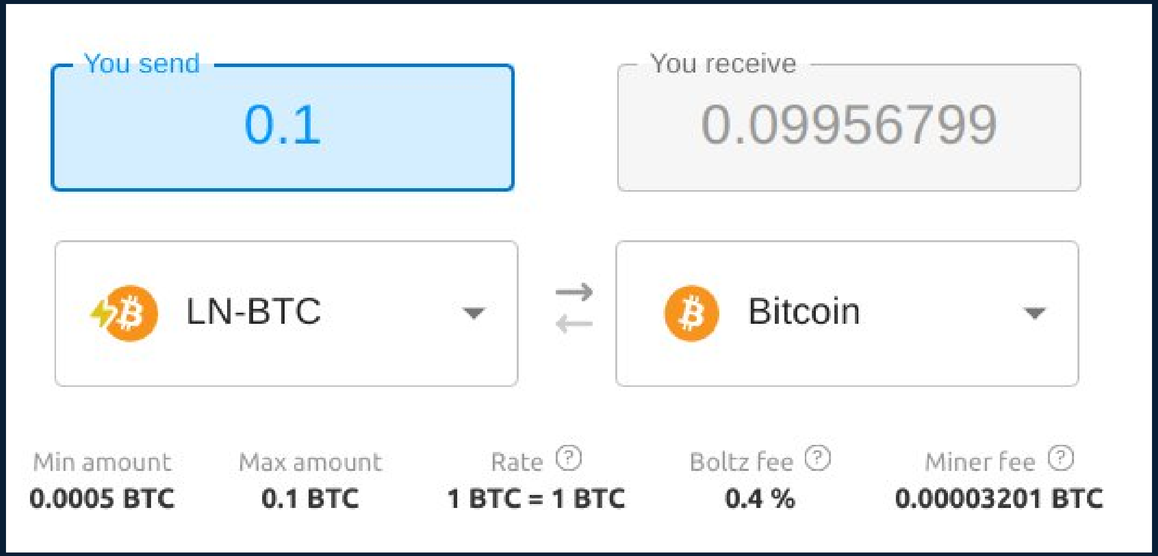
“Send: 0.1 BTC”

“Receive: 0.09 BTC”

Reverse Submarine Swaps (⚡-BTC -> BTC)



“Send: 0.1 BTC”



You send: 0.1

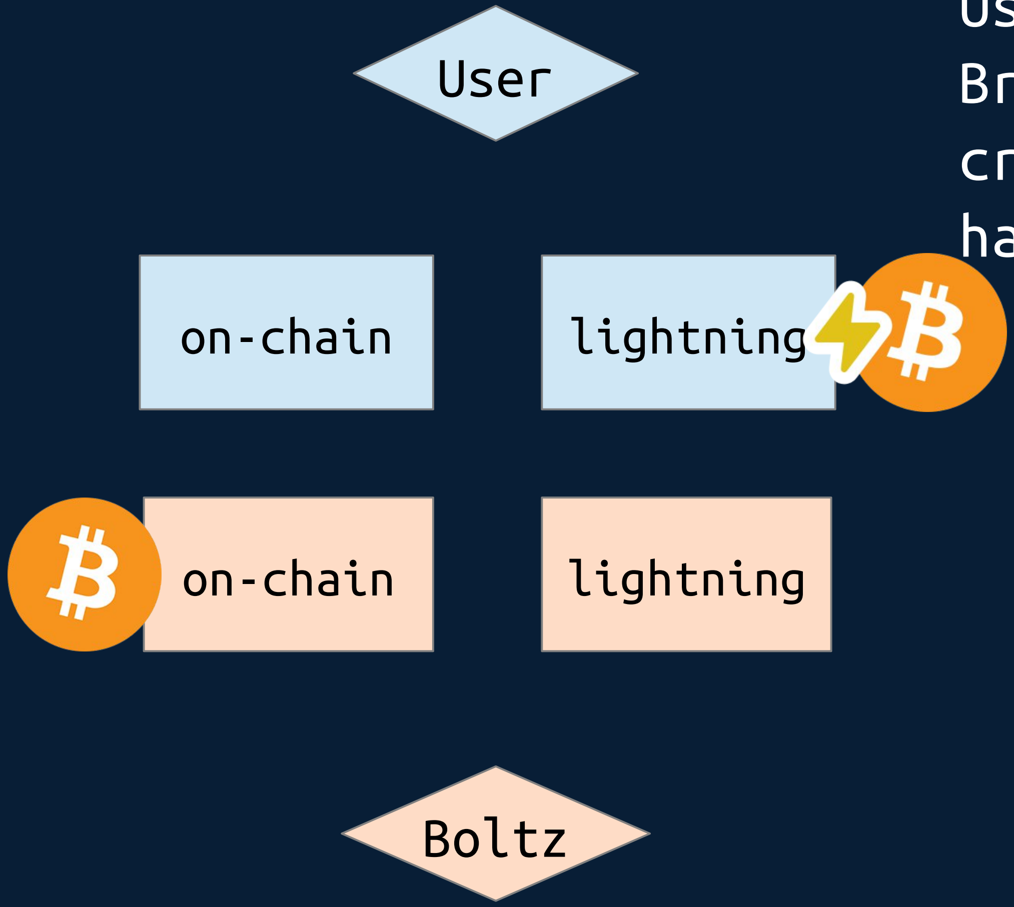
You receive: 0.09956799

LN-BTC ⇄ Bitcoin

Min amount	Max amount	Rate	Boltz fee	Miner fee
0.0005 BTC	0.1 BTC	1 BTC = 1 BTC	0.4 %	0.00003201 BTC

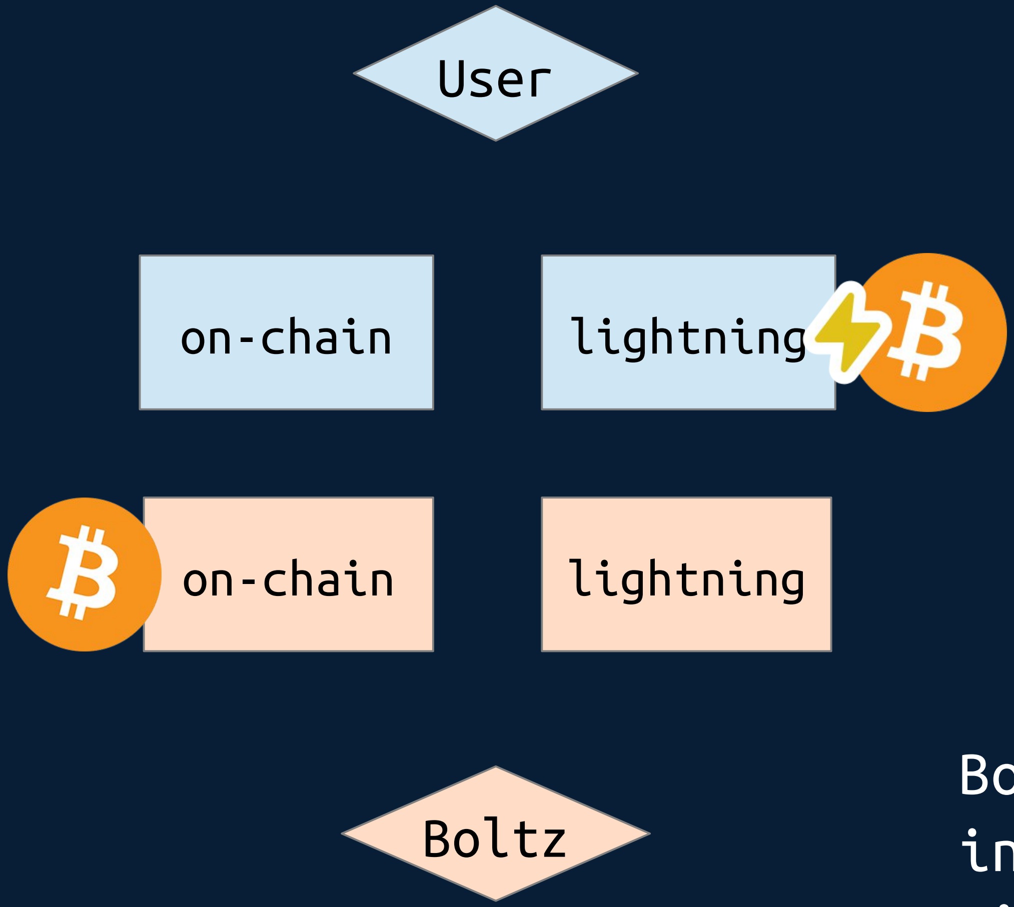
“Receive: 0.09 BTC”

Reverse Submarine Swaps (⚡-BTC -> BTC)



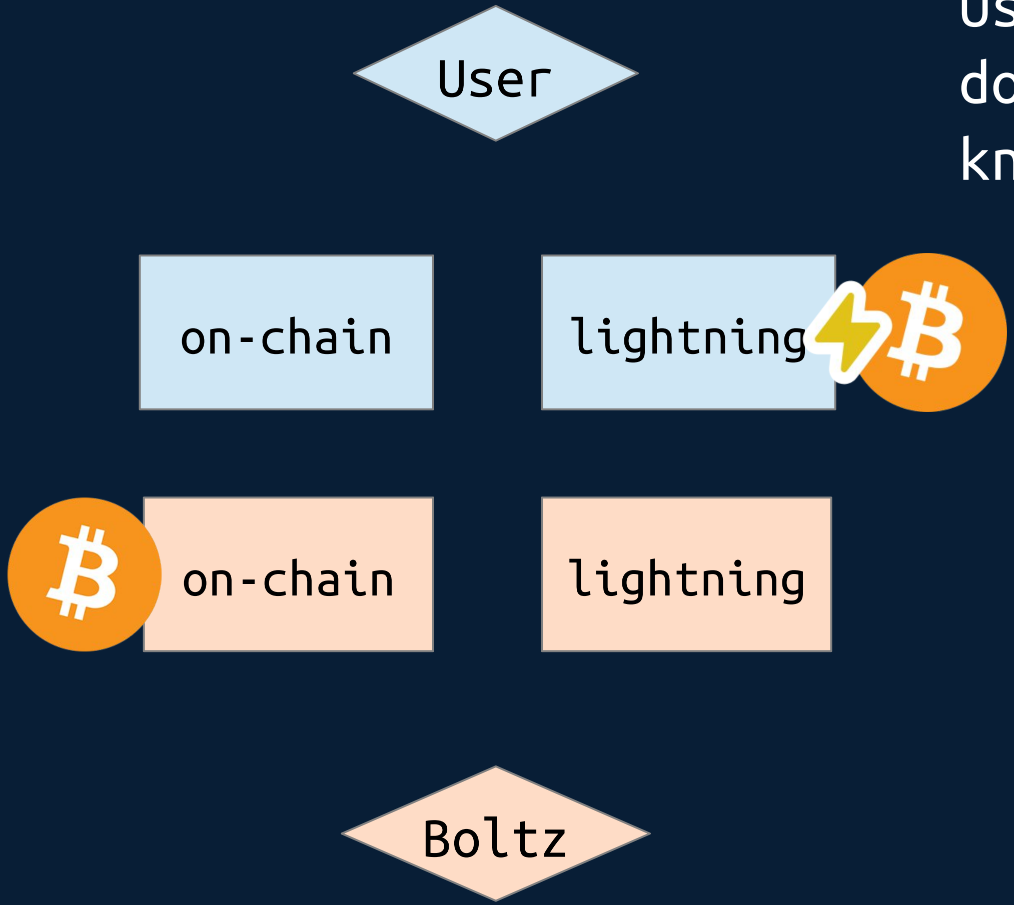
User’s app (e.g. boltz.exchange or Breez Wallet) generates a preimage, creates SHA256 hash of it and sends hash to Boltz

Reverse Submarine Swaps (⚡-BTC -> BTC)



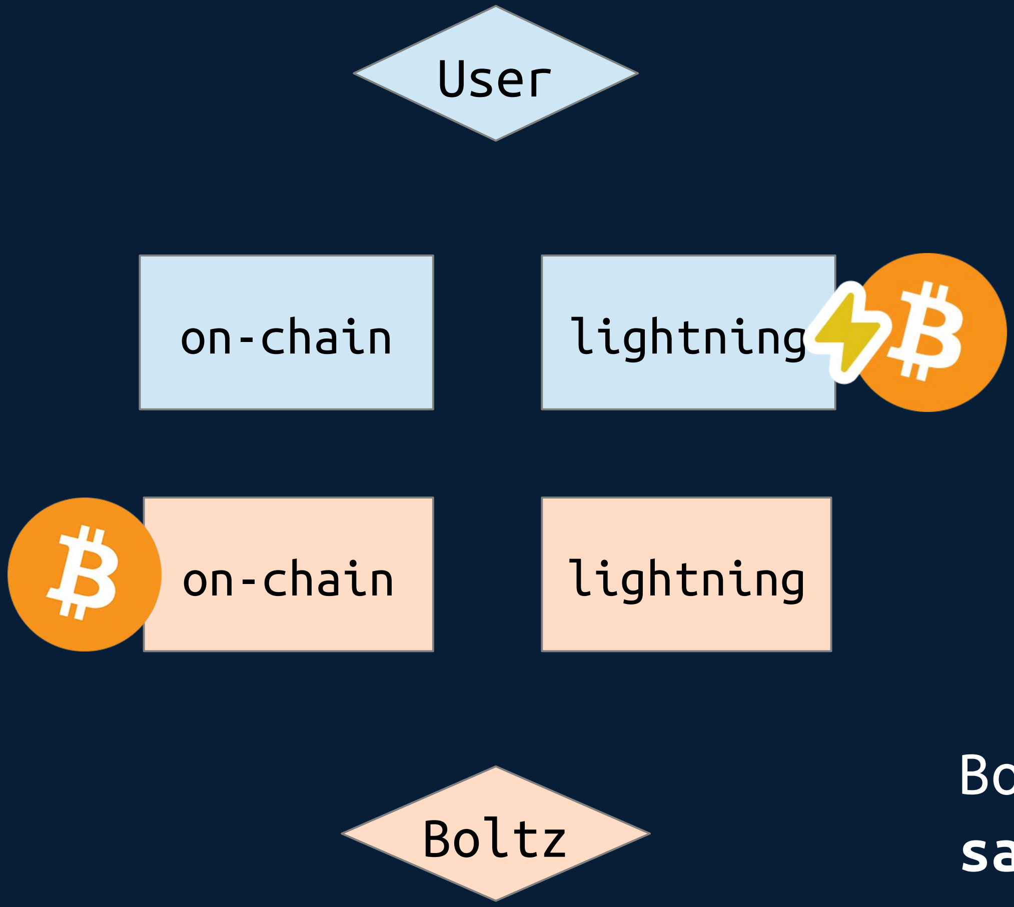
Boltz creates a so-called “hold invoice” about 0.1 BTC
with hash received from user

Reverse Submarine Swaps (⚡-BTC -> BTC)



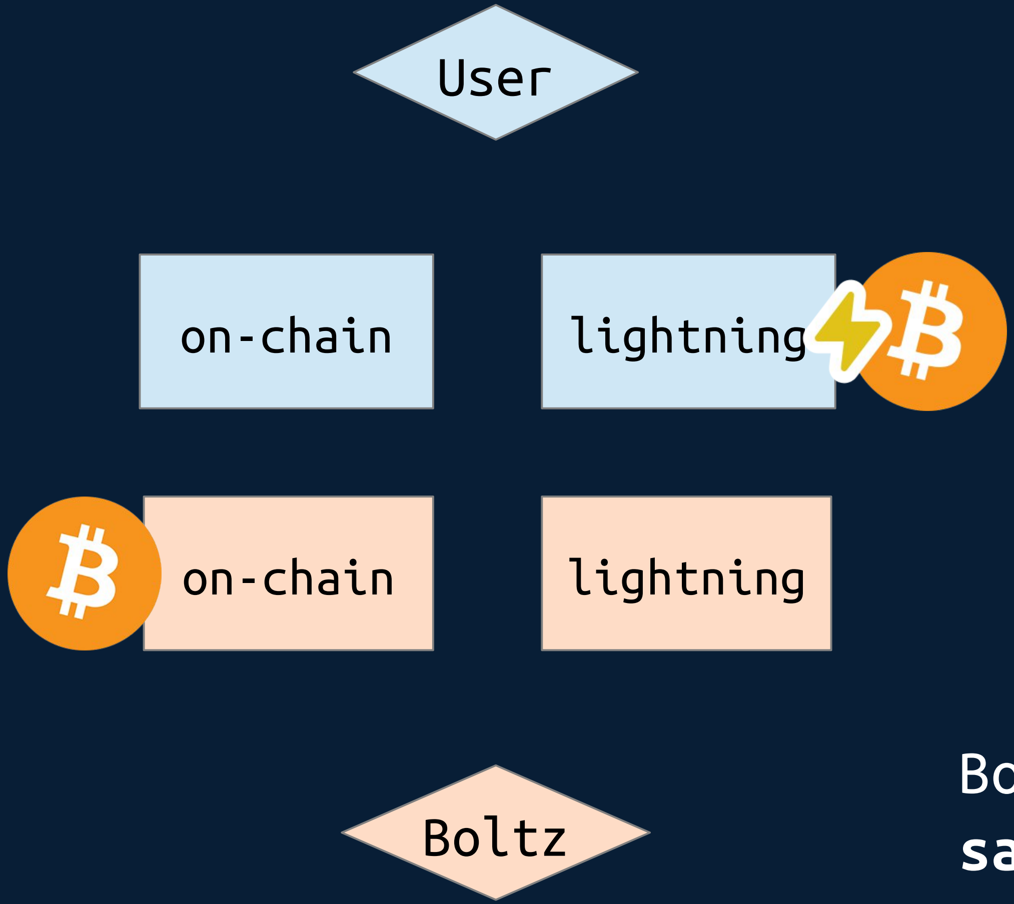
User pays Boltz’ invoice, but invoice does not settle because Boltz doesn’t know preimage to do so yet

Reverse Submarine Swaps (⚡-BTC -> BTC)



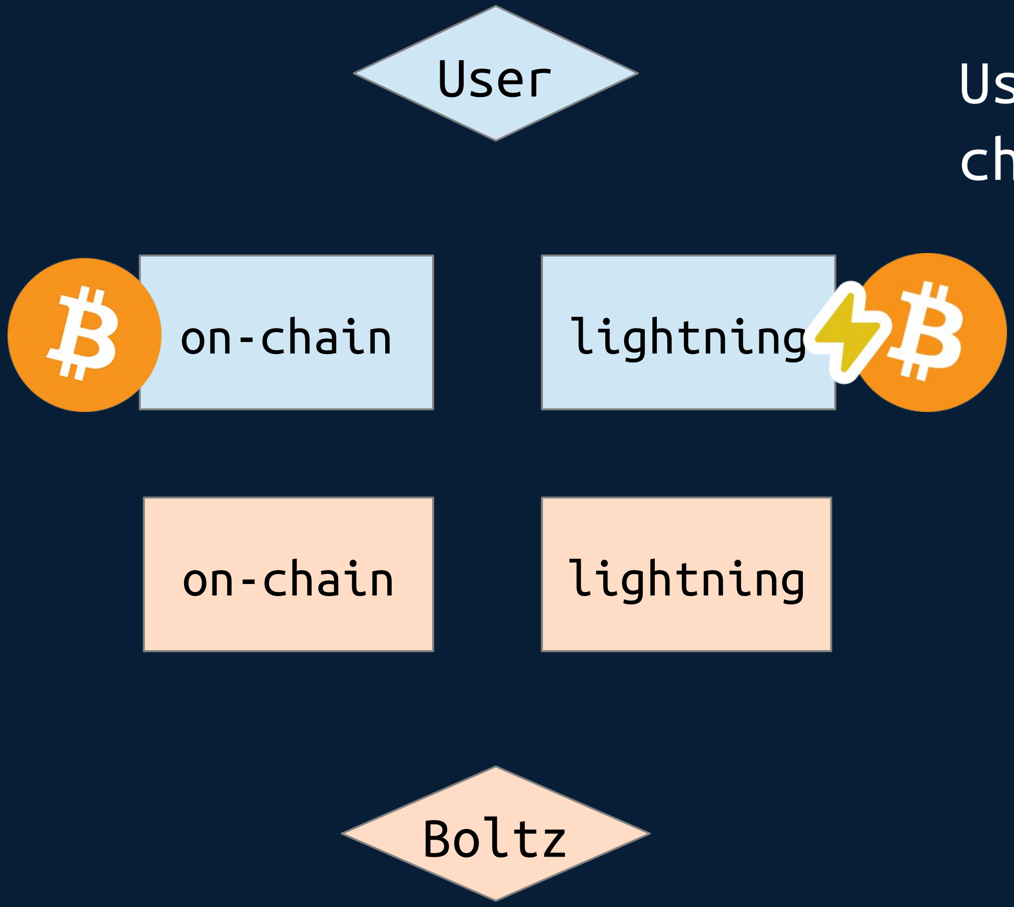
Boltz locks up 0.09 BTC on-chain using **same hash from user**

Reverse Submarine Swaps (⚡-BTC -> BTC)



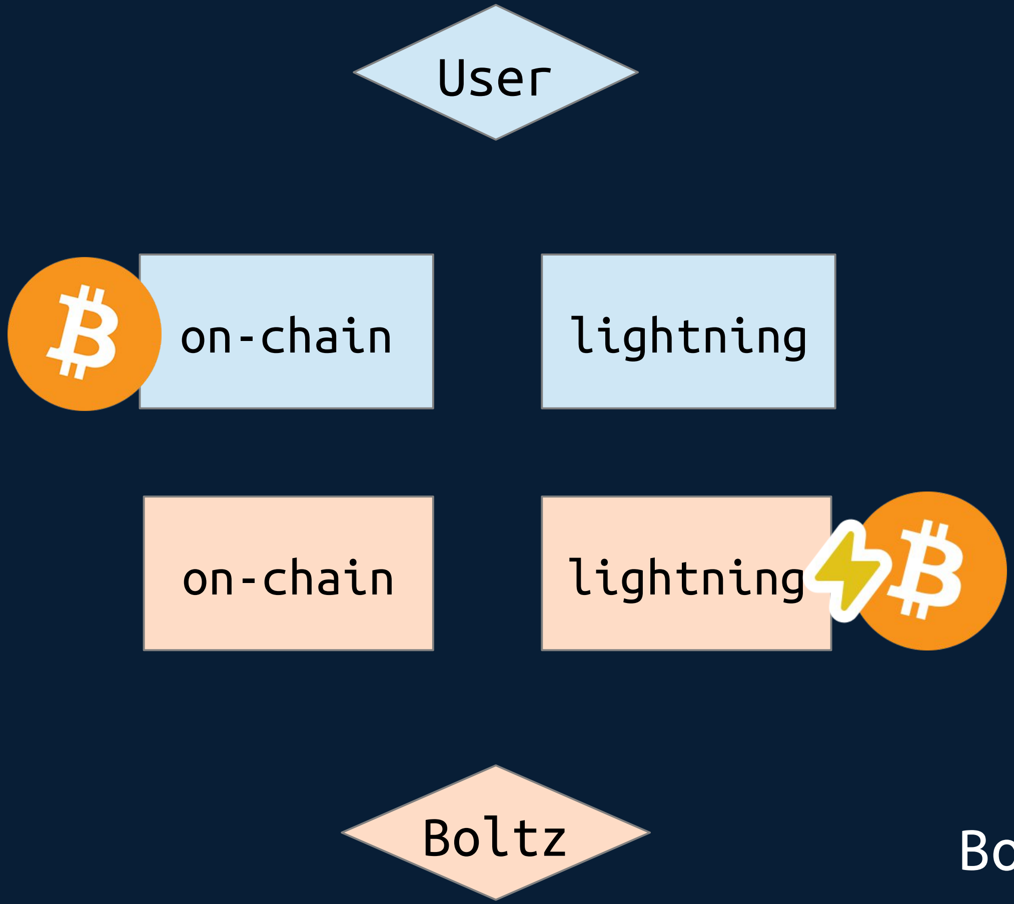
Boltz locks up 0.09 BTC on-chain using **same hash from user**

Reverse Submarine Swaps (⚡-BTC -> BTC)



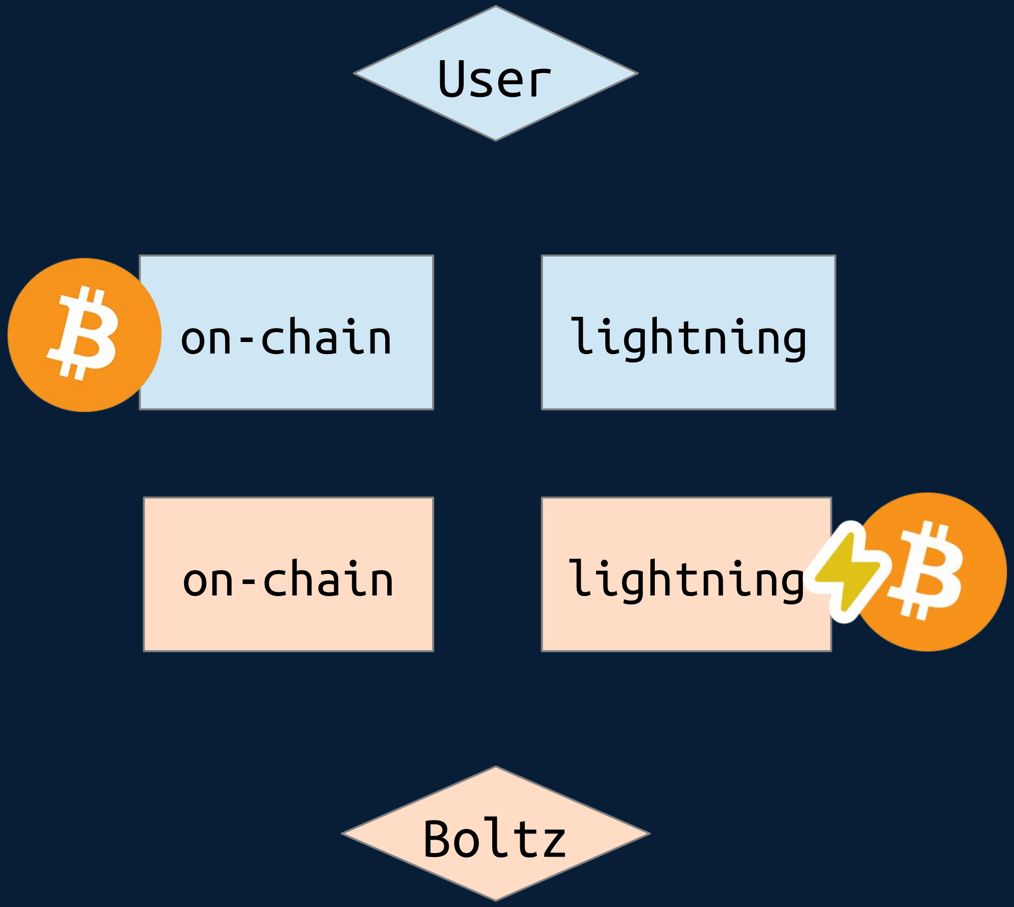
User broadcasts claim transaction on-chain and receives 0.09 BTC

Reverse Submarine Swaps (⚡-BTC -> BTC)



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

Reverse Submarine Swaps (⚡-BTC -> BTC)



SWAP COMPLETED

That’s it!

Resources

boltz.exchange

docs.boltz.exchange

github.com/BoltzExchange

twitter.com/boltzhq