The Basics of Taproot Swaps

What?

 Lightning  Liquid  Rootstock

---

Mainchain

Why?

- Cheaper DCAing
- Use Financial Products
- Lightning Channel Rebalancing
- Spending
- ...

How?

HTLCs

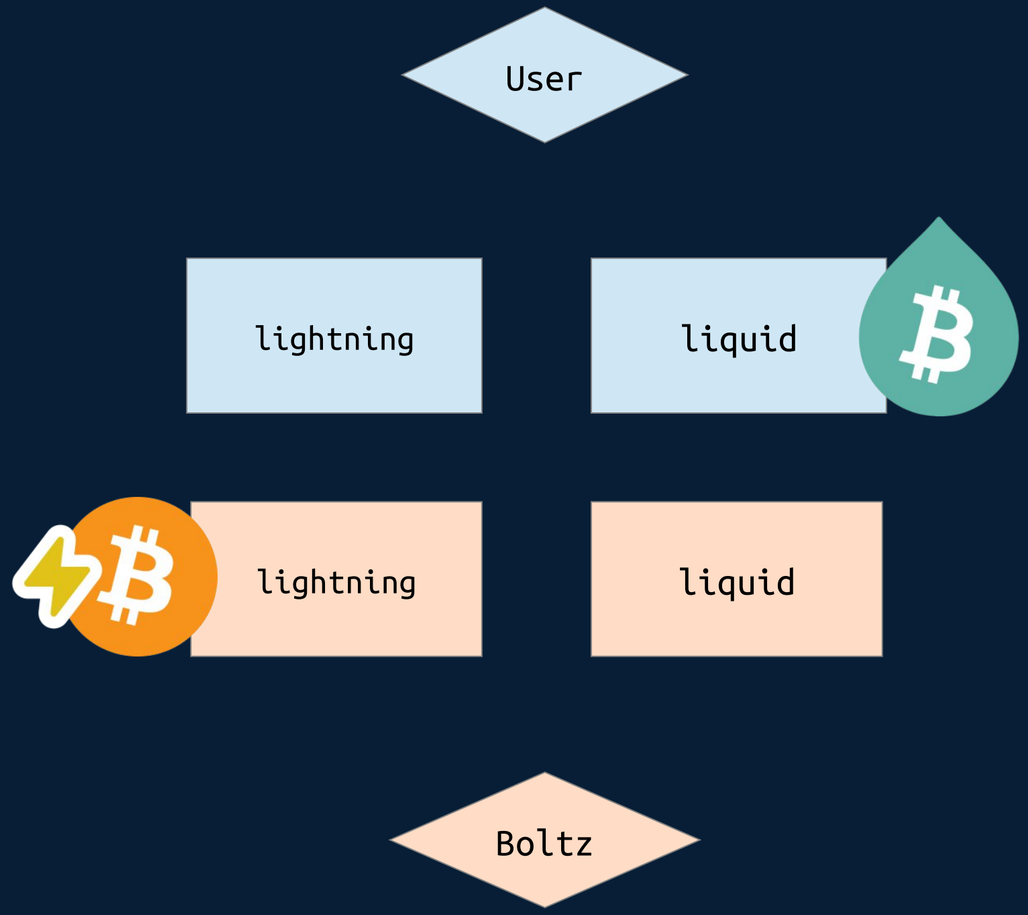
We need

- Hash lock
- Time lock

Payments on Lightning

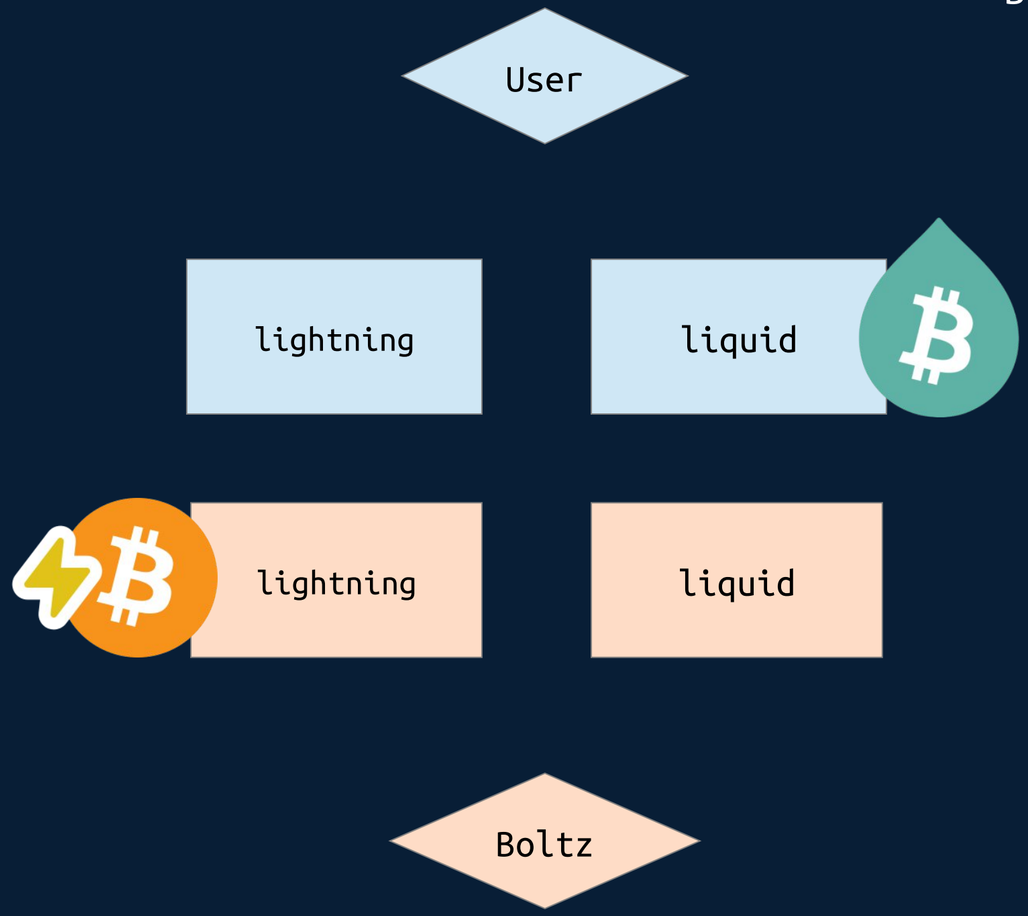
Swaps on Lightning

Atomic Swaps – Submarine Swaps

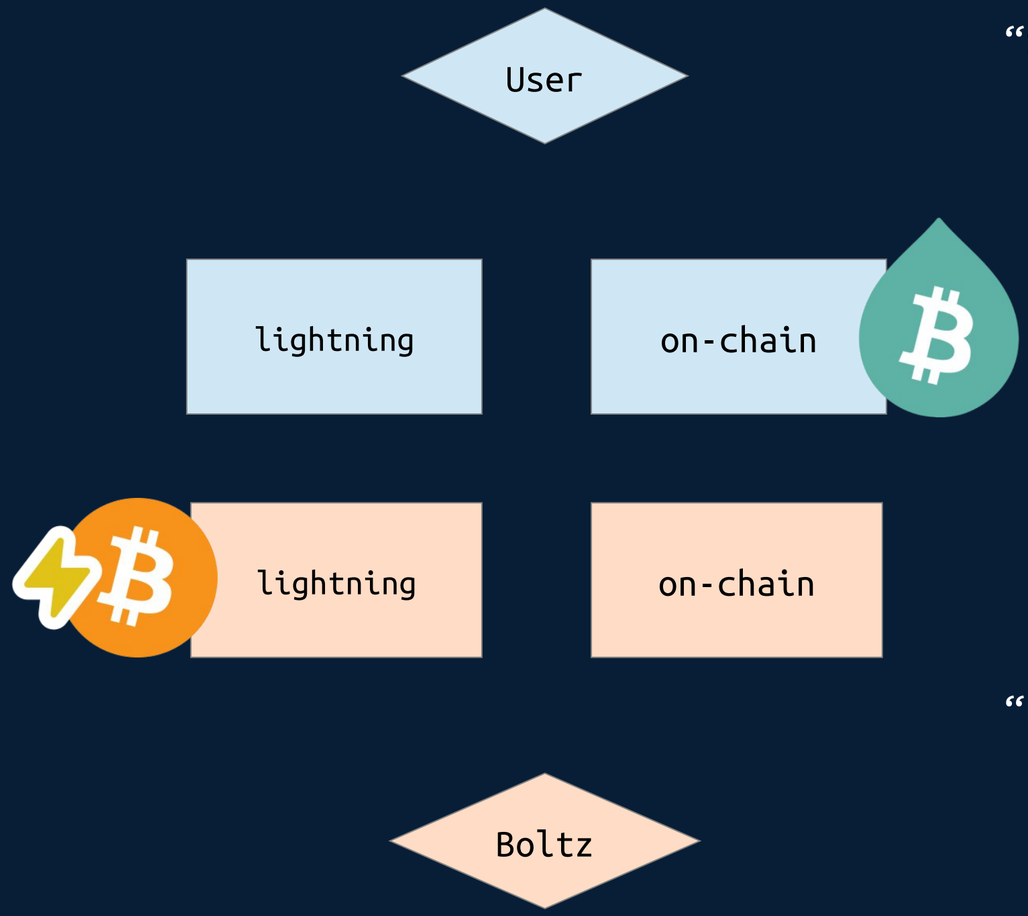


Submarine Swaps (L-BTC -> ⚡-BTC)

Boltz Swap Protocol (simplified):



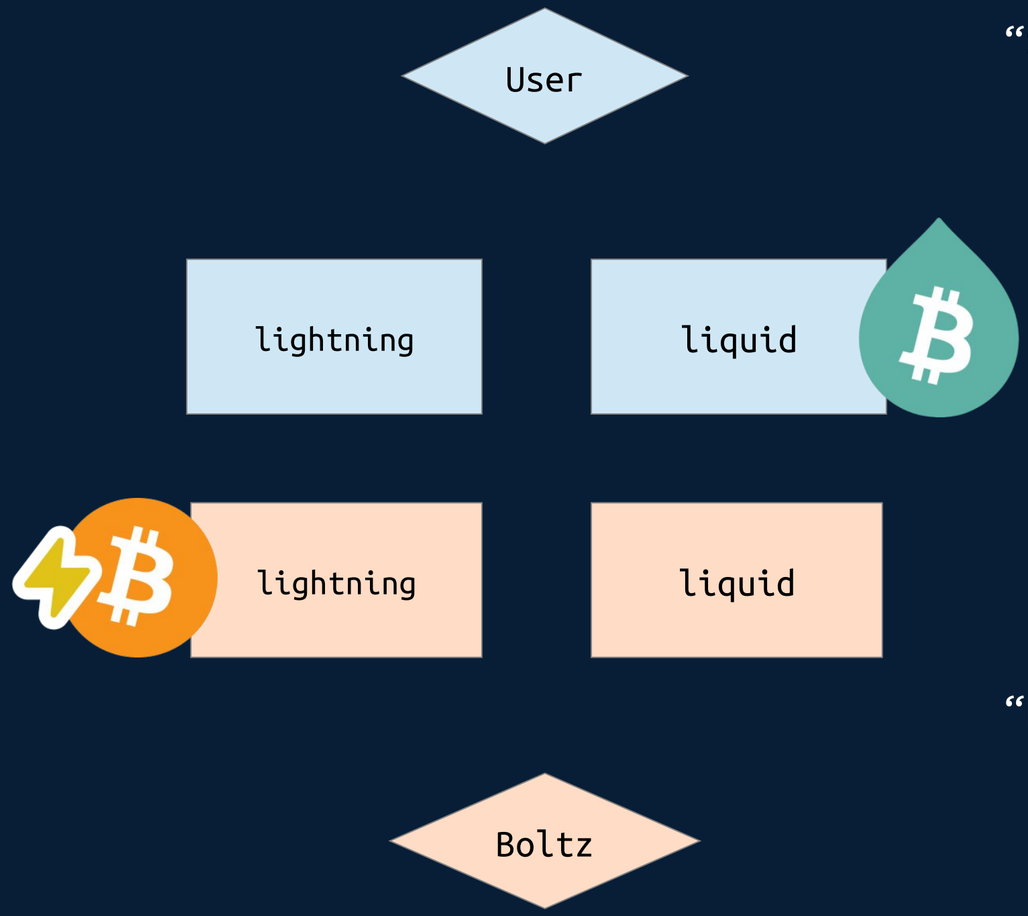
Submarine Swaps (L-BTC -> ⚡-BTC)



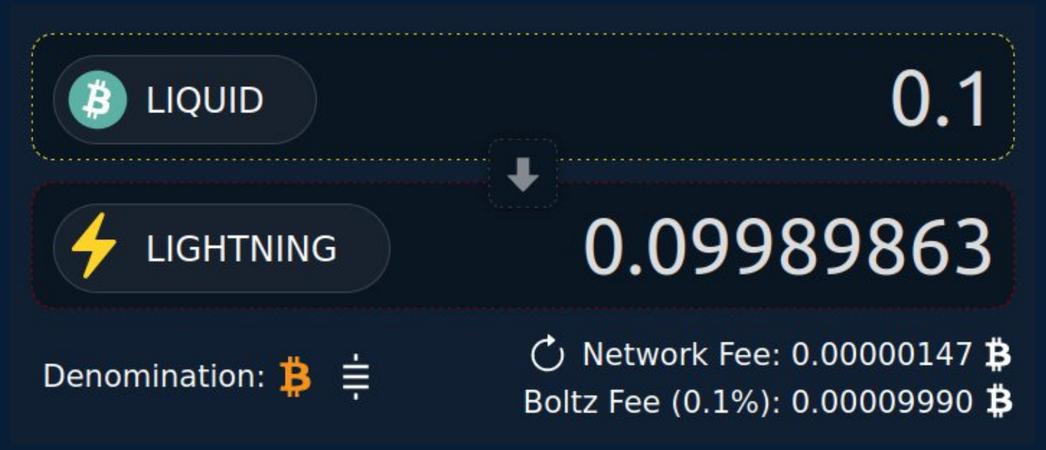
“Send: 0.1 L-BTC”

“Receive: 0.099 ⚡-BTC”

Submarine Swaps (L-BTC -> ⚡-BTC)

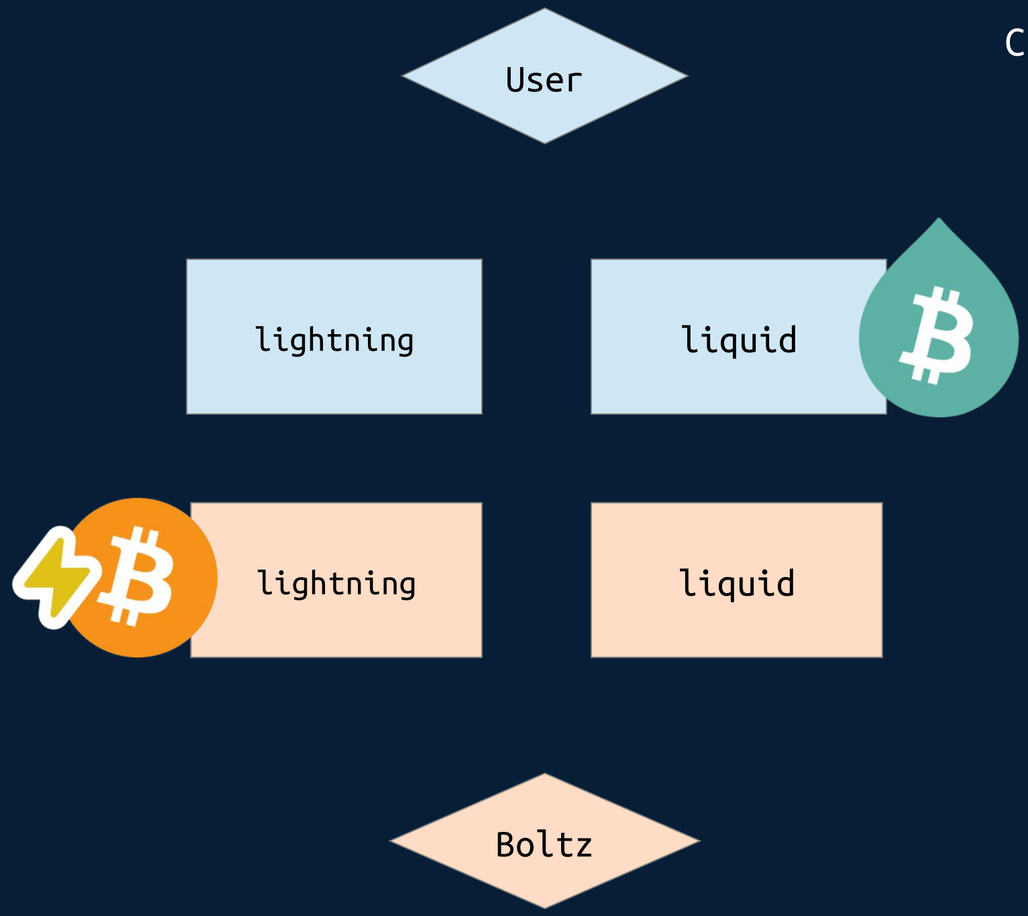


“Send: 0.1 L-BTC”



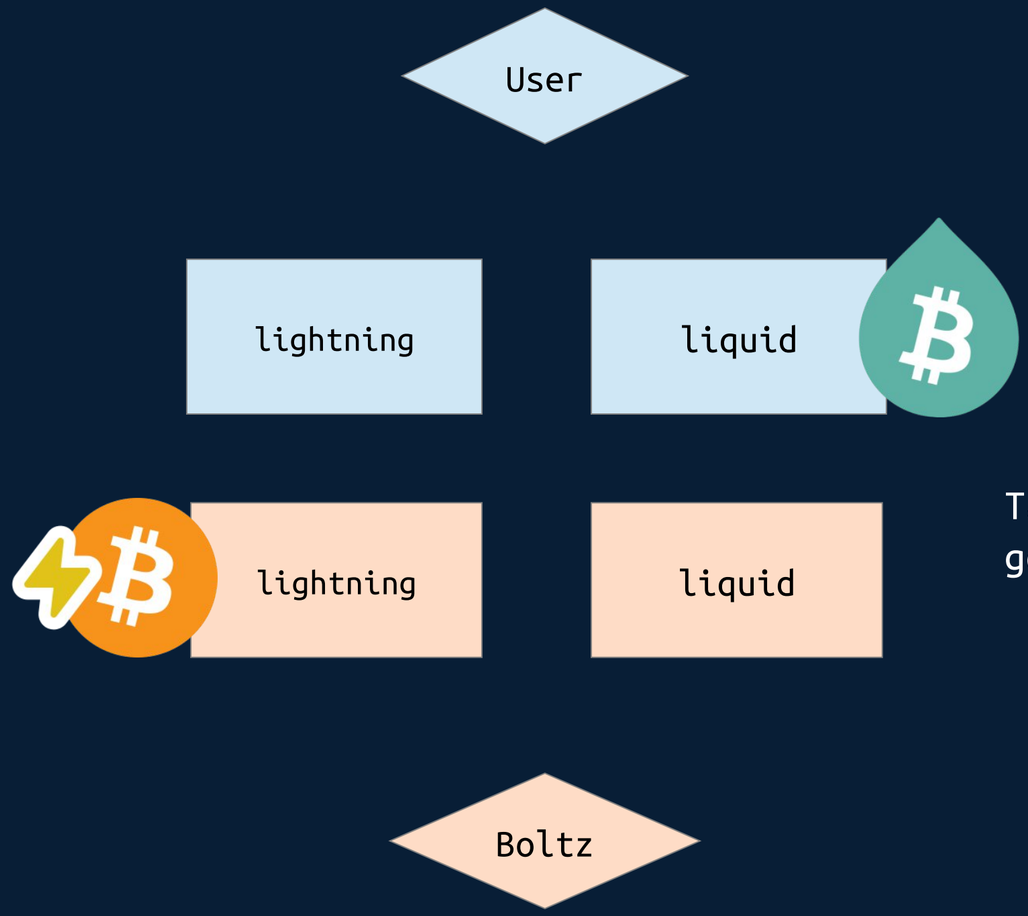
“Receive: 0.099 ⚡-BTC”

Submarine Swaps (L-BTC -> ⚡-BTC)



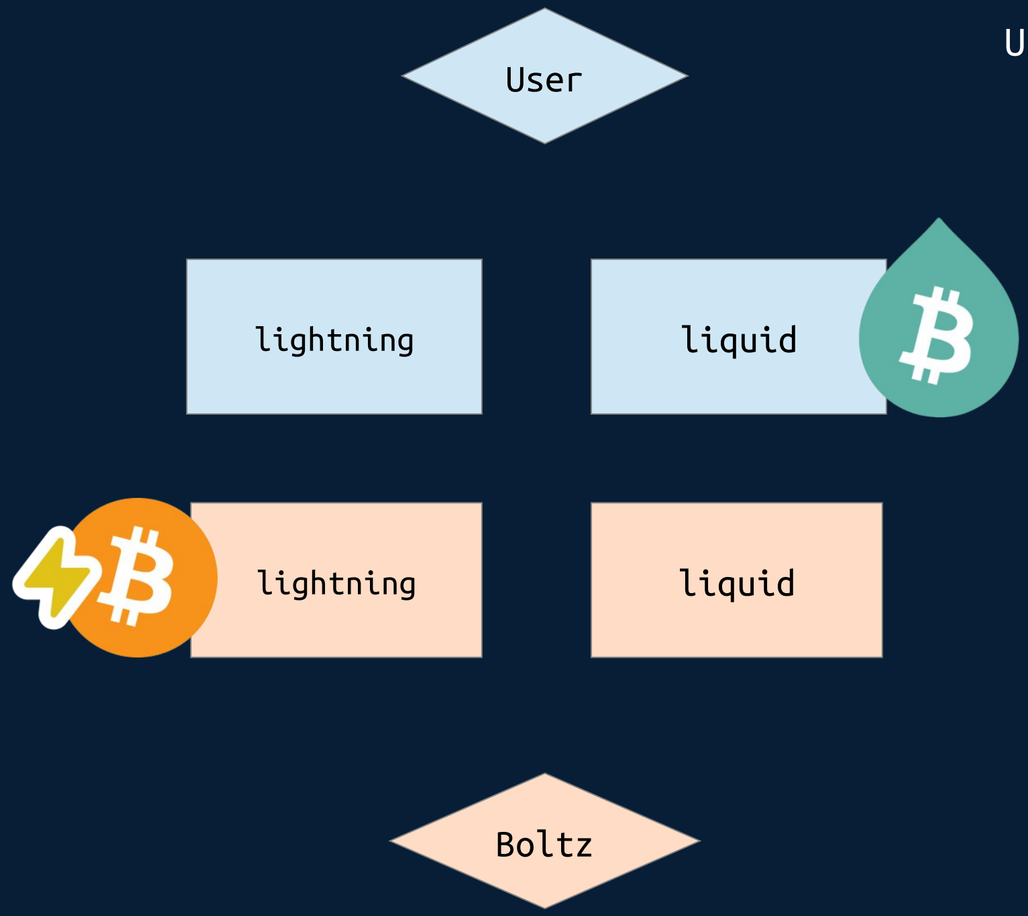
Create ⚡-invoice for 0.099 ⚡-BTC

Submarine Swaps (L-BTC -> ⚡-BTC)



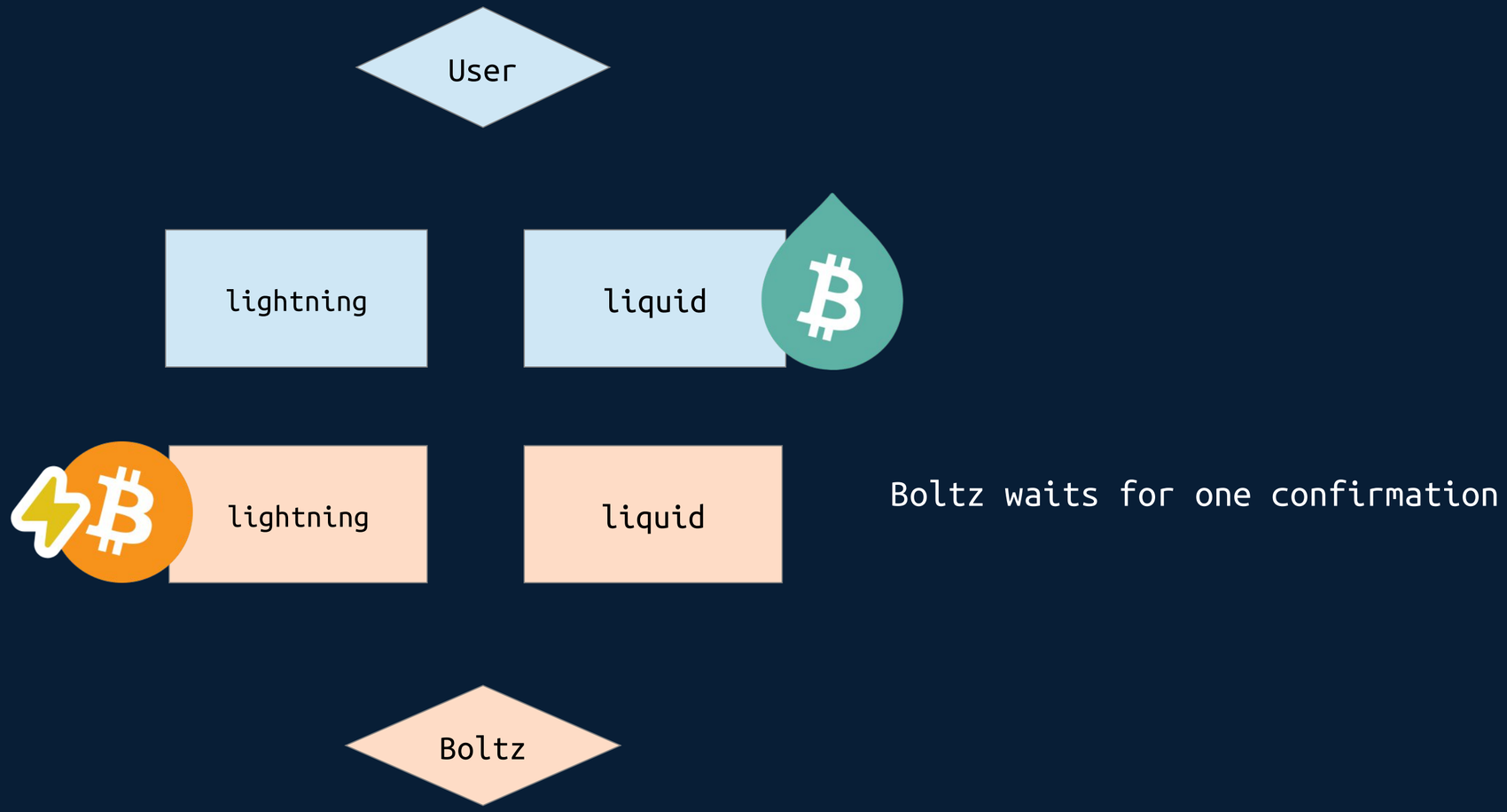
Take invoice preimage hash and create redeem script to generate liquid address for user to send 0.1 L-BTC to

Submarine Swaps (L-BTC -> ⚡-BTC)

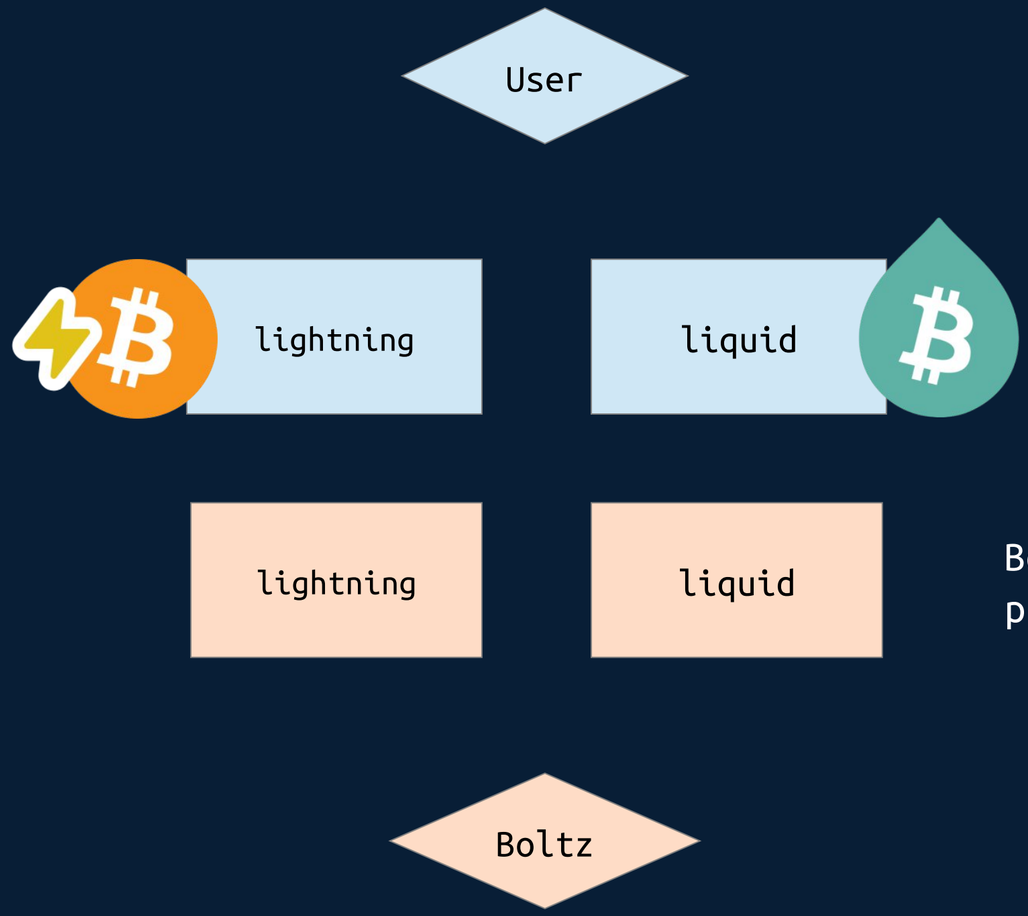


User sends 0.1 L-BTC to this address

Submarine Swaps (L-BTC -> ⚡-BTC)

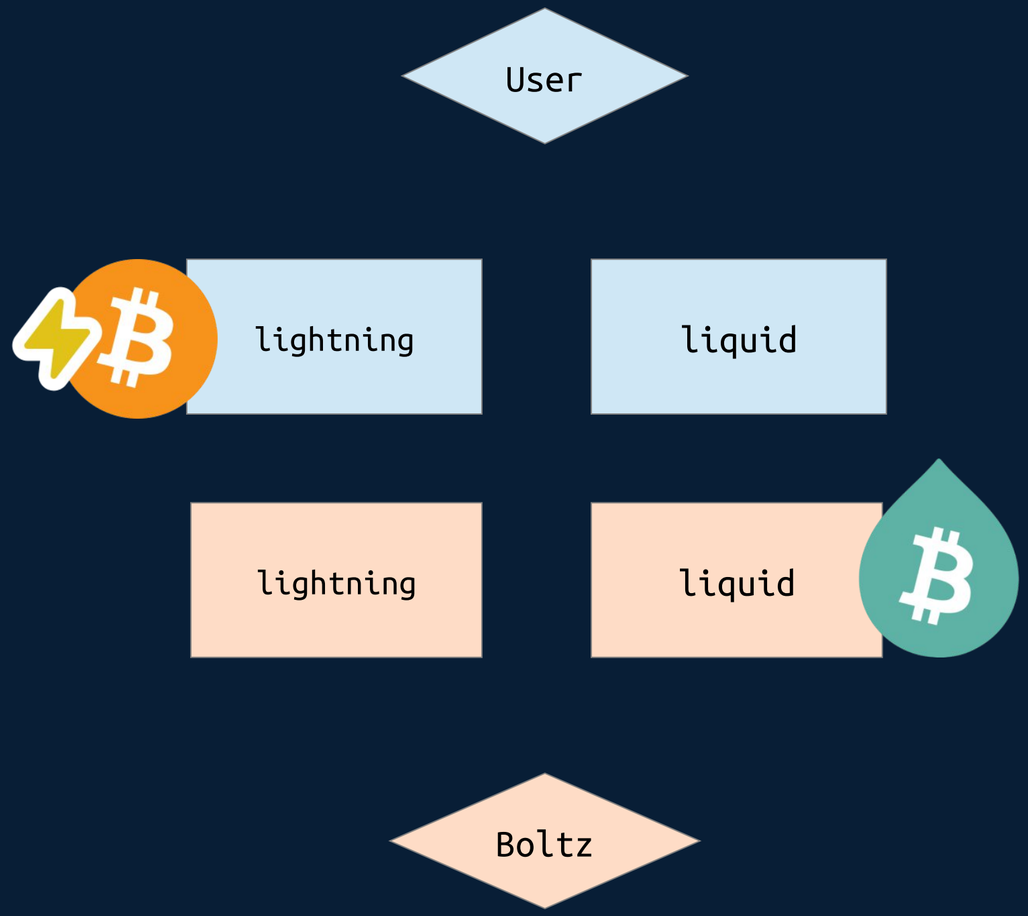


Submarine Swaps (L-BTC -> ⚡-BTC)



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

Submarine Swaps (L-BTC -> ⚡-BTC)



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

Swap completed!

SegWit V0

```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUAL
OP_IF
  OP_HASH160
  OP_PUSHBYTES_20 <preimage hash>
  OP_EQUALVERIFY
  OP_PUSHBYTES_33 <user public key>
OP_ELSE
  OP_DROP
  OP_PUSHBYTES_3 <timeout block height>
  OP_CLTV
  OP_DROP
  OP_PUSHBYTES_33 <Boltz public key>
OP_ENDIF
OP_CHECKSIG
```

SegWit V0

Hash lock

```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUAL
OP_IF
  OP_HASH160
  OP_PUSHBYTES_20 <preimage hash>
  OP_EQUALVERIFY
  OP_PUSHBYTES_33 <user public key>
OP_ELSE
  OP_DROP
  OP_PUSHBYTES_3 <timeout block height>
  OP_CLTV
  OP_DROP
  OP_PUSHBYTES_33 <Boltz public key>
OP_ENDIF
OP_CHECKSIG
```

SegWit V0

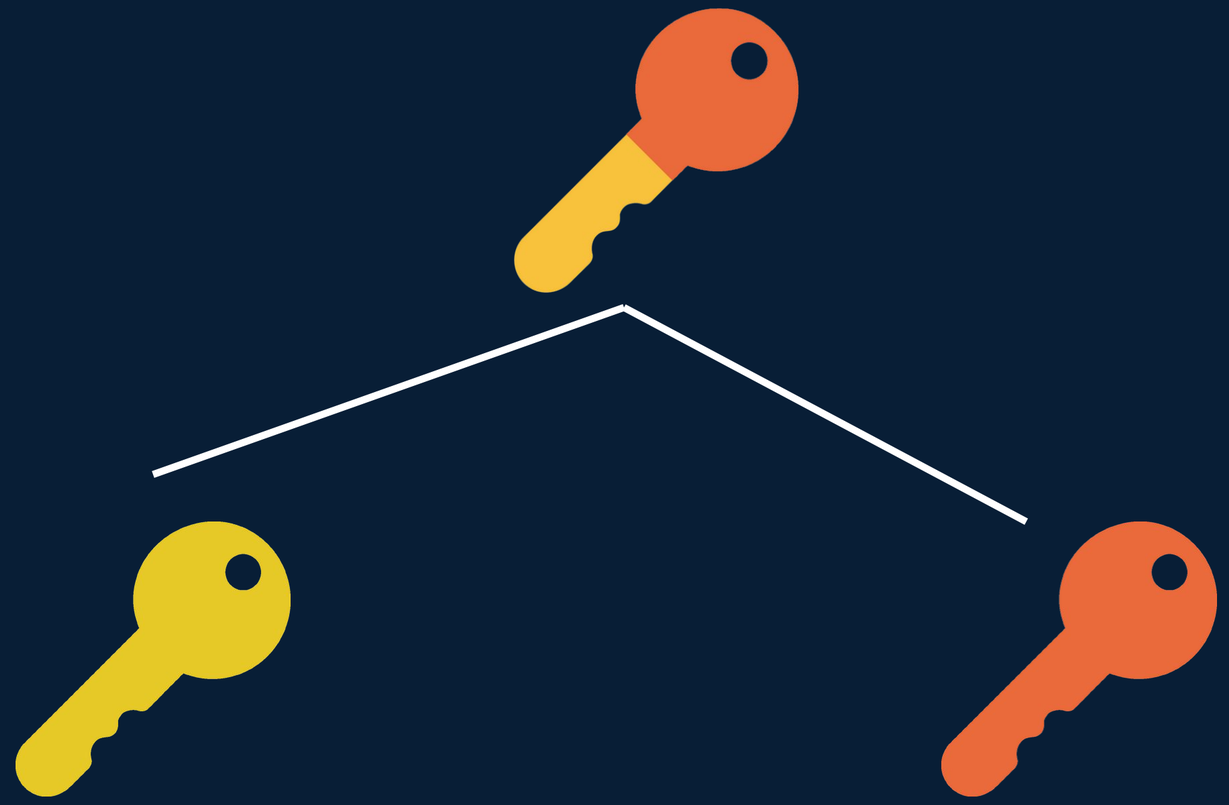
Hash lock

Time lock

```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUAL
OP_IF
  OP_HASH160
  OP_PUSHBYTES_20 <preimage hash>
  OP_EQUALVERIFY
  OP_PUSHBYTES_33 <user public key>
OP_ELSE
  OP_DROP
  OP_PUSHBYTES_3 <timeout block height>
  OP_CLTV
  OP_DROP
  OP_PUSHBYTES_33 <Boltz public key>
OP_ENDIF
OP_CHECKSIG
```

Taproot

Musig2



Taptree

Hash lock

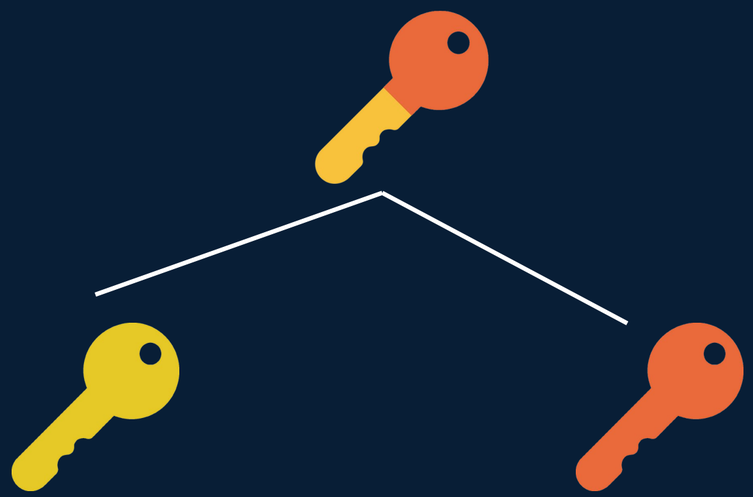
```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUALVERIFY
OP_HASH160
OP_PUSHBYTES_20 <preimage hash>
OP_EQUALVERIFY
OP_PUSHBYTES_33 <user public key>
OP_CHECKSIG
```

Time lock

```
OP_PUSHBYTES_33 <Boltz public key>
OP_CHECKSIGVERIFY
OP_PUSHBYTES_3 <timeout block height>
OP_CLTV
```

Ways to spend

Key path



Script path

Hash lock

```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUALVERIFY
OP_HASH160
OP_PUSHBYTES_20 <preimage hash>
OP_EQUALVERIFY
OP_PUSHBYTES_33 <user public key>
OP_CHECKSIG
```

Time lock

```
OP_PUSHBYTES_33 <Boltz public key>
OP_CHECKSIGVERIFY
OP_PUSHBYTES_3 <timeout block height>
OP_CLTV
```

Advantages

- Immediate Cooperative Refunds
- Lightning Payments more reliable
- Cheaper Network Fees
- Increased Privacy
- Easier script updates

Web App Demo

Aqua Demo


bol.tz