



 Boltz

Conectando capas  
de Bitcoin

# ¿Qué?



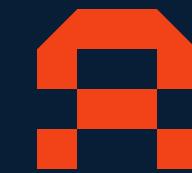
Lightning



Liquid



Rootstock



Arkade

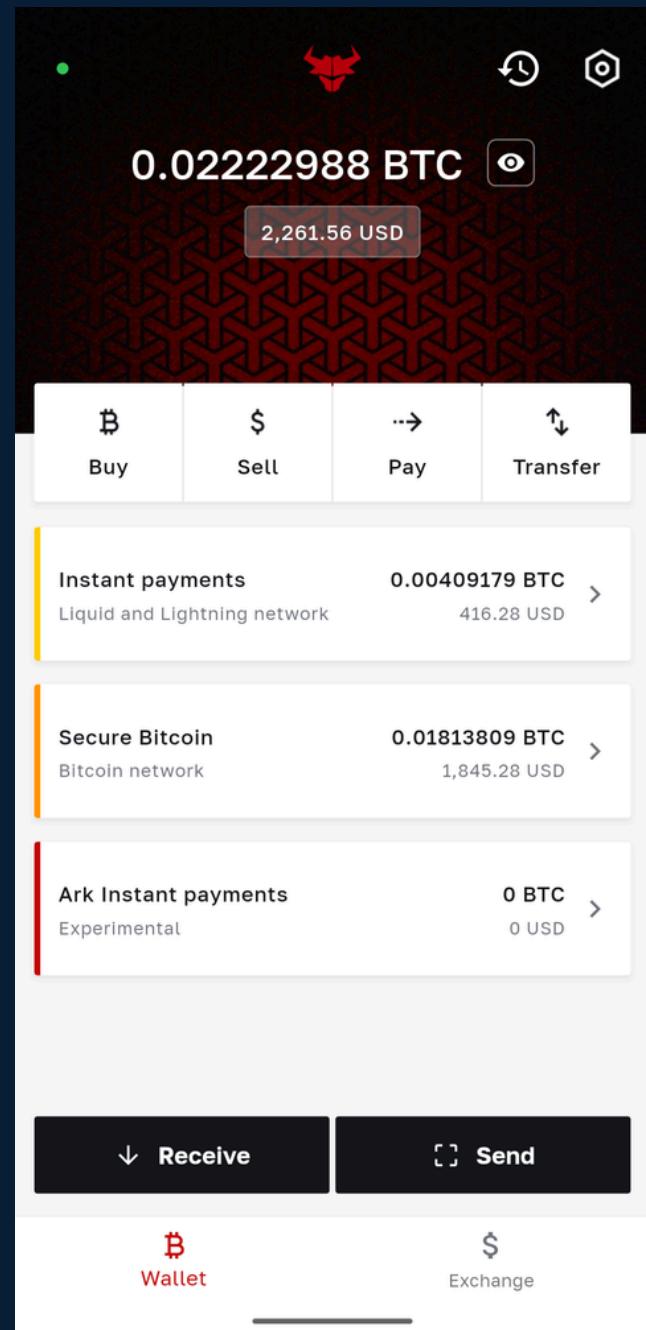


Bitcoin

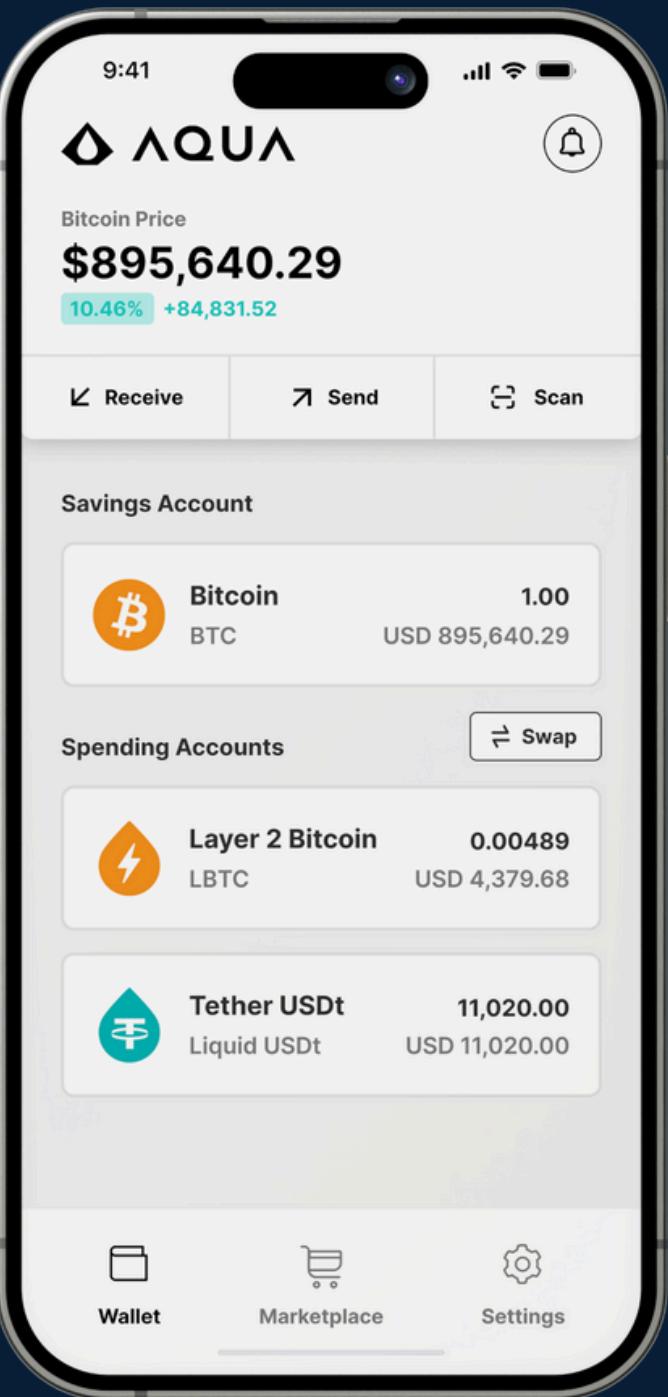
(Cadena Principal)

# Monederos

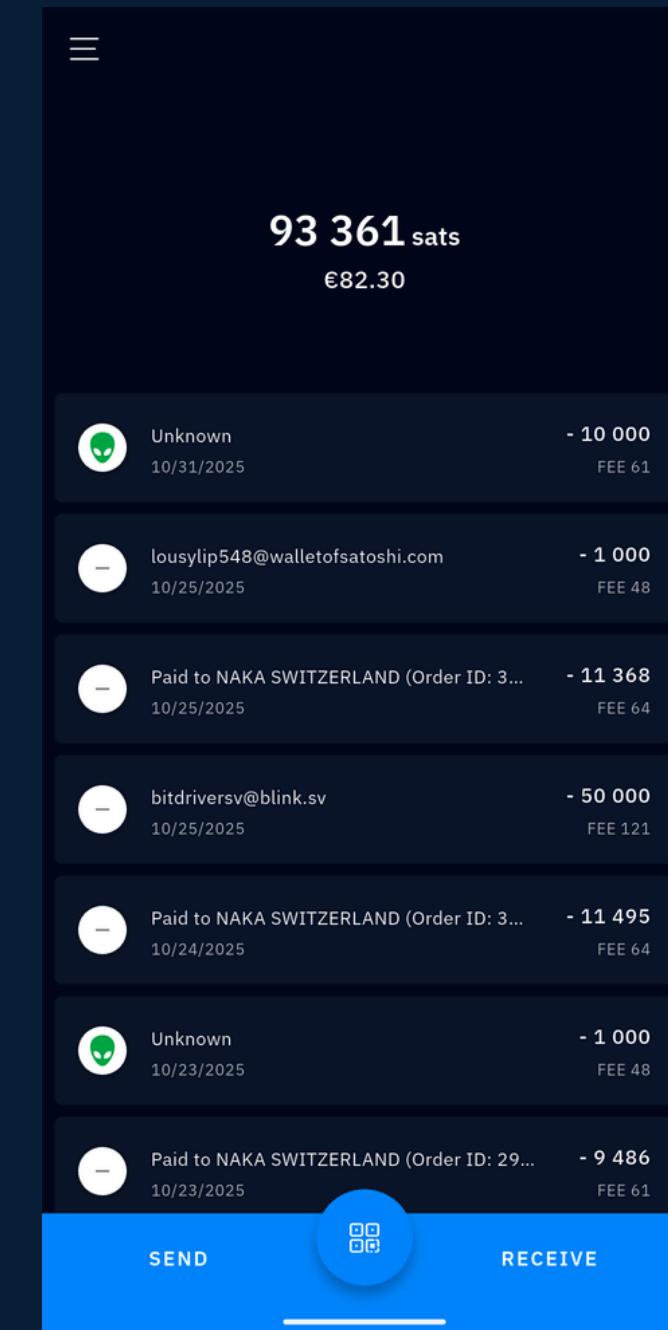
# Bull Bitcoin



# Aqua

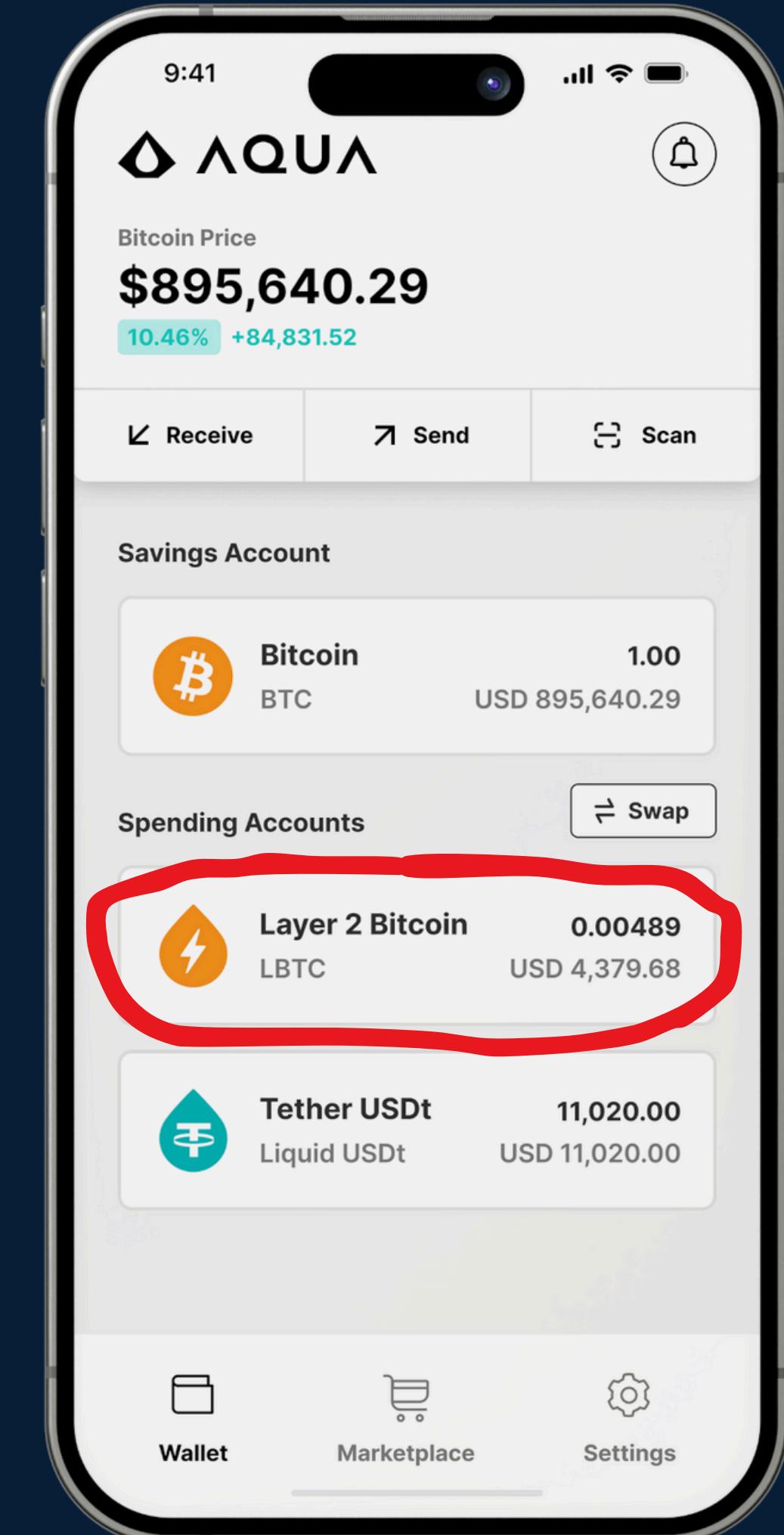


# Misty Breez



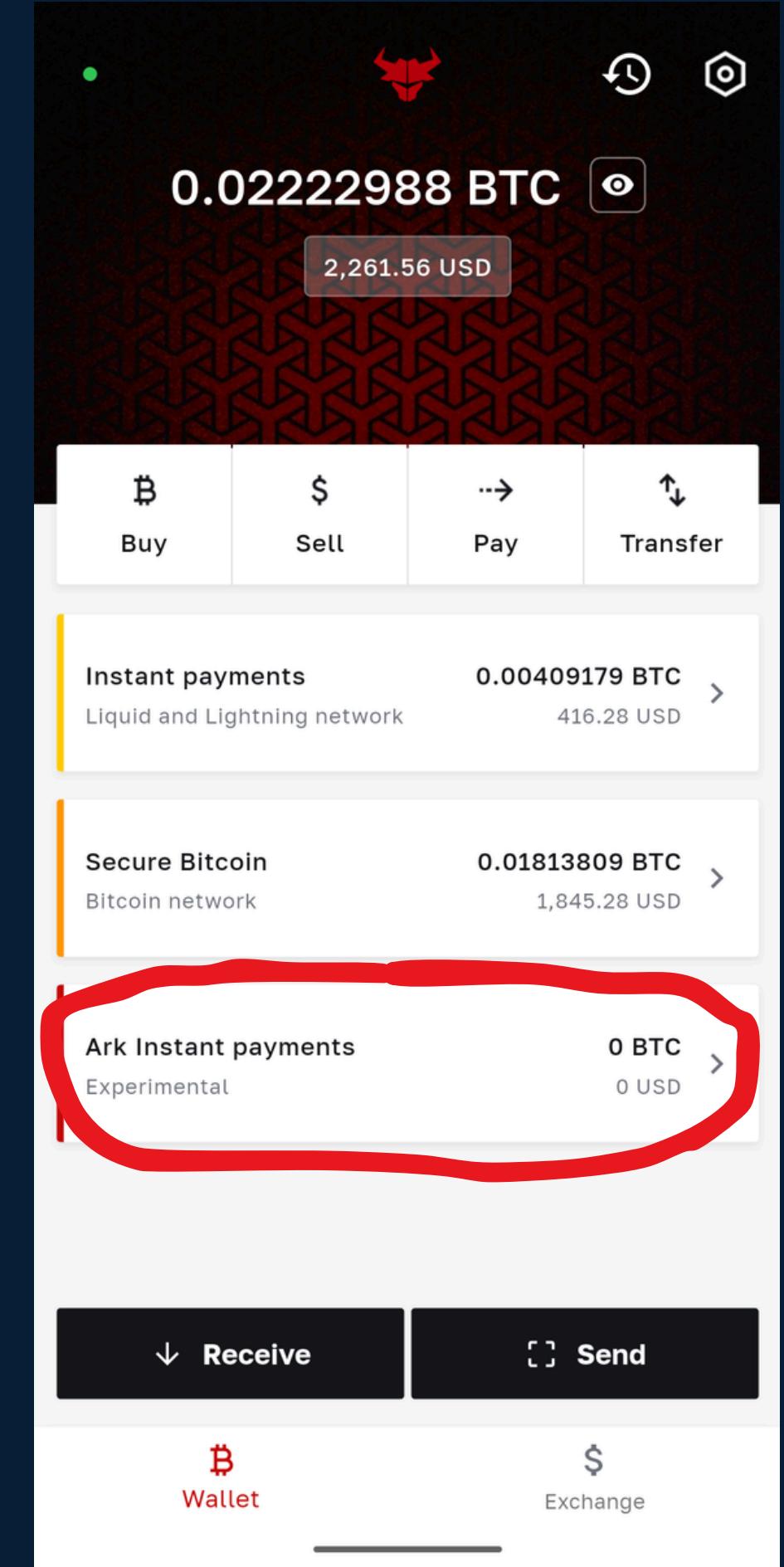
# ¿Cómo funciona?

- Monedero Liquid
- Swapear cuando sea necesario



# ¿Cómo funciona?

- Monedero Arkade
- Swopear cuando sea necesario



# ¿Por qué?

- Bitcoin
- Liquid
- Rootstock
- Ark
- Fedi
- Cashu



## Lightning

### Lightning Is the Common Language of the Bitcoin Economy



Roy Sheinfeld · Follow

Published in Breez Technology · 6 min read · Jun 12, 2024

148 1



One of the best parts about running Breez is the diverse range of people I get to meet and work with. We have partners from [Jamaica](#), the [USA](#), [Switzerland](#), [Germany](#), [Canada](#), [Estonia](#), and who knows where else. We have users in [Finland](#), [Wales](#), [Namibia](#), [India](#), and almost everywhere else. The people behind Breez are split across three continents and come from a broad range of national and ethnic backgrounds.

Agreeing on a communication platform (Telegram? Slack? Zoom? Discord?) sometimes takes a bit of coordination. What never needs coordination, though, is the *language* we use to communicate. It's always automatically English. For many of us, English is our second (or third, or fourth) language, and parts of it are baffling, but it doesn't matter. Every initial contact is in





# Bitcoin Bridge Sin Custodia

¿Cómo?

Atomic Swaps

# ¿Cómo?

## HTLCs

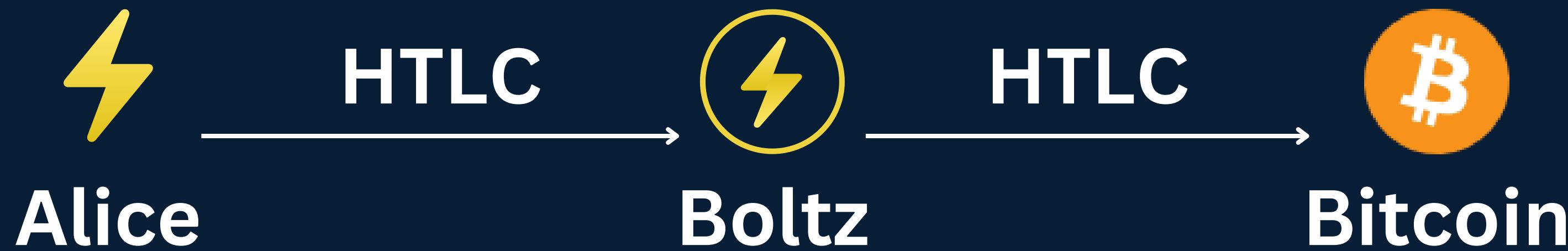
# ¿Qué necesitamos?

- Hash lock
- Time lock

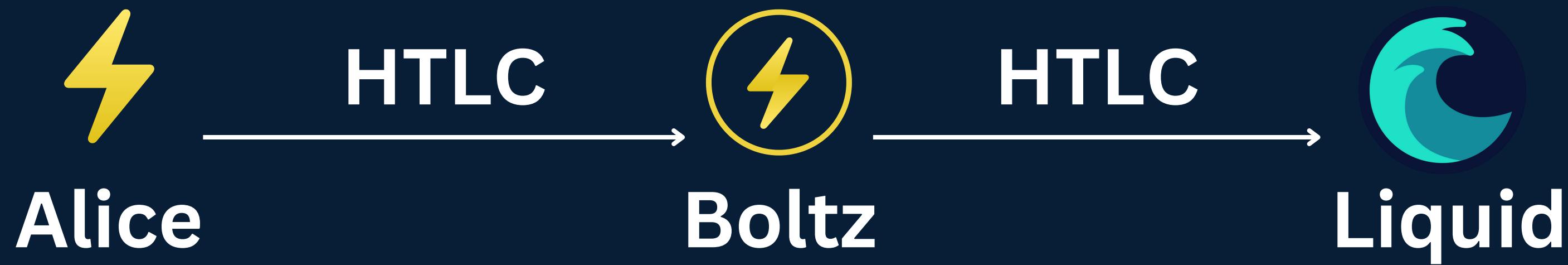
# Pago Lightning



# Swap Lightning



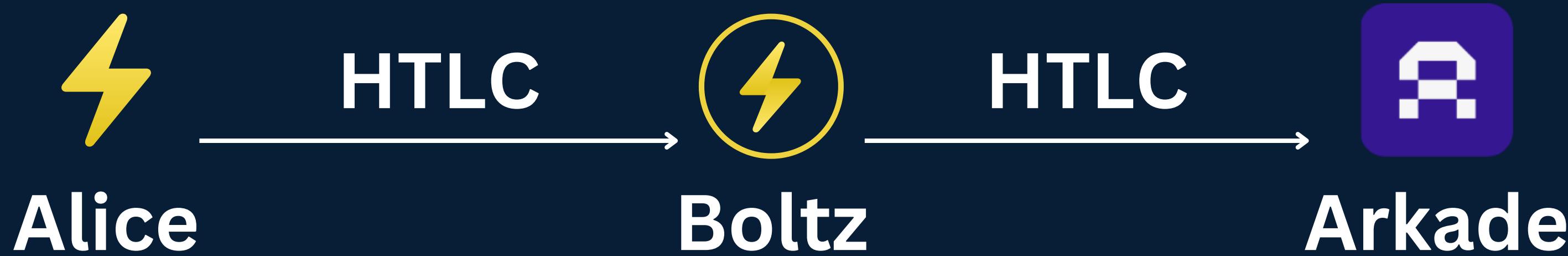
# Swap Lightning



# Swap Lightning



# Swap Lightning



# SegWit VO

```
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

```
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
```

Time lock

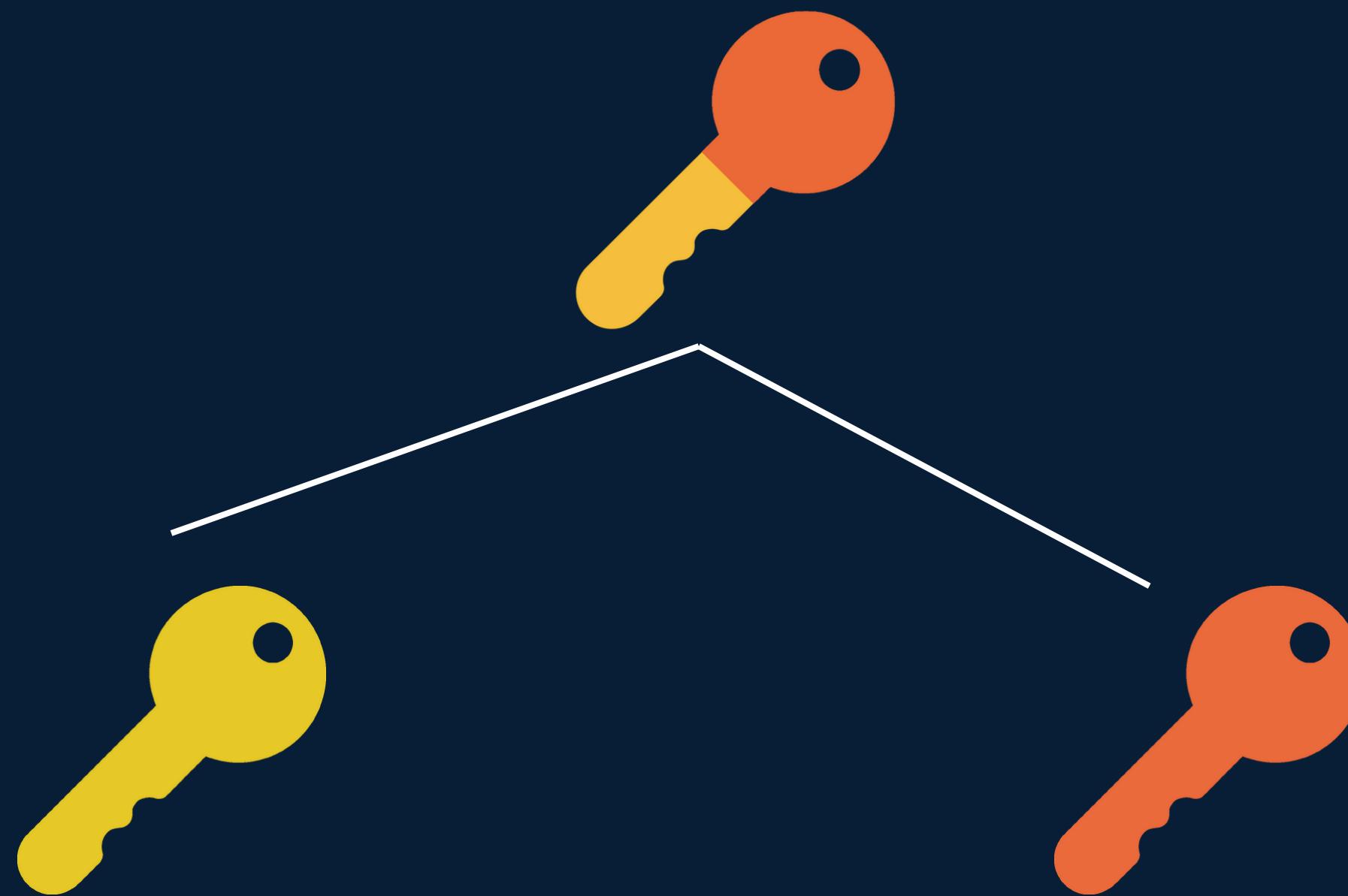
# Taproot Swaps

# ¿Por qué?

- Reembolsos Inmediatos
- Mas barato
- Mas privado

| DETAILS                                                                   |                                                                                                                                                                                                                                                                                                                                                                                                                                 |
|---------------------------------------------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| #0 e686b52008000bb5d0f24ed6a6e4328e1f743a50515211ba59ff703c<br>48967182:0 | 0.01406624 tBTC                                                                                                                                                                                                                                                                                                                                                                                                                 |
| WITNESS                                                                   | 30440220254c31ed1878abe9e210a7fb52a3f7d4195702078f6559fcade372c9f0fe30c402202ee43acc54a8c7fa884e50505af32477ff35b31e77d2e58793c7a075159fe101c20885c313be91980231132ae64f38a76fbbea3dd5ab4fb7a1dc6b5d854a792 82012087639145b3a1c677c40f9af7f879ee95e474707d5a8d4f28821037ecc2b5c8729956014537e22b5b18fc2dbfd9ce92b2855ba9b946cd621484c00677503294927b1752103360d643ed4c56bb463ebf0d910eb42439c1e5cb42d652405281c8ac5fd12b0c968ac |
| P2WSH WITNESS SCRIPT                                                      | OP_SIZE OP_PUSHBYTES_1 20 OP_EQUAL OP_IF OP_HASH160 OP_PUSHBYTES_20 5b3a1c677c40f9af7f879ee95e474707d5a8d4f2 OP_EQUALVERIFY OP_PUSHBYTES_33037ece2b5c8729956014537e22b5b18fc2dbfd9ce92b2855ba9b946cd621484c00 OP_ELSE OP_DROP OP_PUSHBYTES_3 294927OP_CLTV OP_DROP OP_PUSHBYTES_33 03360d643ed4c56bb463ebf0d910eb42439c1e5cb42d62405281c8ac5fd12b0c968ac IF OP_CHECKSIG                                                         |
| NSEQUENCE                                                                 | 0xffffffff                                                                                                                                                                                                                                                                                                                                                                                                                      |
| PREVIOUS OUTPUT SCRIPT                                                    | OP_0 OP_PUSHBYTES_32 6b6ac3a3d331fa dd194af883f69c4db8f23f45fb70de751de4ad45ac22e948c4 (<v0_p2wsh>)                                                                                                                                                                                                                                                                                                                             |
| #0 tb1q8llhuaqm0szsuq4y0n77q4xj986wuzauservl                              | 0.01406478 tBTC                                                                                                                                                                                                                                                                                                                                                                                                                 |
| TYPE                                                                      | V0_P2WPKH                                                                                                                                                                                                                                                                                                                                                                                                                       |
| SCRIPTPUBKEY (ASM)                                                        | OP_0 OP_PUSHBYTES_20 3ffff7e741b7c050e02a47cfde054d229f4ee0bbc                                                                                                                                                                                                                                                                                                                                                                  |
| SCRIPTPUBKEY (HEX)                                                        | 00143ffff7e741b7c050e02a47cfde054d229f4ee0bbc                                                                                                                                                                                                                                                                                                                                                                                   |
| SPENDING TX                                                               | Unspent                                                                                                                                                                                                                                                                                                                                                                                                                         |
| #0 ca19737c64db02fb0f8840fa720ee04b6c6e7c02e5<br>035890ef732af18198ef0    | 0.04974692 tBTC                                                                                                                                                                                                                                                                                                                                                                                                                 |
| WITNESS                                                                   | 2235253c7737eadb797f6cf10920cb0a1541eca2b88f7a5658c7b87aea39d27161941af61ea773ae4d65a3aba8979b20e3bf14daaa58317f52ca80df8d888a                                                                                                                                                                                                                                                                                                  |
| NSEQUENCE                                                                 | 0xffffffff                                                                                                                                                                                                                                                                                                                                                                                                                      |
| PREVIOUS OUTPUT SCRIPT                                                    | OP_PUSHNUM_1 OP_PUSHBYTES_32402660fed5b697fce91a29eebfc4cc4282480920f58033691534d89e78226ce (<v1_p2fe>)                                                                                                                                                                                                                                                                                                                         |
| PREVIOUS OUTPUT ADDRESS                                                   | tb1pgqnxplk4k6tu16dp520wh1xvcs5zfqyjpavqxd532dxneuzym8qsj9dsz                                                                                                                                                                                                                                                                                                                                                                   |
| #0 2N24sf8LGxFKKHqGZNsA7AqFIZzAiQpkURo                                    | 0.04974470 tBTC                                                                                                                                                                                                                                                                                                                                                                                                                 |
| TYPE                                                                      | P2SH                                                                                                                                                                                                                                                                                                                                                                                                                            |
| SCRIPTPUBKEY (ASM)                                                        | OP_HASH160 OP_PUSHBYTES_20 60c40066a3b8cf7ba6e3eca536a4aee82994c8e3 OP_EQUAL                                                                                                                                                                                                                                                                                                                                                    |
| SCRIPTPUBKEY (HEX)                                                        | a91460c40066a3b8cf7ba6e3eca536a4aee82994c8e387                                                                                                                                                                                                                                                                                                                                                                                  |
| SPENDING TX                                                               | Unspent                                                                                                                                                                                                                                                                                                                                                                                                                         |
| 2 CONFIRMATIONS 0.04974470 tBTC                                           |                                                                                                                                                                                                                                                                                                                                                                                                                                 |

# Musig2



# Taptree

## Hash lock

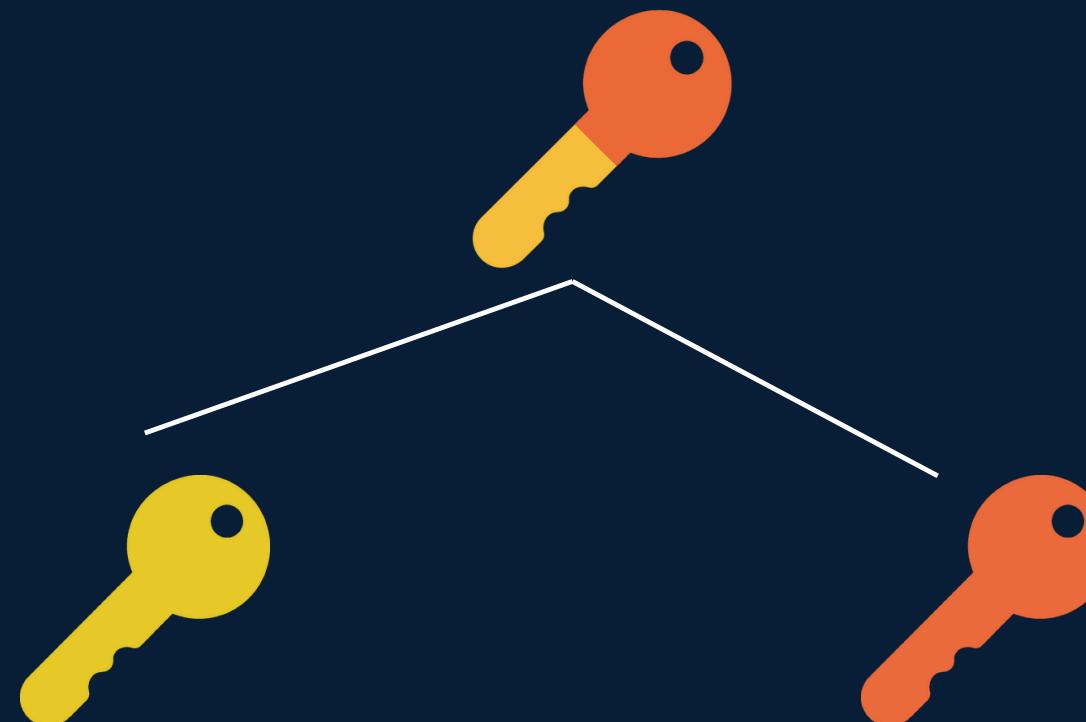
```
OP_SIZE  
OP_PUSHBYTES_1 20  
OP_EQUALVERIFY  
OP_HASH160  
OP_PUSHBYTES_20 <preimage hash>  
OP_EQUALVERIFY  
OP_PUSHBYTES_33 <user public key>  
OP_CHECKSIG
```

## Time lock

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

# Formas de gastar

## Key path



## Script path

### Hash lock

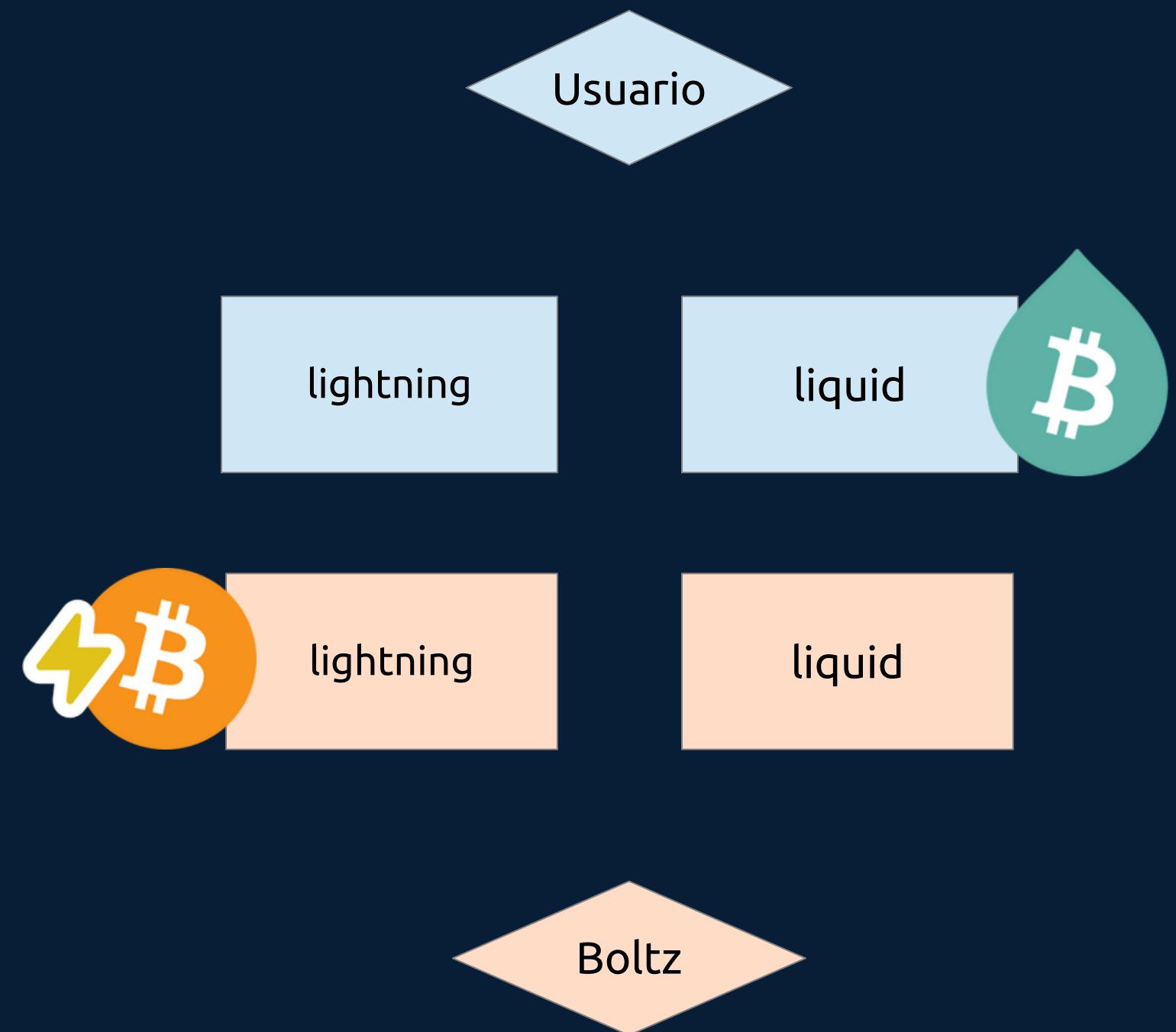
OP\_SIZE  
OP\_PUSHBYTES\_1 20  
OP\_EQUALVERIFY  
OP\_HASH160  
OP\_PUSHBYTES\_20 <preimage hash>  
OP\_EQUALVERIFY  
OP\_PUSHBYTES\_33 <user public key>  
OP\_CHECKSIG

### Time lock

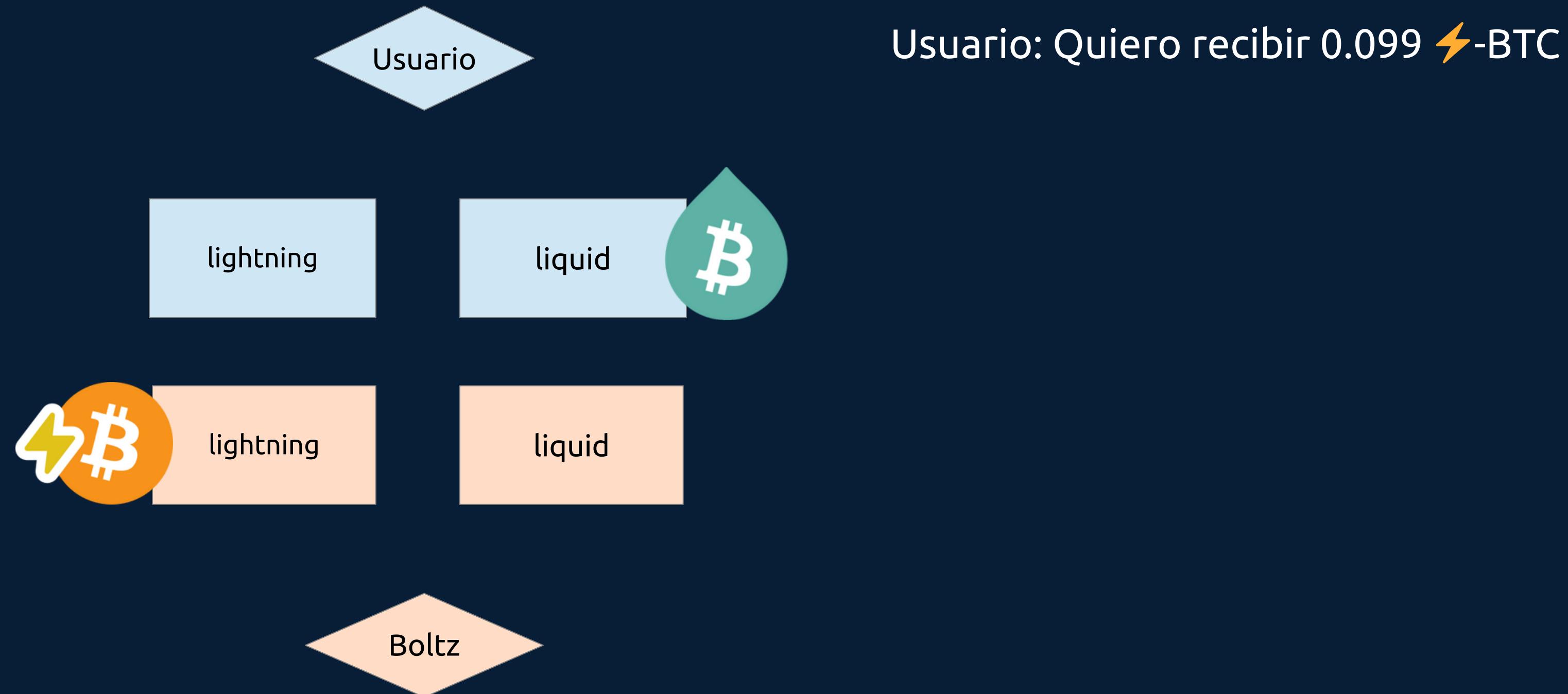
OP\_PUSHBYTES\_33 <Boltz public key>  
OP\_CHECKSIGVERIFY  
OP\_PUSHBYTES\_3 <timeout block height>  
OP\_CLTV

# Flujo

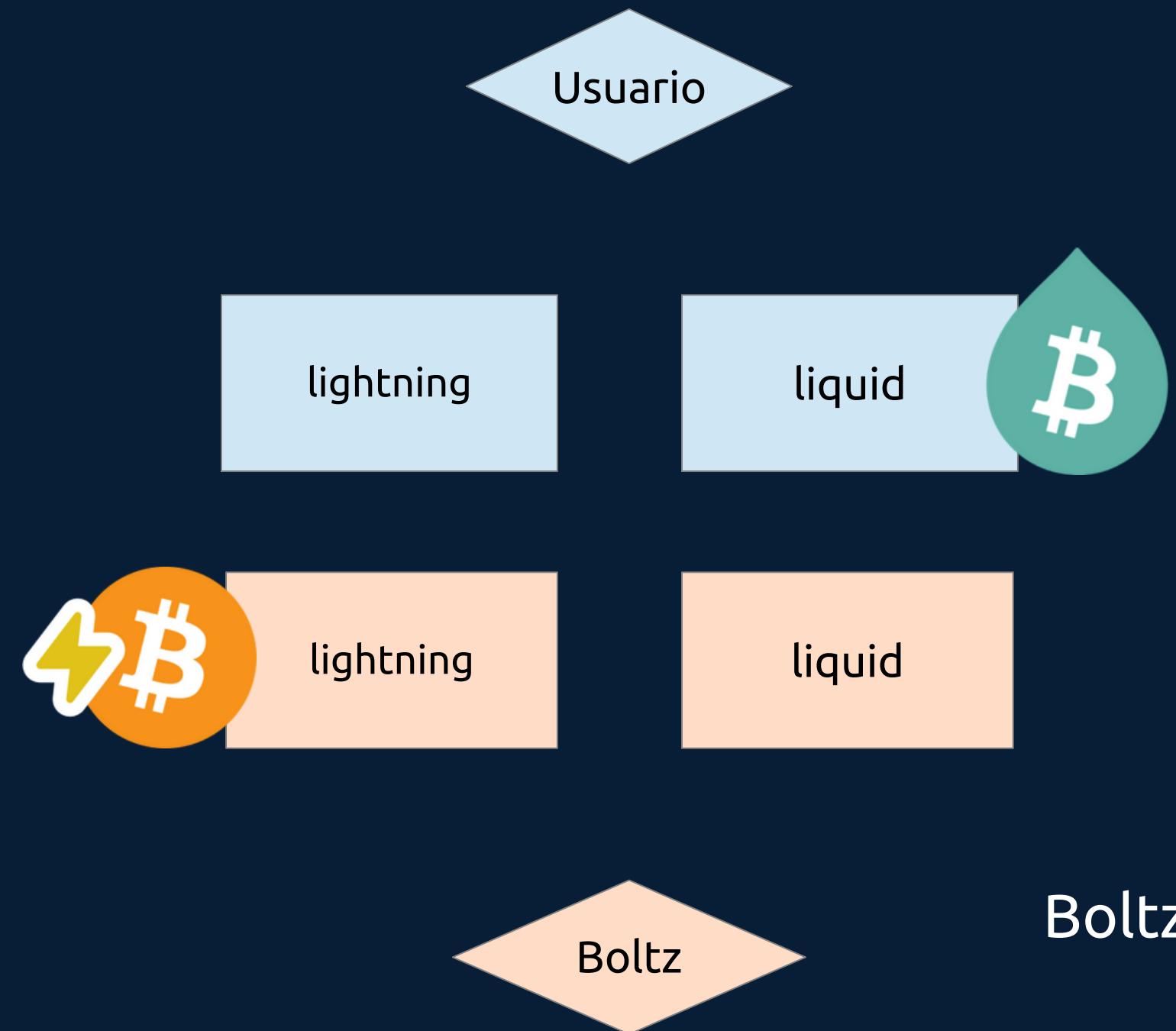
# Submarine Swaps (L-BTC → ⚡-BTC)



# Submarine Swaps (L-BTC $\rightarrow$ ⚡-BTC)

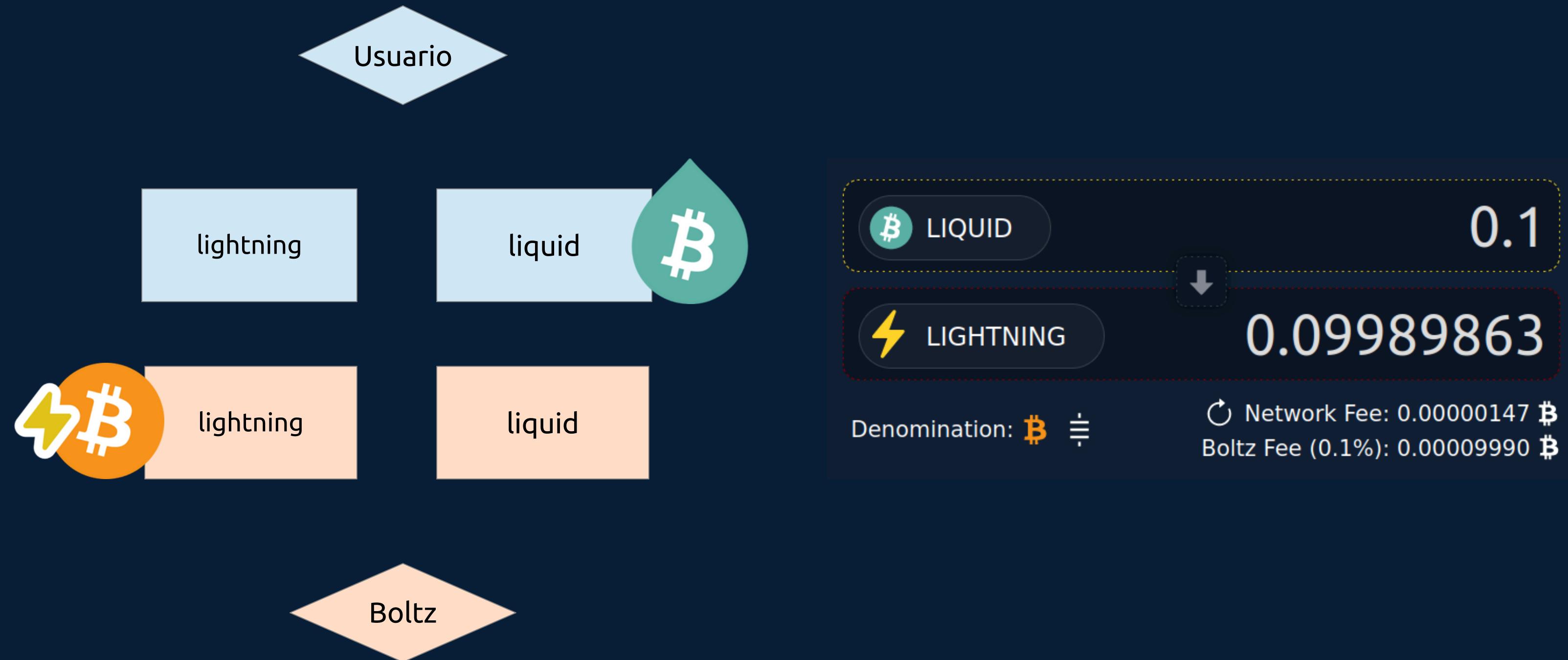


# Submarine Swaps (L-BTC → ⚡-BTC)

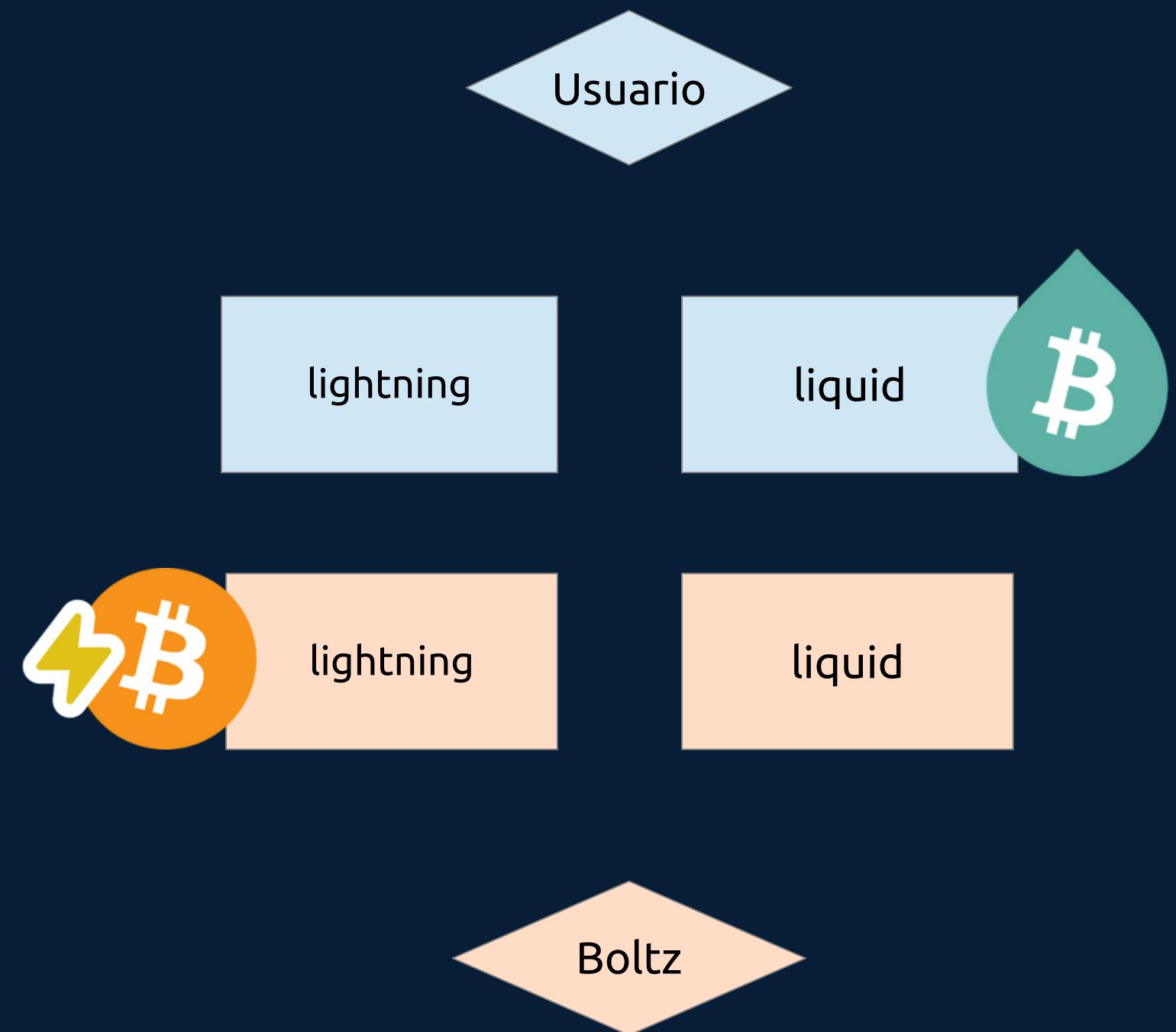


Boltz: Bueno, por eso tienes que enviarme 0.1 L-BTC

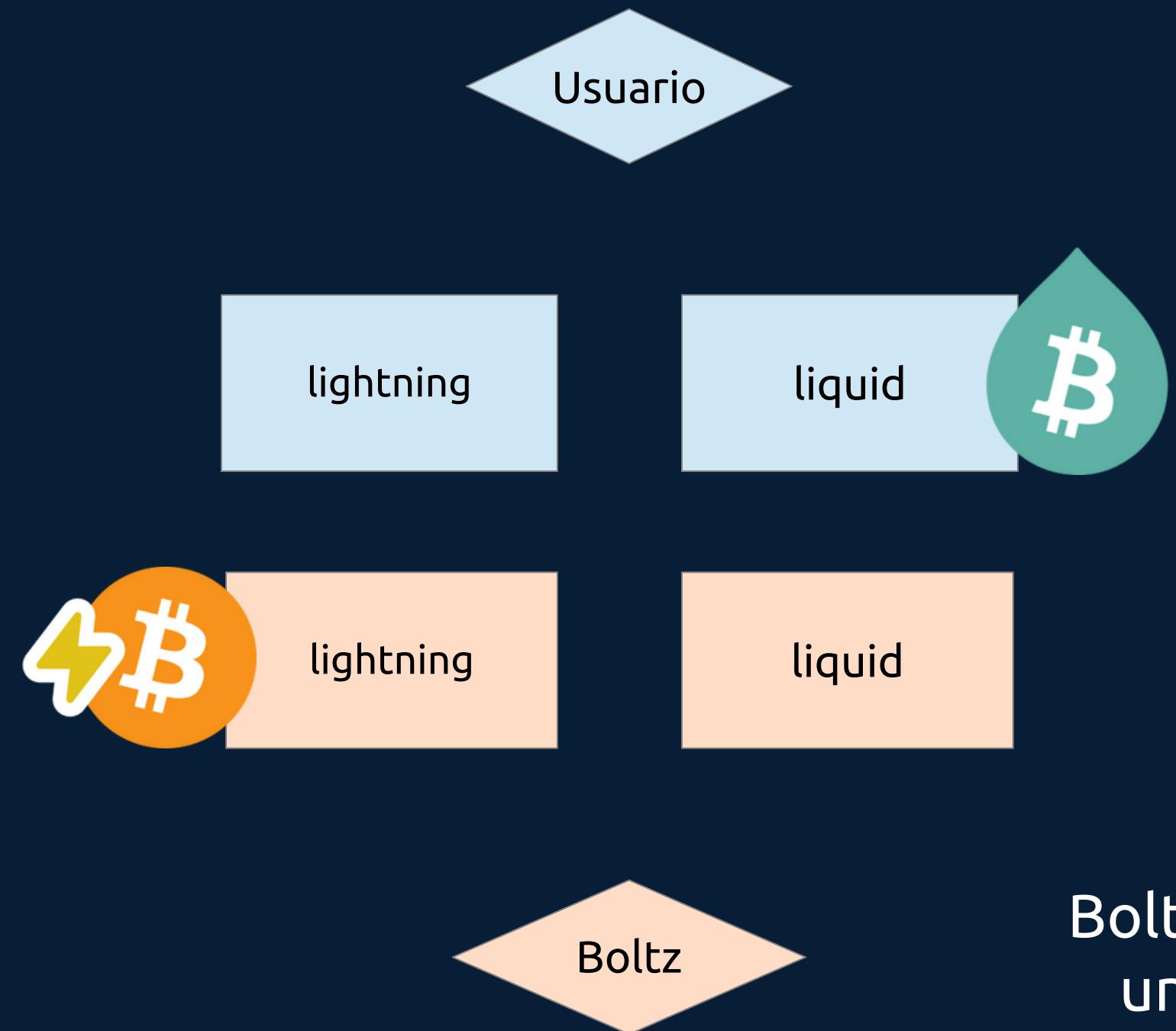
# Submarine Swaps (L-BTC → ⚡-BTC)



# Submarine Swaps (L-BTC $\rightarrow$ ⚡-BTC)

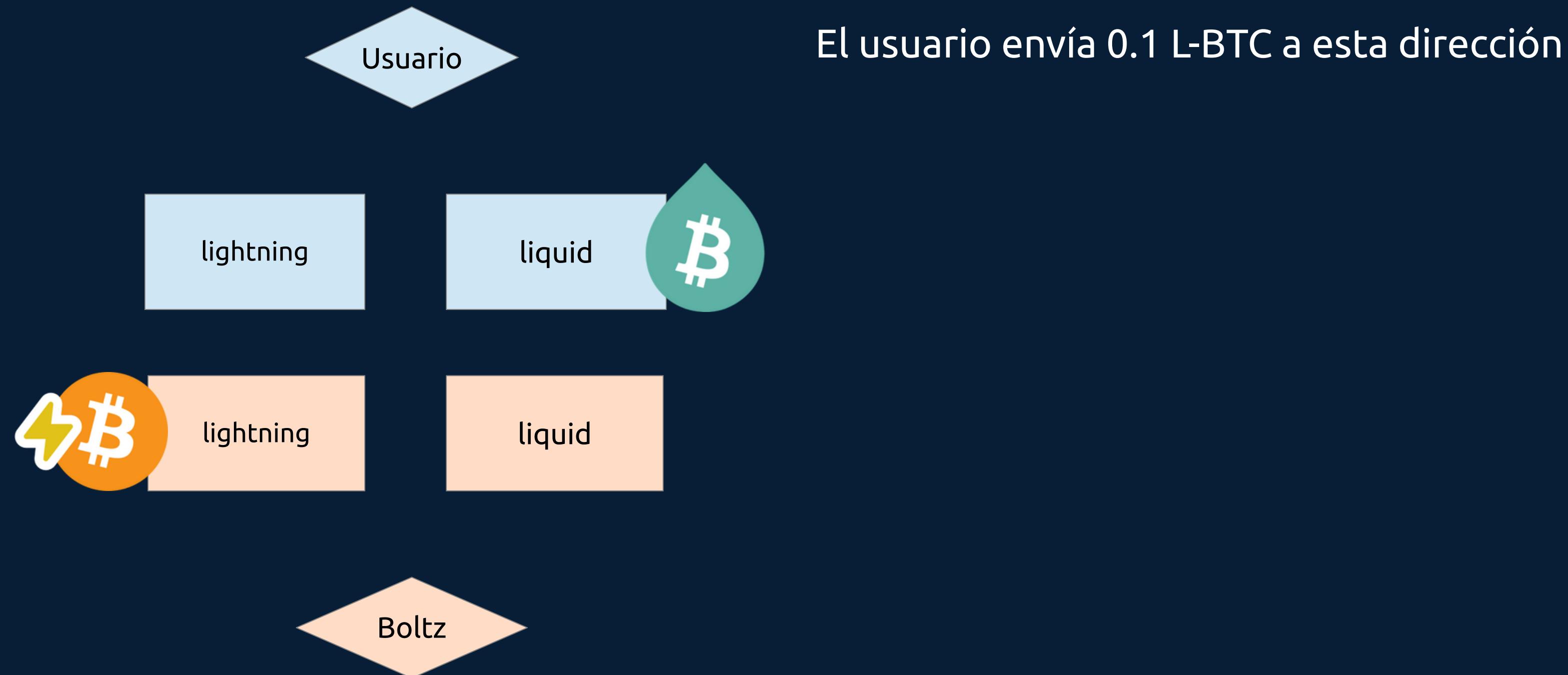


# Submarine Swaps (L-BTC → ⚡-BTC)

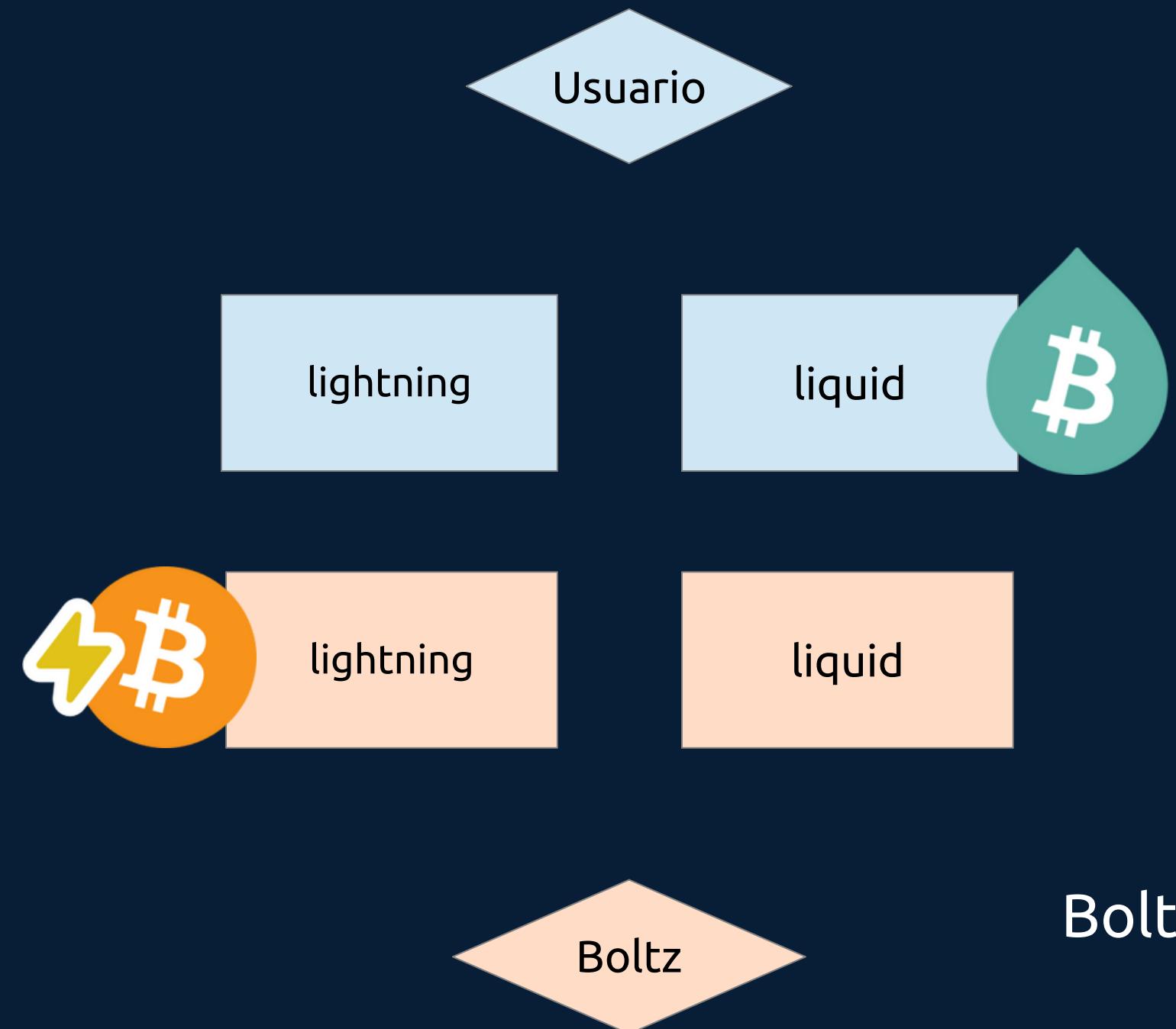


Boltz toma el hash de la preimagen de la factura y crea un redeem script para generar una dirección Liquid

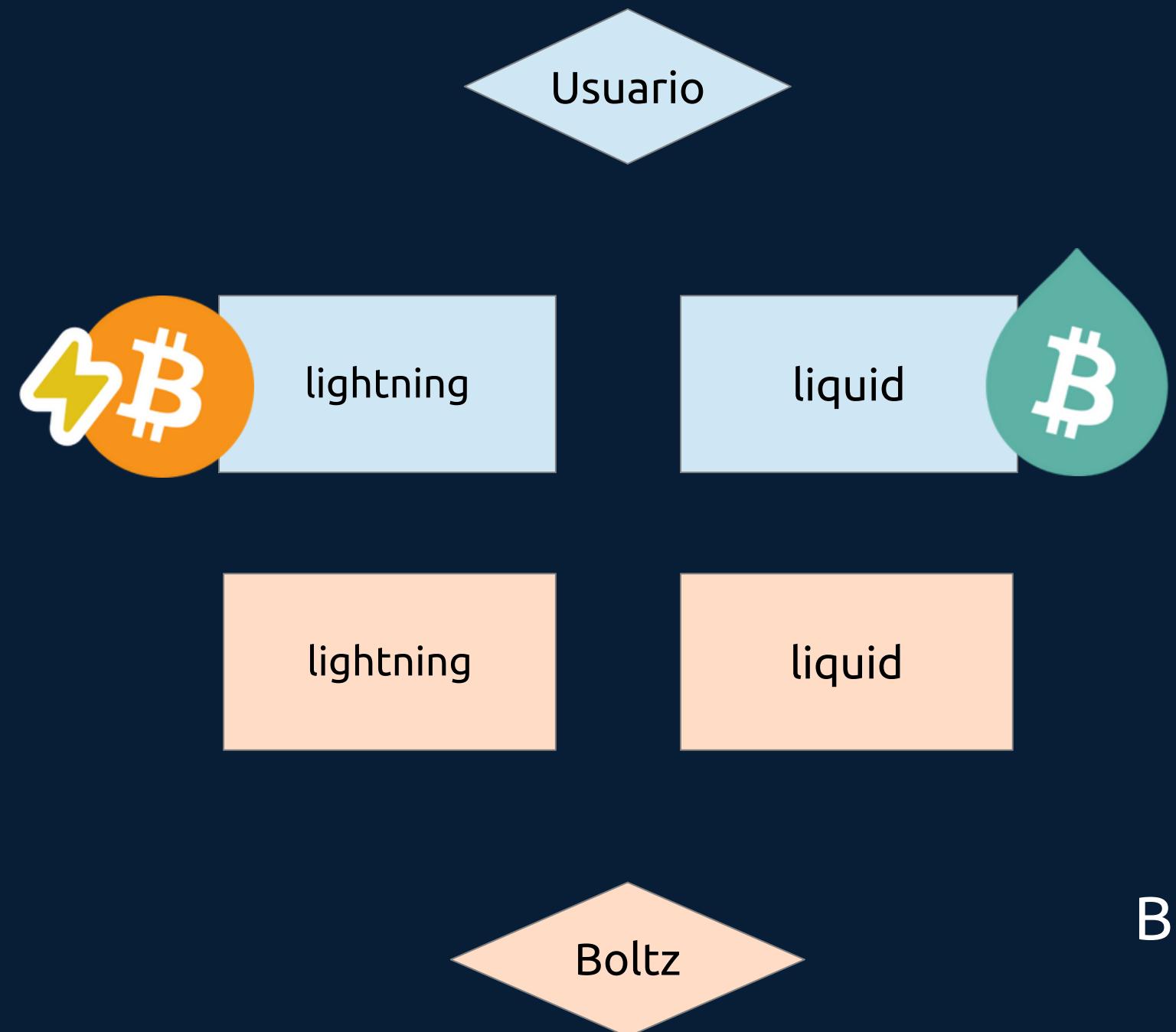
# Submarine Swaps (L-BTC → ⚡-BTC)



# Submarine Swaps (L-BTC → ⚡-BTC)

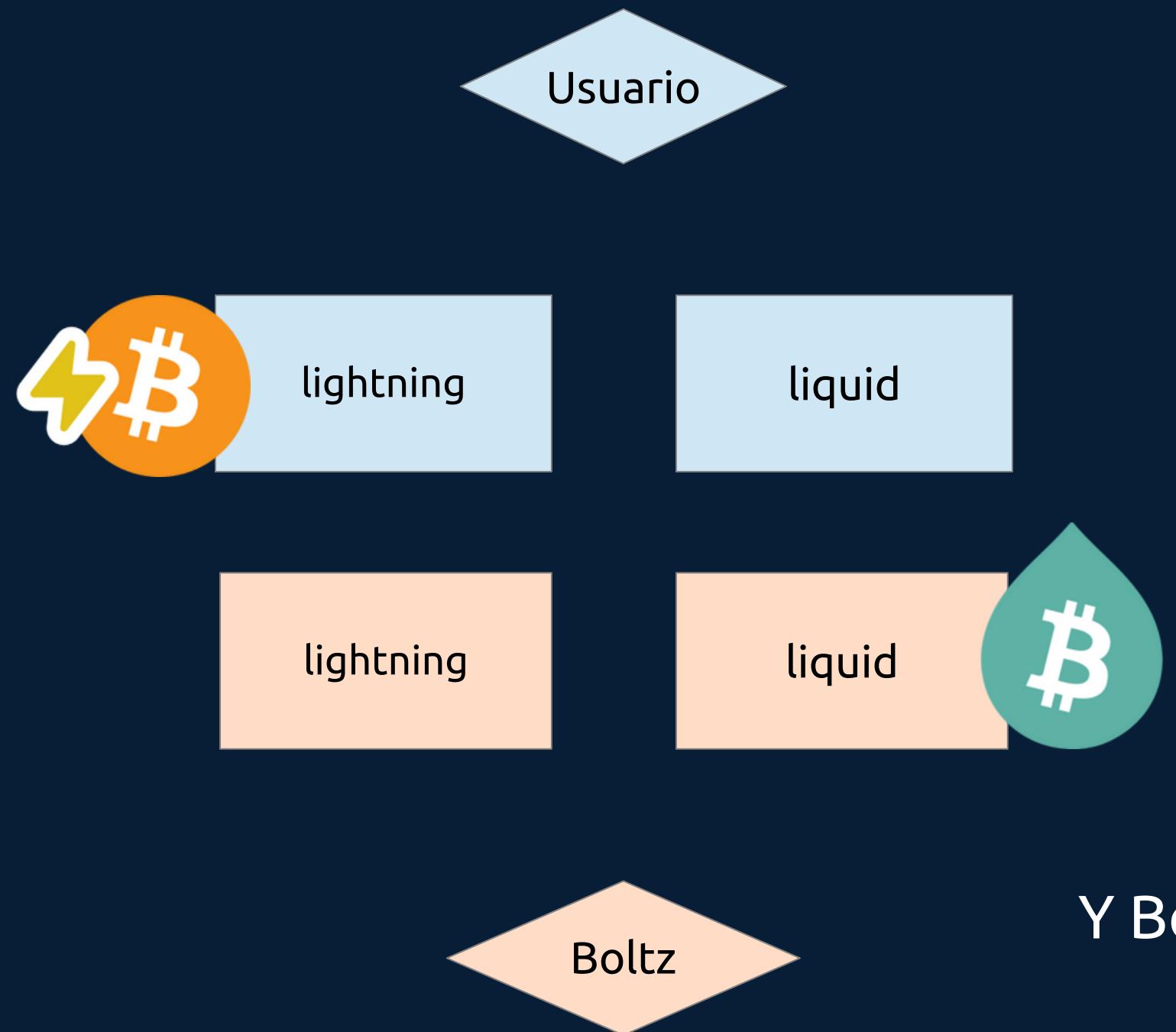


# Submarine Swaps ( $L\text{-BTC} \rightarrow \lightning\text{-BTC}$ )



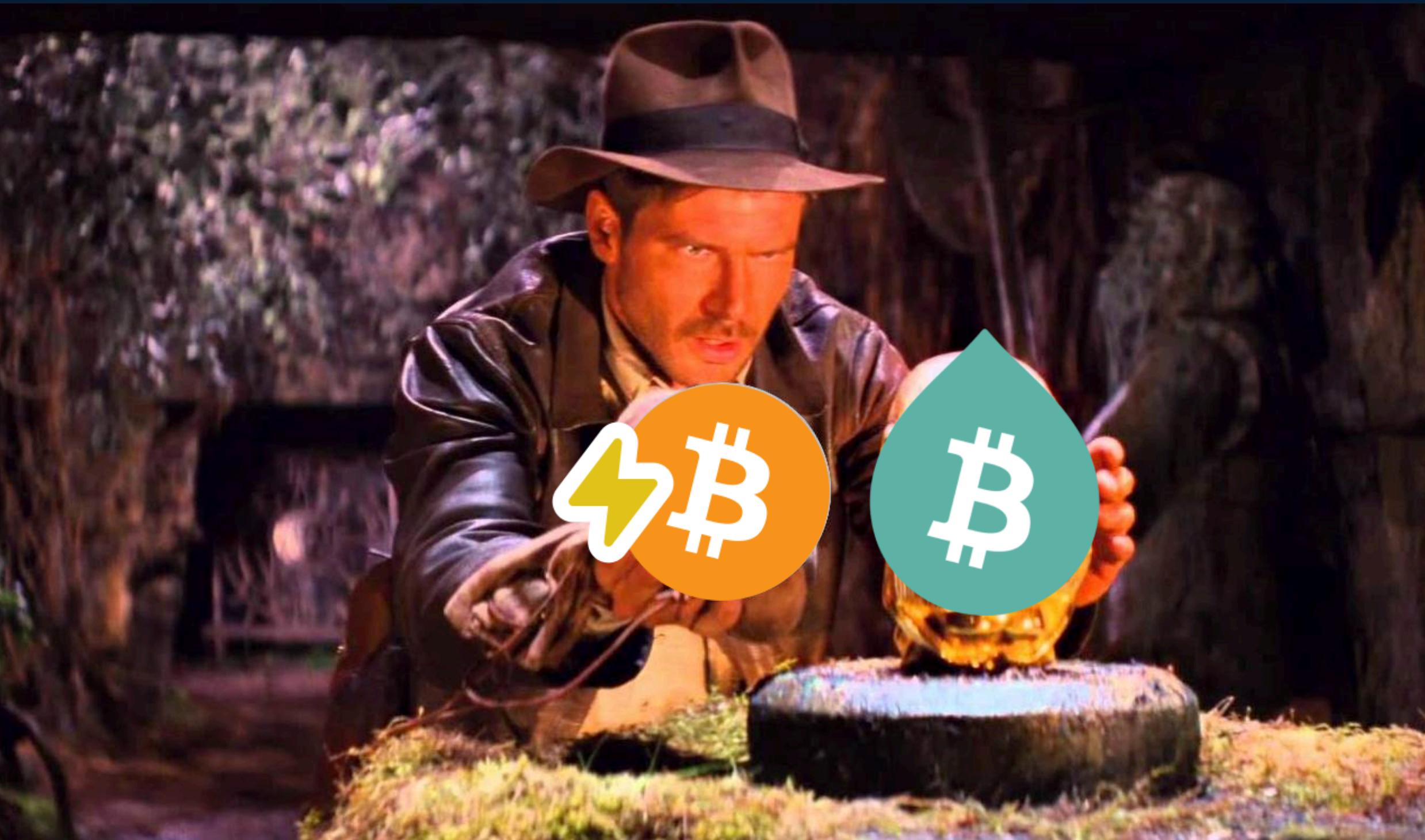
Boltz paga la factura de 0.099  $\lightning\text{-BTC}$ , por lo que se revela la preimagen.

# Submarine Swaps (L-BTC $\rightarrow$ ⚡-BTC)



Y Boltz puede reclamar las 0.1 L-BTC en Liquid desde el redeem script utilizando la preimagen

# Swap completado!



# Demo