Boltz

Conectando capas de Bitcoin

¿Qué?

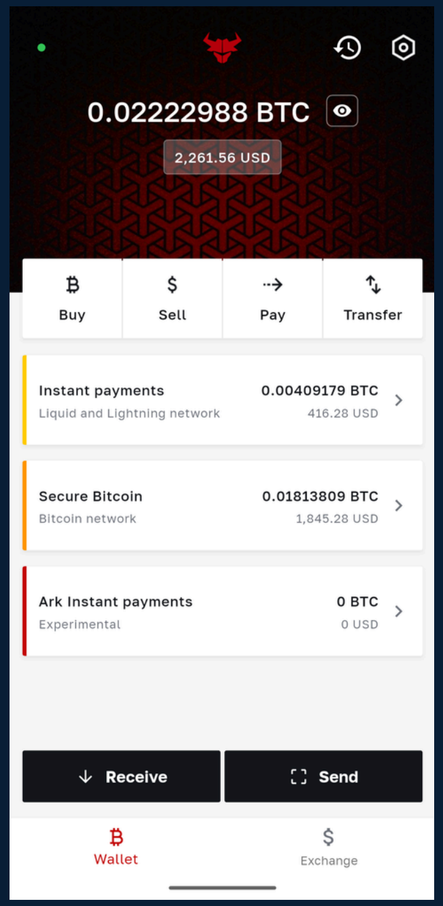
Lightning Liquid Rootstock Arkade

Bitcoin

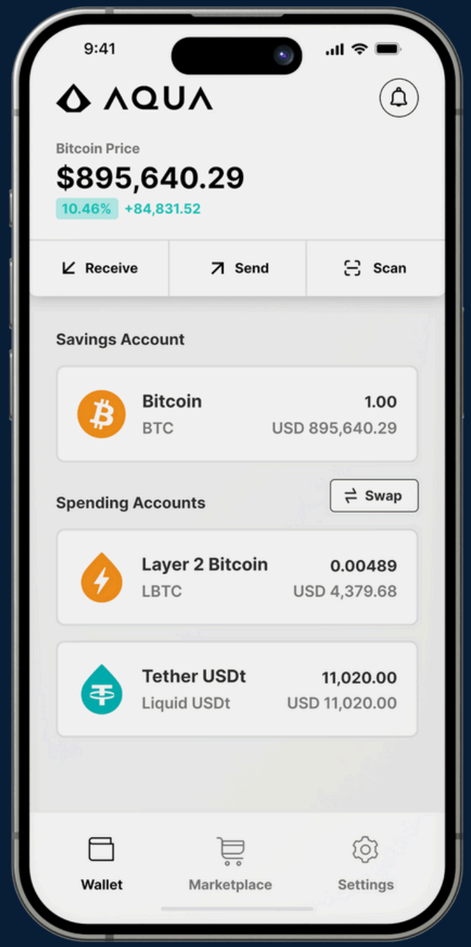
(Cadena Principal)

Monederos

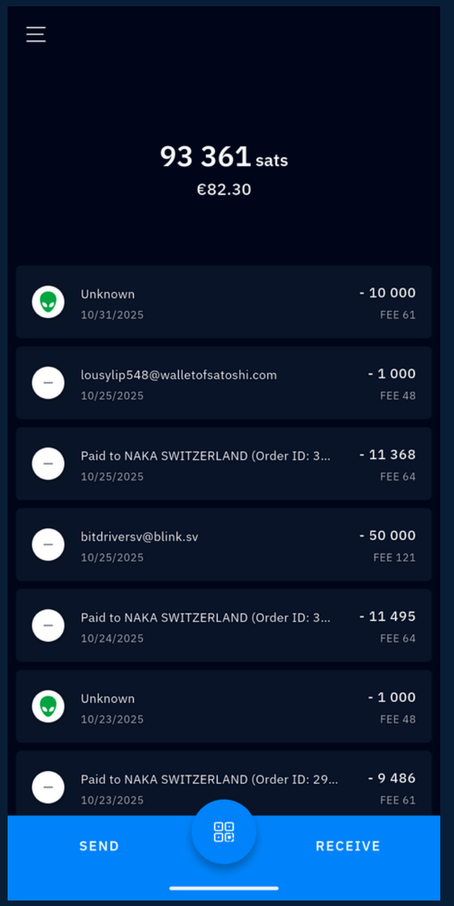
Bull Bitcoin



Aqua

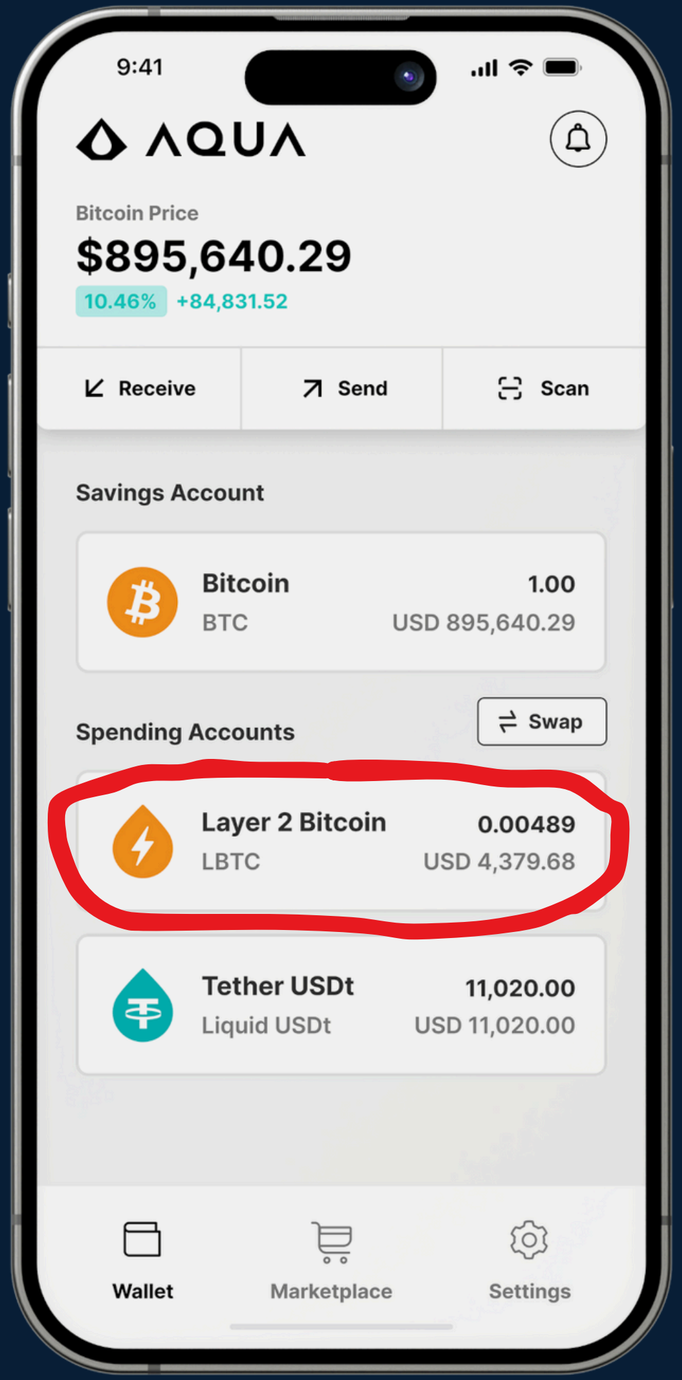


Misty Breez



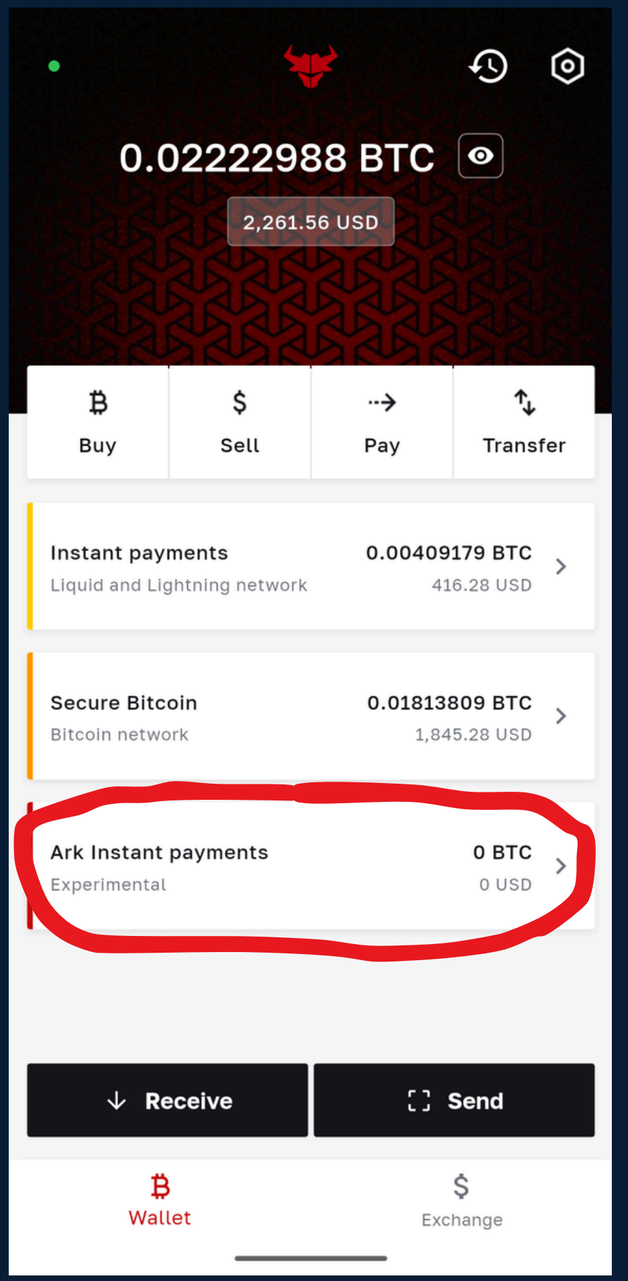
¿Cómo funciona?

- Monedero Liquid
- Swapear cuando sea necesario



¿Cómo funciona?

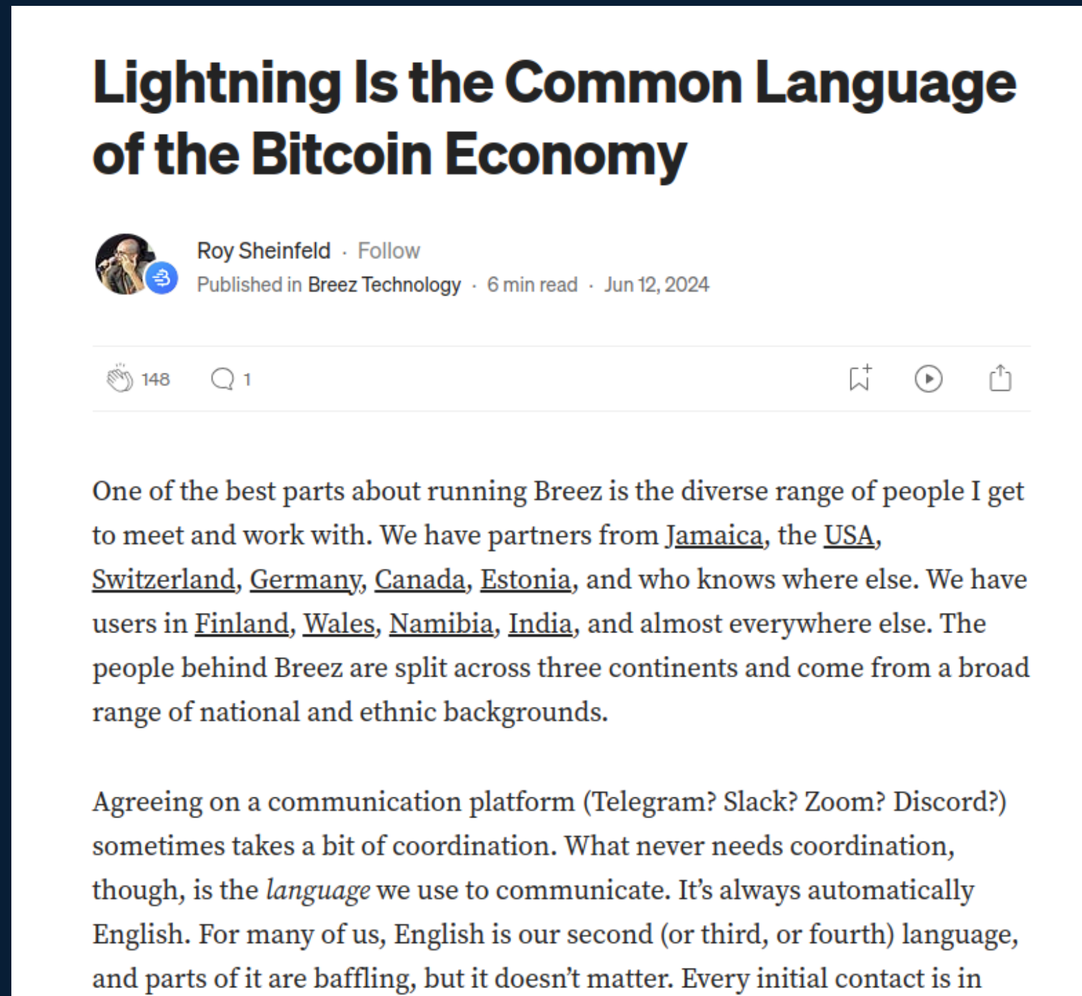
- Monedero Arkade
- Swapear cuando sea necesario



¿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

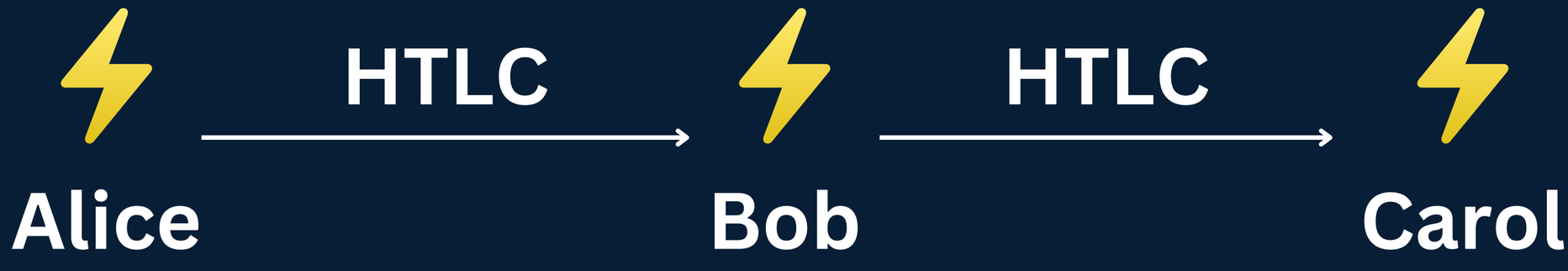
¿Cómo?

HTLCs

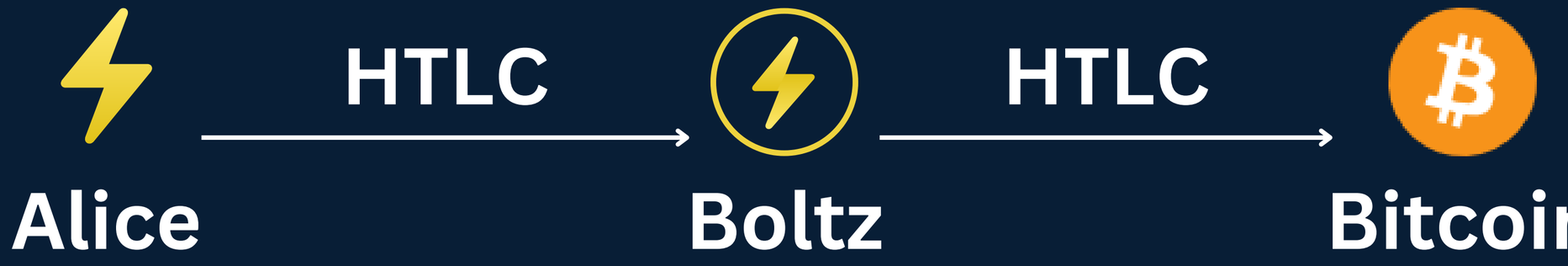
¿Qué necesitamos?

- **Hash lock**
- **Time lock**

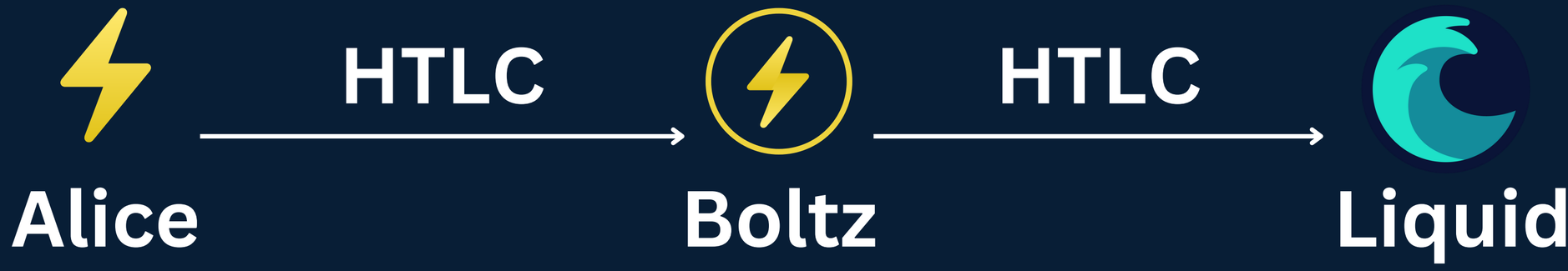
Pago Lightning



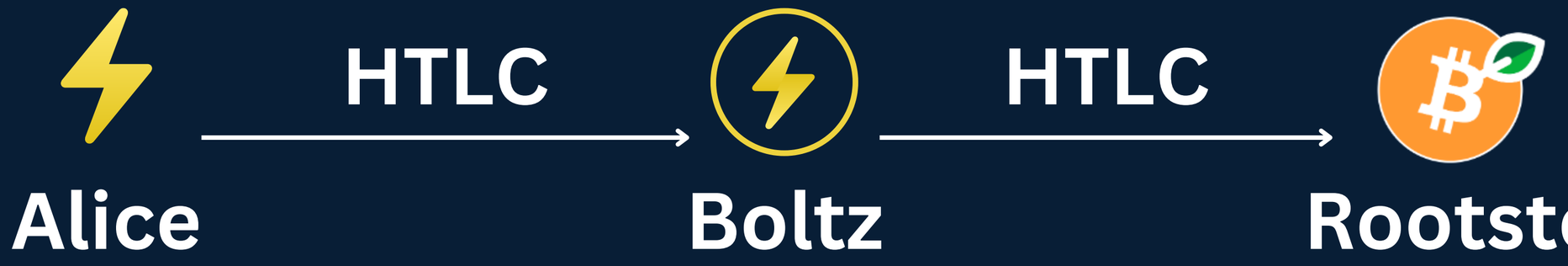
Swap Lightning



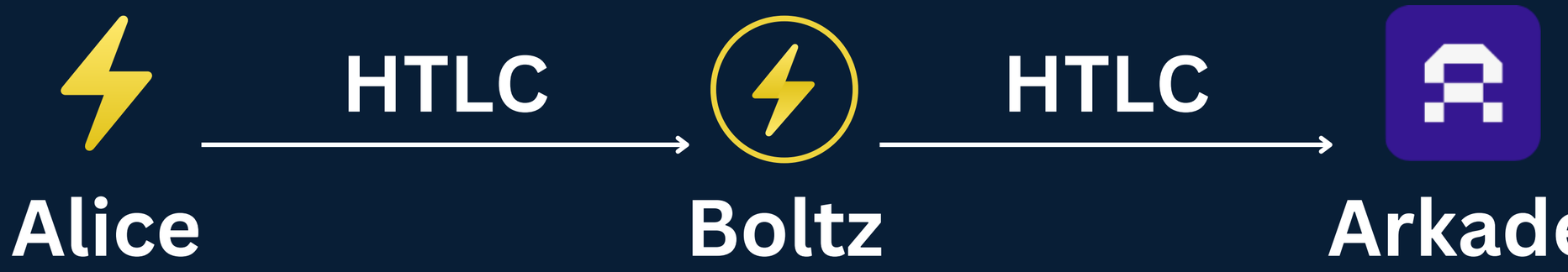
Swap Lightning



Swap Lightning



Swap Lightning



SegWit 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

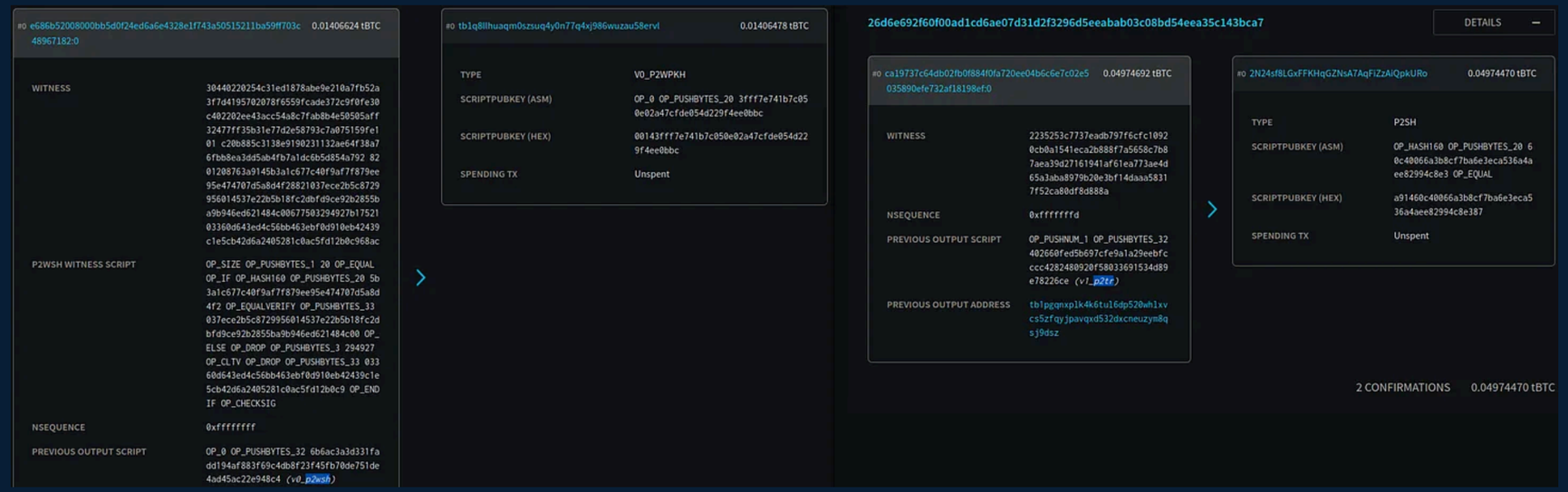
```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUAL
OP_IF
  OP_HASH160
  OP_PUSHBYTES_20 <preimage hash>
  OP_EQUALVERIFY
  OP_PUSHBYTES_33 <user public key>
OP_ELSE
  OP_DROP
  OP_PUSHBYTES_3 <timeout block height>
  OP_CLTV
  OP_DROP
  OP_PUSHBYTES_33 <Boltz public key>
OP_ENDIF
OP_CHECKSIG
```

Time lock

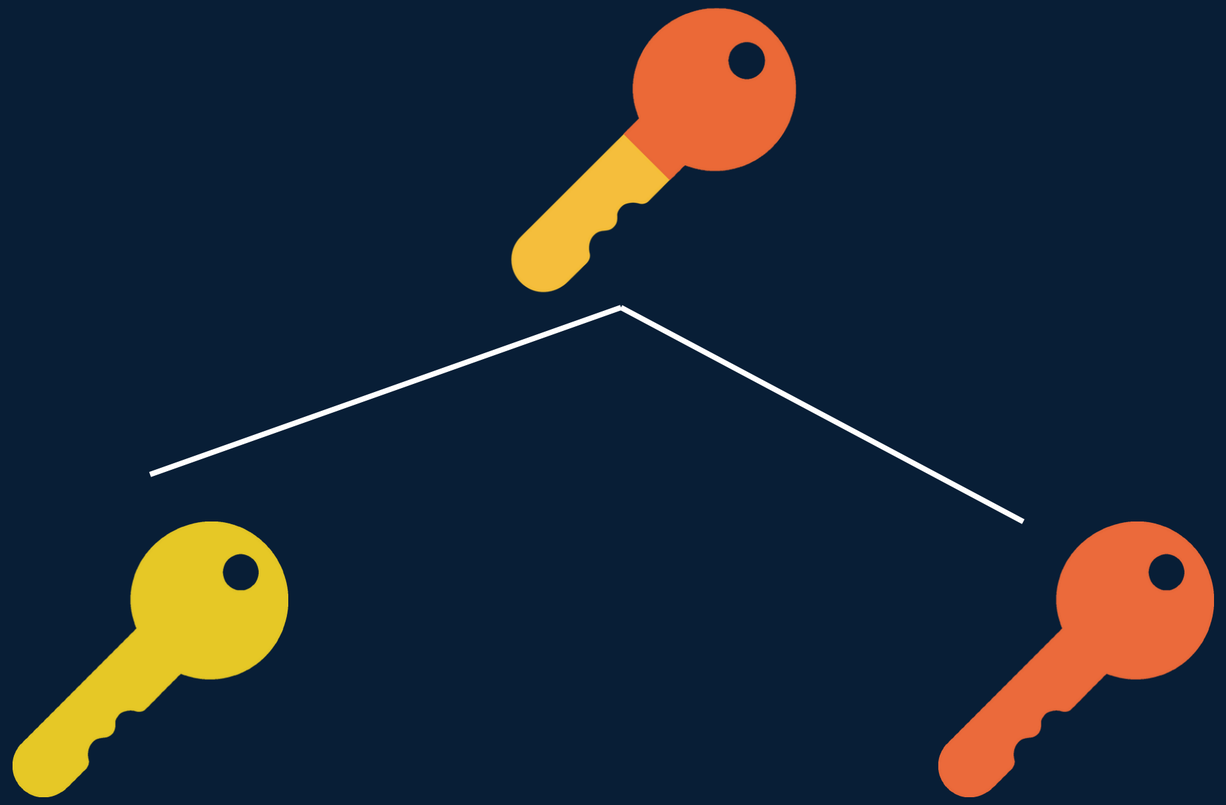
Taproot Swaps

¿Por qué?

- Reembolsos Immediatos
- Mas barrato
- Mas privado



Musig2



Taptree

Hash lock

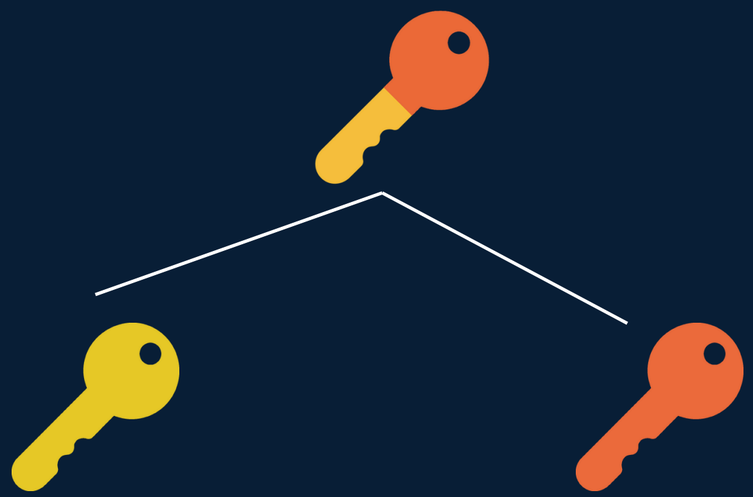
```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUALVERIFY
OP_HASH160
OP_PUSHBYTES_20 <preimage hash>
OP_EQUALVERIFY
OP_PUSHBYTES_33 <user public key>
OP_CHECKSIG
```

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

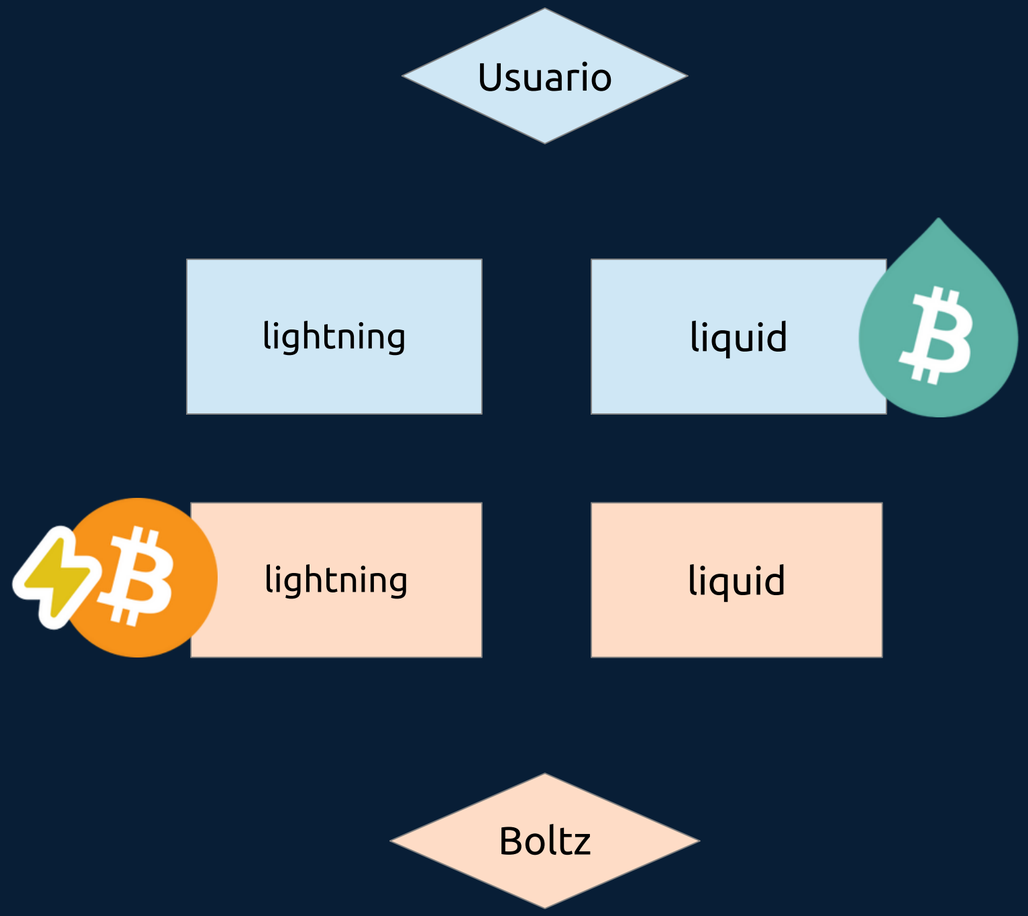
```
OP_SIZE
OP_PUSHBYTES_1 20
OP_EQUALVERIFY
OP_HASH160
OP_PUSHBYTES_20 <preimage hash>
OP_EQUALVERIFY
OP_PUSHBYTES_33 <user public key>
OP_CHECKSIG
```

Time lock

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

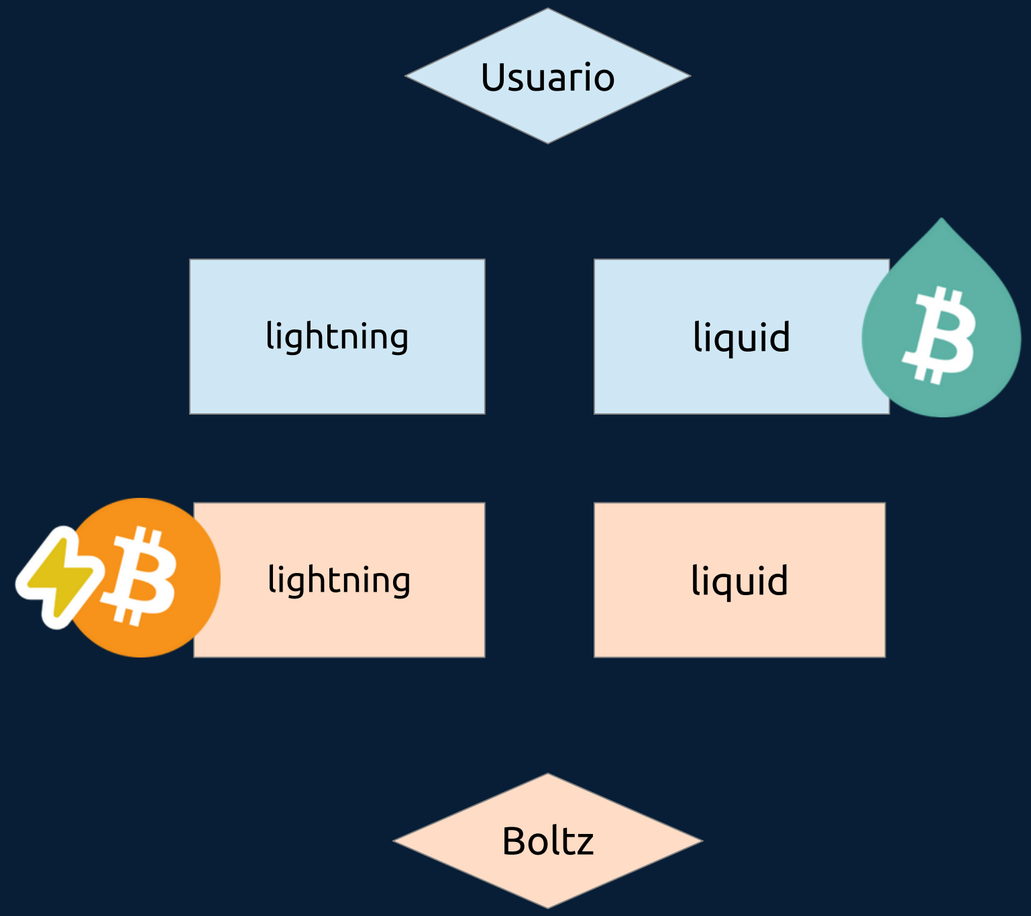
Flujo

Submarine Swaps (L-BTC -> ⚡-BTC)



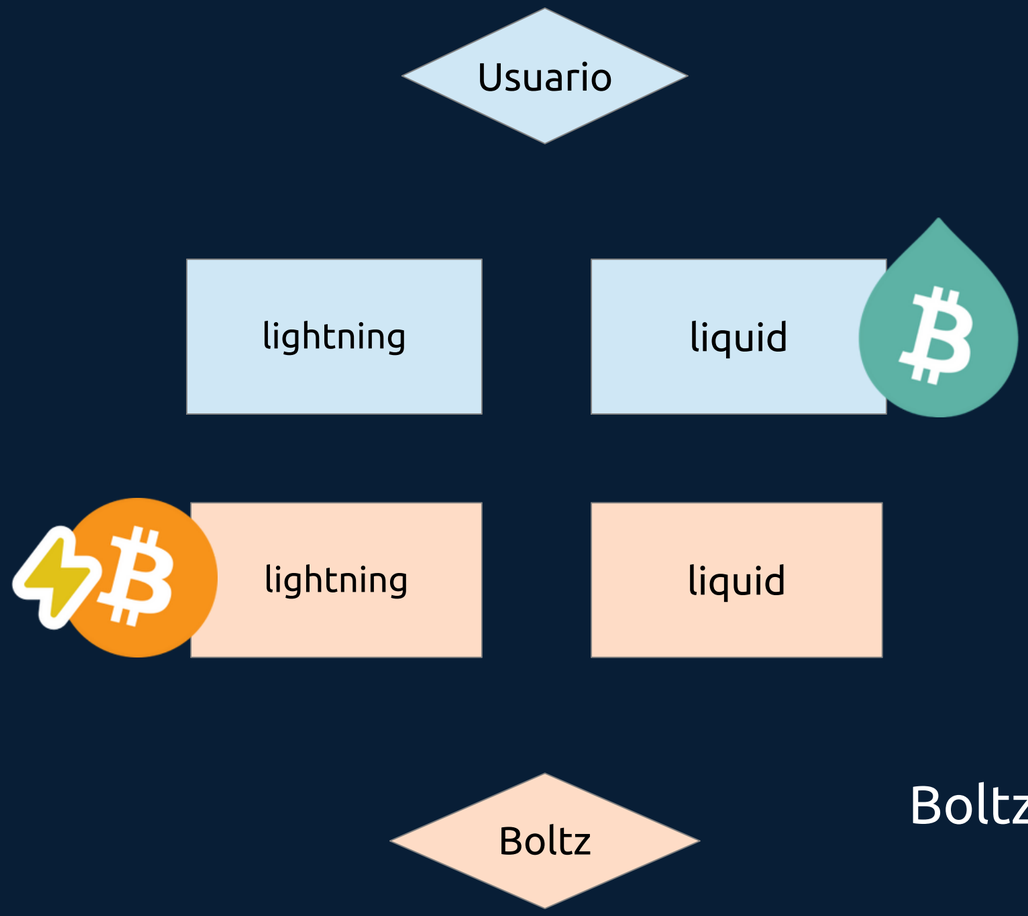
Protocolo Boltz Swap (simplificado):

Submarine Swaps (L-BTC -> ⚡-BTC)



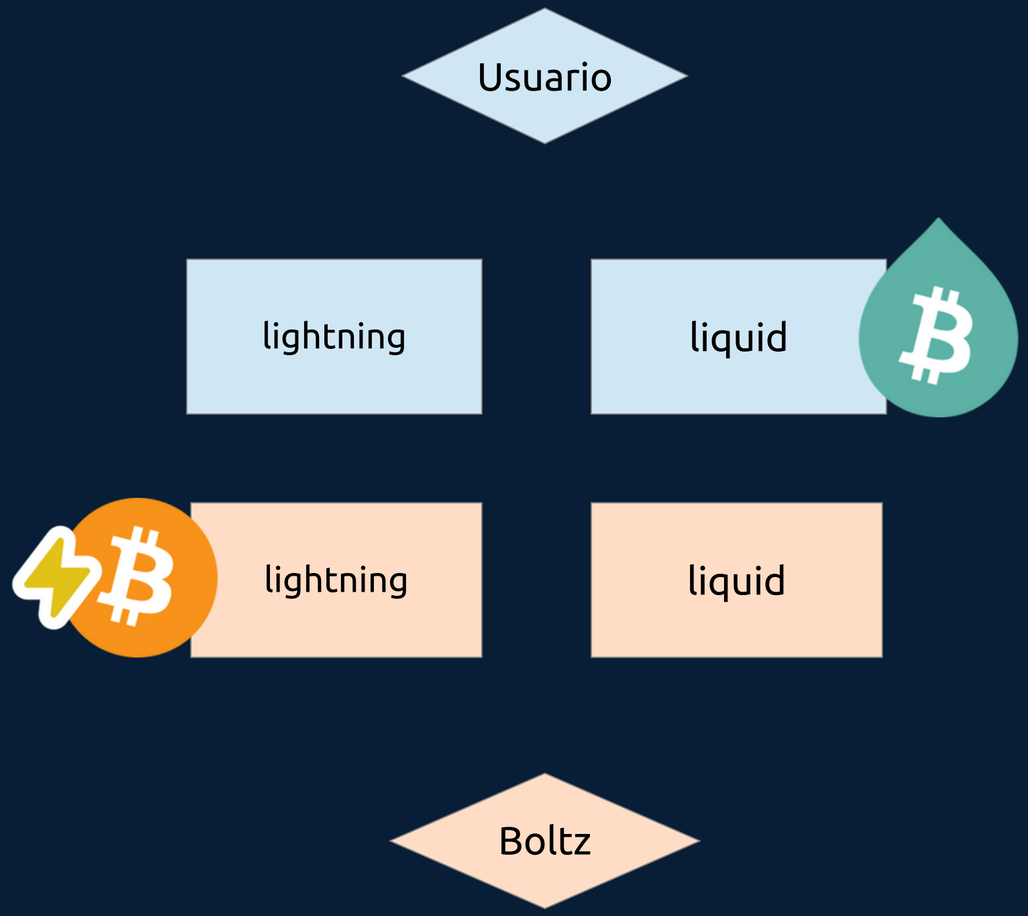
Usuario: Quiero recibir 0.099 ⚡-BTC

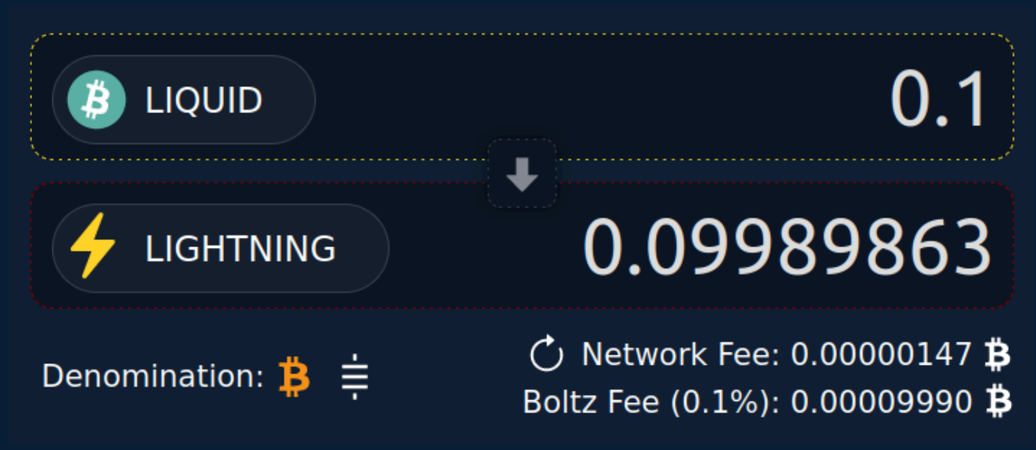
Submarine Swaps (L-BTC -> ⚡-BTC)



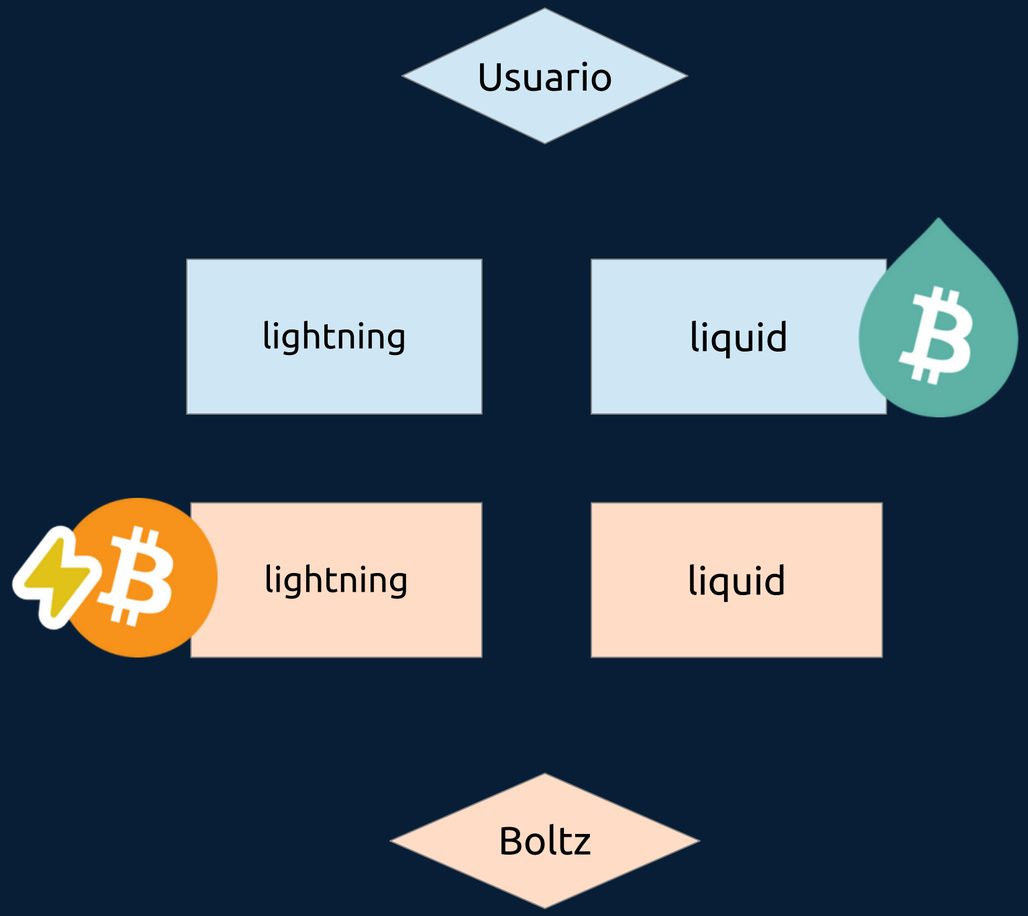
Boltz: Bueno, por eso tienes que enviarme 0.1 L-BTC

Submarine Swaps (L-BTC -> ⚡-BTC)



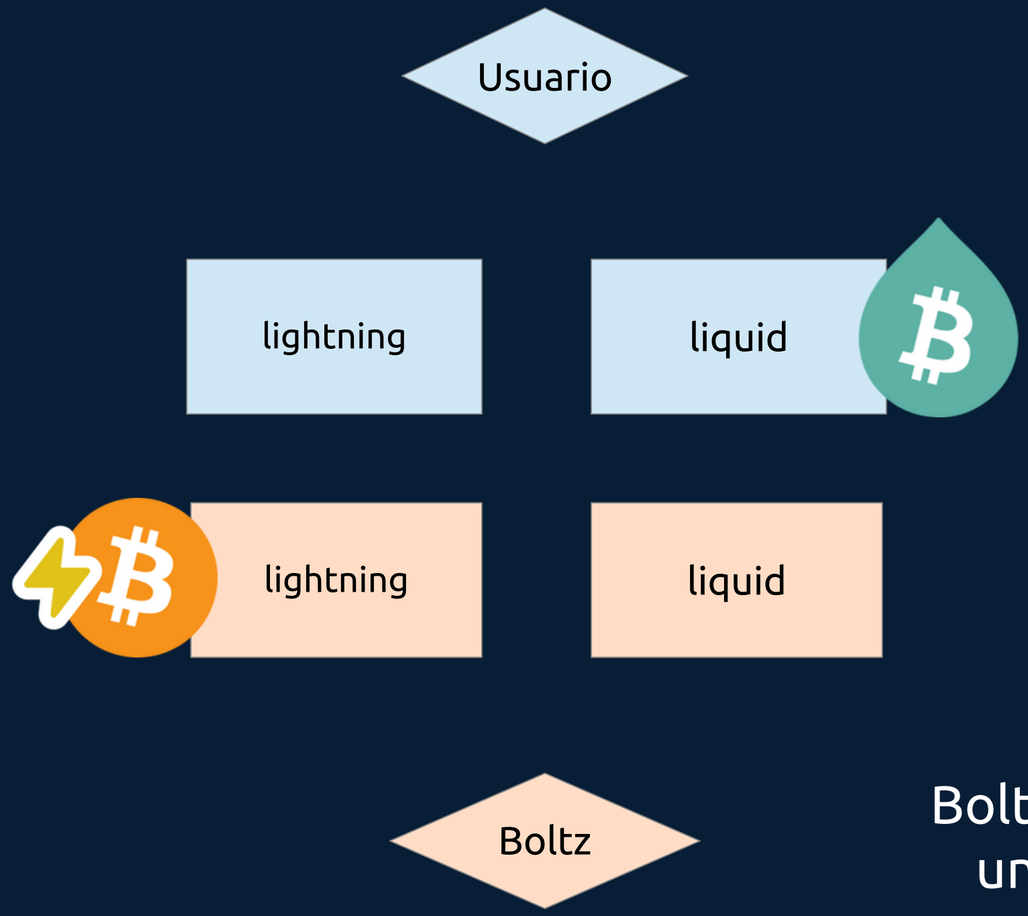


Submarine Swaps (L-BTC -> ⚡-BTC)



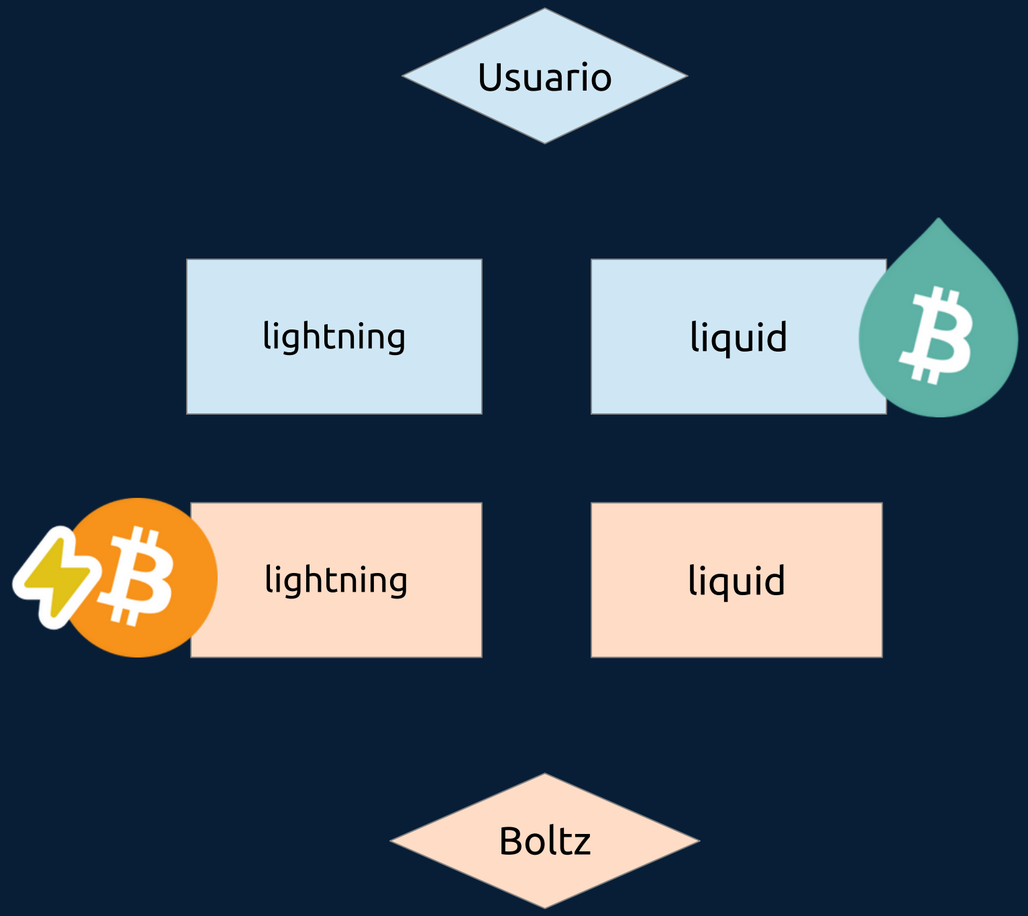
El usuario crea una factura por un importe de 0.099 ⚡-BTC.

Submarine Swaps (L-BTC -> ⚡-BTC)



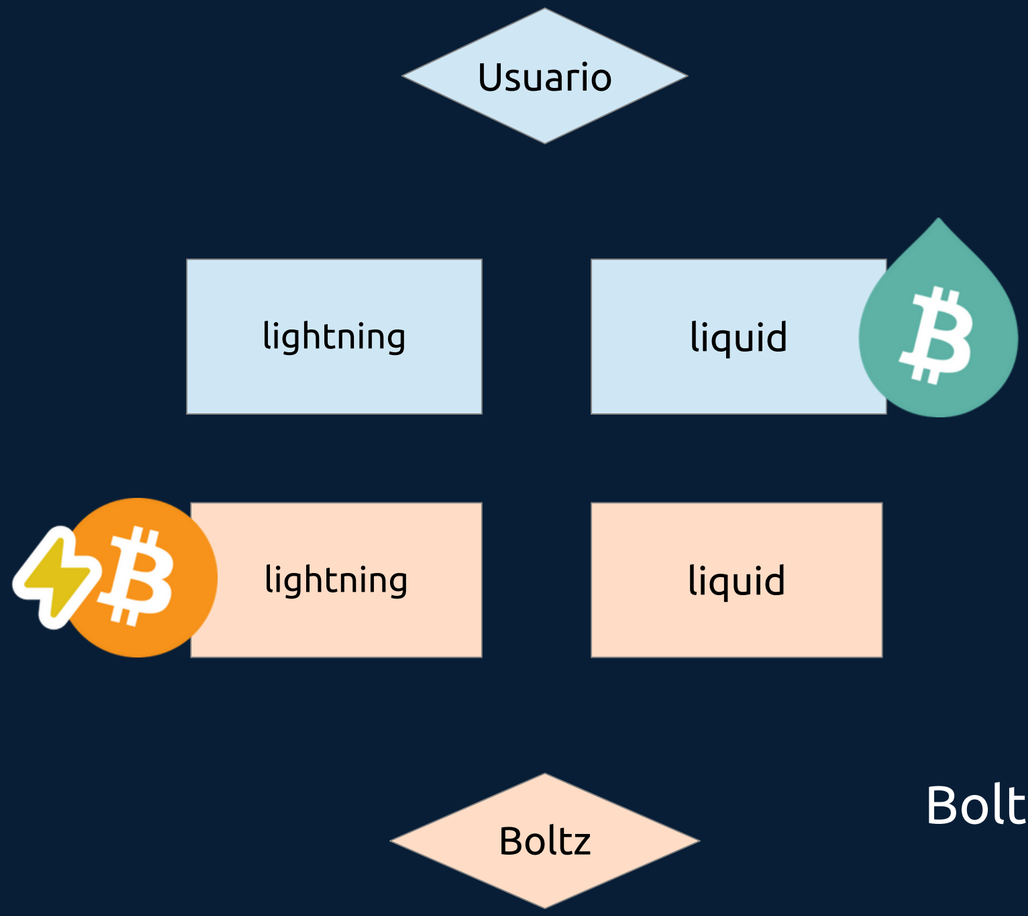
Boltz toma el hash de la preimagen de la factura y crea un redeem script para generar una dirección Liquid

Submarine Swaps (L-BTC -> ⚡-BTC)



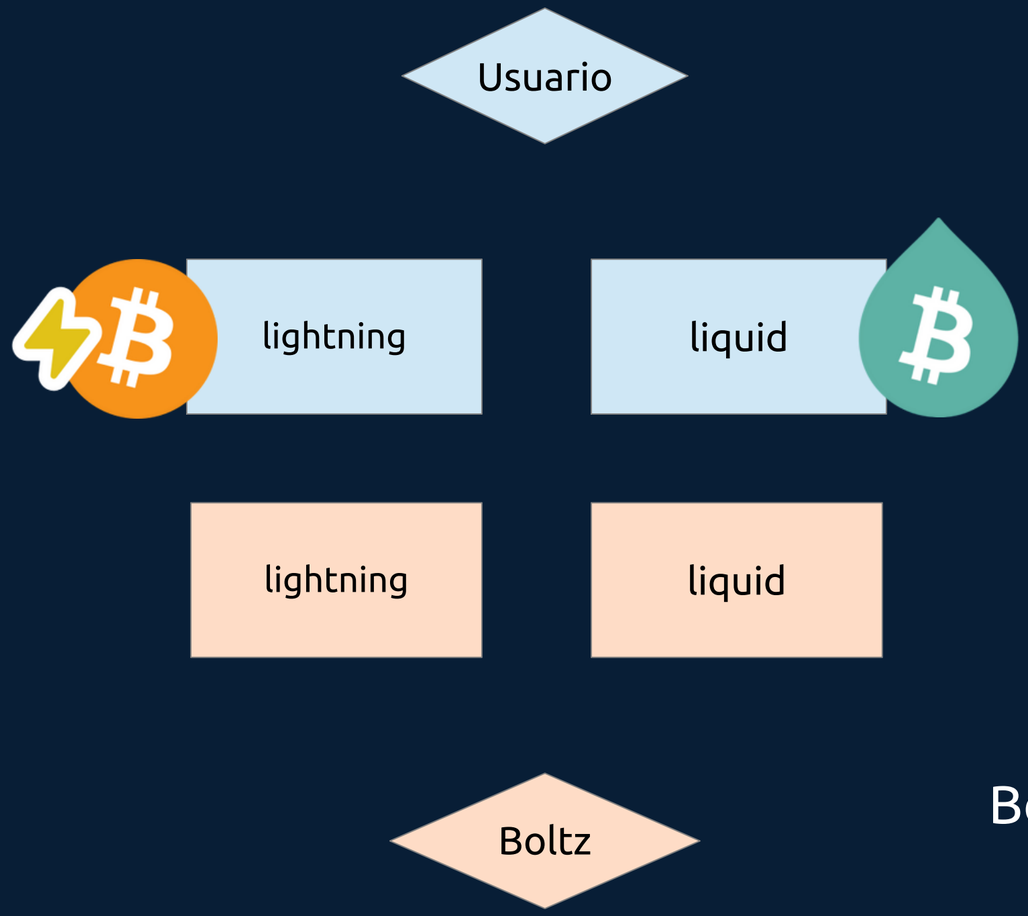
El usuario envía 0.1 L-BTC a esta dirección

Submarine Swaps (L-BTC -> ⚡-BTC)



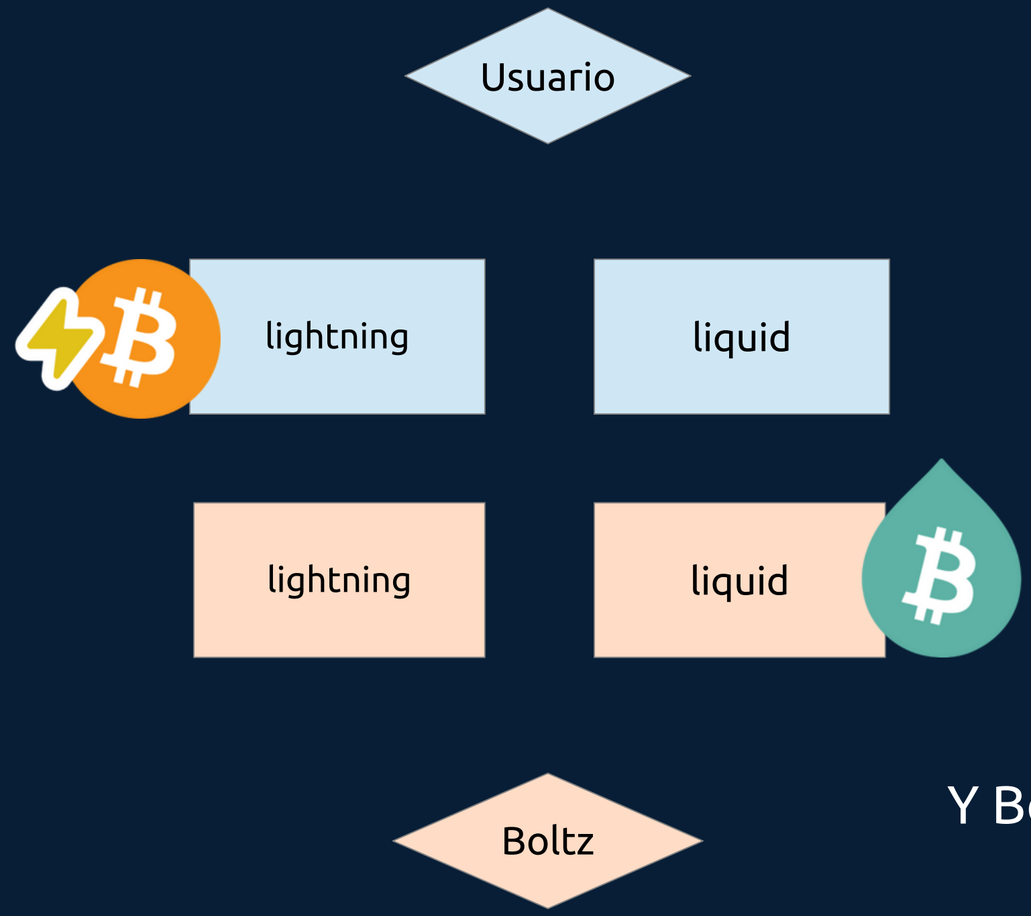
Boltz espera una confirmación de esta transacción (o no)

Submarine Swaps (L-BTC -> ⚡-BTC)



Boltz paga la factura de 0.099 ⚡-BTC, por lo que se revela la preimagen.

Submarine Swaps (L-BTC -> ⚡-BTC)



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

Swap completado!

Demo