Boltz

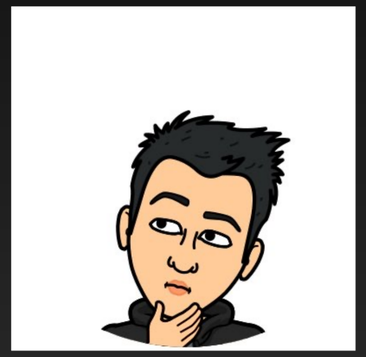
Boltz.exchange

The what, the whys, and the hows.

Ankur and Michael, 17/05/20

Boltz

A short introduction.



Ankur Kumar
Product @ Boltz

Michael
Tech Lead @ Boltz

Boltz

What is Boltz?

Boltz is a privacy first, account free crypto exchange which is completely open-source and natively supports lightning. Boltz also is a Lightning Service Provider for wallets and lapps.

Boltz

Problems with current digital asset exchanges

Boltz

- **Lack of Anonymity** in trading digital assets results in governments having unprecedented control over financial sovereignty of its citizens.

- **Custodial Nature** of popular digital asset exchanges makes them an attractive target for hacks. In a hack users are likely to actually loose their funds.
- **KYC/AML** verifications makes it hard for unbanked population of the world to take part in the crypto-economy.

Boltz

How are we solving these problems?

Boltz

By building a privacy first, account free crypto exchange.

PRIVACY FIRST

never loose funds

ACCOUNT FREE

No email, login, or kyc

SELF CUSTODIAL

all boltz offers are atomic

Boltz

Our Product offerings

Boltz

Exchange Services

boltz.exchange

LSP (Lightning Service Provider)

docs.boltz.exchange

Boltz

Demo

Demo of the new UI: http://testnet.boltz.exchange

Boltz

LSP (Lightning Service Provider)

- Boltz provides several LN services, like normal and reverse submarine swaps via a RESTful API.
- Breez uses Boltz as a LSP for integrating submarine swap powered withdrawal features. Integration with Exchange Union's XUD is in works.
- Boltz is also working on integration with a popular node management tool that we will talk about later.

Boltz

Boltz Architecture & Atomic Swaps

Boltz

Atomic Swaps

- Atomic Swaps are a way to exchange two different crypto currencies. Even if they are on different networks.
- In 2017, after a successful LTC/BTC swap, this method became widely known.

Boltz

Submarine Swaps

- A Submarine Swap allows for exchanging coins not only between networks but also layers (like Lightning and the Bitcoin chain).
- Submarine Swaps are the kind of atomic swaps which are used by Boltz to make its trades atomic and self-custodial.

Boltz

Normal Submarine Swaps

When user trades on-chain coins for lightning ones, Ex: (BTC -> ⚡BTC)

⚡ Boltz

- User starts the swap by pasting a ⚡ invoice.
- Boltz backend gets hash of the preimage from that invoice and generates a P2(W)SH address for the user.

- The redeem script of such a P2(W)SH address looks something like this:

```
HASH160 <hash of the preimage> EQUAL
IF <public key of Boltz>
ELSE <timeout block height> CHECKLOCKTIMEVERIFY
DROP <public key of the user> ENDIF
CHECKSIG
```

Boltz

- Next, user sends funds to this address.
- Boltz pays the invoice the user pasted in the first step and get the preimage.
- With preimage now available, Boltz can claim the on-chain coins sent by the user and normal submarine swap is completed.

Boltz

Reverse Submarine Swaps

When user trades lightning coins for on-chain ones, Ex: (⚡BTC -> BTC)

Boltz

- In reverse subamarine swap, Boltz backend and the users switch roles - from the one they had during normal submarine swap flow.
- User generates a random preimage and sends its hash to Boltz, which then generates a hodl invoice with that hash.

Boltz

- When the user pays the invoice, Boltz locks up on-chain coins that can be claimed by the user using the preimage.
- Boltz gets the preimage from the claim transaction and settles the invoice.
- Boltz automatically refunds the on-chain coin and sends them back to its wallet if something goes awry.

Boltz

Fun fact 🎉

Breez uses reverse submarine swap service from Boltz
to power on-chain BTC withdrawal from their wallet. Also, we were first to bring a production release of reverse submarine swap to the market.

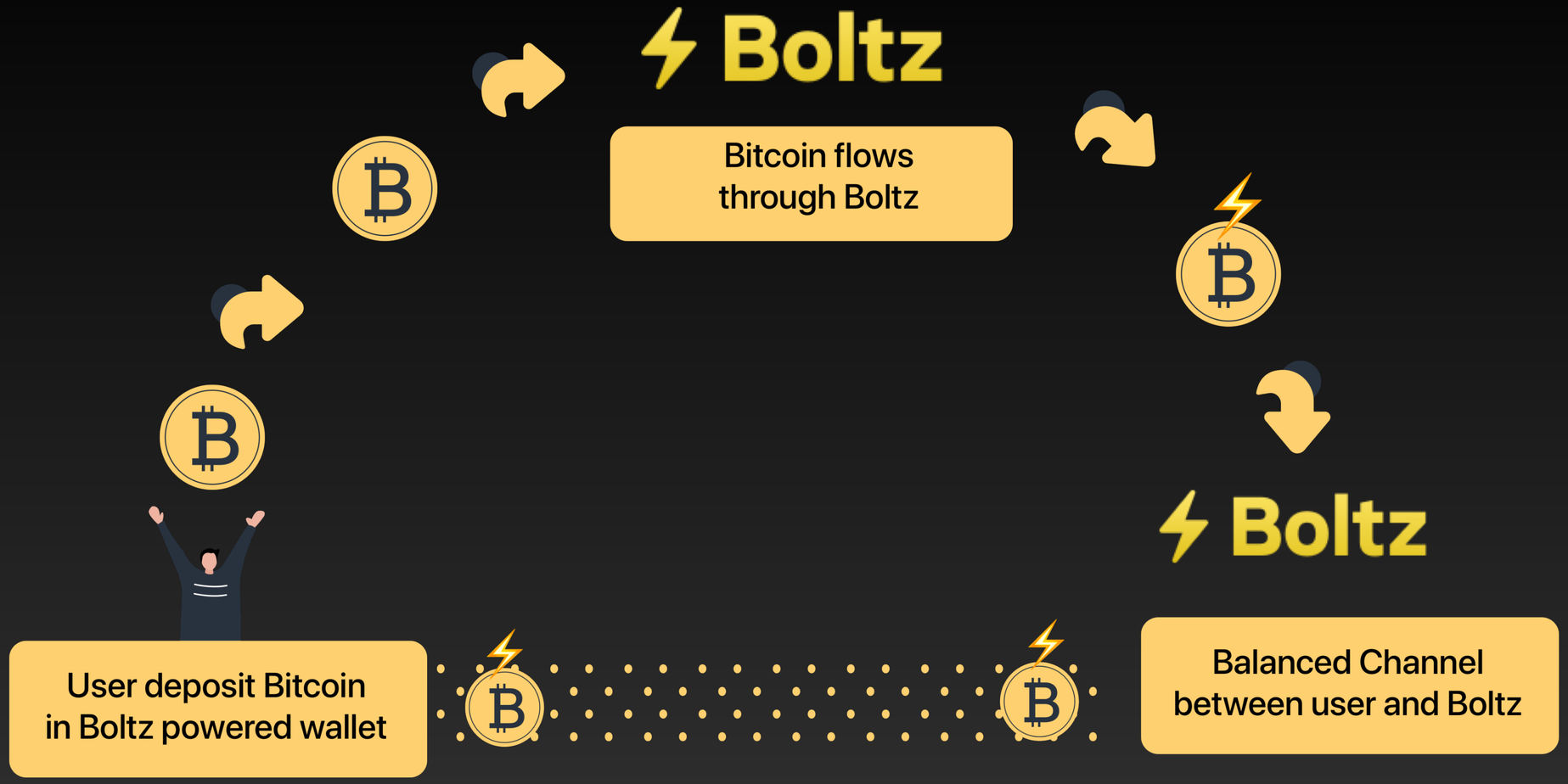
Boltz

One more thing...

Boltz

Channel Creation Swaps

World's first trust minimised channel creation swaps



Depicted: Channel Creation Swap Flow

Boltz

- We are working a Bitrefill-eque channel on demand service, but with one important catch - it is self custodial and trust minimised.
- Channel-creation swaps are similar to the normal submarine swap, however, with the help of hodl invoices, we were able to build a channel creation service that works on the fly.

Boltz

- Channel creation swaps helps with on-boarding new users to the lightning economy.
- Boltz is the first to deploy and release a production grade implementation of self-custodial channel creation swaps.

- From end user perspective, channel creation swap flow goes like this -> user funds a Boltz powered wallet with on-chain Bitcoin, which gets circled through Boltz and results in a balanced channel between user and Boltz.

Boltz

Demo

Channel Creation Swap Demonstration

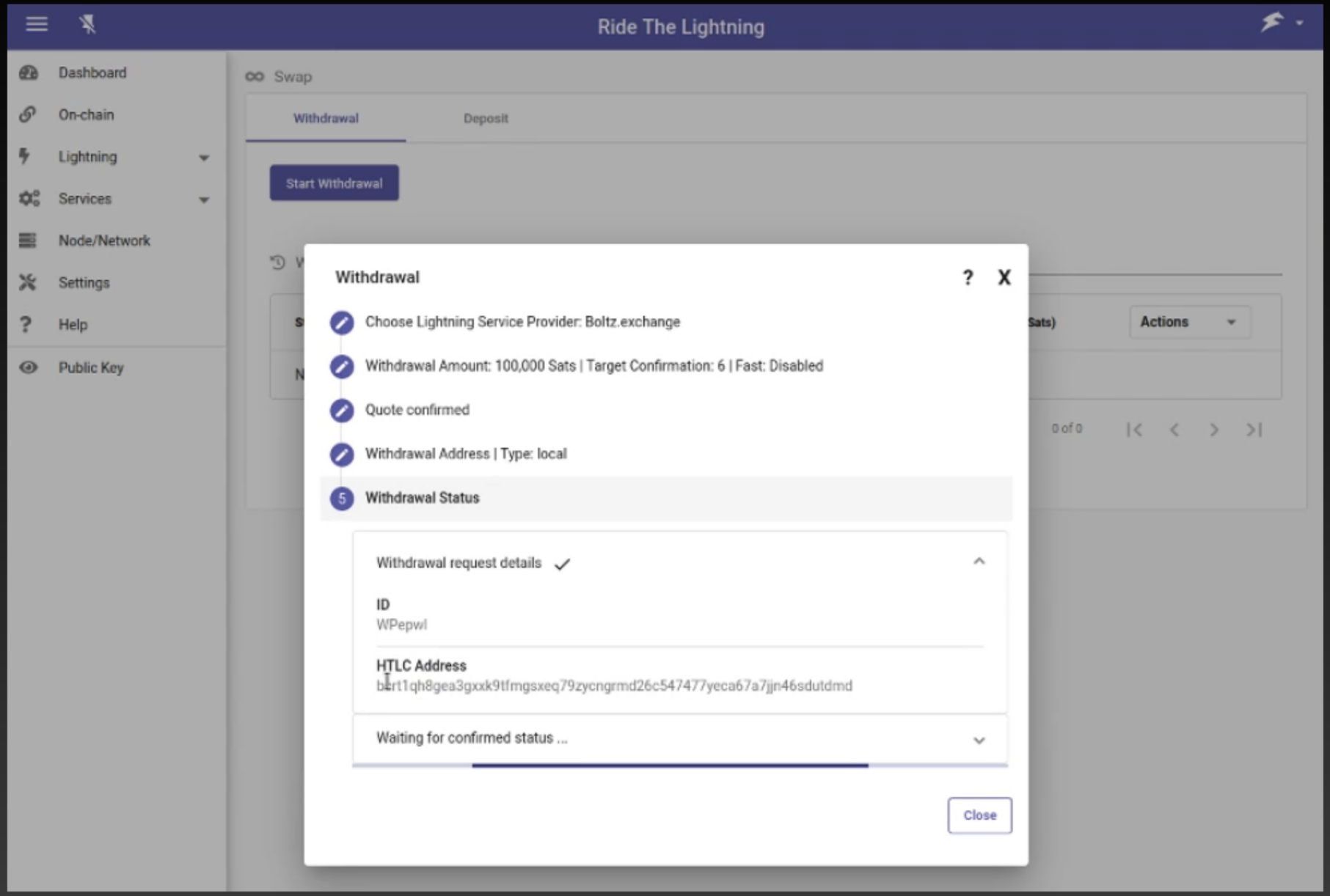
Boltz

A little news for LN power users 🎉

We’re currently also working on a integration of Boltz Lightning Services into RTL (Ride the lightning) that will bring all these cool Boltz features, alongside the already available Lightning Loop alternatives.

Sneak peak..

Boltz



Boltz

Questions?

Thank you!