Itchysats: Bitcoin CFDs

Lucas Soriano del Pino

COMIT, CoBloX

2022-01-25

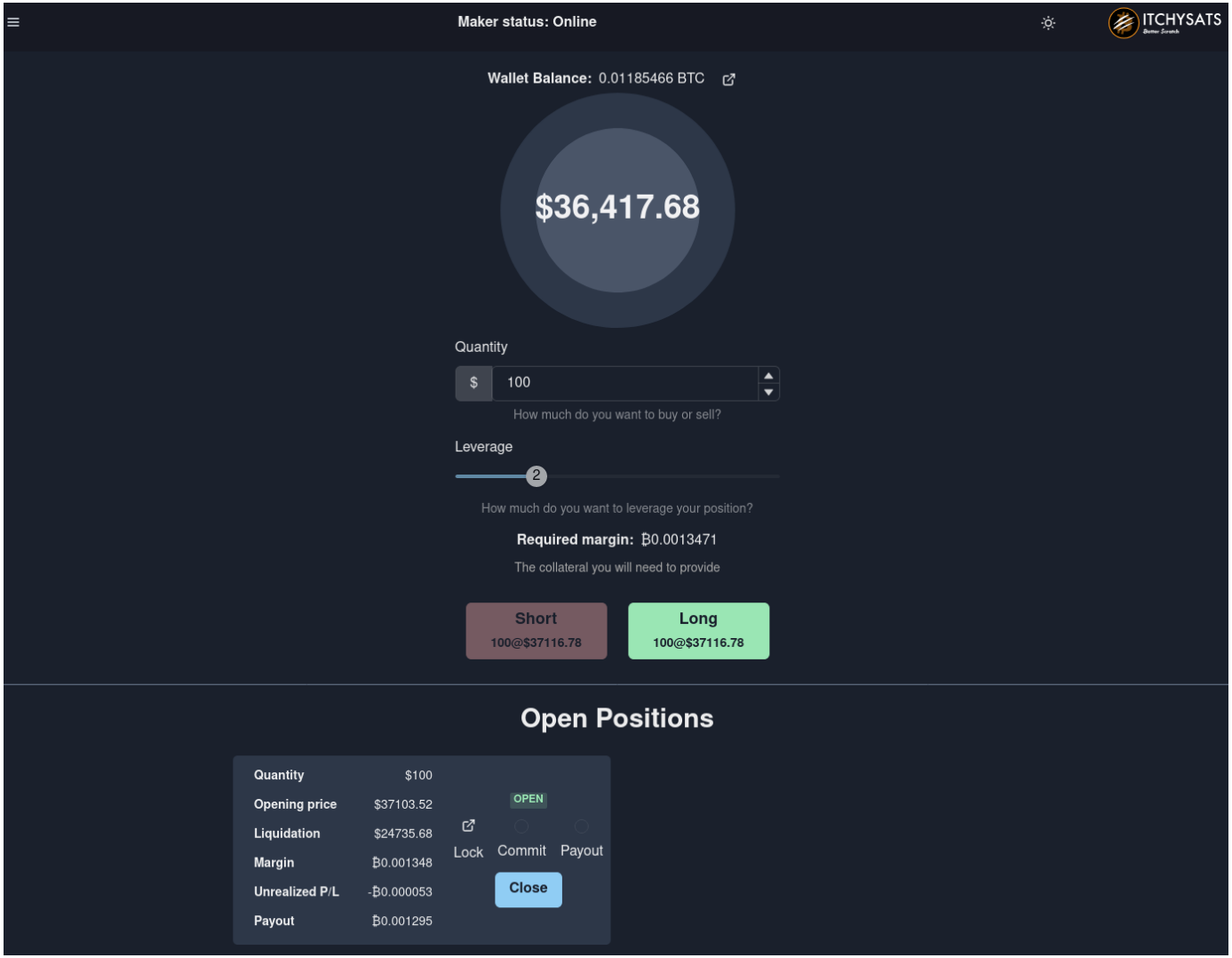
Outline

1. What is Itchysats?
2. How does it work?
3. Roadmap
4. Demo
5. Questions

Outline

1. What is Itchysats?
2. How does it work?
3. Roadmap
4. Demo
5. Questions

What is Itchysats?



What is a CFD?

- Derivative

What is a CFD?

- Derivative
- Bet on the price of an asset in the future

What is a CFD?

- Derivative
- Bet on the price of an asset in the future
- Leverage

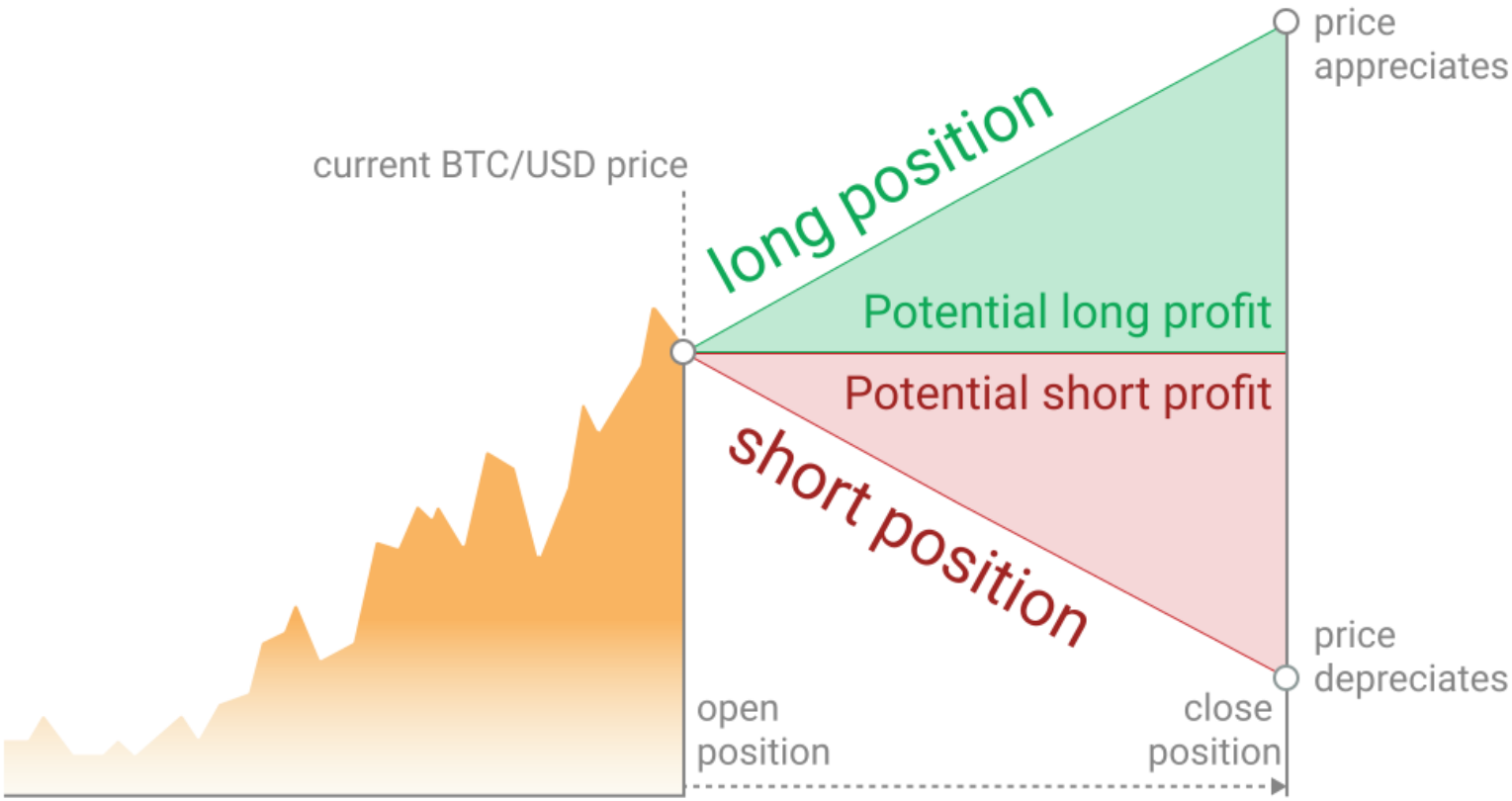
What is a CFD?

- Derivative
- Bet on the price of an asset in the future
- Leverage
- No expiry date

What is a CFD?

- Derivative
- Bet on the price of an asset in the future
- Leverage
- No expiry date
- Margin call

Potential profits (and losses)



Bitcoin CFDs on Itchysats

- Like conventional CFDs

Bitcoin CFDs on Itchysats

- Like conventional CFDs
- Bitcoin as underlying asset

Bitcoin CFDs on Itchysats

- Like conventional CFDs
- Bitcoin as underlying asset
- Can only go long (shorting soon TM)

Bitcoin CFDs on Itchysats

- Like conventional CFDs
- Bitcoin as underlying asset
- Can only go long (shorting soon TM)
- Long can *double-dip*

BitMEX already does this!

But Itchysats is:

- Non-custodial

BitMEX already does this!

But Itchysats is:

- Non-custodial
- Peer-to-peer

BitMEX already does this!

But Itchysats is:

- Non-custodial
- Peer-to-peer
- Built on top of Bitcoin

BitMEX already does this!

But Itchysats is:

- Non-custodial
- Peer-to-peer
- Built on top of Bitcoin
- Free of counterparty risk

BitMEX already does this!

But Itchysats is:

- Non-custodial
- Peer-to-peer
- Built on top of Bitcoin
- Free of counterparty risk
- Accountless

Outline

1. What is Itchysats?
2. How does it work?
3. Roadmap
4. Demo
5. Questions

Example

- Taker goes long: bets 0.5 BTC that BTC >= 40k USD

Example

- Taker goes long: bets 0.5 BTC that BTC >= 40k USD
- Maker goes short: bets 0.5 BTC that BTC < 40k USD

Example

- Taker goes long: bets 0.5 BTC that BTC >= 40k USD
- Maker goes short: bets 0.5 BTC that BTC < 40k USD
- Winner takes all

Counterparty risk

- 1st step on chain: lock up margin as collateral

Counterparty risk

- 1st step on chain: lock up margin as collateral
- 2-of-2 multisig output

Enforcing the bet

- Spend condition based on external information

Enforcing the bet

- Spend condition based on external information
- Settle bet without collaboration

DLC (Discreet Log Contract)

- 2-of-2 multisig

DLC (Discreet Log Contract)

- 2-of-2 multisig
- Spent according to an oracle

DLC (Discreet Log Contract)

- 2-of-2 multisig
- Spent according to an oracle
- Oracle is oblivious

DLC (Discreet Log Contract)

- 2-of-2 multisig
- Spent according to an oracle
- Oracle is oblivious
- Privacy-preserving

DLC (Discreet Log Contract)

- 2-of-2 multisig
- Spent according to an oracle
- Oracle is oblivious
- Privacy-preserving
- *dlcspecs*

Olivia

Oracle server made and hosted by Lloyd!

In practice

Olivia

Oracle server made and hosted by Lloyd!

In practice

- Olivia identified by `P`

Olivia

Oracle server made and hosted by Lloyd!

In practice

- Olivia identified by `P`
- Olivia announces future attestation, including a public nonce `R`

Olivia

Oracle server made and hosted by Lloyd!

In practice

- Olivia identified by `P`
- Olivia announces future attestation, including a public nonce `R`
- Itchysats uses `P`, `R` and prices to lock spending conditions for DLC

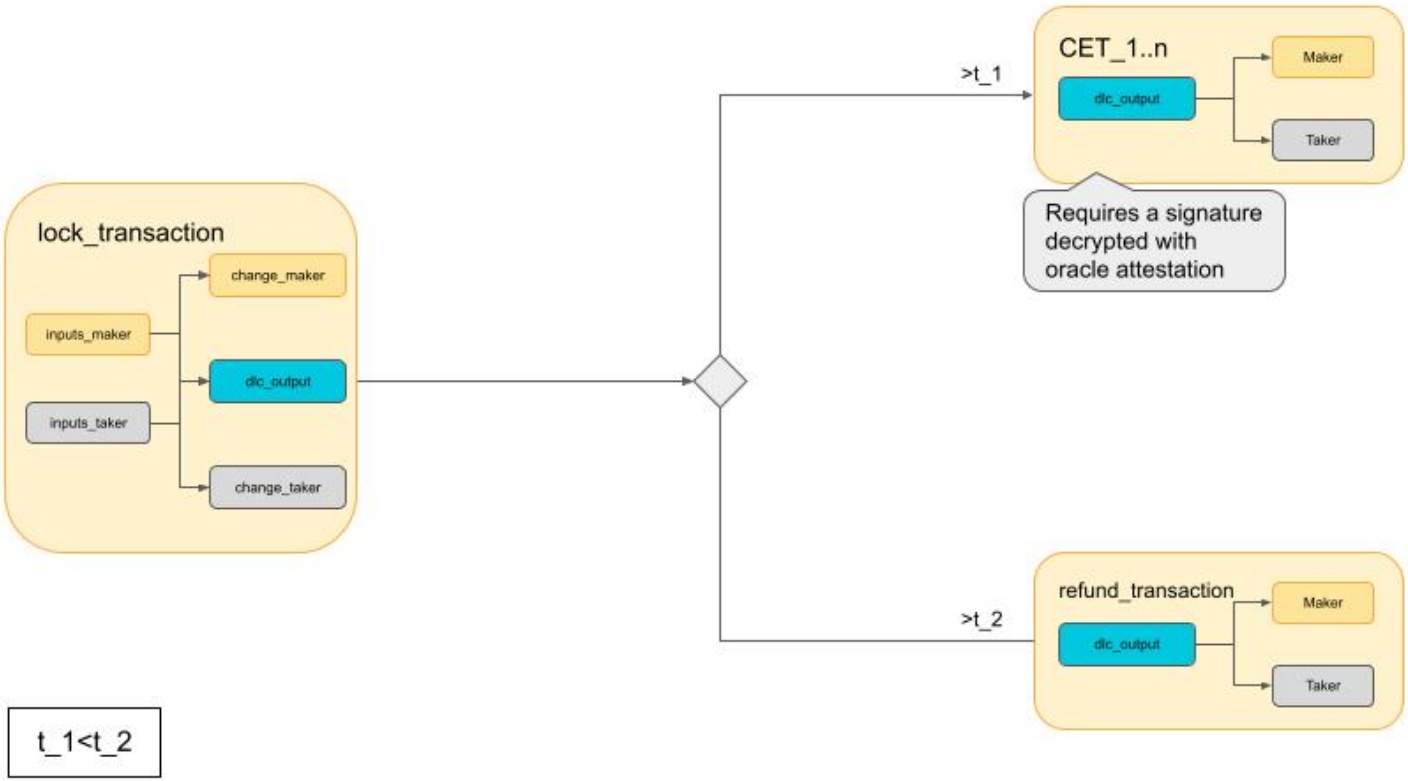
Olivia

Oracle server made and hosted by Lloyd!

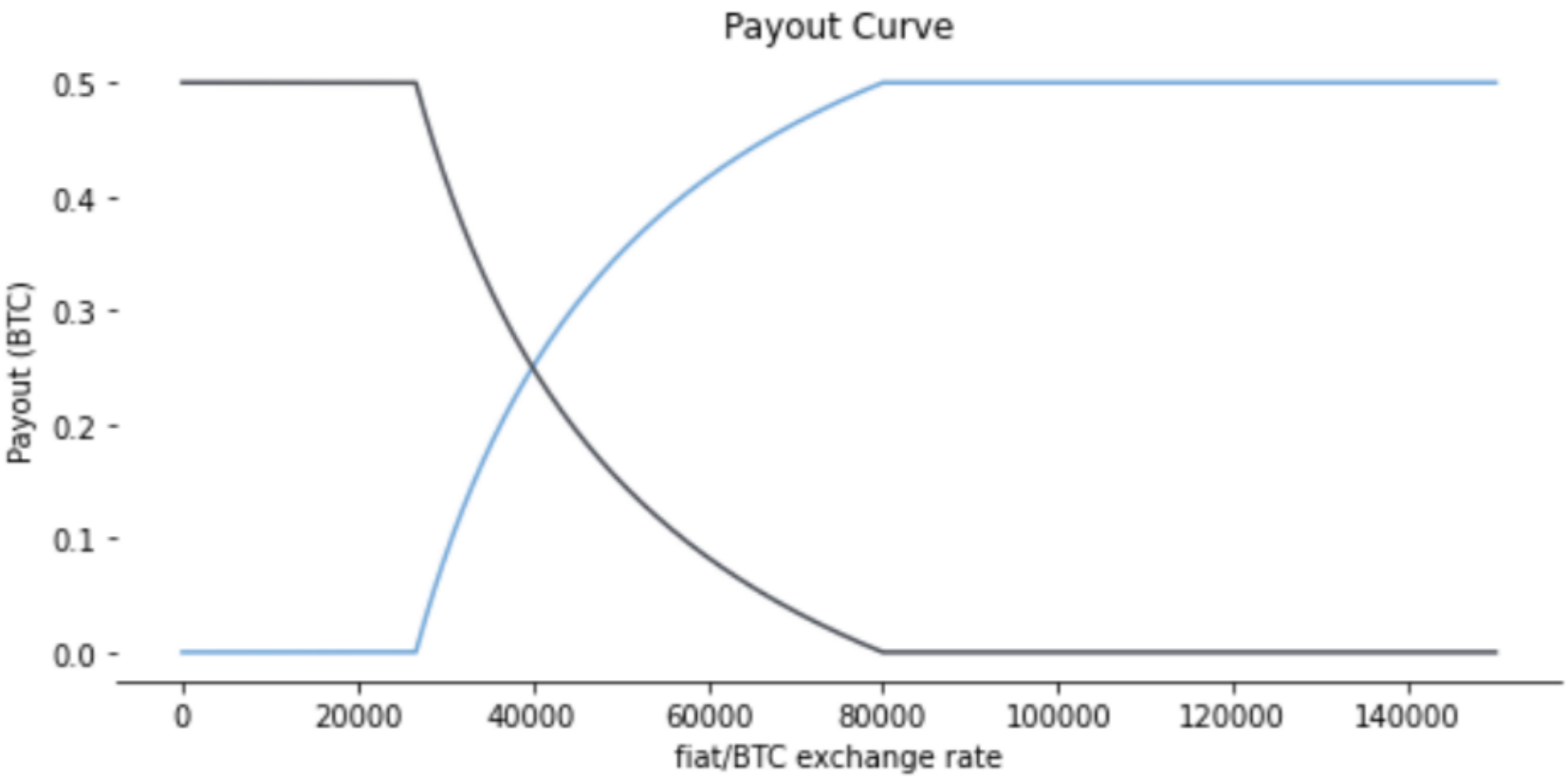
In practice

- Olivia identified by `P`
- Olivia announces future attestation, including a public nonce `R`
- Itchysats uses `P`, `R` and prices to lock spending conditions for DLC
- Olivia attests to price using `p` and `r`, enabling one spending path

Transactions



Payout curve



Perpetual CFDs

- CFDs aren't meant to expire

Perpetual CFDs

- CFDs aren't meant to expire
- Can't get rid of the deadline

Perpetual CFDs

- CFDs aren't meant to expire
- Can't get rid of the deadline
- Can we push the deadline?

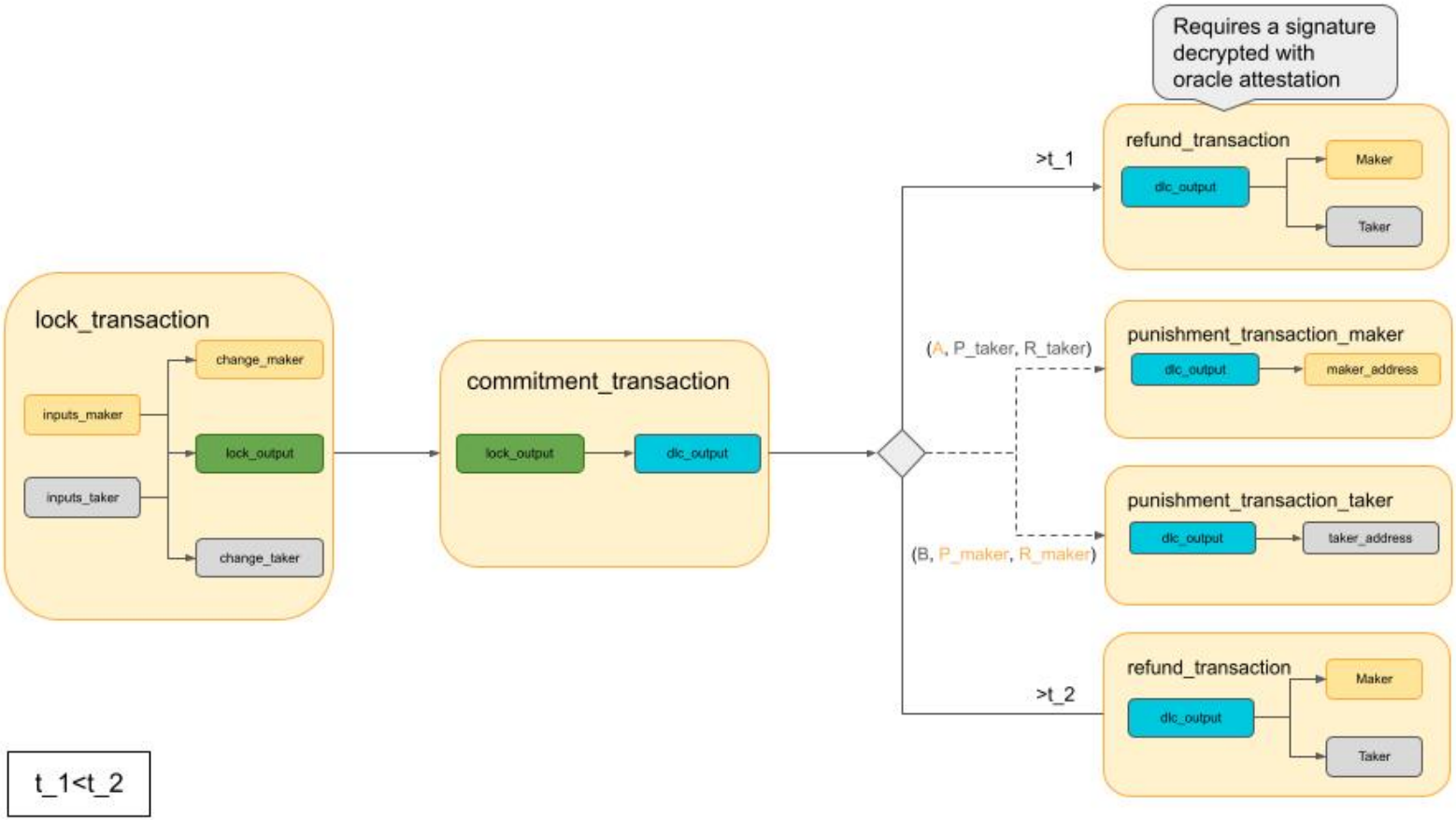
Using channels

- Look at Lightning

Using channels

- Look at Lightning
- We have experience: implemented Generalized Bitcoin-Compatible Channels PoC

More transactions



Optional collaboration

- We have to wait to close our position

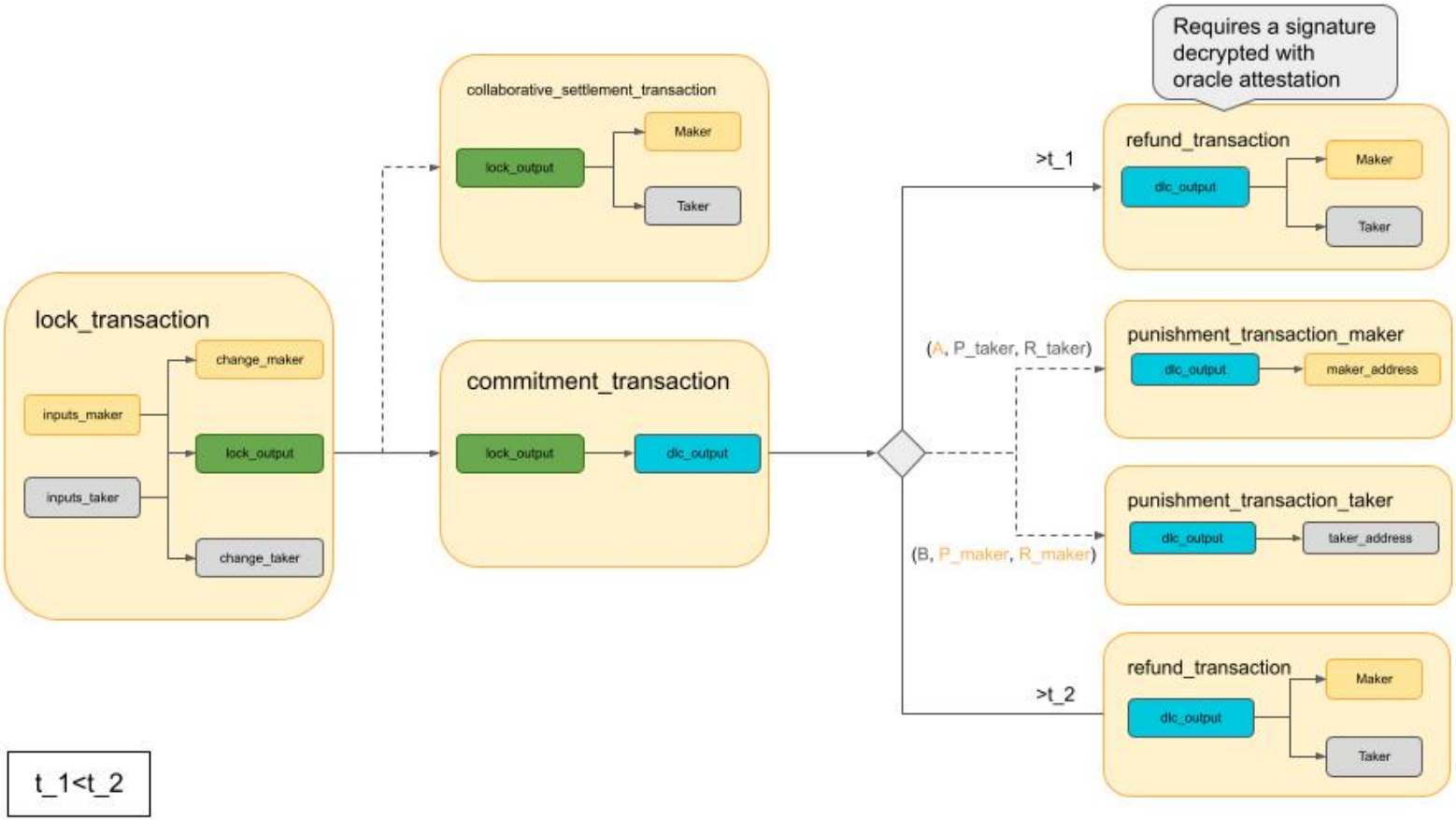
Optional collaboration

- We have to wait to close our position
- Introduce optional transaction

Optional collaboration

- We have to wait to close our position
- Introduce optional transaction
- Olivia isn't involved

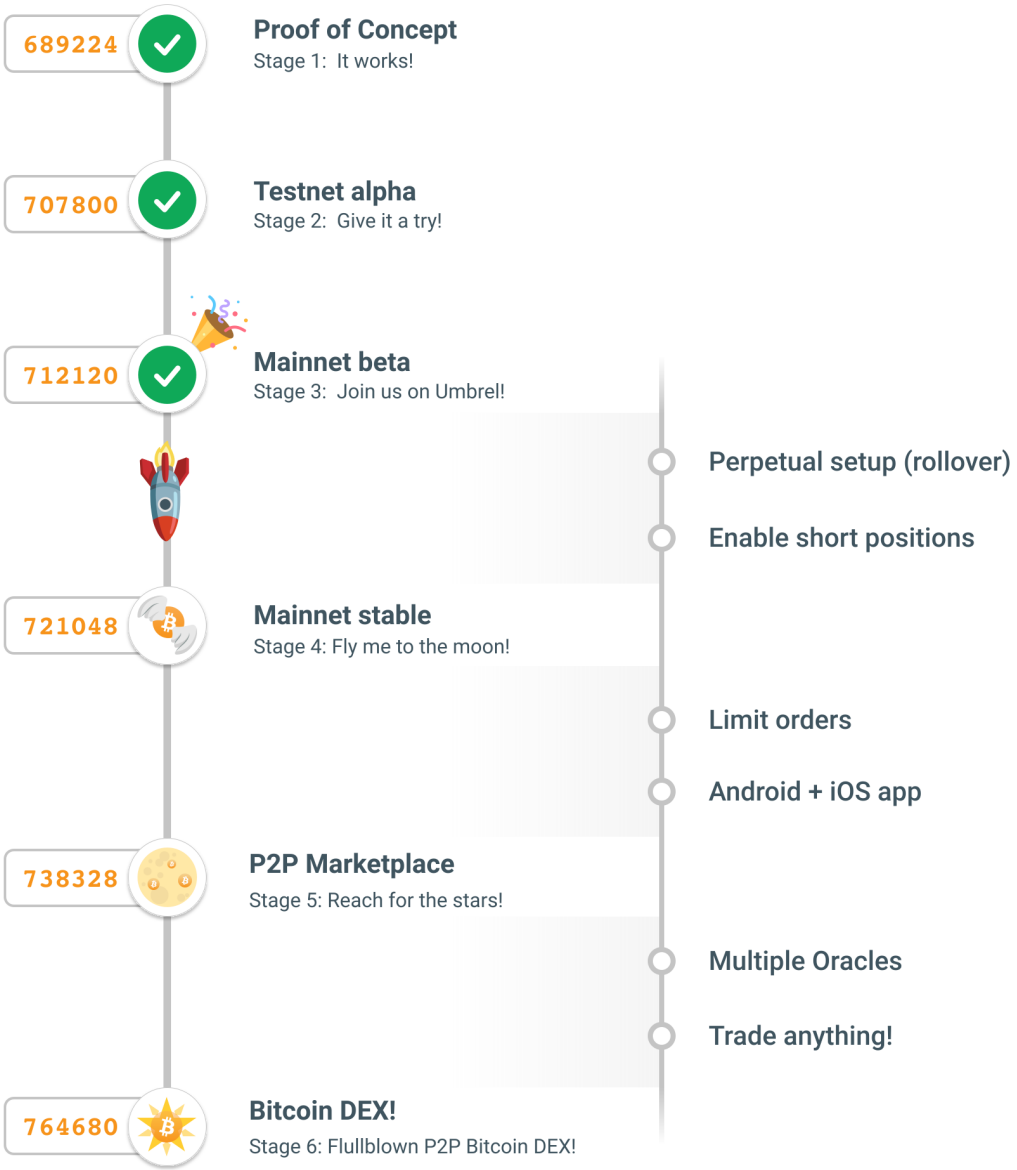
All of the transactions



Outline

1. What is Itchysats?
2. How does it work?
3. Roadmap
4. Demo
5. Questions

Roadmap


689224
Proof of Concept
Stage 1: It works!
707800
Testnet alpha
Stage 2: Give it a try!
712120
Mainnet beta
Stage 3: Join us on Umbrel!
Perpetual setup (rollover)
Enable short positions
721048
Mainnet stable
Stage 4: Fly me to the moon!
Limit orders
Android + iOS app
738328
P2P Marketplace
Stage 5: Reach for the stars!
Multiple Oracles
Trade anything!
764680
Bitcoin DEX!
Stage 6: Flullblown P2P Bitcoin DEX!

Outline

1. What is Itchysats?
2. How does it work?
3. Roadmap
4. Demo
5. Questions

Outline

1. What is Itchysats?
2. How does it work?
3. Roadmap
4. Demo
5. Questions

Ask us anything