Farcaster

Rust + Microservices + Crypto(graphy) + Crypto(currency)

Past - Present - Future

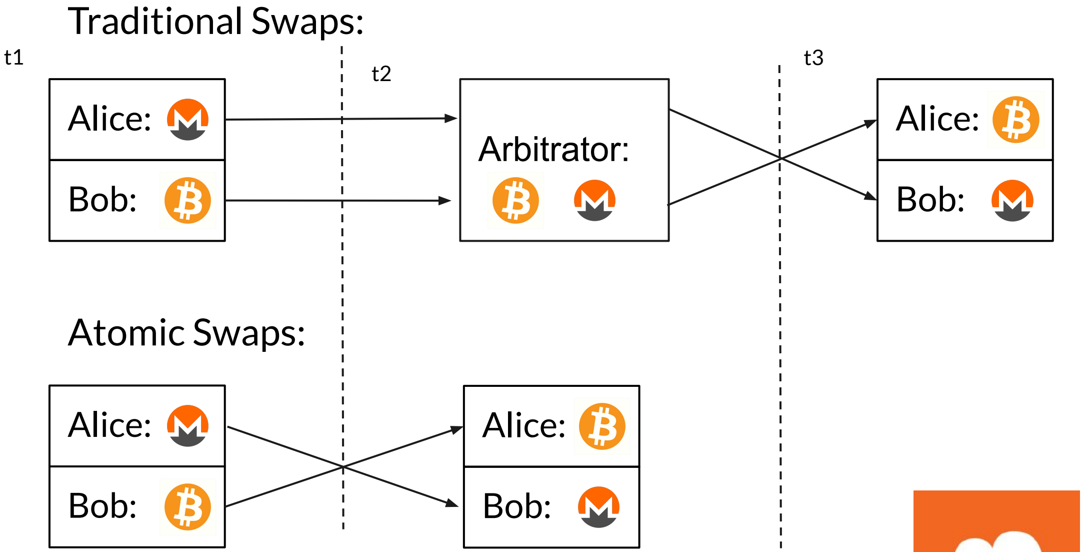
Farcaster Project Description

- CCS funded project
- Goal: Bitcoin <-> Monero atomic swaps
- Project taken on by Cryp GmbH, a Swiss cryptocurrency R&D company
- Open source, MIT licensed
- Specced in a 9-part RFC

cryp

Atomic Swaps

- Traditional asset swaps require a trusted 3rd party to ensure neither party ever holds both assets simultaneously (and can defraud their counterparty)
- Atomic swaps use cryptography instead of a trusted 3rd party to ensure the above

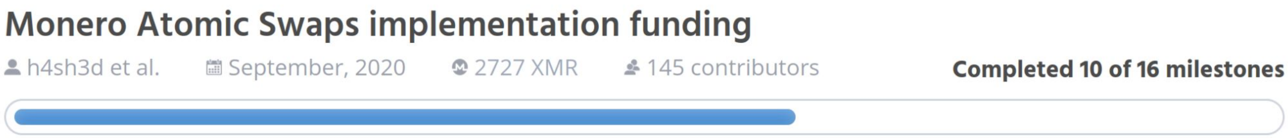


CCS - Community Crowd System

- CCS funded with great enthusiasm
- Expected delivery in Q2 2021, budgeted for 5 developers

But

- Project is delayed
- Never had more than 3 developers working at a time
- Comit released atomic swaps before us - though currently unmaintained

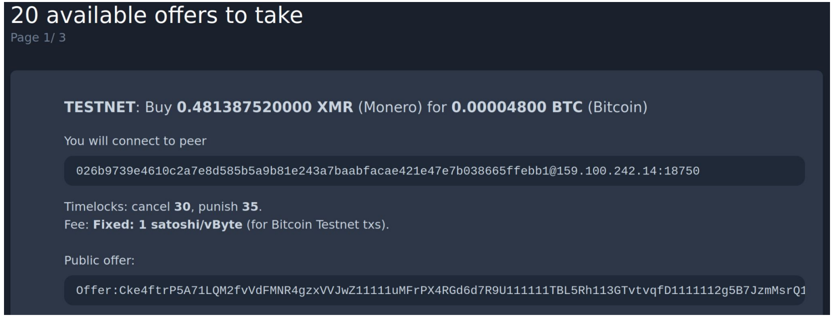


Monero Atomic Swaps implementation funding

h4sh3d et al. September, 2020 2727 XMR 145 contributors **Completed 10 of 16 milestones**

Why Farcaster?

- Farcaster’s swap implementation is symmetric, it handles both buying and selling XMR and BTC
- Sweep XMR to a destination address once swap is done
- Core architecture extendable towards future assets
- Scalable microservice architecture
- Monero light wallet server support
- Farcaster.dev - automated swap offer maker website



20 available offers to take

Page 1/ 3

TESTNET: Buy **0.481387520000 XMR** (Monero) for **0.00004800 BTC** (Bitcoin)

You will connect to peer

```
026b9739e4610c2a7e8d585b5a9b81e243a7baabfacae421e47e7b038665ffebb1@159.100.242.14:18750
```

Timelocks: cancel **30**, punish **35**.
Fee: **Fixed: 1 satoshi/vByte** (for Bitcoin Testnet txs).

Public offer:

```
Offer:Cke4ftrP5A71LQM2fvVdFMNR4gzxVVJwZ11111uMFrPX4RGd6d7R9U111111TBL5Rh113GTvtvqfD1111112g5B7JzmMsrQ1
```

Architecture

- Broadly: Rust microservices communicating over ZeroMQ message busses
- Services are isolated by function, e.g.
  - Swap state machines
  - Cryptography module
  - Database
  - etc.
- Swaps can be managed by a command line application

Current State

- Pushing for mainnet release soon™
  - seriously expect a mainnet release within 1-2 months
- Ensure users can recover funds no matter what
  - Learning from competitors and early lightning network
- API is nearly complete, GUI development will commence in a few weeks

Future Challenges

- Free Option problem -> Bitcoin has to lock first
  - Up front cost to reputable counterparty
  - Delay puzzles and proof of ownership
  - Reputation networks
  - Monero transaction chaining?
- More assets!