

Atomic swaps

crypto251.0 Cryptocurrency and the Smileycoin

Gunnar Stefansson (editor)

November 29, 2020

Background

- There is a considerable demand for exchanging coins
- This is mostly done on cryptocurrency exchanges
- An exchange is a **honeypot** and hacks are common
- Some exchanges are now **decentralised**

In a truly decentralised exchange the exchange should not hold any user funds: The transaction should be solely between users

The atomic swap is an important concept

Atomic swaps need timeout mechanisms to replace trust

timeouts

A timeout on a transaction implies that it can not be transmitted before the time limit
A timeout on a UTXO implies that it can not be spent before the time limit

CLTV is `OP_CHECKLOCKTIMEVERIFY`

See Handout and Example for more detail

an atomic swap algorithm

by TierNolan
(see Handout)

Alternatives

Several decentralised exchanges (DEXs) exist, but the definition of a DEX is not clear

Examples:

Barterdex: <https://komodoplatfrom.com/decentralized-exchange/>

Bit Square (bisq): <https://bisq.network/>

etc

Further reading on atomic swaps etc:

Vitalin Buterik: <https://static1.squarespace.com/static/55f73743e4>

Kyle Samani: <https://www.coindesk.com/opportunity-interoperable>

Adrian Mathieu/Viacoin: <https://ethereumworldnews.com/viacoin-dev>

The missing link: Information flow

Recall the process:

- A creates TX1: “Pay w BTC to $\langle B$'s public key \rangle if (x for $H(x)$ known and signed by B) or (signed by A and B)”
- B creates TX3: “Pay v alt-coins to $\langle A$ -public-key \rangle if (x for $H(x)$ known and signed by A) or (signed by A and B)”

So **before any exchange is set up**,

- A needs to know that B wants to buy w BTC
- B needs to know that A will sell for v alt-coins

Then, to be able to **start the exchange**

- A needs to know B's BTC public key
- B needs to know A's alt-coin public key

This information exchange needs to be done outside the transactions, as an MoU or “announcement(s) of intent”. The info exchange does NOT need to be binding. The info exchange should cost something to avoid

Announcing the atomic swap

- Use a forum (telegram etc)?
- Use a specialised channel (BarterDex/Bisq)?
- Use an existing coin (mempool)?
- Alice should in principle be able to use the Smileycoin blockchain to announce
 - *SELL 1000 SMLY for 1 LTC*
- and Bob could accept the offer by responding
 - *ACCEPT offer TxId'*
- etc.

Could be done through modifications of smileycoin-qt

A draft proposal: <https://tutor-web.info/news-1/announcing-intent>

Dedicated wallets? <https://atomicwallet.io/> (or scam?)


Atomic swaps between chains: Litecoin and Bitcoin

One of the first ones: <https://twitter.com/SatoshiLite/status/911328>



Following

Did a cross-chain atomic swap with LTC/BTC! 😊
10 LTC for 0.1137 BTC with @JStefanop1.

 [insight.litecore.io/address/ML9CNJ ...](https://insight.litecore.io/address/ML9CNJ...)
[insight.bitpay.com/address/3HRWsf ...](https://insight.bitpay.com/address/3HRWsf...)



1:36 PM - 22 Sep 2017

1,209 Retweets 3,156 Likes



10 LTC for 0.1137 BTC

The Litecoin side: <https://insight.litecore.io/address/ML9CNJBtSPM>

The Bitcoin side: <https://insight.bitpay.com/address/3HRWsfjpbHiJ>

See also <https://github.com/topics/atomic-swap> for many, many atomic swap projects.

Copyright 2020, Gunnar Stefansson (editor)

This work is licensed under the Creative Commons Attribution-ShareAlike License. To view a copy of this license, visit

<http://creativecommons.org/licenses/by-sa/1.0/> or send a letter to

Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.