Atomic Swaps

No Author Given

No Institute Given

Abstract.

1 Introduction

1.1 The Evolution of Atomic Swaps[1]:

Atomic swaps enables trade across blockchains safely and quickly. This idea is being discussed since 2013. Atomic means that if the swap is not successful neither part loses anything. In other words, the swaps is either executed or not. Atomic swaps can be on-chain or off-chain. Off-chain swaps are instant, private and they require almost zero-fee. Both type of swaps utilize hashed-time-locked-contracts (HTLCs). This guarantees that a party can't take any funds before it offers its own.

Decred is the **first on-chain atomic swap** [2]. One challenge to be overcome in Decred is that new blocks should be mined to show the change of ownership (it makes the system slower).

The first on-chain EthereumBitcoin atomic swap is realized by Altcoin.io. Swaps take 2-3 mins.

The first off-chain atomic swap over the lightning network is realized by Lightning Labs. Lightning network enables the exchange of coins, off-chain. It creates payment channels. After the transaction is completed, the chains are updated and the channels are closed. It is scalable.

Their next goal: atomically swap any token for any other token, regardless of the blockchain it resides on.

1.2 Atomic Swap of ERC20 Tokens on the Raiden Network [3]:

Raiden Network is similar to Bitcoins Lightning Network, but for Ethereums blockchain. It will enable instant, low-fee and scalable micro payments of ERC20 compliant tokens.

Problem in decentralised exchanges: sacrificing transaction speed for settlement on-chain.

1.3 Republic Protocol [4]:

Republic: a decentralized open-source dark pool protocol facilitating atomic swaps between cryptocurrency pairs across the Bitcoin and Ethereum blockchains.

Trades are on a hidden orderbook and the matching is done using secure multiparty computation. It is a secure, decentralized, scalable dark pool protocol capable of handling billions in trading volume daily. It facilitates the exchange of Ethereum, ERC20 and Bitcoin cryptocurrencies through a decentralized dark pool.

execution without exposing price and volume no trusted intermediary to operate a dark pool (dark pool = private exchanges where financial assets and instruments are traded and matched by an engine running on a hidden order book)

2 Our Implementation

- ETH to ERC20 token atomic swap is implemented.
- ERC20 to ERC20 token atomic swap is implemented.
- One contract can perform several swaps. Each swap is assigned a swapID.
- Each swap has three states: OPEN, CLOSED or EXPIRED.

References

1. "The Evolution of Atomic Swaps," https://blog.altcoin.io/the-evolution-of-atomic-swaps-e33ad3af8818, 2017.
2. "Decred cross-chain atomic swapping," https://github.com/decred/atomicswap, 2017.
3. "Atomic Swap of ERC20 Tokens on the Raiden Network," https://medium.com/@dopetard/atomic-swap-of-erc20-tokens-on-the-raiden-network-a9890c4957d7.
4. T. Zhang and L. Wang, "Republic protocol," 2017.