Atomic Swaps

No Author Given

No Institute Given

Abstract.

1 Introduction

An atomic swap enables involving parties to exchange cryptocurrencies, tokens on or off-chain without the involvement of a third party. Atomicity guarantees that either both sides of the swap happen, or neither. The risk of one party losing their assets is minimized. The concept of atomic swaps, which provides safe and quick trades, is being discussed since 2013[1]. Atomic swaps can be on-chain or off-chain. Off-chain swaps are instant, private and they almost doesn't incur any fees. Both type of swaps utilize hashed-time-locked-contracts (HTLCs) to guarantee that a party can't take any funds before providing his fund.

2 Related Work

Decred realized **the first on-chain atomic swap** between Decred and Litecoin [2]. The need to mine new blocks to show the change of ownership can make the Decred's system slower. **The first on-chain Ethereum-Bitcoin atomic swap** is realized by Altcoin.io(REF!!). Lightning Labs performed **the first off-chain atomic swap** over the lightning network. Lightning network enables the off-chain exchange of coins by creating payment channels between the trading parties. After the transaction is completed, the chains are updated and the channels are closed. Lightning network enables fast and scalable transactions and the involving parties don't have to pay transaction fees for every transaction.

Ethereum's Raiden Network is analogous to Bitcoin's Lightning Network and it provides instant, low-fee and scalable exchanges [3]. The atomic swap of ERC20 tokens are performed on Raiden network.Zhang et al. propose Republic Protocol, which is a decentralized open-source dark pool protocol that provides atomic swaps of cryptocurrencies across Bitcoin and Ethereum blockchains [4].Their proposed system enables the exchange of Ether, ERC20 and Bitcoin over a decentralized dark pool. In an atomic cross-chain swap setting, involving parties perform exchange across different blockchains like exchanging Bitcoin for Ether. In [5], a cross-chain swap is modeled as a directed graph where vertices correspond to the parties in the protocol and the arcs represent the transfers between them.

3 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.

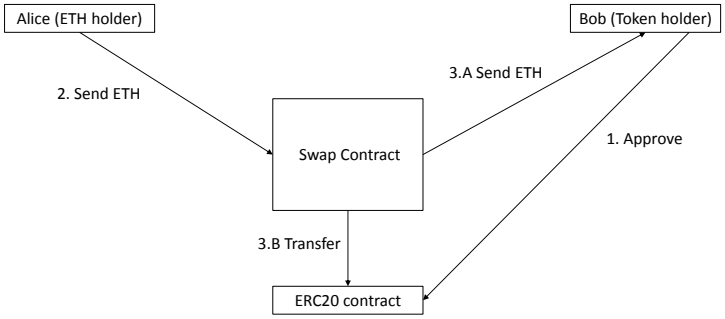

Fig. 1: approve

4 Comparison of Token Standards

4.1 ERC721

non-fungible, ERC20 compatible

4.2 ERC223

ERC20 has the problem of "non-recovarable" coins ERC20 needs to execute two functions to transfer coins: approve and transferFrom. ERC223 consumes half the amount of gas than the amount needed to transfer an ERC20 token. ERC223 offers 3 improvements:

- no lost tokens
- reject non-supported tokens
- energy saving

tokenFallback: the receiving contract has a chance to do some work.

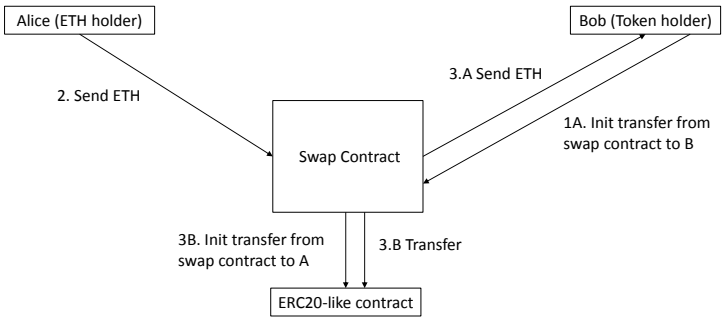

Fig. 2: without approve

4.3 ERC777

TO-DO:

- explain how we count transactions and the difference between margin and fixed transactions
- introduce more settings in the table

5 Atomic swaps with different settings

maker	taker	class	order transactions (margin)	account (onetime) transactions (fixed)
ERC20	ETH	approve	2	3
ERC20	ERC20	approve	3	4
ERC20-like	ETH	w/o approve		
ERC20-like	ERC20-like	w/o approve		
ERC223	ETH			
ERC20	ETH	collateralized		
ERC20	ETH	partially collateralized		
ERC20	ERC223			

Table 1: swaps

ERC20 to ETH: Somebody sets up the swap. Token holder calls approve on the ERC20 contract with the swap contract as the target/allowance holder/spender. The holder of the ETH calls a settle function, sending their ETH

along with it. This triggers the swap and the swap contract calls transferFrom on the ERC20 contract, transferring the tokens from the token holder to the ETH holder. The swap contract at this stage also sends the ETH to the token holder. The atomic swap is now complete. Hence, approving on the ERC20 contract and calling the settle function are counted as the order transactions. When the one-time transactions are also considered, deploying the swap contract should also be counted, which in total makes 4 transactions. We assume that the token contract already exists.

ERC20 to ERC20: For the order transactions, we have 3 in total as the other token holder should also approve the amount of tokens to be spent.

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.
5. M. Herlihy, "Atomic cross-chain swaps," *arXiv preprint arXiv:1801.09515*, 2018.