Mechanism for Exchanging Cryptocurrency and ERC20 Tokens

0v1se

November 5, 2017

This paper explains a mechanism for exchanging ERC20 [1] tokens issued through the Ethereum [3] network for other cryptocurrencies (btc, ltc, etc).

1 Problem

There needs to be a method of exchanging ERC20 tokens issued on Ethereum platform for cryptocurrencies other than Ether. This is particularly important for Initial Coin Offerings (ICO) [4], when the issuer of the token wants to accept Bitcoins as payment for issued tokens or any other coins besides Ether.

2 Concepts and Definitions

1. α - coin from an arbitrary blockchain (other than Ethereum blockchain) for exchange
2. $\widehat{\alpha}$ - an ERC223 [2] token issued on the Ethereum platform, representing same value as α
3. τ - the ERC20 token issued on the Ethereum platform for exchange on coin α
4. A - the owner of coin α
5. B - owner of the τ tokens

3 Solution

For the exchange to work, the Service must occur outside of any blockchain. The Service must also be integrated with the cryptocurrencies blockchains to be exchanged. In order

to carry out the exchange, the Service issues a special $\widehat{\alpha}$ token through the Ethereum platform, which represents the cryptocurrency α involved in the exchange. The System guarantees it will exchange cryptocurrency α to an equal volume of $\widehat{\alpha}$ tokens for all owners of $\widehat{\alpha}$ tokens in response to a corresponding request to the System.

Thus, the System functions:

1. As a generator of tokens to balance blockchain currencies
2. As a temporary depository of the cryptocurrencies participating in the exchange

4 The Process

The exchange occurs in the following order:

1. B requests a temporary wallet from the Service, and informs A
2. A requests a transfer of an amount of α to the temporary wallet
3. The System receives notification of the transfer and releases a corresponding and equal number $\widehat{\alpha}$ tokens to the α coins received.
4. The System transfers the released $\widehat{\alpha}$ tokens to B wallet.
5. B independently calculates the amount of τ tokens that correspond to the $\widehat{\alpha}$ tokens, and transfers that volume to A wallet.
6. B transfers the $\widehat{\alpha}$ tokens to the System's purse, after which the System transfers the α coins to B wallet.

5 Security

As ERC223 tokens are used for the exchange, all accounting data is automatically placed under safe storage in the Ethereum blockchain. The System's bottleneck is the temporary storage of cryptocurrency. The risk of compromisation is offset by the short stay of the cryptocurrency in storage. As the period the cryptocurrency is in storage is limited to the time necessary for the exchange operation, large sums do not accumulate in storage, thus making labor costs for hacking inefficient.

References

[1] *ERC20 Token Standard*. URL: `https://theethereum.wiki/w/index.php/ERC20_Token_Standard`.

[2] *ERC223 Token Standard*. URL: https://github.com/ethereum/EIPs/issues/223.
[3] *Ethereum Project*. URL: https://ethereum.org.
[4] *Initial Coin Offering*. URL: https://en.wikipedia.org/wiki/Initial_coin_offering.