Wrapped Ocvcoin

security@ocvcoin.com

ocvcoin.com

github.com/ocvcoin/Wrapped-Ocvcoin

Abstract: In the current era of widespread usage of cryptocurrencies, an increasing number of cryptocurrency exchanges have been established. However, these platforms tend to be selective in their listings, often prioritizing only high-volume cryptocurrencies while disregarding new ones. To address this issue, decentralized exchanges have emerged as a viable solution. This has led to the development of Wrapped Ocvcoin, which functions as an exact equivalent to the native Ocvcoin and is nearly lossless in terms of interchangeability. The network utilized for Wrapped Ocvcoin is Binance Smart Chain, which boasts notably low gas prices, though alternative options can be considered and implemented as necessary.

Contract Design

The Wrapped Ocvcoin contract adheres to the widely recognized EIP-20 Token Standard and has been designed using Secure OpenZeppelin ready-made contract code. Minimal modifications have been made to the code, with the sole addition of a small function (multiMint) intended to facilitate cost-effective, bulk token transfers without compromising security. The contract is also equipped with support for EIP-3156 Flash Loans and EIP-2612 permit. Notably, functions deemed unsuitable for the cryptocurrency realm, such as the "pause" function, have been omitted from the contract design.

Native Coin -> Wrapped Token Conversion

For this conversion, the cross transfer service (bridge.ocvcoin.com) requests client's wallet address. The service creates an address using the following formula:

```
createmultisig 2 ["public key 1","public key 2"] legacy
```

public key 1 is created with our private key

public key 2 is created with the client's wallet address

(public key 2's private key: "00000000000000000000000000" + "client's wallet address without 0x prefix")

(all public keys are compressed)

Wrapped Token -> Native Coin Conversion

For this conversion, the cross transfer service (bridge.ocvcoin.com) requests client's native wallet address. The service creates an address using the following formula:

"0x" + ripemd160("client's native wallet address")

The implication of this is that tokens that are sent to the said address will be permanently locked and burned. As the address is not a legitimate one, any tokens sent there will remain inaccessible indefinitely. Hence, the information displayed under "Total Supply" on explorer sites can be erroneous. To obtain an accurate representation of the tokens in circulation, it is necessary to examine the balance of the reserve account on the native Ocvcoin platform.

Transparency

Transparency constitutes one of the foremost priorities, where the release of free tokens into the network shall be deemed unacceptable. As such, each address generated via bridge.ocvcoin.com will be readily accessible to the relevant discord channel, thereby empowering the community to exercise adequate oversight.

Security

One of the most pressing issues is security. To ensure utmost protection, private keys are stored on a device that is not connected to the internet. In addition, automation software exclusively operates on a device with no internet access and will continue to do so.