HighTechBlock

Smart Contract Security Review

Introduction

This document summarizes HighTechBlock's opinion on: a) IvyKoinContract.sol smart contract; b) whitelisting process; c) fund management & key storage.

The smart contract review is based on the analysis of the revisions made to the suggestions made to the IvyKoinContract.sol file sent on March 28th, 2018, having a SHA-256 fingerprint of "ecffd1747d3379aa336cf2dc80ef15687a2e4f147fd55cd3a64b94f4772017c0"

Limitations: Smart contract security reviews cannot cover all existing vulnerabilities. There is no guarantee that the smart contracts will be secure in the future. This analysis excludes any express or implied warranties and is purely an opinion on the items analyzed above.

Executive Summary

Smart contract review

We reviewed the IvyKoin smart contract and found 0 critical, 0 important, 0 medium and 1 low severity issues, in regards to upgrading to ERC223 from ERC20. Main benefits and improvements are:

1) Eliminates problem of lost tokens. This happens when users mistakenly use a contract instead of a wallet address when transferring tokens. This leads to tokens being lost. ERC223 allows users to send their tokens to either a wallet or contract.
2) Allows developers to handle incoming token transfers, and reject non-supported tokens
3) Energy savings. Transfer of ERC223 tokens to a contract is a one step process, instead of a 2 step for ERC20. This leads to less gas required for the operation.
4) Additional public functions such as symbol(), name(), decimals(), totalSupply() increase transparency and ease of retrieving these commonly used variables.

Tested known vulnerabilities

1) The methods of StandardToken use the proper protection mechanisms to protect against the short address size attack of ERC20.

2) Usage of SafeMath library and operations.

3) No usage of transaction origin in the contract.

4) No reliance on block timestamps.

5) Proper usage of checks-effects-interactions pattern.

6) Proper usage of function visibility modifiers.

7) Proper handling of fallback functions.

8) Proper protection against reentrancy attacks.

Limitations

Only the Solidity source code of the smart contract was reviewed. The usage, migration, and deployment of the smart contract can also affect the crowdsale.

Whitelisting process review

Moderate

#1 No whitelisting process

There was no whitelisting process through the smart contracts. Instead, it was conducted primarily to sophisticated & institutional investors, through Discovery Capital.

Fund management & private key storage review

The fund management process consisted of the following steps:

1) Funds were collected directly to the Discovery Capital (DC) wallets.
2) Discovery Capital kept an internal ledger of the contributors and amounts contributed. The process of creating and maintaining this ledger was not reviewed by HTB.
3) DC would communicate to IvyKoin the amount of coins to be minted.

4) Once deployed, the IvyKoinContract would create the exact number of coins and assign all of them to the hardcoded DC treasury wallet address.
5) DC would use a series of "allocators" to load balance the assignment of tokens to based on the internal ledger that was created.

The internal process used by Discovery Capital was not analyzed by HTB, focusing instead on the overall approach and integration with DC.