STO Coin Audit

by MonteLabs

June 13, 2018

1 Introduction

This document is a report representing the security audit conducted on the STO Coin smart contract, and discusses potential issues that we found while analysing and testing the code.

The code was written by Validity Labs, the SHA3-256 of the StoToken.sol is 126050cd5e9f6f36615f2a5dc5d3260d43f682add9c44076536fbdde0940afed. Figure 1 shows the inheritance relations between the used smart contract, where the red nodes are external libraries and the green node is the newly implemented smart contract, object of this audit.

The inherited contracts use OpenZeppelin smart contract libraries which are considered standard and have been heavily audited and used by the community in general.

The code can be summarized as a ERC827 token with a pausable feature. There are one million token units, with 18 decimal units. At creation time all coins are issued to a specified account.

Section 2.1 lists the issues found during this audit. No major vulnerabilities were found, and we list minor suggestions. Section 3 presents our concluding thoughts on the audit.

2 Issues

2.1 Suggestions

Some OpenZeppelin contracts hashes are not checked.

The `hashChecker` tool does not check the hash for some of the used OpenZeppelin contracts `ERC827Token` and `ERC827` We suggest this to be checked.

Solidity version.

Solidity's latest version is 0.4.24, but 0.4.21 is used. We suggest the use of laters versions since they contain new features and bugfixes, and the OpenZeppelin smart contracts are already using version 0.4.23.

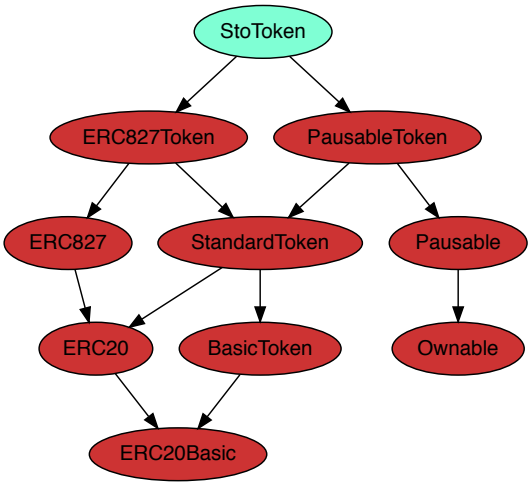

Figure 1: Inheritance relationship between the smart contracts.

3 Conclusion

We have found no security vulnerabilities in the STO Coin smart contract, and provide minor improvement suggestions.

This document is stored on IPFS as a security evidence. This audit also implies that MonteLabs issues an on-chain audit verification seal that can be accessed directly via the smart contract or at montelabs.com/audits as soon as the contracts are deployed, where all the security evidences can be fetched.