Domus Coin Contract: Final Review

Mikhail Vladimirov and Dmitry Khovratovich

27th March, 2018

This document describes issues found in DomusCoin contract system during code review performed by ABDK Consulting.

1. Introduction

We were asked to review the DomusCoin Contract from the link. We got additional documentation on the contract from the whitepaper. We found quite many issues, and all of them were resolved over the long discussion with the DomusCoin project leaders and contract developers. In the final report we analyze the state of contracts in the commit 79682.

2. DomusCoins

Several major issues were identified, primarily to the use of Oraclize, but they all have been fixed.

2.1 EIP-20 Compliance Issues

The code permits small deviation of declared total supply from the actual one, but with current constants there is no such problem.

2.2 Documentation Issues

All documentation issues were fixed.

2.3 Readability Issues

All documentation issues were fixed.

2.4 Unclear Behavior

There were places, where the contract behavior is unclear: the business logic might be violated here, but the documentation and functional requirements are not sufficiently documented to make a clear decision. All such issues were fixed

2.6 Suboptimal Code

All suboptimal code patterns found in the smart contract were fixed.

2.7 Major Flaws

There were major flaws related to elusive ICO addresses, dividend functionality, and internal sold token counting. They were all fixed.

2.8 Moderate Flaws

There were moderate flaws related to the rounding errors and dividends. They were all fixed.

2.9 Other Issues

The fallback function consumes more than 2300 gas, which is common for crowdsale contracts but formally violates Solidity guidelines.