Coinspect Source Code Review 3

Prepared for Krypton Capital • October 2017

V1.0

1. Table of Contents

2. Executive Summary

In October 2017, Krypton Capital engaged Coinspect to perform a first security audit of the Jury token contract created on October 18th, 2017. The contract was audited and 3 minor issues were found. These issues were corrected in October 19th. A second audit was conducted on the corrected version on October 20th and no additional issues were found. The token contract was improved again on October 20th and a third audit was performed on the same date.

The audited source code corresponds is the commit:
F8ee19034ed459f023474cc3e2609f12e177a55e
Repository: https://github.com/juryonline/contracts

The objective of each audit was to evaluate the security of the token smart contract implementation. During this third assessment, Coinspect did not identified any issues.

3. Introduction

The contract “JOT.sol” is an ERC-20 token contract with the feature of minting and multi-minting by an authorized owner. A whitebox security audit was conducted on these smart contracts.

The following checks, related to best practices, were performed:

- Confusion of the different method calling possibilities: send(), transfer(), and call.value()

- Missing error handling of external calls
- Erroneous control flow assumptions after external calls
- The use of push over pull for external calls
- Lack of enforcement of invariants with assert() and require()
- Rounding errors in integer division
- Fallback functions with higher gas limit than 2300
- Functions and state variables without explicitly visibility
- Missing pragmas to for compiler version
- Race conditions, such as contract Reentrancy
- Transaction front running
- Timestamp dependence
- Integer overflow and underflow
- Code blocks that consumes a non-constant amount of gas, that grows over block gas limit.
- Denial of Service attacks
- Suspicious code or underhanded code.
- Non-standard implementations of standardized EIPs

The present report was completed on October 20th, 2017, by Coinspect. The report includes all issues identified in the second audit.

4. Findings

No issues were found in the second audit.

5. Closing Remarks

It has been a pleasure to work with Krypton.Capital. The issues reported in the first audit were corrected promptly. We believe the last release of the token contract is free from defects. The scope of the present security audit is limited to smart contract code. It does not cover the technologies and designs related to these smart contracts, nor the frameworks and wallets that communicate with the contracts, nor the operational security of the company that created and will deploy the audited contracts. This document should not be read as investment or legal advice.