SmartDec

DSG Smart Contracts Security Analysis

This report is public.

Published: March 10, 2019

In this report, we consider the security of the Decentralization Smart Games (DSG) project. Our task is to find and describe security issues in the smart contracts of the platform.

Disclaimer

The audit does not give any warranties on the security of the code. One audit cannot be considered enough. We always recommend proceeding with several independent audits and a public bug bounty program to ensure the security of smart contracts. Besides, security audit is not an investment advice.

Project description

In our analysis, we consider DSG smart contracts code (“code.sol”, sha1sum 2522b681c47879f2b3cbd701a226a2415d631253).

Summary

In this report, we considered the security of DSG smart contracts. The contracts code is of medium code quality. The audit has shown no issues that endanger project security. However, we recommend implementing tests.

Checklist

Security

The audit showed no vulnerabilities.
Here by vulnerabilities we mean security issues that can be exploited by an external attacker. This does not include low severity issues, documentation mismatches, and some other kinds of bugs.

Safe arithmetics

Token smart contract is secure from arithmetics issues.

ERC20 compliance

We checked ERC20 compliance during the audit. The audit has shown that **DSG** token is fully ERC20 compliant.

ERC20 MUST

The audit showed ERC20 “MUST” requirements violations.

ERC20 SHOULD

The audit showed ERC20 “SHOULD” requirements violations.

Tests

The audit showed that the code is not covered with tests.

Owners' powers

We found that the owners have the following permissions:

- They can manage ETH funds from charity pool (line 391):

```
function charitytWithdraw(address recipient) onlyOwners
check0x(recipient) public
```

  There is balance that is used for charity.

- They can manage ETH funds from development pool (line 397):

```
function developmentWithdraw(address recipient) onlyOwners
check0x(recipient) public
```

  There is balance that is used to support the project and games development.

- They can appoint new owners (line 379):

```
function transferOwnership(address candidate, uint8 k)
check0x(candidate) onlyOwners public
```

- They can add a new address of the game contract (line 319):

```
function setGame(address gameAddress, bool active) onlyOwners
public returns(bool){
```

This analysis was performed by SmartDec.

Boris Nikashin, Project Manager
Alexander Drygin, Analyst

March 10, 2019