Audit of the SMV projects
Executive Summary

By OCamlPro
Contact: @fabrice_dune

August 20, 2021

1 Introduction

This set of documents is a submission for the 14th contest of the Formal Methods sub-governance, called "Contest Proposal: SMV Smart Contract Informal Audit Respin".

The projects to be audited were:

- DENS-SMV Project, at `https://github.com/RSquad/dens-smv` at branch master with hash code equal to fbdfe4bca3c372b02cacf9788b4ad37112d0da2c
- BFTG Project (SMV part only) at `https://github.com/RSquad/BFTG` (SMV part only) at branch master with hash code equal to 7c6ec7d811bcc1f228a3499ab19f6d20652ca94b

The contest ended at Aug 20, 2021, 23:59:59 UTC.
This submission includes 3 documents:

- This executive summary
- A detailed audit report for DENS-SMV project
- A detailed audit report for BFTG project

Both detailed reports start with an index of major and critical issues, with hyper-links to detailed explanations.

2 Methodology

The methodology used for this audit is the following:

1. Process all solidity files through an analyzer to generate a document with the code source ready for annotations
2. Read all the code source in the document, reporting any issue found in the code. For some issues, test whether the issue can happen on the testnet.

3. Following requests from jurors from previous audits, remove all functions without any interesting comments.

Issues are sorted into 3 kinds:

- Critical issues: these issues could be used by a malicious user to steal tokens, or change the behavior of the service, making its results useless
- Major issues: these issues can degrade the quality of the service
- Minor issues: these issues have no real impact on the service, but could improve its development (for example, remarks on coding style, etc.)

We submitted some of the major and critical issues to the development team (Roman @inyellowbus), but got no returns.

We audited all the contracts of the 2 projects, though only the SMV part of the BFTG project was required to be audited.

3 Results

3.1 DENS-SMV Project

We reported 5 critical issues, and 3 major issues in this project (see the Table of Major and Critical Issues in the second page of the corresponding report, with hyperlinks to the issues)

3.2 BFTG Project

We reported 15 critical issues, and 8 major issues in this project (see the Table of Major and Critical Issues in the second page of the corresponding report, with hyperlinks to the issues)