Gnosis Chain SBC Withdrawals Smart Contracts Redesign Review

By: ChainSafe Systems

July 2023

Gnosis Chain SBC Withdrawals Smart Contracts Redesign Review

Auditors: Tanya Bushenyova, Anderson Lee, Oleksii Matiiasevych

WARRANTY

This Code Review is provided on an “as is” basis, without warranty of any kind, express or implied. It is not intended to provide legal advice, and any information, assessments, summaries, or recommendations are provided only for convenience (each, and collectively a “recommendation”). Recommendations are not intended to be comprehensive or applicable in all situations. ChainSafe Systems does not guarantee that the Code Review will identify all instances of security vulnerabilities or other related issues.

Introduction

Gnosis Chain requested ChainSafe Systems to perform a review of the contracts used for SBC (Stake Beacon Chain) deposit and withdrawal. The contracts in scope can be identified as the following git commit hash:

```
961df1be316f472b55960a785a7696c7aa02f18a
```

Gnosis Chain has the following contracts in scope:

```
SBCWrapper.sol (unwrap() function)
SBCDepositContract.sol (diff since
63d522e40dfaacde5f00891ca45c86ad474e6184)
```

After the initial review, Gnosis Chain team applied a number of updates which can be identified by the following git commit hash:

```
24f9fcfdff4ef04fd47d459aaa88741c66c5dba4
```

Additional verification was performed after that.

Disclaimer

The review makes no statements or warranties about the utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about the fitness of the contracts for any specific purpose, or their bug free status.

Executive Summary

There are no known compiler bugs for the specified compiler version (0.8.9), that might affect the contracts' logic.

There were no critical, major or minor issues found. 2 informational/optimizational issues were identified in the contracts. Redesign resulted in a simpler implementation eliminating the possibility of side effects and external calls.

Critical Bugs and Vulnerabilities

No critical bugs or vulnerabilities were identified in the contracts.

Line by Line Review. Fixed Issues

1. SBCDepositContract, line 260. Note, the `executeSystemWithdrawls()` function has an outdated description in the comments section, left from a previous implementation.

Line by Line Review. Acknowledged Findings.

1. SBCDepositContract, line 283. Optimization, the `executeSystemWithdrawls()` function reads `_amounts.length` from calldata multiple times, it would be cheaper to store it in a local variable.

Anderson Lee

Tanya Bushenyova

Oleksii Matiiasevych