SOLIDIFIED

Audit Report for Hop Protocol - June 25, 2021

Summary

Audit Report prepared by Solidified covering two updates to the Hop Protocol smart contracts.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code below. The debrief took place on June 25, 2021, and the results are presented here.

Audited Files

The updates audited have been supplied in two GitHub commits:

https://github.com/hop-protocol/contracts/commit/3d5ce6423c2bd492cbabf41c08e7e7439376b15a

https://github.com/hop-protocol/contracts/commit/0bd6a39d5f6023abdd49ef155425bb528194cb16

Intended Behavior

The first update substitutes the OpenZeppelin merkle tree implementation in the verification code with the same library already used for constructing merkle trees in codebase.

The second update fixes an issue in which the chainBalnce variable was not incremented on the destination L2 chain when sending a TransferRoots across.

Code Complexity and Test Coverage

Smart contract audits are an important step to improve the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of a smart contract system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**.

Note, that high complexity or lower test coverage does equate to a higher risk. Certain bugs are more easily detected in unit testing than a security audit and vice versa. It is, therefore, more likely that undetected issues remain if the test coverage is low or non-existent.

Criteria	Status	Comment
Code complexity	Medium	-
Code readability and clarity	High	-
Level of Documentation	Medium-High	-
Test Coverage	Medium-High	-

Audit Report for Hop Protocol - June 25, 2021

Issues Found

Solidified found that the Hop protocol updates contain no issues.

Audit Report for Hop Protocol - June 25, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Authereum / Hop Protocol or its products. This audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

Solidified Technologies Inc.