Summary

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

Process and Delivery

Three (3) independent Solidified experts performed an unbiased and isolated audit of the code below. The debrief took place on March 22, 2021, and the results are presented here.

An extension audit widening the scope was concluded on May 05, 2021.

Audited Files

The source code has been supplied in the form of a GitHub repository:

https://github.com/hop-exchange/contracts

Commit number covered by this report: `74a828a33d77a92cd69e93b8b807e4448894b39c`

The scope of the audit was limited to the following files:

```
contracts
├── admin
│   └── Timelock.sol
├── bridges
│   ├── Accounting.sol
│   ├── Bridge.sol
│   ├── HopBridgeToken.sol
│   ├── L1_Bridge.sol
│   ├── L1_ERC20_Bridge.sol
│   ├── L1_ETH_Bridge.sol
│   ├── L2_Bridge.sol
│   ├── L2_OptimismBridge.sol
│   ├── L2_UniswapWrapper.sol
│   ├── L2_AmmWrapper.sol
│   ├── L2_PolygonBridge.sol
│   ├── L2_PolygonMessengerProxy.sol
│   └── L2_XDaiBridge.sol
├── interfaces
│   ├── IMessengerWrapper.sol
│   ├── IWETH.sol
│   ├── arbitrum
│   │   └── messengers
│   │       ├── IArbSys.sol
│   │       ├── IBridge.sol
│   │       ├── IGlobalInbox.sol
│   │       ├── IInbox.sol
│   │       ├── IMessageProvider.sol
│   │       └── IOutbox.sol
│   ├── optimism
│   │   └── messengers
│   │       ├── iOVM_BaseCrossDomainMessenger.sol
│   │       ├── iOVM_L1CrossDomainMessenger.sol
│   │       └── iOVM_L2CrossDomainMessenger.sol
│   └── xDai
│       └── messengers
│           └── iArbitraryMessageBridge.sol
├── libraries
│   └── MerkleUtils.sol
└── wrappers
    ├── MessengerWrapper.sol
    ├── OptimismMessengerWrapper.sol
    ├── PolygonWrapper.sol
    └── XDaiMessengerWrapper.sol
```

Intended Behavior

The smart contracts implement a protocol that allows users to move funds between different L2 solutions and between L1 and L2, without users having to wait for the L2 exit period for each cross-layer transaction.

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	-

Test coverage report:

```
------------------------------------|----------|----------|----------|----------|----------------|
File                                |  % Stmts | % Branch |  % Funcs |  % Lines |Uncovered Lines |
------------------------------------|----------|----------|----------|----------|----------------|
 admin/                             |        0 |        0 |        0 |        0 |                |
  Timelock.sol                      |        0 |        0 |        0 |        0 |... 287,289,294 |
 bridges/                           |    94.46 |    73.08 |    92.63 |    93.98 |                |
  Accounting.sol                    |      100 |      100 |      100 |      100 |                |
  Bridge.sol                        |      100 |    77.27 |    94.12 |    96.77 |        116,117 |
  HopBridgeToken.sol                |      100 |      100 |      100 |      100 |                |
  L1_Bridge.sol                     |      100 |    97.73 |      100 |      100 |                |
  L1_ERC20_Bridge.sol               |      100 |      100 |      100 |      100 |                |
  L1_ETH_Bridge.sol                 |        0 |        0 |        0 |        0 |       16,17,21 |
  L2_Bridge.sol                     |      100 |       65 |      100 |      100 |                |
  L2_OptimismBridge.sol             |      100 |      100 |      100 |      100 |                |
  L2_UniswapWrapper.sol             |    82.35 |       40 |      100 |    82.35 |... 1,88,98,104 |
  L2_XDaiBridge.sol                 |        0 |        0 |        0 |        0 |... 46,54,55,59 |
 interfaces/                        |      100 |      100 |      100 |      100 |                |
  IMessengerWrapper.sol             |      100 |      100 |      100 |      100 |                |
  IWETH.sol                         |      100 |      100 |      100 |      100 |                |
 interfaces/arbitrum/messengers/    |      100 |      100 |      100 |      100 |                |
  IArbSys.sol                       |      100 |      100 |      100 |      100 |                |
  IBridge.sol                       |      100 |      100 |      100 |      100 |                |
  IGlobalInbox.sol                  |      100 |      100 |      100 |      100 |                |
  IInbox.sol                        |      100 |      100 |      100 |      100 |                |
  IMessageProvider.sol              |      100 |      100 |      100 |      100 |                |
  IOutbox.sol                       |      100 |      100 |      100 |      100 |                |
 interfaces/optimism/messengers/    |      100 |      100 |      100 |      100 |                |
  iOVM_BaseCrossDomainMessenger.sol |      100 |      100 |      100 |      100 |                |
  iOVM_L1CrossDomainMessenger.sol   |      100 |      100 |      100 |      100 |                |
  iOVM_L2CrossDomainMessenger.sol   |      100 |      100 |      100 |      100 |                |
 interfaces/xDai/messengers/        |      100 |      100 |      100 |      100 |                |
  iArbitraryMessageBridge.sol       |      100 |      100 |      100 |      100 |                |
 libraries/                         |    82.76 |       70 |      100 |    82.76 |                |
  MerkleUtils.sol                   |    82.76 |       70 |      100 |    82.76 | 33,34,35,43,44 |
 wrappers/                          |    44.44 |       25 |    57.14 |    47.37 |                |
  MessengerWrapper.sol              |      100 |       50 |      100 |      100 |                |
  OptimismMessengerWrapper.sol      |      100 |       50 |      100 |      100 |                |
  XDaiMessengerWrapper.sol          |        0 |        0 |        0 |        0 |... 44,53,54,58 |
------------------------------------|----------|----------|----------|----------|----------------|
All files                           |     75.5 |    51.98 |    76.61 |    75.66 |                |
------------------------------------|----------|----------|----------|----------|----------------|
```

Issues Found

Solidified found that the Hop protocol contracts contain 1 critical issue, no major issue, 1 minor issue, in addition to 6 informational notes.

We recommend all issues are amended, while the notes are up to the team's discretion, as they refer to best practices.

Issue #	Description	Severity	Status
1	L1_ETH_Bridge.sol: _transferFromBridge() can be griefed	Critical	Resolved
2	Bridge.sol: timeSlotSize not bounded	Minor	Acknowledged
3	L1_ETH_Bridge.sol: incorrect revert messages	Note	-
5	No reentrancy guards	Note	-
6	Note on the economic model for challenges	Note	-
7	L2_Bridge.sol: l2CanonicalToken not used	Note	-
8	Duplicate SafeMath implementations	Note	-
9	L2_AmmWrapper.sol - should use SafeERC20 to interact with external ERC-20 tokens	Note	-
10	L2_AmmWrapper.sol - does not support ERC-20 tokens which charge transfer fees	Note	-

Critical Issues

1. `L1_ETH_Bridge.sol`: `_transferFromBridge()` can be griefed

The function `_transferFromBridge()` sends ETH out and reverts on failure. This may cause permanent failure of certain kinds of `resolveChallenge()` flows. If the challenger is malicious, for example, the challenger address being a smart contract that reverts on the fallback function unless a variable is set, this flow can be used to ransom bonders and hold their credit hostage.

Recommendation

Consider using a withdrawal pattern.

Major Issues

No major issues have been identified.

Minor Issues

2. `Bridge.sol`: `timeSlotSize` not bounded

The variable `timeSlotSize` can be set to a value that causes the contract to just be unable to execute due to hitting the block gas limit.

Recommendation

Consider using a guard to make sure this cannot happen by accident.

Team Response

We have chosen to make no change. The reason being that this is a governance-controlled parameter and would only be changed with gas costs in mind. If governance is making this change maliciously, that is within our threat model.

Informative Notes

3. L1_ETH_Bridge.sol: incorrect revert messages

The revert message texts in functions `_transferFromBridge()` and `_transferToBridge()` relate to the ERC20 bridge contract.

Recommendation
Adjust the strings to reflect the correct contract.

4. No reentrancy guards

Given that bridge code calls out to messenger interfaces and calls out to token transfer functions which pass the full gas flow, it might be prudent to include reentrancy guards in critical functions just as a precaution, especially if in the future functionality is implemented that allows users to specify custom smart contract execution targets on the cross-layer tx.

Recommendation
Consider using reentrancy protection for critical functions.

5. Note on the economic model for challenges

Depending on the economics of the bonder and how the HOP exchange is used, a 10% deposit to lock up credit for the exit time duration might be too low, or worth it to the challenger to profit in some other way. There's the possibility of blackmailing a bonder if they really need the credit, and asking for ransom otherwise, they will submit a challenge, as well, and even losing 10% might not be enough to dissuade that depending on second-order effects that the bonder might experience by having that credit locked up for long periods of time, especially in the "future" cases where the bonder set is larger or open.

Recommendation
There is no specific recommendation for this beyond suggesting that the economic model could use a curve to calculate the challenger deposit percentage.

6. L2_Bridge.sol: l2CanonicalToken not used

The variable l2CanonicalToken is unused. This may be leftover from a previous version.

Recommendation
Consider removing unused variables.

7. Mixed compiler versions

The codebase uses a number of compiler versions, which may have different behavior.

Recommendation
We recommend locking the whole codebase to a single compiler version.

8. Duplicate SafeMath implementations

The codebase uses OpenZeppelin's version of SafeMath in most places. However, `Timelock.sol` implements its own version.

Recommendation
Consider using a single version of the library.

9. L2_AmmWrapper.sol - should use SafeERC20 to interact with external ERC-20 tokens

The `L2_AmmWrapper.sol` does not use OpenZeppelin `SafeERC20.sol` library to interact with ERC-20 tokens. This is not consistent with the rest of the codebase and might prevent some implementation of ERC20 tokens from being used with `L2_AmmWrapper`

Recommendation
Use OpenZeppelin `SafeERC20.sol` library to interact with ERC-20 tokens

10. `L2_AmmWrapper.sol` - does not support ERC-20 tokens which charge transfer fees

The `L2_AmmWrapper.sol` swaps would fail if used with ERC-20 tokens which charge transfer fees, because the actual amount of tokens received in the contract would be less than specified `amount` parameter for the functions `swapAndSend()` and `attemptSwap()`.

Recommendation

Assess if this limitation is of any importance.

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.