1Inch LimitOrderProtocol Audit

Solidity Compiler Downgrade

September 2021

By CoinFabrik

Introduction

CoinFabrik was asked to audit changes made to contracts for 1Inch's LimitOrderProtocol project. The project was updated to run in the Optimism network and in order to do this, the solidity compiler pragma was modified (downgrading version), together with some of the contracts. In this audit we validated that no issues were introduced with the downgrade. No other threats were considered.

No issues were found during our analysis. Next, we explain the process.

Summary

The contracts audited are from the GitHub repository at https://github.com/1inch/limit-order-protocol/. The audit is based on the commit `9d3ee4b51e3b4108137b8cf84e379c9748193c32` (pull/35).

Contracts

The audited contracts are:

- contracts/LimitOrderProtocol.sol: main functions
- contracts/helpers/AmountCalculator.sol: helper functions calculating maker and taker amounts
- contracts/helpers/PredicateHelper.sol: helper functions for building predicates
- contracts/helpers/ImmutableOwner.sol: modifier
- contracts/helpers/ERC20Proxy.sol: proxy helper
- contracts/helpers/ERC1155Proxy.sol: proxy helper
- contracts/helpers/ERC721Proxy.sol: proxy helper
- contracts/helpers/NonceManager.sol: nonces
- contracts/libraries/ArgumentsDecoder.sol: help decoding arguments
- contracts/libraries/UncheckedAddress.sol: includes calls to (external) token functions,

- contracts/libraries/SilentECDSA.sol: includes calls to (external) token functions
- contracts/interfaces/IEIP1271.sol: interface
- contracts/interfaces/InteractiveMaker.sol: interface

Analyses

For this scope, we went through Solidity's changelog analysing change by change and its potential impact in the code base. In particular, this includes validating that arithmetic operations do not underflow or overflow as safeMath is used everywhere, and sweeping for problems introduced by changes in functions introduced after v0.7.6 (e.g., `chainid()` vs `block.chainid`).

Issues Found by Severity

Critical severity

No issues were found.

Medium severity

No issues were found.

Minor severity

No issues were found.

Security Considerations

When deploying contracts, it is best to use the latest released version of Solidity. The development team has chosen to use the older v.0.7.6, which is the latest of the v.0.7.*, due to unexpected increases in gas cost for the v0.8.* versions.

Conclusion

We found the contracts to be simple and straightforward and have an adequate amount of documentation. The changes introduced were small. No issues were found with the solidity downgrade.