

Summary

Audit report prepared by Solidified for Gnosis covering the 2.0 release of their DutchX (a simultaneous dutch auction based exchange).

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the below contracts. The debrief took place on February 4, 2019 and the final results are presented here.

Audited Files

The following files were covered during the audit:

```
contracts
├── base
│   ├── AuctioneerManaged.sol
│   ├── DxMath.sol
│   ├── DxUpgrade.sol
│   ├── EthOracle.sol
│   ├── SafeTransfer.sol
│   └── TokenWhitelist.sol
├── DutchExchange.sol
├── DutchExchangeHelper.sol
├── DutchExchangeProxy.sol
├── TokenFRT.sol
└── TokenFRTProxy.sol
```

Intended Behavior

This release consists of refactoring and usability improvements to the DutchX, the core behavior of the auctions remains the same. A full specification can be found [here](#).

The audit was based on commit `c9a9bd0d73f96eed65dca5c5a947451adb8e80b6`.

Issues Found

Note

1. When passing token pairs as parameters, could be more gas efficient to pass in canonical order

Functions `setAuctionStart` & `resetAuctionStart` are calling `getTokenOrder` to enforce the expected order of parameters in the following function calls, however since they're internal functions (won't be called directly) could potentially save gas by refactoring them to expect the tokens passed in the canonical order.

Recommendation

Investigate the efficiency of the stated refactor.

Closing Summary

No security issues were discovered in the course of this audit. One informational issue concerning gas efficiency was reported.

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Gnosis or its products. This audit does not provide a security or correctness guarantee of the audited smart contracts. 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.