SOLIDIFIED

Audit Report for Gnosis. February 4, 2019.

Summary

Audit report prepared by Solidified for Gnosis covering a price oracle which sources its prices from the DutchX.

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
 ├──── DutchXPriceOracle.sol
 └──── IDutchX.sol
```

Intended Behavior

This price oracle queries the DutchX for the ending price (in ETH) of n-auctions of a given token in a given range and returns the median.

The audit was based on commit `a4977d9fad444a24d673c7a8b11a5eee67affe29`.

Issues Found

Minor

1. Median returned incorrectly when amount of values to medianize is even

---

When the number of auctions is even, the median will be incorrectly reported: the median when there's an even number of values is the arithmetic mean of the two middle values, but the code currently reports half a price movement higher for an even `numberOfAuctions`, i.e. `priceAt((numberOfAuctions)/2 + 1)`
There is a comment referencing this, but the justification doesn't make much sense to us.

Recommendation
When the amount of values to medianize is even, return the arithmetic mean of the two middle values.

Note

2. Algorithm used to find median is inefficient

In the course of finding the median, a linked list is constructed. Constructing a linked list to find nth largest value of an unsorted array doesn't seem like the most efficient approach, likely want quickselect instead.

Recommendation
Investigate the efficiency of the current approach, and if feasible implement a robust selection algorithm (such as quickselect) in its stead.

Closing Summary

No security vulnerabilities were discovered in the course of this audit. One minor issue concerning an error in the calculation of medians was reported. One informational issue concerning gas efficiency was reported.

Disclaimer