DYAD Audit Report

Reviewed by:

0x52

Reviewed on:

3-17-23

Summary

The DyadStablecoin/contract-v3 repo was reviewed at the following commit:

a31d33588501a190ab3e47c1e8ac0c2f28db572a

Scope

src/core/DNft.sol

src/core/Dyad.sol

Findings

Severity	# of findings
Medium	1

Medium Severity Findings

[M-01] Price feed is hard-coded to 8 dp but oracle is Chainlink aggregator

Summary

The oracle used to price Ethereum is a Chainlink aggregator proxy, meaning that the underlying oracle contract can be upgraded at any time, changing the number of decimals.

Proof of Concept

AggregatorProxy.sol#L355-L360

```
function proposeAggregator(address _aggregator)
  external
  onlyOwner()
{
  proposedAggregator = AggregatorV2V3Interface(_aggregator);
}
```

Aggregator proxy can be updated at any time by owner. This means that the decimals of the aggregator can also change. All price calculations are hard coded for 8 dp and there is no way to change the oracle. The result of this is that a change in decimals would be catastrophic to DNFT.sol.

Lines of Code

DNft.sol#L149

DNft.sol#L195

Recommendation

Use oracle.decimals() in place of 1e8 when calculating price

Review

Fixed in PR #40