DECENTER

Audit report for Wyvern Protocol

DECENTER

1. Summary

Wyvern Protocol has engaged Decenter in the period starting on December 18th and ending on December 28th 2018 to assess and audit their platform's Solidity smart contracts. This document describes the issues discovered during the audit. Decenter's assessment is focused primarily on code review of the contract, with an emphasis on security, gas usage optimization and overall code quality.

2. Audit

2.1 Authenticity

The audited contracts can be found in the GitHub repository: https://github.com/wyvernprotocol/wyvern-v3; the version used has commit hash *ef787c534f06d0144998ebb112e97de658a83d6d*.

2.2 Scope

This audit covered only the *.sol files linked to in the previous section.

2.3 Legend

- 🔴 Critical issues
- 🟠 High priority issues
- 🟡 Medium issues and optimisations
- 🟢 Minor issues, notes and recommendations

3. Issues Found

---

1. ProxyRegistryInterface contract should be an interface instead

Contract: ProxyRegistryInterface;

As of now, ProxyRegistryInterface is declared as a contract. We recommend turning it into an interface and declaring all contained functions as external, which would be the standard practice.

Additionally, the ProxyRegistry contract should extend ProxyRegistryInterface.

2. Typos in comments

Contract: ProxyRegistry;
Line: 64;

The word “enable” is misspelled as “nable” in comment at line 64.

3. Older version of Solidity used

As of now the latest stable version is 0.5.2 and we recommend updating to and using the latest stable version.

4. Audit

The audit makes no statements or warranties about utility of the code, safety of the code, suitability of business model, or any other statements about fitness of the contracts to purpose or their bugfree status. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

5. Closing Summary

It is the conclusion of this audit that the codebase of the platform is well organized and modular. In general, the smart contract code adopts all the relevant best practices and has clean, legible and well-documented code. Aside for the minor remarks reported in this audit, the security of the contracts is on the extremely high level, given the assumed requirements. The main issue found by the audit is the item marked as medium priority.