Primitive

Primitive Bits, Inc.
New York, NY
primitive.xyz

February 22, 2024

Arbiter Security Review

Engagement II

Waylon Jepsen	Lead
Colin Roberts	Lead
Could be you	Researcher

1 Executive Summary

Over the course of X days in total, Primitive has reviewed the DFMM protocol Protocolname protocol.

We found a total of X issues with DFMM.

Repository	Commit
Projectname	commithash

Summary

Type of Project	TYPE
Timeline	Feb 29, 2022 - Feb 31, 2022
Methods	Manual Review
Documentation	High
Testing Coverage	High

Total Issues

Critical Risk	1
High Risk	1
Medium Risk	0
Low Risk	0
Gas Optimizations and Informational	0

Contents

2 Primitive

Primitive is a team of deeply technical passionate indciduals, building the future of finance. You can find more information about us at primitive.finance.

3 Introduction

This report is a security review of the Dynamic Function Market Maker smart contracts.

3.1 Agent Based Modeling

Arbiter uses agent based modeling with the rust evm to provide security and risk analysis insights that are traditionally more difficult to audit.

3.2 Simulation Components

The system is composed of several agents and contracts. Below is a summary of the components:

- **Agents:**
  - Arbitrage Agent: The Arbitrage Agent is responsible for swaping against DFMM pools and the external market.
  - Liquidity Provider Agent: The Liquidity Provider Agent is responsible for providing liquidity to the DFMM pools.
  - Price Changer Agent: The Price Changer Agent is responsible for changing the price of the external market.

- **Contracts:**
  - TODO
- **Oracle:**
  - The Oracle we will perturb is the liquid exchange (lex) contract.

3.3 Simulation Setup

3.4 Risk Modeling

We will perturb over the infinite space of price paths to look for anomoly behavior. and perform financial analysis on the system.

4 Findings

4.1 Critical Risk

4.2 High Risk

4.2.1 Issue title (Only first word should be capitalized; titles should never end with punctuation)

Severity: High

Context: `Contract.sol#L160-L165`

Description:

Recommendation:

Project: Fixed in PR #1.

Arbiter: Resolved.

4.3 Medium Risk

4.4 Low Risk

4.5 Gas Optimizations

5 Additional Comments

\clearpage

6 Appendix