



Three Sigma

Code Audit



Ojo A cross-chain oracle built as a blockchain

Disclaimer

Code Audit

Ojo A cross-chain oracle built as a blockchain

Disclaimer

The ensuing audit offers no assertions or assurances about the code's security. It cannot be deemed an adequate judgment of the contract's correctness on its own. The authors of this audit present it solely as an informational exercise, reporting the thorough research involved in the secure development of the intended contracts, and make no material claims or guarantees regarding the contract's post-deployment operation. The authors of this report disclaim all liability for all kinds of potential consequences of the contract's deployment or use. Due to the possibility of human error occurring during the code's manual review process, we advise the client team to commission several independent audits in addition to a public bug bounty program.

Table of Contents

Code Audit

Ojo A cross-chain oracle built as a blockchain

Table of Contents

<i>Disclaimer</i>	<i>3</i>
<i>Summary</i>	<i>7</i>
<i>Scope</i>	<i>9</i>
<i>Methodology</i>	<i>11</i>
<i>Project Dashboard</i>	<i>13</i>
<i>Code Maturity Evaluation</i>	<i>16</i>
<i>Findings</i>	<i>19</i>
3S-Ojo-L01	19
3S-Ojo-N01	20

Summary

Code Audit

Ojo A cross-chain oracle built as a blockchain

Summary

Three Sigma audited Ojo in a 2 day engagement. The audit was conducted from 16-10-2024 to 17-10-2024.

Protocol Description

Ojo has created an exchange-rate oracle contract for LRTs curated by Mellow. This oracle is intended to output the exchange rate between an LRT and a particular base asset, while having an interface that is compatible with Morpho markets. Since Mellow accepts multiple asset types in its vaults, this contract takes the underlying TVL of the vault into consideration and is compatible with vaults which contain multiple currencies, rather than strictly pegging the LRT to the underlying token with a 1:1 ratio.

000000010	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000000020	00 00 00 00 3B A3 ED FD	7A 7B 12 B2 7A C7 2C 3E	:Eiÿz{.
000000030	67 76 8F 61 7F C8 1B C3	88 8A 51 32 3A 9F B8 AA	gv.a.Ê.Ã~SQ
000000040	4B 1E 5E 4A 29 AB 5F 49	FF FF 00 1D 1D AC 2B 7C	K.^J)«_Iyy.
000000050	01 01 00 00 00 01 00 00	00 00 00 00 00 00 00 00	
000000060	00 00 00 00 00 00 00 00	00 00 00 00 00 00 00 00	
000000070	00 00 00 00 00 00 FF FF	FF FF 4D 04 FF FF 00 1D	ÿÿÿÿ
000000080	01 04 45 54 68 65 20 54	69 6D 65 73 20 30 33 2F	..EThe Tim
000000090	4A 61 6E 2F 32 30 30 39	20 43 68 61 6E 63 65 6C	Jan/2009 CH
0000000A0	6C 6F 72 20 6F 6E 20 62	72 69 6E 6B 20 6F 66 20	lor on brin
0000000B0	73 65 63 6F 6E 64 20 62	61 69 6C 6F 75 74 20 66	second bail
0000000C0	6F 72 20 62 61 6E 6B 73	FF FF FF FF 01 00 F2 05	or banksÿÿÿÿ
0000000D0	2A 01 00 00 00 43 41 04	67 8A FD B0 FE 55 48 27	*....CA.gŠÿ
0000000E0	19 67 F1 A6 71 30 B7 10	5C D6 A8 28 E0 39 09 A6	.gñ q0·.\Ö"
0000000F0	79 62 E0 EA 1F 61 DE B6	49 F6 BC 3F 4C EF 38 C4	ybaê.ab¶IÖ%
00000100	F3 55 04 E5 1E C1 12 DE	5C 38 4D F7 BA 0B 8D 57	óU.ã.Á.Þ\8M
00000110	8A 4C 70 2B 6B F1 1D 5F	AC 00 00 00 00	ŠLp+kñ._~..
000000000	30 31 30 30 30 30 30 30	36 66 65 32 38 63 30 61	01000000006f
000000010	61 65 66 31 62 33 37 32	63 31 61 36 61 32 34 36	b6f1b3726c1
000000020	61 65 36 33 66 37 34 66	39 33 31 65 38 33 36 35	ae63f7f4639
000000030	65 31 35 61 30 38 39 63	36 38 64 36 31 39 30 30	e15a089c638
000000040	30 30 30 30 30 30 30 30	39 38 32 30 35 31 66 64	00000009820
000000050	30 30 30 30 30 30 30 30	38 30 65	1e4ba7445bb
000000060	31 66 65 65 31 34 36 37	37 62 61 31 61 33 63 33	1fee1456376
000000070	35 34 30 62 66 37 62 31	63 64 62 36 30 36 65 38	5400bfb1bcd
000000080	35 37 32 33 33 65 30 65	36 31 62 63 36 36 34 39	57233e0e6bc
000000090	66 66 66 66 30 30 31 64	30 31 65 33 36 32 39 39	fff0001d01e
0000000A0	30 31 30 31 30 30 30 30	30 30 30 31 30 30 30 30	01010000000
0000000B0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
0000000C0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
0000000D0	30 30 30 30 30 30 30 30	30 30 30 30 30 30 30 30	00000000000
0000000E0	30 30 30 30 30 30 30 30	30 30 30 30 66 66 66 66	00000000000
0000000F0	66 66 66 66 30 37 30 34	66 66 66 66 30 30 31 64	ffff074ffff
00000100	30 31 30 34 66 66 66 66	66 66 66 66 30 31 30 30	0104ffffffffff
00000110	66 32 30 35 32 61 30 31	30 30 30 30 30 30 34 33	f2052a01000
00000120	34 31 30 34 39 36 62 35	33 38 65 38 35 33 35 31	4104946b538
00000130	39 63 37 32 36 61 32 63	39 31 65 36 31 65 63 31	9c726ac91e6
00000140	31 36 30 30 61 65 31 33	39 30 38 31 33 61 36 32	16000ae1390
00000150	37 63 36 36 66 62 38 62	65 37 39 34 37 62 65 36	7c66fb8be79
00000160	33 63 35 32 64 61 37 35	38 39 33 37 39 35 31 35	3c52da73589
00000170	64 34 65 30 61 36 30 34	66 38 31 34 31 37 38 31	d4e0a646381
00000180	65 36 32 32 39 34 37 32	31 31 36 36 62 66 36 32	e6224947321
00000190	31 65 37 33 61 38 32 63	62 66 32 33 34 32 63 38	1e73a823cbf
000001A0	35 38 65 65 61 63 30 30	30 30 30 30 30 30	58eacc00000
000000000	30 31 30 30 30 30 30 30	34 38 36 30 65 62 31 38	010000000486

Scope

Code Audit

Ojo A cross-chain oracle built as a blockchain

Scope

CloneFactory

MellowPriceFeed

Assumptions

External libraries are assumed to be secure.

Methodology

Code Audit

Ojo A cross-chain oracle built as a blockchain

Methodology

To begin, we reasoned meticulously about the contract's business logic, checking security-critical features to ensure that there were no gaps in the business logic and/or inconsistencies between the aforementioned logic and the implementation. Second, we thoroughly examined the code for known security flaws and attack vectors. Finally, we discussed the most catastrophic situations with the team and reasoned backwards to ensure they are not reachable in any unintentional form.

Taxonomy

In this audit we report our findings using as a guideline Immunefi's vulnerability taxonomy, which can be found at immunefi.com/severity-updated/. The final classification takes into account the severity, according to the previous link, and likelihood of the exploit. The following table summarizes the general expected classification according to severity and likelihood; however, each issue will be evaluated on a case-by-case basis and may not strictly follow it.

Severity / Likelihood	LOW	MEDIUM	HIGH
NONE	None		
LOW	Low		
MEDIUM	Low	Medium	Medium
HIGH	Medium	High	High
CRITICAL	High	Critical	Critical

Project Dashboard

Code Audit

Ojo A cross-chain oracle built as a blockchain

Project Dashboard

Application Summary

Name	Ojo
Commit	e2ff96624afea24fbc9d79f5cc30f4ae2e8c530b
Language	Solidity
Platform	Ethereum

Engagement Summary

Timeline	16-10-2024 to 17-10-2024
Nº of Auditors	1
Review Time	2 days

Vulnerability Summary

Issue Classification	Found	Addressed	Acknowledged
Critical	0	0	0
High	0	0	0
Medium	0	0	0
Low	1	1	0

None	1	1	0
------	---	---	---

Category Breakdown

Suggestion	1
Documentation	0
Bug	1
Optimization	0
Good Code Practices	0

Code Maturity Evaluation

Code Audit

Ojo A cross-chain oracle built as a blockchain

Code Maturity Evaluation

Code Maturity Evaluation Guidelines

Category	Evaluation
Access Controls	The use of robust access controls to handle identification and authorization and to ensure safe interactions with the system.
Arithmetic	The proper use of mathematical operations and semantics.
Centralization	The presence of a decentralized governance structure for mitigating insider threats and managing risks posed by contract upgrades
Code Stability	The extent to which the code was altered during the audit.
Upgradeability	The presence of parameterizations of the system that allow modifications after deployment.
Function Composition	The functions are generally small and have clear purposes.
Front-Running	The system's resistance to front-running attacks.
Monitoring	All operations that change the state of the system emit events, making it simple to monitor the state of the system. These events need to be correctly emitted.
Specification	The presence of comprehensive and readable codebase documentation.
Testing and Verification	The presence of robust testing procedures (e.g., unit tests, integration tests, and verification methods) and sufficient test coverage.

Code Maturity Evaluation Results

Category	Evaluation
Access Controls	Satisfactory . The codebase has a strong access control mechanism.
Arithmetic	Satisfactory . The codebase uses Solidity version >0.8.0 implementing safe arithmetic.
Centralization	Satisfactory . The protocol has no centralization points.
Code Stability	Satisfactory . The codebase was stable during the course of the audit.
Upgradeability	Weak . The price feed is not upgradeable.
Function Composition	Satisfactory . Functionality is well split into different helpers.
Front-Running	Satisfactory . No front-running issues were found.
Monitoring	Satisfactory . Events were correctly emitted.
Specification	Satisfactory . The code matched the design specifications.
Testing and Verification	Satisfactory . Although tests were not present the codebase is very simple.

Findings

Code Audit

Ojo A cross-chain oracle built as a blockchain

Findings

3S-Ojo-L01

Hardcoded **1e18** ratio calculation regardless of decimals

Id	3S-Ojo-L01
Classification	Low
Severity	Low
Likelihood	Low
Category	Bug
Status	Addressed in #ad88fe1 .

Description

MellowPriceFeed gets the ratio by doing `answer = int256(uint256(ratiosX96[0])) * 1e18 / int256(managedRatiosOracle.Q96());`, hardcoding the decimals to **1e18**. However, the decimals are set in the **constructor** and stored in **priceFeedDecimals**, and could differ from **1e18**.

Recommendation

```
answer = int256(uint256(ratiosX96[0])) * 10**priceFeedDecimals /  
int256(managedRatiosOracle.Q96());
```

3S-Ojo-N01

The number of underlying tokens may be modified in the **Vault** leading to inconsistent exchange rate

Id	3S-Ojo-N01
Classification	None
Category	Suggestion
Status	Addressed in 065a63f .

Description

The price is calculated based on the ratio from **managedRatiosOracle.getTargetRatiosX96()**. Currently the vault has only 1 underlying token, which means the ratio will always be **1e18**. However, the vault may add more tokens, which would change this.

Recommendation

Clarify the behaviour if more tokens are added.