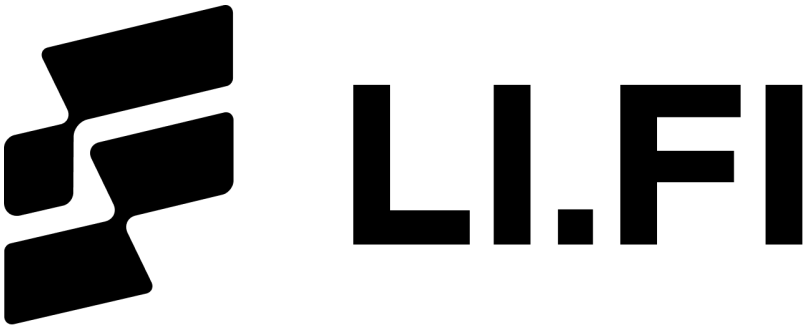

LI.FI Security Review

LiFiDEXAggregator(v1.8.0)

Security Researcher

Sujith Somraaj (somraajsujith@gmail.com)

Report prepared by: Sujith Somraaj

April 22, 2025

Contents

1 About Researcher

Sujith Somraaj is a distinguished security researcher and protocol engineer with over eight years of comprehensive experience in the Web3 ecosystem.

In addition to working as a Security researcher at Spearbit, Sujith is also the security researcher and advisor for leading bridge protocol LI.FI and also is a former founding engineer and current CISO at Superform, a yield aggregator with over $170M in TVL.

Sujith has experience working with protocols including Berachain, Optimism, Fantom, Monad, Blast, ZkSync, Decent, Drips, SuperSushi Samurai, DistrictOne, Omni-X, Centrifuge, Superform-V2, Tea.xyz, Paintswap, Bitcorn, Sweep n' Flip, Byzantine Finance, Variational Finance, Satsbridge, Earthfast and Angles

Learn more about Sujith on sujithsomraaj.xyz or on cantina.xyz

2 Disclaimer

Note that this security audit is not designed to replace functional tests required before any software release, and does not give any warranties on finding all possible security issues of that given smart contract(s) or blockchain software. i.e., the evaluation result does not guarantee against a hack (or) the non existence of any further findings of security issues. As one audit-based assessment cannot be considered comprehensive, I always recommend proceeding with several audits and a public bug bounty program to ensure the security of smart contract(s). Lastly, the security audit is not an investment advice.

This review is done independently by the reviewer and is not entitled to any of the security agencies the researcher worked / may work with.

3 Scope

- src/Periphery/LiFiDEXAggregator.sol(v1.8.0)

4 Risk classification

Severity level	**Impact: High**	**Impact: Medium**	**Impact: Low**
Likelihood: high	Critical	High	Medium
Likelihood: medium	High	Medium	Low
Likelihood: low	Medium	Low	Low

4.1 Impact

High leads to a loss of a significant portion (>10%) of assets in the protocol, or significant harm to a majority of users.

Medium global losses <10% or losses to only a subset of users, but still unacceptable.

Low losses will be annoying but bearable — applies to things like griefing attacks that can be easily repaired or even gas inefficiencies.

4.2 Likelihood

High almost certain to happen, easy to perform, or not easy but highly incentivized

Medium only conditionally possible or incentivized, but still relatively likely

Low requires stars to align, or little-to-no incentive

4.3 Action required for severity levels

Critical Must fix as soon as possible (if already deployed)

High Must fix (before deployment if not already deployed)

Medium Should fix

Low Could fix

5 Executive Summary

Over the course of 1 hours in total, LI.FI engaged with the researcher to audit the contracts described in section 3 of this document ("scope").

In this period of time a total of 2 issues were found. This review focussed only on the changes made from the previous version (v1.7.0), not the code on its entirety.

Project Summary	
Project Name	LI.FI
Repository	lifinance/contracts
Commit	eef8eac61b8c.....910e25adb91
Audit Timeline	April 21, 2025
Methods	Manual Review

Issues Found	
Critical Risk	0
High Risk	0
Medium Risk	0
Low Risk	0
Gas Optimizations	0
Informational	2
Total Issues	**2**

6 Findings

6.1 Informational

6.1.1 Use of magic number in `swapVelodromeV2()` callback flag

Context: LiFiDEXAggregator.sol#L783

Description: In the `swapVelodromeV2()` function, a magic number `1` is used to determine if a callback should be executed after the swap:

```
bool callback = stream.readUint8() == 1; // if true then run callback after swap with tokenIn as
↪  flashloan data
```

Using hardcoded values reduces code readability and maintainability.

Recommendation: Define a constant for this value at the contract level, similar to other constants in the contract:

```
uint8 constant CALLBACK_ENABLED = 1;

bool callback = stream.readUint8() == CALLBACK_ENABLED;
```

LI.FI: Fixed in 70f430629770c853f5cadfb6f835ab7a5c2b3380

Researcher: Verified fix

6.1.2 Incorrect code comment in `swapVelodromeV2()` function

Context: LiFiDEXAggregator.sol#L769

Description: The `swapVelodromeV2()` function comment indicates that the steam parameter contains pool, direction, to, fee, stable, and callback.

However, the function stream does not contain a fee and stable parameter, which is misleading and causes confusion.

Recommendation: Consider fixing the code comment as follows:

```
- /// @param stream [pool, direction, to, fee (not used), stable (not used), callback]
+ /// @param stream [pool, direction, to, callback]
```

LI.FI: Fixed in 4f5eec7d5d10a4c9e0d812daf53941c85e0b0542

Researcher: Verified fix