Security Assessment

ether.fi – Bridging Contracts Combined Audit Report

October 2025

Table of contents

Project Summary

Project Scope

Project Name	Initial Commit Hash	Latest Commit Hash	Platform	Start Date	End Date
weETH OFT Role Improvements	7352faef	7352faef	EVM	06/10/2025	07/10/2025
beHYPE OFT contracts	9646c2	9646c2	EVM	06/10/2025	07/10/2025
CCTP Adapter	76f0ad	3545ec	EVM	07/10/2025	08/10/2025

Project Overview

This document describes the manual code review of several changes to the bridging contracts throughout the **cash-v3**, **weETH-cross-chain** & the **beHYPE** repositories.

The work was a 2 day effort undertaken between **06/10/2025** and **08/10/2025**

The team performed a manual audit of the Solidity smart contracts. During the manual audit, the Certora team discovered bugs in the Solidity smart contracts code, as listed on the following page.

Findings Summary

The table below summarizes the findings of the review, including type and severity details.

Severity	Discovered	Confirmed	Fixed
Critical	-	-	-
High	-	-	-
Medium	-	-	-
Low	-	-	-
Informational	1	1	1
Total	1	1	1

Severity Matrix

Impact	High	Medium	High	Critical
	Medium	Low	Medium	High
	Low	Low	Low	Medium
		Low	Medium	High
		Likelihood		

Detailed Findings

ID	Title	Severity	Status
weETH OFT Role Improvements			
–	–	–	–
beHYPE OFT contracts			
–	–	–	–
CCTP Adapter			
I-01	Discrepancy between the finality and fee parameter	Info	Fixed

weETH OFT Role Improvements

Project Overview

This report presents the findings of a manual code review for the **weETH OFT Role Improvements** audit within the **EtherFi weETH-cross-chain** repository. The work was undertaken between **October 6th 2025** and **October 7th 2025**

The following contract list is included in the scope of this audit:

- `contracts/EtherfiOFTUpgradeable.sol`

The code modifications examined during this review were implemented in the following pull request - PR#62

beHYPE OFT contracts

Project Overview

This report presents the findings of a manual code review for the **beHYPE OFT contracts** audit within the **EtherFi beHYPE** repository. The work was undertaken between **October 6th 2025** and **October 7th 2025**

The following contract list is included in the scope of this audit:

- `src/BeHYPEOFT.sol`
- `src/BeHYPEOFTAdapter.sol`

The code modifications examined during this review were implemented in the following pull request - PR#19

CCTP Adapter

Project Overview

This report presents the findings of a manual code review for the **CCTP Adapter** audit within the **EtherFi cash-v3** repository. The work was undertaken between **October 7th 2025** and **October 8th 2025**

The following contract list is included in the scope of this audit:

- `src/top-up/bridge/CCTPAdapter.sol`

The code modifications examined during this review were implemented in the following pull request - PR#55

Informational Issues

I-01. Discrepancy between the finality and fee parameter

Description: Within the bridge function, minFinalityThreshold parameter is provided to indicate whether a fast or standard transfer should be performed. However, the depositForBurn() call uses a hardcoded fee value of 0, which effectively enforces standard transfers only. As a result, fast transfers cannot be executed on the following supported chains:

- Arbitrum, Base, Codex, Ethereum, Ink, Linea, OPMainnet, Plume, Solana, Unichain, WorldChain.

Recommendation: If more flexibility is intended for the CCTPAdapter, consider allowing for arbitrary fee to be provided. Alternatively, hardcode the minFinalityThreshold to 2000, in order to indicate that only standard transfers can be performed.

Given the permissionless nature of the bridging function in TopUpFactory, it is recommended that the protocol configures for standard transfers, to prevent potential griefing attacks due to fee deduction for fast transfers currently

Customer's response: Fixed in commit 6ecec6 - *"We will only use this contract for standard transfers"*

Fix Review: Fixed

Disclaimer

Even though we hope this information is helpful, we provide no warranty of any kind, explicit or implied. The contents of this report should not be construed as a complete guarantee that the contract is secure in all dimensions. In no event shall Certora or any of its employees be liable for any claim, damages, or other liability, whether in an action of contract, tort, or otherwise, arising from, out of, or in connection with the results reported here.

About Certora

Certora is a Web3 security company that provides industry-leading formal verification tools and smart contract audits. Certora's flagship security product, Certora Prover, is a unique SaaS product that automatically locates even the most rare & hard-to-find bugs on your smart contracts or mathematically proves their absence. The Certora Prover plugs into your standard deployment pipeline. It is helpful for smart contract developers and security researchers during auditing and bug bounties.

Certora also provides services such as auditing, formal verification projects, and incident response.