



Offchain Custom Fee Token Exchange Rate

Security Assessment (Summary Report)

March 12, 2025

Prepared for:

Harry Kalodner, Lee Bousfield, Steven Goldfeder, and Ed Felten

Offchain Labs

Prepared by: **Gustavo Grieco and Tarun Bansal**

Table of Contents

Table of Contents	1
Project Summary	2
Executive Summary	3
A. Code Quality Recommendations	4
About Trail of Bits	5
Notices and Remarks	6

Project Summary

Contact Information

The following project manager was associated with this project:

Mary O'Brien, Project Manager
mary.obrien@trailofbits.com

The following engineering director was associated with this project:

Josselin Feist, Engineering Director, Blockchain
josselin.feist@trailofbits.com

The following consultants were associated with this project:

Gustavo Grieco, Consultant
gustavo.grieco@trailofbits.com

Tarun Bansal, Consultant
tarun.bansal@trailofbits.com

Project Timeline

The significant events and milestones of the project are listed below.

Date	Event
February 10, 2025	Delivery of report draft
February 14, 2025	Report readout meeting
March 12, 2025	Delivery of final summary report

Executive Summary

Engagement Overview

Offchain Labs engaged Trail of Bits to review the security of the changes made to the Nitro contracts to support an exchange rate for the custom fee token. These changes correspond to [PR #252](#) (c4ee8b8) and [PR #281](#) (13f2cac).

The commits in scope involve a number of changes that allow Arbitrum rollups using ERC-20 tokens as a fee token to properly reimburse the batch poster. Essentially, the gas price needs to be adjusted based on the relative price of the custom token. In order to compute this price, a number of alternatives are offered for the rollup owners to implement, from manually adjusted fixed prices to complex oracles based on external data. Only the infrastructure smart contract-related changes were in scope, so testing and example code was excluded.

A team of two consultants conducted the review from February 5 to February 10, 2025, for a total of five engineer-days of effort. With full access to source code and documentation, we performed a manual review of the code in scope.

Observations and Impact

This engagement did not reveal any issues in the code in scope. However, we provide some recommendations for improving the code quality in the [Code Quality Recommendations appendix](#).

Recommendations

Based on the security review, Trail of Bits recommends that Offchain Labs take the following step:

- Review the items in the [Code Quality Recommendations appendix](#) and consider taking action on each one.

A. Code Quality Recommendations

The following is a list of findings that were not identified as immediate security issues but may warrant further investigation.

- The batch poster will need additional trust assumptions if they can directly or indirectly influence the exchange rate for getting refunds. While this is documented in the `fee-token-pricer` README, it must also be included in [the official sequencer/batch poster documentation](#).
- Be careful while moving the storage variables in upgradeable smart contracts to avoid storage slot collision risks. The `buffer` storage variable has been moved from the last position to above all the immutable variables. This movement does not introduce storage collision vulnerabilities because immutable variables are not stored in the storage slots.

About Trail of Bits

Founded in 2012 and headquartered in New York, Trail of Bits provides technical security assessment and advisory services to some of the world's most targeted organizations. We combine high-end security research with a real-world attacker mentality to reduce risk and fortify code. With 100+ employees around the globe, we've helped secure critical software elements that support billions of end users, including Kubernetes and the Linux kernel.

We maintain an exhaustive list of publications at <https://github.com/trailofbits/publications>, with links to papers, presentations, public audit reports, and podcast appearances.

In recent years, Trail of Bits consultants have showcased cutting-edge research through presentations at CanSecWest, HCSS, Devcon, Empire Hacking, GrrCon, LangSec, NorthSec, the O'Reilly Security Conference, PyCon, REcon, Security BSides, and SummerCon.

We specialize in software testing and code review projects, supporting client organizations in the technology, defense, and finance industries, as well as government entities. Notable clients include HashiCorp, Google, Microsoft, Western Digital, and Zoom.

Trail of Bits also operates a center of excellence with regard to blockchain security. Notable projects include audits of Algorand, Bitcoin SV, Chainlink, Compound, Ethereum 2.0, MakerDAO, Matic, Uniswap, Web3, and Zcash.

To keep up to date with our latest news and announcements, please follow [@trailofbits](#) on Twitter and explore our public repositories at <https://github.com/trailofbits>. To engage us directly, visit our "Contact" page at <https://www.trailofbits.com/contact>, or email us at info@trailofbits.com.

Trail of Bits, Inc.

228 Park Ave S #80688

New York, NY 10003

<https://www.trailofbits.com>

info@trailofbits.com

Notices and Remarks

Copyright and Distribution

© 2025 by Trail of Bits, Inc.

All rights reserved. Trail of Bits hereby asserts its right to be identified as the creator of this report in the United Kingdom.

Trail of Bits considers this report public information; it is licensed to Offchain Labs under the terms of the project statement of work and has been made public at Offchain Labs' request. Material within this report may not be reproduced or distributed in part or in whole without Trail of Bits' express written permission.

The sole canonical source for Trail of Bits publications is the [Trail of Bits Publications page](#). Reports accessed through sources other than that page may have been modified and should not be considered authentic.

Test Coverage Disclaimer

All activities undertaken by Trail of Bits in association with this project were performed in accordance with a statement of work and agreed upon project plan.

Security assessment projects are time-boxed and often reliant on information that may be provided by a client, its affiliates, or its partners. As a result, the findings documented in this report should not be considered a comprehensive list of security issues, flaws, or defects in the target system or codebase.

Trail of Bits uses automated testing techniques to rapidly test the controls and security properties of software. These techniques augment our manual security review work, but each has its limitations: for example, a tool may not generate a random edge case that violates a property or may not fully complete its analysis during the allotted time. Their use is also limited by the time and resource constraints of a project.