cLabs Equivalent Tokens Review

Security Assessment (Summary Report)

February 21, 2024

Prepared for:
Benjamin Speckien
cLabs

Prepared by: **Kurt Willis**

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

The sole canonical source for Trail of Bits publications is the Trail of Bits Publications page. Reports accessed through any source 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.

Table of Contents

Project Summary

Contact Information

The following project manager was associated with this project:

Jeff Braswell, Project Manager
jeff.braswell@trailofbits.com

The following engineering director was associated with this project:

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

The following consultant was associated with this project:

Kurt Willis, Consultant
kurt.willis@trailofbits.com

Project Timeline

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

Date	Event
January 30, 2024	Pre-project kickoff call
February 6, 2024	Delivery of report draft
February 6, 2024	Report readout meeting
February 13, 2024	Delivery of summary report
February 21, 2024	Delivery of summary report with fix review appendix

Project Targets

The engagement involved a review and testing of the differential targets contained in the Core Contracts Release 11 notes.

Release: Sorted oracles update

Repository	https://github.com/celo-org/celo-monorepo/pull/10891
Version	PR #10891 (`8e0a1d87ab1c2512cf0bf635f62b3a83f9311dc9`)
Type	Solidity
Platform	EVM

FeeCurrency Adapter

Repository	https://github.com/celo-org/celo-monorepo/pull/10907
Version	PR #10907 (`71796dad0d99465c7061e761c704cf0ab1c46927`)
Type	Solidity
Platform	EVM

Calculation of unlockable gold

Repository	https://github.com/celo-org/celo-monorepo/pull/10731
Version	PR #10731 (`eba4fffe6648f0273db8a005432ac740ba978a7f`)
Type	Solidity
Platform	EVM

Gas Price Minimum should never be zero

Repository	https://github.com/celo-org/celo-monorepo/pull/10909
Version	PR #10909 (`d9630651862a0ec73ad82d890c29c0dcf140b1ff`)
Type	Solidity
Platform	EVM

Add logic for getTotalPendingWithdrawalsCount

Repository	https://github.com/celo-org/celo-monorepo/pull/10488
Version	PR #10488 (`d82334002afa560faf5d818f302b394151064da9`)
Type	Solidity
Platform	EVM

Migrate Governance Tests

Repository	https://github.com/celo-org/celo-monorepo/pull/10697
Version	PR #10697 (`bee30b80a42ac59c351b100d875509f2f8502a21`)
Type	Solidity
Platform	EVM

Executive Summary

Engagement Overview

cLabs engaged Trail of Bits to review the security of the equivalent tokens added to the core contracts as part of release 11.

One consultant conducted the review from January 30 to February 5, 2024, for a total of one engineer-week of effort. With full access to source code and documentation, we performed static and dynamic testing of the project targets, using automated and manual processes.

Observations and Impact

The main focus of the engagement was to assess the security of the upgrade to the `SortedOracles` contract, which introduced the notion of equivalent tokens. We also reviewed the new `FeeCurrencyAdapter` contract for vulnerabilities.

The coverage was limited to additional features (changes only) contained in Solidity files that were part of release 11 of the core contracts.

We identified several high- and medium-severity issues related to the fact that the protocol does not round arithmetic operations in its favor. We also found medium- and low-severity issues related to unclear handling of edge case scenarios. Finally, we identified ways to improve the testing patterns and documentation.

Recommendations

Trail of Bits recommends that cLabs remediate the findings disclosed in this report. These findings should be addressed as part of a direct remediation or as part of any refactor that may occur when addressing other recommendations.

Summary of Findings

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

ID	Title	Type	Severity
1	Minimum gas price does not round up for equivalent tokens	Data Validation	**Medium**
2	Fixed point multiplication does not round up for median rate	Data Validation	**Medium**
3	Absolute minimum gas price does not guard against DoS	Denial of Service	**Medium**
4	Panic is thrown when no oracle rates are available	Undefined Behavior	**Low**
5	debitGasFees does not round up	Data Validation	**High**
6	debitGasFees could result in a zero value	Data Validation	**Low**
7	Risk of value loss due to hard-coded multiplier	Undefined Behavior	**Medium**
8	Adapter does not handle decimals larger than or equal to expected decimals	Undefined Behavior	**Informational**
9	Storage gaps are not used for upgradeable contracts	Auditing and Logging	**Informational**
10	Dangerous testing pattern	Auditing and Logging	**Informational**
11	Unclear units for equivalent token multiplier	Auditing and Logging	**Informational**

12	Compiler warnings are not addressed	Auditing and Logging	**Informational**

A. Vulnerability Categories

The following tables describe the vulnerability categories, severity levels, and difficulty levels used in this document.

Vulnerability Categories	
Category	**Description**
Access Controls	Insufficient authorization or assessment of rights
Auditing and Logging	Insufficient auditing of actions or logging of problems
Authentication	Improper identification of users
Configuration	Misconfigured servers, devices, or software components
Cryptography	A breach of system confidentiality or integrity
Data Exposure	Exposure of sensitive information
Data Validation	Improper reliance on the structure or values of data
Denial of Service	A system failure with an availability impact
Error Reporting	Insecure or insufficient reporting of error conditions
Patching	Use of an outdated software package or library
Session Management	Improper identification of authenticated users
Testing	Insufficient test methodology or test coverage
Timing	Race conditions or other order-of-operations flaws
Undefined Behavior	Undefined behavior triggered within the system

Severity Levels	
Severity	Description
Informational	The issue does not pose an immediate risk but is relevant to security best practices.
Undetermined	The extent of the risk was not determined during this engagement.
Low	The risk is small or is not one the client has indicated is important.
Medium	User information is at risk; exploitation could pose reputational, legal, or moderate financial risks.
High	The flaw could affect numerous users and have serious reputational, legal, or financial implications.

B. Fix Review Results

When undertaking a fix review, Trail of Bits reviews the fixes implemented for issues identified in the original report. This work involves a review of specific areas of the source code and system configuration, not comprehensive analysis of the system.

On February 21, Trail of Bits reviewed the fixes and mitigations implemented by the cLabs team for the issues identified in this report. We reviewed each fix to determine its effectiveness in resolving the associated issue.

In summary, of the 12 issues described in this report, cLabs has resolved six issues, has partially resolved three issues, and has not resolved the remaining three issues. For additional information, please see the Detailed Fix Review Results below.

ID	Title	Status
1	Minimum gas price does not round up for equivalent tokens	**Partially Resolved**
2	Fixed point multiplication does not round up for median rate	**Resolved**
3	Absolute minimum gas price does not guard against DoS	**Unresolved**
4	Panic is thrown when no oracle rates are available	**Resolved**
5	debitGasFees does not round up	**Resolved**
6	debitGasFees could result in a zero value	**Resolved**
7	Risk of value loss due to hard-coded multiplier	**Partially Resolved**
8	Adapter does not handle decimals larger than or equal to expected decimals	**Resolved**
9	Storage gaps are not used for upgradeable contracts	**Partially Resolved**
10	Dangerous testing pattern	**Unresolved**

11	Unclear units for equivalent token multiplier	**Resolved**
12	Compiler warnings are not addressed	**Unresolved**

Detailed Fix Review Results

TOB-CELO-1: Minimum gas price does not round up for equivalent tokens
Partially resolved in PR #10932 (`76f106d`). The `SortedOracles` contract now always returns a constant/fixed denominator of `1e24` for the median rate. However, the operation still does not round up.

The client provided the following context for this finding's fix status:

> *We removed the multiplier altogether in this PR. Otherwise we decided not to round up GasPrice since it might cause tx price to be higher than the user agreed to.*

TOB-CELO-2: Fixed point multiplication does not round up for median rate
Resolved in PR #10931 (`8de3e94`). The equivalent token's multiplier feature was removed.

TOB-CELO-3: Absolute minimum gas price does not guard against DoS
Unresolved. The recommendation is to have the code revert when the oracle rate returns `0`. Currently, it maps the value `0` to a minimal value of 1 WEI instead of reverting.

The client provided the following context for this finding's fix status:

> *Prerequisite of SortedOracles having a bug (or rather having full control over SortedOracles) is problematic and it would cause huge issues in general (including Mento protocol). In such a case returning 1 could be forced attacked in the same way as returning 0.*
>
> *We will keep ABSOLUTE_MINIMAL_GAS_PRICE since it allows for potential future high-value FeeCurrencies to be used. It would be rather expensive for the user, but it would be their choice to use it.*

TOB-CELO-4: Panic is thrown when no oracle rates are available
Resolved in PR #10932 (`76f106d`). `SortedOracles` now always returns a constant/fixed denominator of `1e24`.

TOB-CELO-5: debitGasFees does not round up
Resolved in PR #10940 (`bedbac1`). The debited value is now rounded up.

TOB-CELO-6: debitGasFees could result in a zero value
Resolved in PR #10930 (`b8ba85b`). A check for whether the amount to be debited is zero has been included.

TOB-CELO-7: Risk of value loss due to hard-coded multiplier
Partially resolved. The client provided the following context for this finding's fix status:

> *This issue was considered a worst case scenario; Celo network will be DDoSed because of a depeg of one of the FeeCurrencies. We have the following countermeasures in such a case:*
>
> - *Celo network restricts the percentage of transactions that can be paid in FeeCurrencies (other than Celo).*
> - *We can remove FeeCurrency from the whitelist with a Governance proposal (it takes 7 days).*
> - *We can introduce hotifix (70% of validators need to agree) and remove FeeCurrency from the whitelist (instant).*

There is still a risk that a token could be depegged while still being tied to another token's value; however, a network restriction can reduce the damage in the case of a DoS attack.

TOB-CELO-8: Adapter does not handle decimals larger than or equal to expected decimals
Resolved in PR #10943 (`d1250d1`). A NatSpec comment explaining that `_expectedDecimals` must be bigger than `_adaptedToken.decimals()` was added.

TOB-CELO-9: Storage gaps are not used for upgradeable contracts
Partially resolved in PR #10933 (`97b1324`). Storage gaps were introduced; however, the convention is to count the remaining gap from 50, and this convention is not kept.

TOB-CELO-10: Dangerous testing pattern
Unresolved. cLabs will consider removing this pattern in a future upgrade.

The client provided the following context for this finding's fix status:

> *We are using this testing pattern throughout the whole protocol and we will be considering addressing it in future releases.*

TOB-CELO-11: Unclear units for equivalent token multiplier
Resolved in PR #10931 (`8de3e94`). The equivalent token's multiplier feature was removed.

TOB-CELO-12: Compiler warnings are not addressed
Unresolved. However, the issue is being tracked in issue #10942.

C. Fix Review Status Categories

The following table describes the statuses used to indicate whether an issue has been sufficiently addressed.

Fix Status	
Status	**Description**
Undetermined	The status of the issue was not determined during this engagement.
Unresolved	The issue persists and has not been resolved.
Partially Resolved	The issue persists but has been partially resolved.
Resolved	The issue has been sufficiently resolved.