Linea Custom Bridged Token

Date	December 2023
Auditors	Rai Yang

1 Executive Summary

This report presents the results of our engagement with **Consensys Linea** to review **Linea Custom Bridged Token**.

The review was conducted over two days, from **November 30, 2023** to **December 1, 2023**, by **Rai Yang**. A total of 1 person-days were spent.
No issues are found, however the deployer of the custom bridged token should take caution to initialize the token with the correct initialization function version and parameters.

2 Scope

Our review focused on the commit hash 3cf85529fd4539eb06ba998030c37e47f98c528a. The list of files in scope can be found in the Appendix.

2.1 Objectives

Together with the **Linea** team, we identified the following priorities for our review:

1. Correctness of the implementation, consistent with the intended functionality and without unintended edge cases.
2. Identify known vulnerabilities particular to smart contract systems, as outlined in our Smart Contract Best Practices, and the Smart Contract Weakness Classification Registry.
3. The correct initialization of the bridged token

3 System Overview

The Linea custom bridged token is inherited from Linea `BridgedToken` contract, it's used as same purpose as `BridgedToken`. The only difference is the custom bridged token allows token issuer to deploy the token or original deployer to transfer the ownership (usually is the proxy admin of a proxy contract behind which the bridged token is deployed) to the issuer so that they can later governance tasks such as upgrades as needed. In Lido's `wstETH` case, the ownership will be transfered from the orginal deployer (a Multisig controlled by Linea team) to `LineaBridgeExecutor`, a contract which is controlled by the `Ethereum Governance Executor` contract on Ethereum to execute governance tasks. While the original deployer of the `BridgedToken` is always the `TokenBridge` contract.

4 Security Specification

This section describes, **from a security perspective**, the expected behavior of the system under audit. It is not a substitute for documentation. The purpose of this section is to identify specific security properties that were validated by the audit team.

4.1 Actors

The relevant actors are listed below with their respective abilities:

- Token issuer: deploys bridged token and performs governance tasks (e.g. upgrade)
- Original bridged token deployer: deploys bridged token and transfers the ownership to token issuer or LineaBridgeExecutor

4.2 Trust Model

In any system, it's important to identify what trust is expected/required between various actors. For this audit, we established the following trust model:

- Token issuer deploys and initializes the token with the correct initalization function `initializeV2` and parameters especially `_bridge` (address of canonical token bridge) and performs governance tasks correctly.
- Original bridged token deployer deploys the token and transfers the ownership correctly.
- `LineaBridgeExecutor` relays and executes governance tasks correctly.

Appendix 1 - Files in Scope

This audit covered the following files:

File	SHA-1 hash
contracts/tokenBridge/CustomBridgedToken.sol	`7c856bbc41696b45dfb571c84984693818c1682a`

Appendix 2 - Disclosure

Consensys Diligence (“CD”) typically receives compensation from one or more clients (the “Clients”) for performing the analysis contained in these reports (the “Reports”). The Reports may be distributed through other means, including via Consensys publications and other distributions.

The Reports are not an endorsement or indictment of any particular project or team, and the Reports do not guarantee the security of any particular project. This Report does not consider, and should not be interpreted as considering or having any bearing on, the potential economics of a token, token sale or any other product, service or other asset. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. No Report provides any warranty or representation to any third party in any respect, including regarding the bug-free nature of code, the business model or proprietors of any such business model, and the legal compliance of any such business. No third party should rely on the Reports in any way, including for the purpose of making any decisions to buy or sell any token, product, service or other asset. Specifically, for the avoidance of doubt, this Report does not constitute investment advice, is not intended to be relied upon as investment advice, is not an endorsement of this project or team, and it is not a guarantee as to the absolute security of the project. CD owes no duty to any third party by virtue of publishing these Reports.

A.2.1 Purpose of Reports

The Reports and the analysis described therein are created solely for Clients and published with their consent. The scope of our review is limited to a review of code and only the code we note as being within the scope of our review within this report. Any Solidity code itself presents unique and unquantifiable risks as the Solidity language itself remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond specified code that could present security risks. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. In some instances, we may perform penetration testing or infrastructure assessments depending on the scope of the particular engagement.

CD makes the Reports available to parties other than the Clients (i.e., “third parties”) on its website. CD hopes that by making these analyses publicly available, it can help the blockchain ecosystem develop technical best practices in this rapidly evolving area of innovation.

A.2.2 Links to Other Web Sites from This Web Site

You may, through hypertext or other computer links, gain access to web sites operated by persons other than Consensys and CD. Such hyperlinks are provided for your reference and convenience only, and are the exclusive responsibility of such web sites’ owners. You agree that Consensys and CD are not responsible for the content or operation of such Web sites, and that Consensys and CD shall have no liability to you or any other person or entity for the use of third party Web sites. Except as described below, a hyperlink from this web Site to another web site does not imply or mean that Consensys and CD endorses the content on that Web site or the operator or operations of that site. You are solely responsible for determining the extent to which you may use any content at any other web sites to which you link from the Reports. Consensys and CD assumes no responsibility for the use of third-party software on the Web Site and shall have no liability whatsoever to any person or entity for the accuracy or completeness of any outcome generated by such software.

A.2.3 Timeliness of Content

The content contained in the Reports is current as of the date appearing on the Report and is subject to change without notice unless indicated otherwise, by Consensys and CD.