Linea Cross-Chain Governance Executor

Date	October 2023
Auditors	George Kobakhidze, Rai Yang

1 Executive Summary

This report presents the results of our engagement with **Linea** to review **Linea Cross-Chain Governance Executor**.

The review was conducted over half a week, from **October 9, 2023** to **October 11, 2023**, by **George Kobakhidze** and **Rai Yang**. A total of 5 person-days were spent.

2 Scope

Our review focused on the commit hash 7d4fd35e92688d7aa56ae2f94872f851bacae50c. The list of files in scope can be found in the Appendix.

> *Note: The commit that includes the audit remediation is 315308a2640c6969371857321 59b130417f29997, and the* `LineaBridgeExecutor.sol` *file's updated hash is* `f79108241daf6891b2f7db52ec4af2d3c16feaff`.

The focus was on a single contract file `LineaBridgeExecutor` and an interface `IMessageService`. The contract is built upon Aave's cross-chain governance executor set of contracts that enable DAOs and other entities to take control of contracts from their native chain on destination chains, in this case the Linea network.

While the contract's immediate use may be specifically for Lido's governance to control the `wstETH` token on Linea, this contract may be used for managing any contract with cross-chain governance.

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 Document Change Log

Version	Date	Description
1.0	2023-10-11	Initial report
1.1	2023-11-28	Added audit remediation commit and associated updated file hash in the scope section

4 Recommendations

4.1 Adjust NatSpec Author ✓ Fixed

Resolution

Remediated in 315308a2640c6969371857321 59b130417f29997 by referencing Linea as the author.

Description

The NatSpec provided for the file has a minor inconsistency with the actual properties. The `author` tag is assigned to Aave whereas this contract was written by the Linea team, though of course built on by work made by the Aave team.

contracts/bridges/LineaBridgeExecutor.sol:L9

```
* @author Aave
```

Recommendation

Adjust the NatSpec as appropriate.

5 System Overview

This system allows entities, such as DAOs, from Ethereum (or other source chains) to control contracts on destination chains using a bridge message service (like the Linea message service) and a bridge executor contract that can execute transactions on behalf of those entities. Typically, the bridge executor contract is given special permissions on target contracts, such as the `Owner` role, so when bridge tasks are executed - they are executed with these permissions. In effect, the bridge executor contract acts as a cross-chain governance proxy that allows for use cases such as managing bridged token contracts and multi-chain protocol deployments. In this system, the entity that queues up and executes the tasks on the bridge executor is known as the Ethereum Governance Executor.

More technically, the `LineaBridgeExecutor` is a contract that inherits the majority of its functionality from the `L2BridgeExecutor` and `BridgeExecutorBase` contracts.

The functionality contained in `LineaBridgeExecutor` is concerned with establishing correct access control for the rest of the core logic. Specifically, this contract defines the relevant message service address for the destination chain - `LINEA_MESSAGE_SERVICE` in our case – and the access control modifier for the function that queues up tasks for the executor – `onlyEthereumGovernanceExecutor`.

The `LINEA_MESSAGE_SERVICE` address variable is set directly in the constructor as an immutable contract variable, a common implementation choice for such bridge executors. The `onlyEthereumGovernanceExecutor` modifier contains access control logic. This logic can vary based on the parameters of the destination chain. In our case, the Linea network's message service allows contracts to query the original sender of the transaction that is being claimed on Linea, so the modifier makes use of that and ensures that any transactions not sent by the Linea message service (`msg.sender != LINEA_MESSAGE_SERVICE`) or transactions not initiated by the Ethereum Governance Executor on the source chain (`IMessageService(LINEA_MESSAGE_SERVICE).sender() != _ethereumGovernanceExecutor`) are reverted.

The `L2BridgeExecutor` contract defines the access control logic around the aforementioned Ethereum Governance Executor, such as wrapping its ownership around the `queue()` function and managing changes to that address. Finally, the `BridgeExecutorBase` contract defines all the core logic around queuing and actually executing the transactions.

6 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.

6.1 Actors

The relevant actors are listed below with their respective abilities:

- Bridge executor deployer team. Deploys and configures the `LineaBridgeExecutor` contract.
- The target contract deployer team. Deploys and configures the target contract to be managed on the destination chain (Linea).
- Ethereum Governance Executor, the contract on Ethereum that has permission to execute relevant governance tasks on Linea.

6.2 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:

- The bridge executor deployer team is trusted to deploy the contracts with correct parameters to ensure correct functionality such as the address of the relevant managing contract on Ethereum (Ethereum Governance Executor) and the address of the Linea Message Service, which is an immutable contract variable.
- The target contract team correctly transfers the contract ownership on Linea (for example - `wstETH` token contract ownership from Linea's security council) to `LineaBridgeExecutor` contract.
- The Ethereum Governance Executor manages contracts on Linea owned by the `LineaBridgeExecutor` contract from Ethereum. Therefore, users should also treat (and therefore trust) the Ethereum Governance Executor as the owner of those contracts.

Appendix 1 - Files in Scope

This audit covered the following files:

File	SHA-1 hash
contracts/bridges/LineaBridgeExecutor.sol	`8f2cec19e6ee5b6fd5f65a15b4abd82325b59b95`
contracts/dependencies/linea/interfaces/IMessageService.sol	`0ecc11d7612b6e9511cbaf1d8a1717f0b120c864`

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.