Security Assessment Report

Aave StatAToken Oracle

04/24

Prepared for
Aave

Table of content

Project Summary

Project Scope

Repo Name	Repository	Commits	Compiler version	Platform
static-a-token-v3	Github Repository	34ae7ab		

Project Overview

This document describes the manual code review for the **StaticAToken Oracle**. The work was undertaken on **17 April 2024**.

The following contract list is included in our scope:

- `StataOracle.sol`

Protocol Overview

StataOracle is a contract that provides a canonical way for third parties to fetch the current staticAToken prices.

Audit Goals

1. Check that the call to *getAssetPrice* can be used as a substitute for a Chain Link oracle:
    a. Check the return value's economic units are adequate.
    b. Check that the result of a call to *getAssetPrice* is given in the relevant Chain Link precision.

2. Check that a call to *getAssetPrice* returns the base currency value equal to 1 statAToken if we were to redeem it from the staticAToken contract.

3. Check that a call to *getAssetsPrices* is a trivial extension of *getAssetPrice*

Coverage and Conclusions

1. The party who's calling *getAssetsPrice* can safely use the contract as a substitute for a Chain Link oracle, given that they expect the following output:
    a. The return value answers the question, "What is the exchange ratio between statAToken and base currency?" i.e. "What is the base currency value of 1 statAToken?".
    b. The return value is given in the underlying-to-base-currency Chain Link oracle precision.

2. *getAssetPrice* is rounding the result down, corresponding to the rounding direction applied when calling *redeem* of staticAToken. This means the oracle correctly answers the question, "What is the current base currency value of 1 statAToken if I am to redeem it right now?".

3. *getAssetsPrices* builds and returns an array of multiple statATokens exchange rates corresponding to the list of assets enquired by the user. Calling the function is equivalent to performing multiple separate calls to *getAssetsPrice* with the same list of inputs.

Disclaimer

The Certora Prover takes a contract and a specification as input and formally proves that the contract satisfies the specification in all scenarios. Notably, the guarantees of the Certora Prover are scoped to the provided specification and the Certora Prover does not check any cases not covered by the specification.

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.