A CONSENSYS DILIGENCE AUDIT REPORT

Aave CPM Price Provider

Date	May 2020

1 Document Change Log

Version	Date	Description
1.0	2020-05-05	Initial report
1.1	2020-05-20	Updated for fixes

2 Executive Summary

This report presents the results of our assessment of Aave's Constant Product Market Price Provider (CPMPP), which is an extension to the existing protocol. The CPMPP acts as an oracle, calculating the price in ETH of a liquidity token, which enables the holder to withdraw a portion of the liquidity from an on-chain automated market maker (AMM) such as Uniswap.

The assesment was conducted from May 1 to May 18, 2020 by John Mardlin and Alexander Wade as part of an ongoing engagement between Aave and ConsenSys Diligence. The objective of this collaboration is a more agile and iterative approach to smart contract security vs. the 'security last' approach currently dominating in the industry.

A total of 20 hours were spent on the assessment. Although the code assessed is quite small, time was allocated towards learning about the role of this contract in the larger Aave system, as well as Chainlink and the security properties necessary for an on-chain oracle.

3 Scope

Our review focused on a single file `CmpPriceProvider.sol`. We looked at two iterations of the file.

3.1 Objectives

We focused on the following objectives for our review of the `CmpPriceProvider`:

1. Ensure the absence of known security vulnerabilities
2. Ensure the contract satisfies the critical requirements of an oracle:
   1. **Availability:** it returns a value when requested.
   2. **Integrity/Authenticity:** it returns the correct value.

In particular, the Aave team requested that we confirm that the CPMPP is not subject to oracle manipulation attacks such as those which have been recently observed using flash loans.

4 Discussion

4.1 Assessment of Price Manipulation Attack Feasibility

The `CpmPriceProvider` contract calculates the price in ETH of a Uniswap liquidity token (UNI) using data from Uniswap and Chainlink. Ignoring constants, the formula is roughly:

`LiqPrice = (EthReserve + TokenReserve*Price)/Liquidity`

Where the symbols above are defined as:

Symbol	Property	Data Source

Symbol	Property	Data Source
`EthReserve`	Eth Value in Reserve	`exchange.balance`
`TokenReserve`	Tokens in Reserve	`Token.balanceOf(exchange)`
`Price`	Price of Token in ETH	Chainlink Oracle
`Liquidity`	Total supply of liquidity tokens	`exchange.totalSupply()`
`LiqPrice`	Price of Liquidity Tokens in Eth	calculated

An attacker could attempt to manipulate the value of `LiqPrice` in one of two ways:

1. Trade Eth/Tokens
2. Add or remove liquidity tokens

Our investigation concluded that manipulation was indeed possible, (see issue 6.1).

In the follow up review, a fix was introduced which detects manipulation by comparing the price derived from the state of the Uniswap exchange to the price provided by the Chainlink oracle. If the prices differ significantly, the Chainlink price is taken as correct, and used to derive the proper asset balance for that price.

The improved design with manipulation detection may still have issues at times of high price volatility. At such times, the ethereum network also tends to be congested, making it likely that the Chainlink oracle will not be current. It is even quite possible that arbitrageurs would rebalance Uniswap before the Chainlink price is updated, so that Uniswap will have a more accurate price.

In the case that Uniswap is more current than Chainlink, the `CPMPriceProvider` would use the incorrect Chainlink price to determine the value of the CPM tokens. However the error margin would be limited to the size of the price change in real world markets, which are much more difficult to manipulate than Uniswap (thought not impossible). A sufficiently large over-collateralization requirement should be enough to protect against opportunistic borrowers seeking to take under-collateralized loans during times of high volatility and chain congestion.

5 Recommendations

5.1 Review Chainlink's performance at times of price volatility

In order to understand the risk of the Chainlink oracle deviating significantly, it would be helpful to compare historical prices on Chainlink when prices are moving rapidly, and see what the largest historical delta is compared to the live price on a large exchange.

Update: The Aave team has evaluated the behavior of the price provider and believes that in the worst case, the CPMPriceProvider's performance will match that of the oracle for the underlying currency (ex. Chainlink's DAI/ETH aggregrator) in the UNI pair.

5.2 Expand on existing code comments

The Natspec comments in the codebase are quite minimal. On the `latestAnswer()` question in particular, additional information on the rationale for the price calculation would be helpful.

Update: More Natspec comments have been added since this reccomendation was first made.

5.3 Provide a specification

Even for small changes, a specification should be created outlining:

1. Motivation for the change
2. High level design details and assumptions
3. Key security properties

This does not need to be a long or formal document, it can fit easily into a Pull Request or Issue message. The important thing is that it provides a description of the intended behavior, and allows other members of the team to review and agree on the details. Including a brief discussion of security properties may help to anticipate and avoid potential vulnerabilities or errors.

Update: A specification was provided along with the change to address the price manipulation issue in the first iteration of this report.

6 Issues

The issues are presented in approximate order of priority from highest to lowest.

6.1 CPM token price is susceptible to manipulation `Addressed`

Resolution
Addressed by checking for deviation from Chainlink price.

Description

The calculation of the CPM token price is based on the combined value of the Ether and ERC20 Token liquidity that can be withdrawn per CPM token.

This can be represented simply as `Price = (EtherValue + TokenAmount*EthPriceOfToken) / CpmTotalSupply`, where `EthPriceOfToken` is taken from the chainlink oracle.

However this calculation does not properly account for the Constant Price Model which is susceptible to price slippage at larger trading volumes. This would enable an attacker to make a large trade (possibly funded by a Flash Loan), shifting the balance of the ETH and Token reserves, and reducing the real value of the liquidity held in the exchange.

One way to think of this is that for any given price, there is a "correct" ratio of ETH to Token in the reserve.

The consequence of this issue is that the wrong price is returned, which breaks the security model of this contract.

6.2 Underflow if TOKEN_DECIMALS are greater than 18 `Addressed`

Resolution

The development team has indicated that less than 18 decimals is a design assumption of the system.

We recommend documenting this assumption clearly in the code.

Description

In `latestAnswer()`, the assumption is made that `TOKEN_DECIMALS` is less than 18:

code/contracts/proxies/CmpPriceProvider.sol:L76

```
(_ethBalanceOfCpmToken.mul(1 ether)  + _tokenBalanceOfCpmToken.mul(_unsignec
```

If there are greater than 18 decimals, then this value will underflow to a number close to MAX_UINT.

Recommendation

Add a simple check to the constructor to ensure the added token has 18 decimals or less.

Appendix 1 - Files in Scope

This assessment covered the following files:

A.1.1 Initial state

File	SHA-1 hash
contracts/proxies/CmpPriceProvider.sol	0e3c925cac3c962ccf3c3affd78fbcde8ceafcf9

A.1.2 Final State

File	SHA-1 hash
contracts/proxies/CmpPriceProvider.sol	82b3d7e7f0fe7ca76e131f4f214fc9f6e81d34ab

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 bugfree 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.

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 Solidity code and only the Solidity code we note as being within the scope of our review within this report. 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 Solidity that could present security risks. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty.

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.

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.

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.