xuwinnie

Orbit Protocol Audit Report

2024-02-25

Scope

https://github.com/orbit-protocol/contracts/tree/41d97950bc56983d4a06d6cafec53ae6e240ffe9

OToken.sol - Blast related diff

PythOracleProxy.sol

Conclusion

During this audit, one medium risk finding and one low risk finding were identified, both of which have been addressed accordingly.

Findings

Medium Risk

M-1 Function `getUnderlyingPrice` should use the decimal of underlying token instead of OToken

```
    /**
      * @notice Get the underlying price of a cToken asset
      * @param oToken The cToken to get the underlying price of
      * @return The underlying asset price mantissa (scaled by 1e18).
      *  Zero means the price is unavailable.
      */
    function getUnderlyingPrice(OToken oToken) virtual external view returns
(uint);
}
```

According to the comment, function `getUnderlyingPrice` should use the decimal of underlying token. However, the decimal of the OToken is used.

```
if (expToUse > 0) {
    return
        FullMath.mulDiv(
            10 ** expToUse,
            uint256(int256(price.price)),
            10 ** oToken.decimals()
        );
}
```

Reaction: Fixed

Low Risk

L-1 Confidence interval of price is not used

According to the pyth doc

> To expand upon the first option, we recommend using the confidence interval to protect your users from these unusual market conditions. The simplest way to do so is to use Pyth's confidence interval to compute a *range* in which the true price probably lies. This principle is common sense. Imagine that you are lending money to a friend, and your friend pledges a bitcoin as collateral. Also imagine that Pyth says the bitcoin price is $50000 +- $1000. (Note that $1000 is an unusually large confidence interval for bitcoin; the confidence interval is typically $50 dollars). You therefore calculate that the true price is between $49000 and $51000. When originating the loan, you would value the bitcoin at $49000. The lower price is conservative in this instance because it limits the amount of borrowing that is possible while the price is uncertain. On the other hand, if you were to issue a loan of bitcoin, you would value the borrowed bitcoin at $51000. The higher price is conservative, as it protects you from allowing someone to borrow in excess during times of increased volatility.

Reaction: Acknowledged