Some information about cryptocurrency rates could be obtained from AMM. The issue is that AMM could be manipulated and this may be the reason of hacks, like 2nd bZx hack. Here I consider some manipulation costs computation for non-time averaged oracle models.

1. Uniswap v1 based oracle

Uniswap oracle manipulation is a composite of two opposite swaps.

$(x,y) \rightarrow (x \sqrt{1+\alpha}, y\sqrt{1+\alpha}^{-1}) \rightarrow (x,y)$

.

Price π_y/π_x

at the middle will be α

times more than the initial.

The total fee for Uniswap v1 will be

$\Phi = \phi (\sqrt{\alpha+1} - 1) x + \phi(1-\sqrt{\alpha+1}^{-1})y$

, neglecting $O(\phi^2)$

.

For the case of the same capitalization of x and y C/2

, the total fee will be:

$\Phi = \phi C \frac{\sqrt{\alpha+1} - \sqrt{\alpha+1}^{-1}}{2}$

, where C

is total pair capitalization and ϕ

is fee rate.

2. Mooniswap based oracle

In Mooniswap there are two independent points, corresponding to opposite swaps. So, Mooniswap could offer upper and lower price bounds estimates. The difference between the points is corresponded to the accuracy of the oracle.

Attacker could shift any of two bounds to corresponding direction:

$(x,y) \rightarrow (\sqrt{\alpha+1} x, \sqrt{\alpha+1}^{-1} y)$

.

Rewards for opposite swap will be split by miners, arbitrage bots, and Mooniswap pool.

So, the cost for attack will be

$\Phi = (\sqrt {\alpha+1} + \sqrt {\alpha+1} ^ {-1} -2) \frac{C}{2} = ((\alpha+1)^\frac{1}{4} - (\alpha+1)^{-\frac{1}{4}})^2 \frac{C}{2}$

Models comparison

Here is comparison of two models for $\phi=0.003$

and C=10000000

(USD).

It is important to emphasize that manipulation(2) does not affect the whole value of the oracle, but only reduces the accuracy.

Manipulation cost is growing faster for the 2nd model, so, it could be used when the contract satisfies the following points:

- small manipulations are not important

- for big manipulations the attack is not cost-efficient
- more complex and time-averaged oracle constructions are vulnerable or too gas-inefficient for the current contract

Links

Uniswap whitepaper

Mooniswap whitepaper