CS251: Cryptocurrencies and Blockchain Technologies **Fall 2022**

Assignment #3

Due: 11:59pm on Thursday, **Nov. 10, 2022**
Submit via Gradescope (each answer on a separate page) code: **DJ66V3**

Problem 1. Oracles. In class we discussed the MakerDAO system, where DAI is intended to be a stable currency governed by MKR token holders. A brief description of the MakerDAO system is available here, and a more in-depth description is available here. The MakerDAO system uses a pricing oracle to tell it the current price of ETH in USD. Suppose that this pricing oracle temporarily malfunctions and advertises that the price of ETH is $1,000, when in reality it is only $100. How might an attacker exploit this situation to make money?

Problem 2. Uniswap. Recall that Uniswap uses the elegant constant product formula, $xy = k$, to determine the exchange rate between two tokens. Assuming no fees ($\phi = 1$), we showed Lecture 10 and in section that if the true exchange rate between two tokens A and B is M_p (i.e., one type A token is worth M_p type B tokens), then the market will drive the Uniswap contract to an equilibrium point where it holds x tokens of type A and y tokens of type B, where $y/x = M_p$. This short writeup explains this further.

a. In some cases, it is beneficial to change the equilibrium point so that the ratio of y to x is some value different from M_p. To do so, suppose we change the product formula to $x^2y = k$. The market will drive this modified Uniswap contract to hold x tokens of type A and y tokens of type B, where y/x is $c \cdot M_p$ for some constant c. What is c? (as before, M_p is the true exchange rate between token A and token B, that is 1 $A = M_p$ B).

b. Let us go back to the curve $xy = k$. Suppose Alice wants to buy Δx type A tokens from Uniswap. We showed in section that she would have to send $\Delta y = y \cdot \Delta x/(x - \Delta x)$ type B tokens to Uniswap to maintain the $xy = k$ invariant (see also the writeup referenced above). Therefore, the exchange rate Alice is getting from Uniswap is

$$\frac{\Delta y}{\Delta x} = \frac{y}{x - \Delta x}.$$

In the open market, the exchange rate is M_p. Let us define the *slippage* s as

$$s = \frac{(\Delta y/\Delta x) - M_p}{M_p}.$$

This measures the difference in exchange rate between Uniswap and the open market (hence the name *slippage*). If $s = 0$ then the Uniswap exchange rate is the same as on the open market. If $s > 0$ then the Uniswap exchange rate is worse.

Show that the slippage s is always positive, and is approximately $s \approx \Delta x/x$, assuming x is much larger than Δx. Use the fact that $M_p = y/x$, and that for a small $\epsilon > 0$ we have $1/(1 - \epsilon) \approx 1 + \epsilon$. Your derivation shows that the exchange rate in Uniswap is always worse than on the open market, however, the larger the liquidity pool, the larger x is, and therefore the smaller the slippage $\Delta x/x$, for a fixed Δx.

Problem 3. Howey test. In lecture 12 we discussed the Howey test that defines what is a security using four conditions that must be met. Now, consider the following situation. Alice is a famous Hollywood producer. To finance her next blockbuster film she creates a new ERC-20 AliceToken and sells fifty million tokens to Hollywood studios at a rate of 1 USD per token. Every month after the film premiers, all proceeds from the film for that month are distributed equally among the token holders. For example, if in its first month the movie makes $100M, then every token holder gets $2 per token at the end of the first month. As an ERC-20 token, AliceTokens can be bought and sold on exchanges like Uniswap, and will have a fluctuating exchange rate relative to the USD, depending on how the movie does once it is released. When Alice first sells her AliceTokens, would they be designated as a security according to the Howey test?