XCS251 Assignment 5: Stablecoins, oracles, and decentralized exchanges

---

Due Sunday, October 23 at 11:59pm PT.

Guidelines

1. If you have a question about this assignment, we encourage you to post your question on slack channel.
2. Familiarize yourself with the collaboration and honor code policy before starting work.

Submission Instructions

You should submit a PDF with your solutions online in Gradescope. As long as the PDF is legible and organized, the course staff has no preference between a handwritten and a typeset LaTeX submission. If you wish to typeset your submission and are new to LaTeX, you can get started with the following:

- Download and install Tex Live or try Overleaf.
- Submit the compiled PDF.

Honor code

We strongly encourage students to form study groups. Students may discuss and work on assignment in groups. However, each student must write down the solutions independently, and without referring to written notes from the joint session. In other words, each student must understand the solution well enough in order to reconstruct it by him/herself. In addition, each student should write on the assignment the set of people with whom s/he collaborated. Further, because we occasionally reuse problem set questions from previous years, we expect students not to copy, refer to, or look at the solutions in preparing their answers. It is an honor code violation to intentionally refer to a previous year's solutions. More information regarding the Stanford honor code can be found at https://communitystandards.stanford.edu/policies-and-guidance/honor-code.

Introduction

In this assignment, there are several questions related to stablecoins, oracles, and decentralized exchanges discussed in the class videos. In particular, we will explore how MakerDAO maintains its decentralized stablecoin, Dai, at a $1 price point and how MakderDAO reacts to potential malfunctions of its pricing oracles. We will also explore Uniswap, a decentralized crypto exchange protocol, to see how different product formulas will change the equilibrium point and compare the exchange rate provided by Uniswap to the open market. By the end of this assignment, you should have a better understanding of stablecoins, oracles, and decentralized exchanges.

Problem 1. Stablecoins. In class we looked at how collateralized stablecoin system work. Some collateralized stablecoin system maintains collateral so that when the price of the stablecoin drops, the collateral can be used to shrink the supply of coins and bring the price back up. Some projects maintain on-chain collateral (like MakerDAO, which uses ETH and other asset types for collateral) while others maintain off-chain collateral (like USDC, which uses fiat currencies such as the US dollar for collateral).

a. In MakerDAO, what is the purpose of the DAI Savings Rate (DSR)? Why is it that a high DSR can be used to bring up the price of DAI, and a low DSR can be used to bring down the price of DAI?

b. In MakerDAO the DSR cannot be negative. Explain what would happen if the DSR were set to -1%. Specifically, what is the impact of the negative DSR for DAI holders and what is the impact of the negative DSR on the price of DAI?

Problem 2. 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 in the Maker protocol white paper is available here. Suppose that the MakerDAO pricing oracle (elected by MKR token holders) temporarily malfunctions and advertises that the price of ETH is $1,000, when in reality it is only $100.

a. How might an attacker exploit this situation to make money?

b. Assuming the error is corrected quickly enough not to destroy MakerDAO, who would bear the losses from such an attack? Describe the mechanism that causes those losses.

Hint: You may want to read the Maker protocol white paper. Specifically, you may want to look at how Maker Vaults work.

Problem 3. 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 in class that if the true exchange rate between two tokens A and B is M_p (i.e., 1 $A = M_p$ B), then the market will drive the Uniswap contract to hold x tokens of type A and y tokens of type B, where $y/x = M_p$.

a. In some cases, it is beneficial to change the equilibrium point to some value other than $y/x = M_p$. 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?

b. Let us go back to the curve $xy = k$. Suppose Alice wants to buy Δx type A tokens from Uniswap. We showed in class that she would have to send $\Delta y = y \cdot \Delta x/(x - \Delta x)$ type B tokens to Uniswap. 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.