Uniswap Report

Thanh-Phuong Nguyen - Tu Phan - Nguyen Anh Tuan
{phuongnguyen, tuphan, tuannguyen}@descartes.network

Senswap

1 Introduction

Automated Market Maker (AMM) is a pricing mechanism that allows digital assets traded automatically. This is an efficient replacement of traditional limit order book, which suffers some flaws such as external manipulations. AMMs are mainly separated into two types. One is governed and set up by professional market makers. The other is fully operated by algorithms allowing any user to take part in by providing liquidity to the smart contract. Recently, there are three most popular AMMs run fully by algorithms, one of them is **Uniswap**, which will be discussed in this article.

Uniswap was released in November 2019. It is the first decentralized AMM introduced to market. Uniswap incentives any user to contribute liquidity to the liquidity pool, and enables other traders to trade tokens on the exchange. A special feature of Uniswap, or any similar AMM, is that the trading price of tokens is totally determined by reserves of pair of traded tokens in the pool. This is possible by employing an algorithm called **constant product formula** as the following

$$R_A \times R_B = k,$$

where R_A and R_B are reserves of token A and token B at the time t respectively. If a trader wish to buy an amount Δ_A of token A by paying an amount Δ_B of token B, which means the pool decreasing Δ_A and increasing Δ_B that satisfies

$$(R_A - \Delta_A) \times (R_B + \Delta_B) = k.$$

The **marginal price** is calculated as the following

$$m_u = \frac{R_B}{R_A}.$$

For example, the pool initially has 100 coins of token A and 20 coins of token B, so $k = 100 \times 20 = 2000$. A trader wants to buy 10 coins A, then he must pay $2000 \div (100 - 10) = \frac{20}{9}$ coins B, and the marginal price will be $\frac{20}{100} = 0.2$.

When a user wish to provide liquidity to the pool, he must deposit an amount of pair of tokens at proportion relative to the price in reference market. If the deposited proportion is away from reference price, it will introduce risky arbitrages. The benefit of being a liquidity provider is gaining returns from accumulating trading fees which is 0.3% on Uniswap. This fee is added to the pool and can be collected at any time. It will be distributed to the liquidity providers responding to their relative percent proportion contribution at the time depositing.

Besides, Uniswap also offers a feature called flash swap. With flash swaps, users are able to withdraw up to full reserves of any token in Uniswap at no upfront cost. Obviating upfront capital requirements encourages users to trade on Uniswap for arbitrageurs. By the end of this type of transaction, obviously, users have to either pay for the withdrawn tokens or return all of them along with a small fee.

2 Advantages

Uniswap employed constant product formula as an AMM to execute transactions. The most important property that this AMM possesses is convexity (readers can find more mathematical details in this paper). "Why is convexity?" you might ask, the trading set in Uniswap is convex, which has been well-studied. The advantage of convexity is that we can solve optimization problems like risk modeling, or bounded loss in an efficient way.

In the aspect of protocol, Uniswap has manipulation-resistant on-chain price oracles. The mechanism is that Uniswap measures the market price before the first trade of each block. This price is difficult to manipulate because it was set by the last transaction of the previous block. Attackers have to make a bad trade at the end of the previous block, but there is no guarantee that they will be able to arbitrage it back at the next block. They may lose money to other arbitrageurs.

Another advantage of Uniswap is that it is difficult to find the best path to trade any pair of tokens. Trying to route transactions via some intermediate tokens may cause a proliferation of pairs of tokens in Uniswap.

3 Disadvantages

However, there exist also some disadvantages in Uniswap. One of them is quadratic slippage rate. The slippage rate of Uniswap is shown in the following

$$\frac{R_B^{(t+1)}}{R_A^{(t+1)}} = \frac{1}{\alpha^2} \frac{R_B^{(t)}}{R_A^{(t)}},$$

where $R_A^{(t)}$ is reserve of token A at the t^{th} transaction, $\alpha = \frac{R_A^{(t+1)}}{R_A^{(t)}}$ is the changing rate of reserve of token A. When a transaction trading an amount nearly full reserve of a token, the price will change very fast. Such transactions are easy to occur when the pool is still small. Since impermanent loss is the decreasing value of liquidity provider's stake when the price changes compared to itself at the time depositing. High slippage rate leads to potentially high impermanent loss for liquidity providers. The relationship between slippage rate and impermanent loss is written as follow (see this)

$$IL = \frac{2\sqrt{SR}}{1 + SR} - 1,$$

where IL is impermanent loss, and SR is slippage rate. Without trading fee, IL is always less than or equal to zero. The equality occurs when the price is the same as it at the time of depositing. Despite of trading fee balancing LPs' returns, they still suffer the risk of loss if the market could not attract enough trades.

Uniswap is decentralized for liquidity provision on Ethereum. Therefore, there exists a gas fee for Uniswap to deploy on Ethereum. Recently, many complains that Uniswap is so expensive (see this). The reason for this is Ethereum fee is getting higher. According to the article, the price of an ETH to DAI transaction on Uniswap is \$55 compared to \$33 on Curve, \$44 on Aave, and over \$80 on Mooniswap. The gas fee problem is making Uniswap less attractive to both traders and liquidity providers.

Another drawback of Uniswap is that it is open for any new tokens. Listing new tokens without monitoring makes Uniswap easy to be scammed by fake tokens. It was reported that a fake Teller token and Uniswap pool had been created on August 19,2020 (see this). Attackers could possibly create new tokens with similar name to real tokens to deceive users to trade worthless tokens.