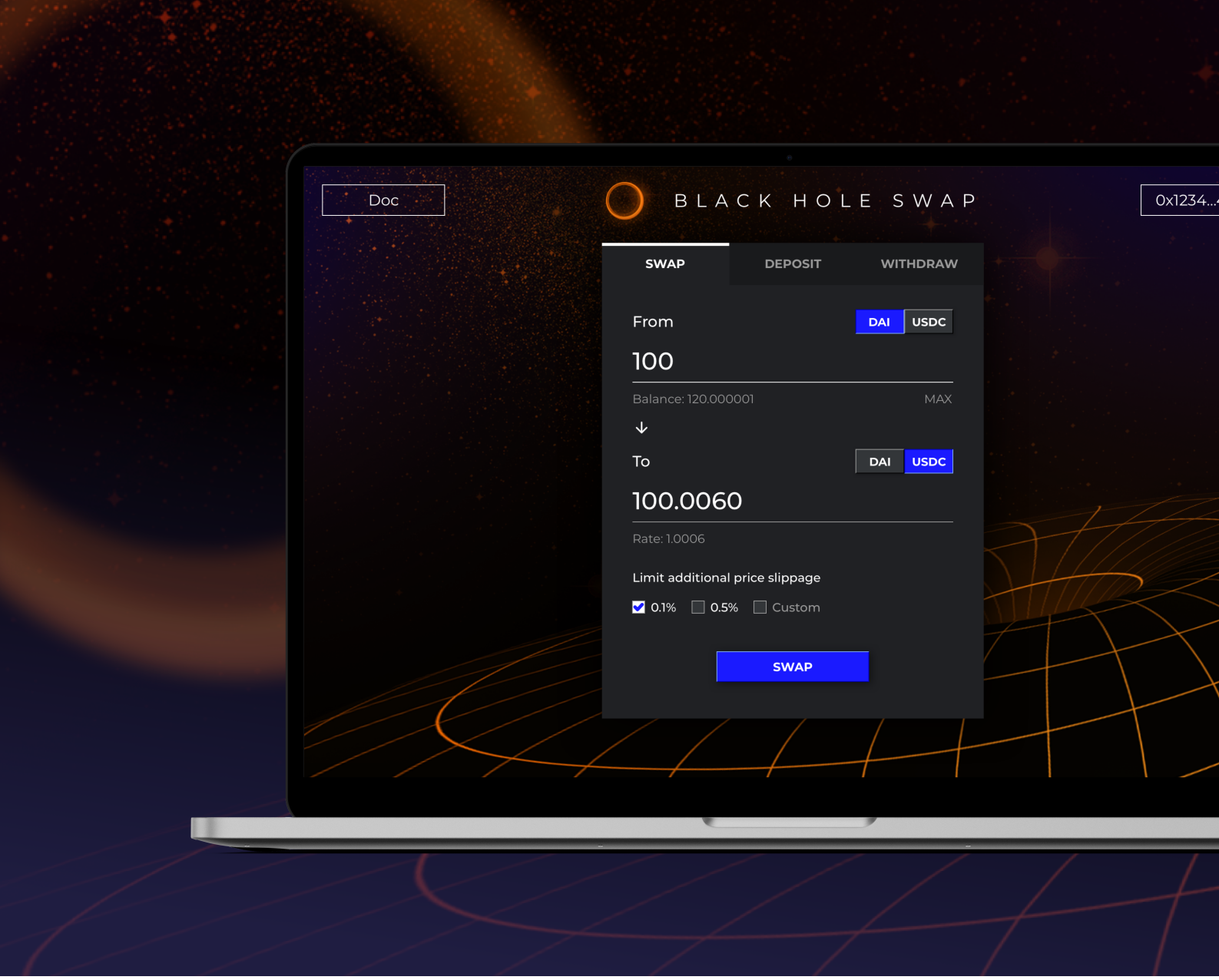


BlackHoleSwap

White Paper

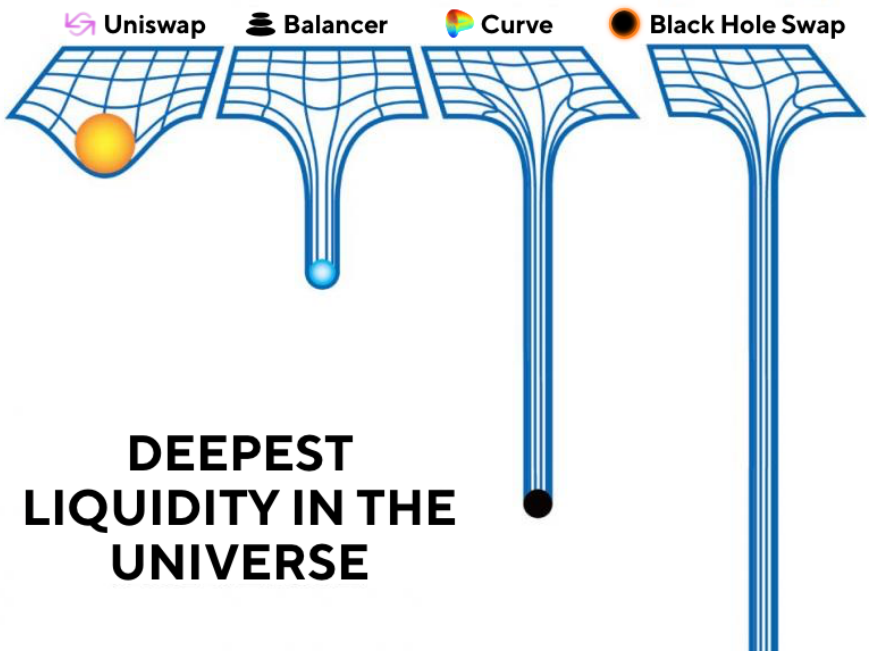
Decentralized Stablecoin Exchange with Unlimited Liquidity

Hakka Finance

July 31, 2020

Abstract

BlackHoleSwap is a decentralized AMM (Automatic Market Making) exchange designed for stablecoins. By integrating lending protocols to leverage the excess supply while borrowing on the inadequate side, It can therefore process transactions far exceeding its existing liquidity. Compared to other AMMs, BlackHoleSwap provides nearly infinite liquidity with the lowest price slippage, maximizing capital utilization.



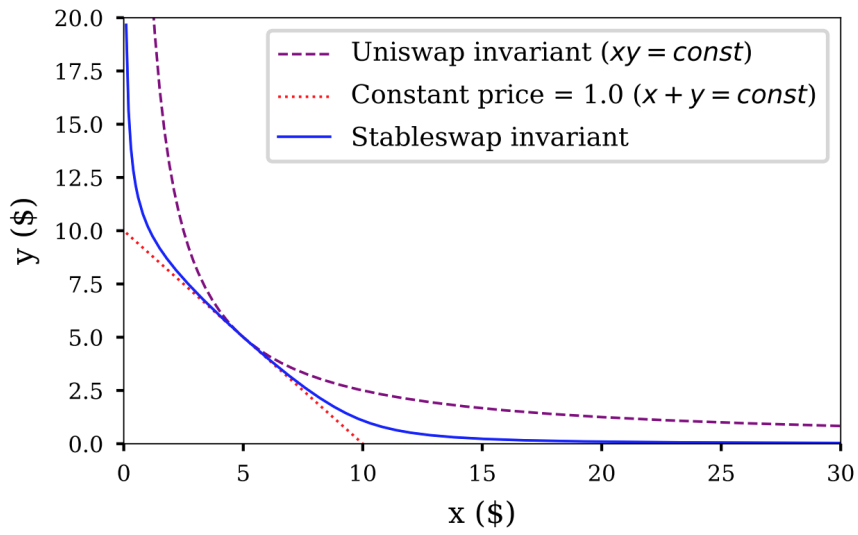
1. Background

The quotation of classic AMM, such as Uniswap, was provided by a "fixed product" formula during the swap between two assets, which makes quoted price very sensitive to stock changes but able to be widely adopted in market making between multiple different assets. However, for exchanges within stablecoins, the fixed product formula of Uniswap is apparently not sufficient enough because the price differences between assets would be quite small.

For exchanges between stablecoins, Curve proposed a specialized model called "Uniswap with leverage," which is a particular formula between constant price (always 1:1 rate) and fixed product of pair volumes (Uniswap). Given the same volume and price difference, the Curve can provide ten times higher liquidity than Uniswap and keep the feature of "always deal."

$$\chi D^{n-1} \sum x_i + \prod x_i = \chi D^n + \left(\frac{D}{n}\right)^n .$$

Even if the model presented by the Curve can provide the excellent trading depth of stablecoins in most situations, colossal price slippage will show up once liquidity of one side is running out. Therefore, when a stablecoin deviates from constant price, liquidity will dry up shortly, resulting in worse performance than Uniswap. This is the side effect of Curve with adjustments for stablecoins.



In an algorithm-based decentralized exchange, the model of Curve is in essence "Reserve-Quote-Deal." A lack of liquidity sometimes occurs due to limited stocks. However, people should have no limitations. BlackHoleSwap has succeeded in the breakthrough of restriction of stocks. Through integrating with decentralized lending protocols (Compound, dYdX, etc.), BlackHoleSwap can provide nearly unlimited liquidity with the lowest price slippage.

2. How It Works

In short, BlackHoleSwap puts reserves into the lending protocol. While running out of the stock on one side of the trading pair, BlackHoleSwap will mortgage the other coin to borrow the required coin to complete the transaction. Hence, BlackHoleSwap will not be limited to its own stocks and safe from the "big turnaround" of Curve while running out of reserves.

The concept of BlackHoleSwap is the same as other AMMs: fulfilling a particular invariant before and after the transaction. The formula of invariant would determine the characteristics of the AMM: the formula of "x + y = k" can provide a fixed price, but the reserves might be drained; "x · y = k" is available for random input, but the price is quite sensitive to the volume of the stocks. Instead, BlackHoleSwap, deriving benefits from lending protocols, can provide the lowest price slippage without the concern of depletion of the reserves.

3. Mathematical Model

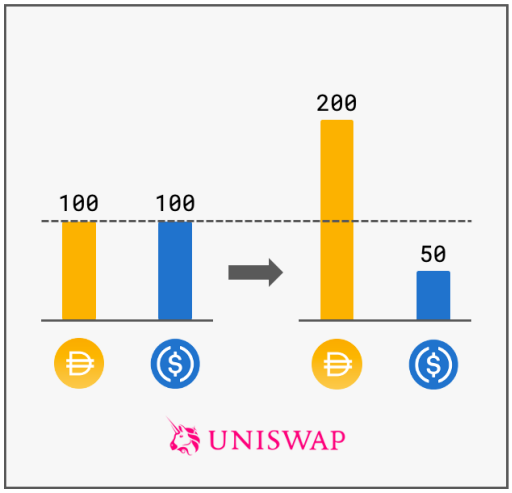
In the design of Uniswap, price slippage of a single transaction is determined by the scale of the reserves. The more mass the reserve has, the less the price slippage will be given the same deal. Therefore, BlackHoleSwap adds "virtual" liquidity in the existing model of Uniswap, just like the structure of the iceberg being more massive underwater. Accordingly, given the same amount of "real" reserves, BlackHoleSwap demonstrates a lower price slippage. Moreover, the number of real reserves can be smaller than 0, which is negative stocks or so-called liability.

Given 100 DAI and 100 USDC in stock in the example below, we present the scenario of swapping 100 DAI (the same amount as stock) for USDC. There will only be 50 USDC in return due to the limitation of "fixed product" in Uniswap. However, BlackHoleSwap, deriving from virtual stocks, can return "98.01 USDC."

(Given 100 DAI and 100 USDC in stock)

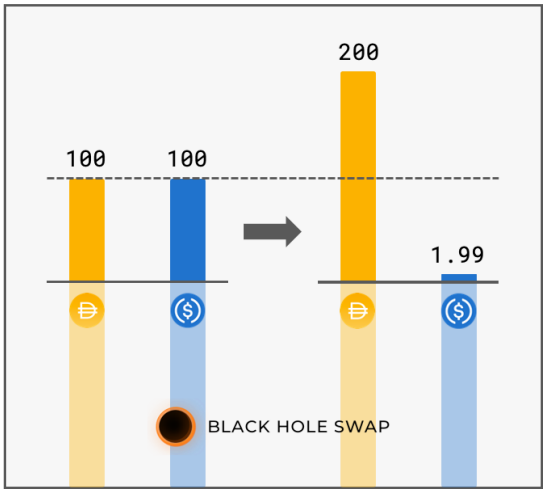
Swap 100 DAI in Uniswap

Get 50 USDC in return



Swap 100 DAI in BlackHoleSwap

Get 98.01 USDC in return



The virtual assets beneath depend on the sum of two stablecoins plus a leverage multiple.
Virtual liquidity S = x + y ; Leverage Multiple: A
Here comes the BlackHoleSwap formula:

$$(x + AS)(y + AS) = k$$

The formula above can be tidied up to:

$$(x + ay)(y + ax) = K$$

Besides,

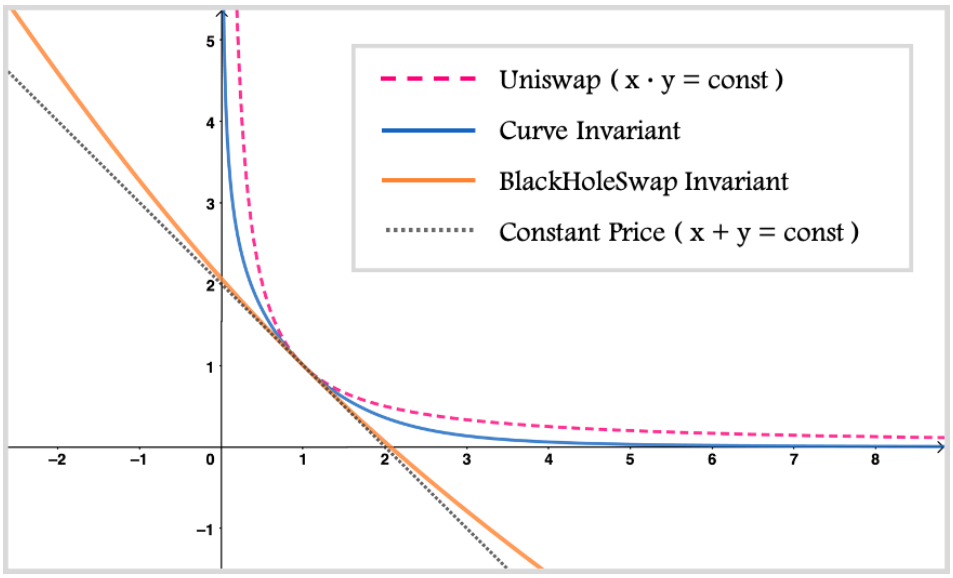
$$a = A/(A + 1),\ 0 < a < 1$$

Therefore, BlackHoleSwap can actually be regarded as implementing a linear transformation to Uniswap, projecting the original curve onto a new coordinate system.

$$\begin{bmatrix} u & v \end{bmatrix} = \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} 1 & a \\ a & 1 \end{bmatrix}$$

Parameter Selection

By observing the identity, we can conclude that when a = 0, BlackHoleSwap would degenerate into Uniswap (x · y = K). While a = 1, the fixed price model (x + y = K) would show up. Through adjusting the parameter "a" BlackHoleSwap (orange line in the below chart) will be a curve warped between x · y = K (pink dotted line) and x + y = K (black dotted line).

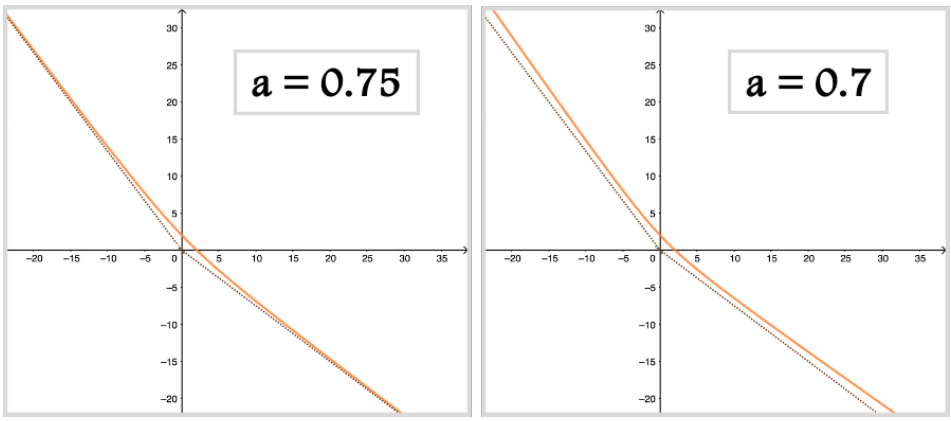


Apparently, when "a" is closer to 1, the slope will be smaller along with better "efficacy" of BlackHoleSwap. However, BlackHoleSwap is required to fulfill external limitations, which is the limitation of liabilities in lending protocols.

Take Compound Finance for example, the collateral factor of stablecoins DAI and USDC is set as 75%, which means the upper bound of the capital available for borrowing is 75% of the mortgage. Otherwise, the loan would be rejected or liquidated due to insufficient mortgages. Therefore, the factor mentioned above is considered as a limitation of BlackHoleSwap.

Look back to the model, BlackHoleSwap is, in fact, a linear transformation of Uniswap, so it inherits some characteristics of Uniswap. $x \cdot y = K$ is a hyperbola with the asymptotes of the x–axis and y–axis. The plot of Uniswap will be infinitely close to $x = 0$ and $y = 0$, but never intersect. For the same reason, the asymptotes of BlackHoleSwap are $x + ay = 0$ and $y + ax = 0$, which is coincidentally analogous to the rule of lending protocols.

When $a = 0.75$, BlackHoleSwap can reach the most effective status in theory with a curve infinitely close to 75% upper bound of borrowing without intersection, providing the best liquidity in an extreme situation.



Considering the different situations we might encounter, including minimal calculating inaccuracy or the interest from liabilities might be more than the interest from deposited assets by the time, we should remain some buffer for BlackHoleSwap rather than riskily setting at extreme (a = 0.75). Otherwise, hackers would be possible of arbitraging BlackHoleSwap via the attack of "Trade–Wait–Liquidate."

A way to buffer is setting "a" as a number slightly smaller than 0.75 so that even if an extreme transaction showing up, the curve remains some distance to the liquidation line. However, a smaller "a" will not only change the shape of the curve but end up in a worse performance.

The other way is to set an upper bound of liability rate while remaining "a = 0.75" unchanged. This solution requires checking the liability rate at every transaction and refuses the transactions, which will put BlackHoleSwap into an over–high liability rate. The advantage of this solution is that the depth of price will not be affected in most situations. On the other hand, unlimited liquidity will be discounted owing to a hard upper bound in the system.

Nevertheless, BlackHoleSwap does not have unlimited liquidity because the reserves in lending protocols are limited. When all DAIs in Compound are all borrowed, the USDC–DAI swap transaction will fail anyway. Therefore, we decided to adopt the liability rate solution with a 62% liability rate upper bound.

4. Risk of Profit and Loss

Any market maker is suffering from certain kinds of risks. Usually, market makers at a lower price slippage and transaction fees market take a higher chance of losing in price fluctuation. The higher utilization rate in the Curve than the Uniswap comes with higher risks. Simultaneously, BlackHoleSwap bears the risks of price fluctuation as well as liquidation due to the borrowing.

In the aspect of system security, the risk in Uniswap is its own codes. However, the Curve and the BlackHoleSwap, deeply integrated with lending protocols, would suffer a wider range of potential attacks including bugs in lending protocols, failing oracles, or the run of mortgage assets in the lending platform.

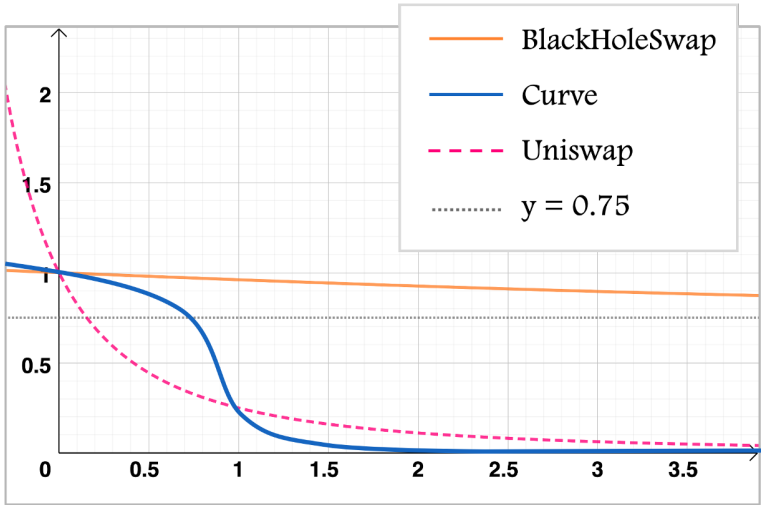
Stablecoin AMM	Depth	Loss in Price Fluctuation	Extra Risks	Utilization Rate
Uniswap	Bad	Low	N/A	Low
Curve	Good (when price within 0.96~1.04)	High	Lending Protocols (ytoken, ctoken)	High
BlackHoleSwap	Best	High	Lending Protocols + Liquidation	Highest

The risk of liquidation and potential flashloan attacks can be prevented by setting an upper bound of liability rate. The system risks of code can also be protected by insurance. However, price fluctuation is the inevitable risk for liquidity providers.

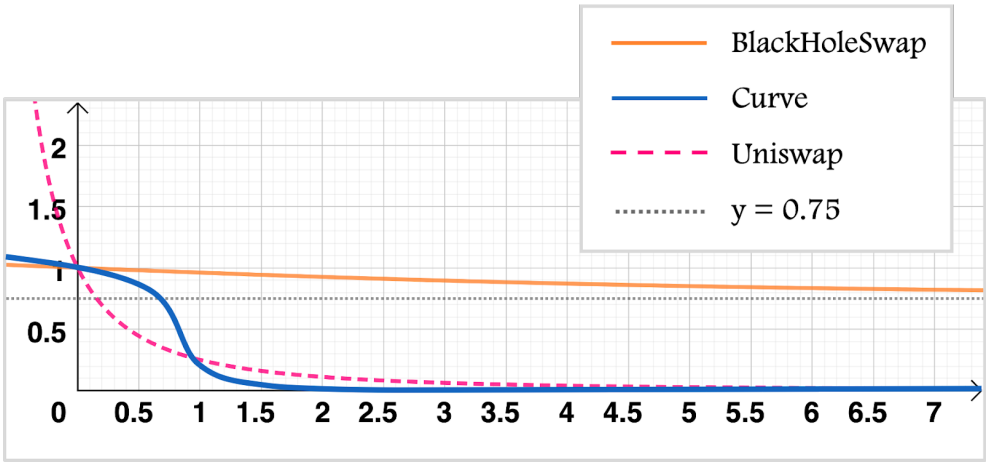
AMM has an especially strong "Buckets Effect," which is that whether the value of an AMM will crash or not is determined by the weakest asset in it. Hence, the failure of either DAI or USDC will result in an enormous loss for liquidity providers.

5. Effectiveness Analysis

Obviously, the performance of BlackHoleSwap in the swap of stablecoins is a lot better than the Uniswap. While swapping the same amount as the reserve in a 1:1 situation in BlackHoleSwap can get ~0.98 of the other coin. The price change of BlackHoleSwap is exceptionally flat, so there will be no phenomenon of precipitous price change in the Curve right before the liquidity runs out.



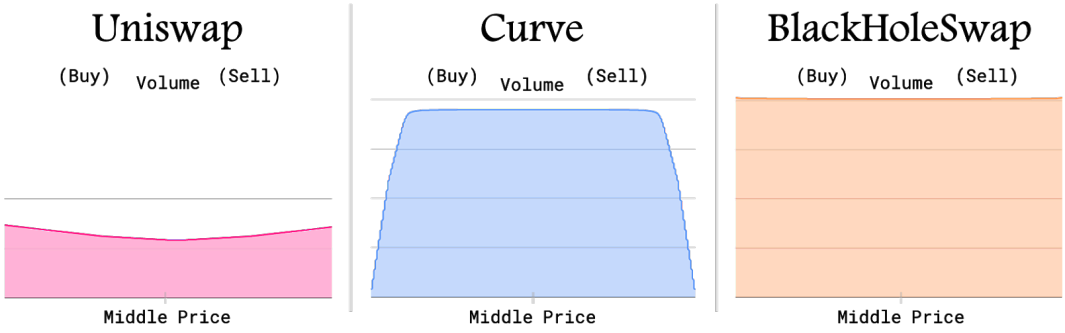
The price in the BlackHoleSwap will be infinitely close to 0.75, which is that all of the inputs are used to mortgage and all the outputs are coming from borrowing.

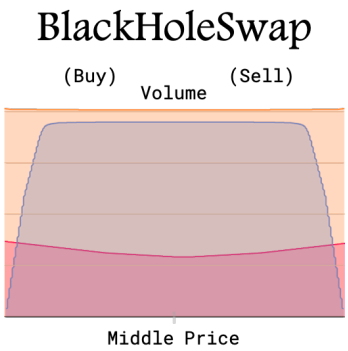


Order Book

If we compare the order books of each protocol, the graph would be shown as below. The x-axis represents the price while the y-axis represents the supplied amount of the stock. On the left side of the middle price is the "ask price" of the protocol; on the right side of the middle price is the "bid price" of the protocol. The area of the painted area is the total supply of the protocol.

Uniswap provides the worst liquidity, but it provides a certain amount of liquidity at every price interval; Curve puts all the liquidity together in the area near the middle price. Once exceeding a boundary, liquidity would steeply fall; Rather than employing either of these liquidity methods, BlockHoleSwap provides extremely stable liquidity at every price, prevailing over all the other methods.





While folding up the three order books, we can conclude that BlackHoleSwap presents an increased performance in all situations compared to Curve and Uniswap.

Extra Profit

BlackHoleSwap currently integrates the lending protocol Compound Finance, which the "Liquidity Mining" mechanism now implements, so there will be some protocol tokens "Comp" mined by BlackHoleSwap. After receiving Comps, BlackHoleSwap will swap it into stablecoins: DAI or USDC and directly add into the pool of capital, making an extra profit for liquidity providers.

6. Future Work

(1) Support more stablecoins

BlackHoleSwap currently only supports limited coins due to lending protocols policy. While Compound Finance or any other lending platform supports other stablecoin as collateral, BlackHoleSwap can onboard more trading pairs.

(2) Apply "black hole" to other AMM models

BlackHoleSwap is basically Uniswap with the linear transformation. By carefully analyzing, a similar method may also apply to other automated market–making mechanisms: BlackholeCurve, BlackHoleBalancer, and so on.