

# BlackHoleSwap

## White Paper

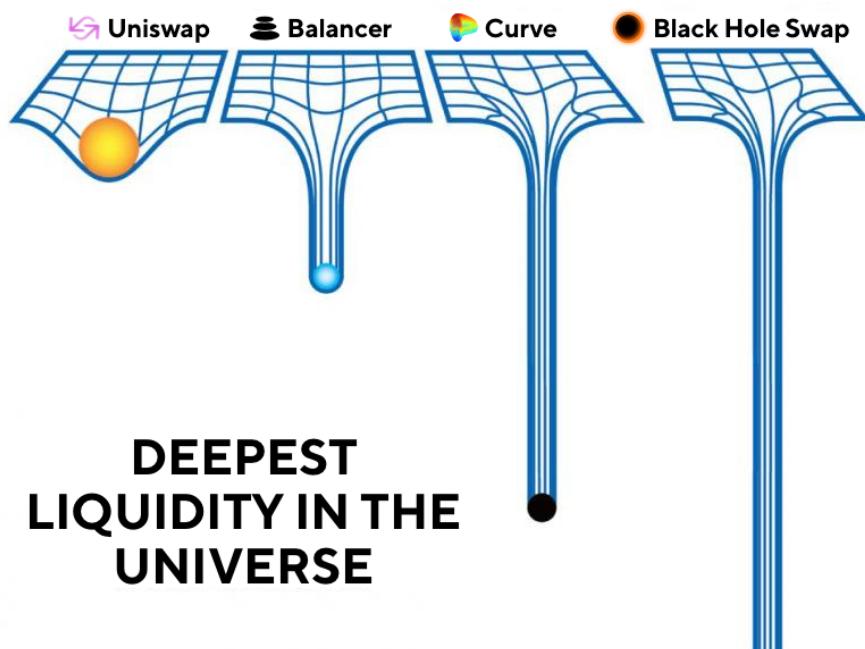
無限流動性的去中心化穩定幣交易所白皮書

Hakka Finance

July 31, 2020

## 摘要

BlackHoleSwap 是一個針對穩定幣設計、由演算法自動報價（Automated Market Making, AMM）的去中心化交易所（DEX）。BlackHoleSwap 最大的特色是允許系統擁有負數的存貨，藉由整合借貸協議的方式，抵押量多的幣，借出不足的幣，可以處理遠超過自身儲備的成交量。相比起其它 AMM，BlackHoleSwap 滑價超低，提供近乎無限的流動性，並極大化資金利用率。

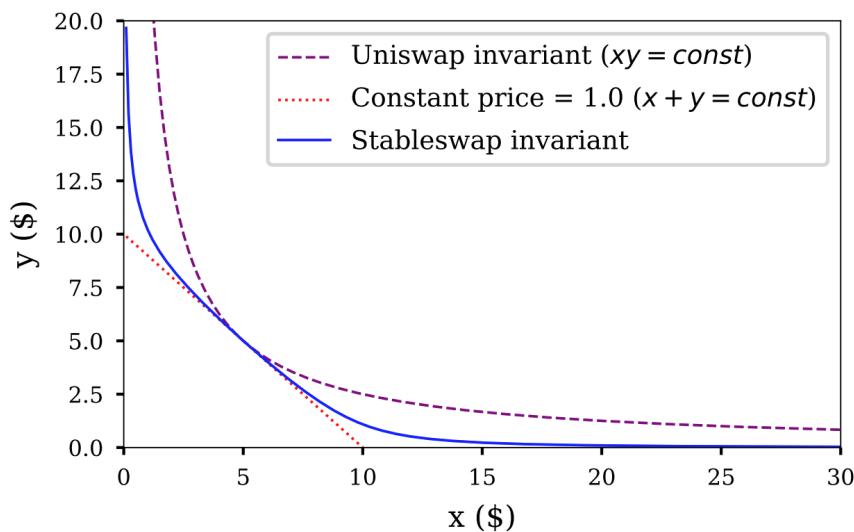


# 1. 背景簡介

經典的 AMM 如 Uniswap 是以「乘積固定」的方式提供兩種資產互換的報價，價格對存貨變化敏感，能廣泛使用在各種不同資產間的自動做市。但對於穩定幣間的交易而言，因為可以合理預期價差不大，使得 Uniswap 的固定乘積演算法顯得不夠有效率。

針對穩定幣的交換，Curve 提出了一個特化的模型，稱為「帶槓桿的 Uniswap」。Curve 使用的是一種介於恆定總量（匯率永遠是 1:1）和恆定乘積（Uniswap）之間的特殊公式。在同樣的資金量、同樣的差價下，Curve 能提供數十倍於 Uniswap 的流動性，同時兼具 Uniswap 永遠可以成交的特性。

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



不過，即便 Curve 提出的模型能在大部分情況下提供很好的穩定幣交易深度，一旦單邊的儲備接近耗盡時，仍會出現巨大的滑價。亦即，當一種穩定幣價格相對偏離時，流動性將迅速萎縮，表現甚至會比 Uniswap 更差，這是 Curve 為穩定幣特化所伴隨的副作用。

做為演算法式的去中心化交易所，Curve 本質上不脫 Uniswap 「儲備–報價–成交」的模式，受制於有限的存貨，總有流動性不足的時候。但是人類是不會安於現狀的，人類生來就要突破限制！

我們的 BlackHoleSwap 突破了 AMM 只能在自身儲備量下交易的限制，藉由整合去中心化借貸協議（Compound, dYdX 等），BlackHoleSwap 能提供超過自己儲備量、超低滑價、接近無限的流動性。

## 2. BlackHoleSwap 設計邏輯

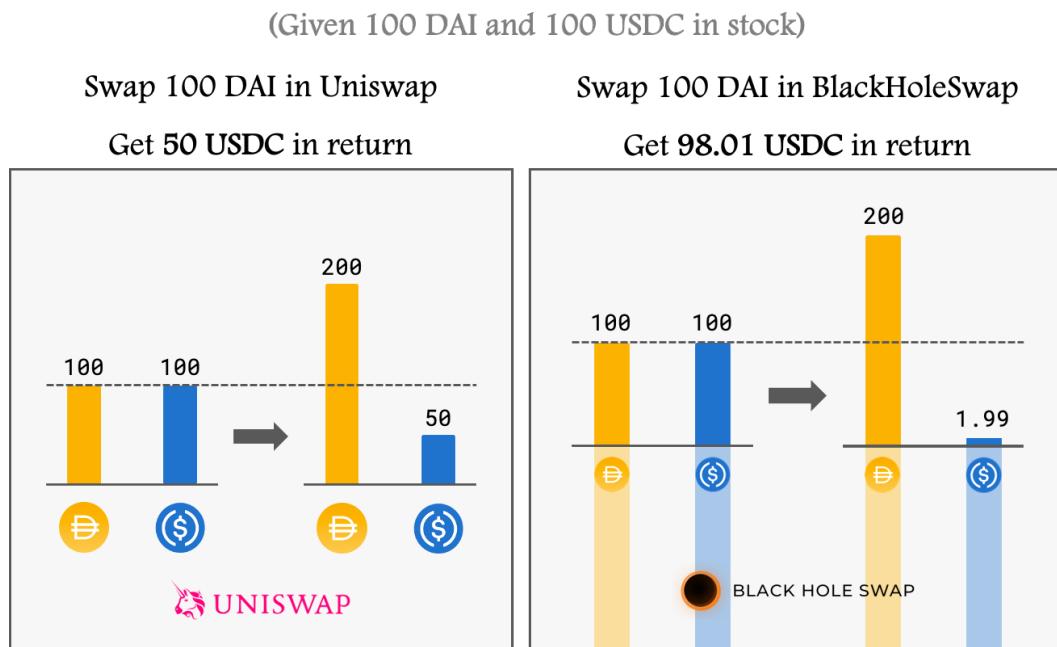
簡而言之，BlackHoleSwap 將儲備貨幣存入借貸平台，當交易對中其中一種貨幣的存貨耗盡，而市場仍有需求時，BlackHoleSwap 會以另一種貨幣做為抵押，從借貸平台中借出需求貨幣以完成交易。因此，BlackHoleSwap 不會受限於自身的存貨量，也就不會有像 Curve 那樣在存貨接近歸零時曲線「大轉彎」的問題。

概念上 BlackHoleSwap 和其他 AMM 相同，都需要在交易前後滿足某個不變量 (invariant)，而這個不變量的計算公式，會決定 AMM 的性質： $x + y = k$  交易價格恆定，但存貨可能被耗盡； $x \cdot y = k$  可以接受任意輸入，但價格對存貨變化敏感。而 BlackHoleSwap 得益於借貸平台，可以在保持低滑價的同時又無須擔心存貨耗盡。

### 3. BlackHoleSwap 的數學模型

在 Uniswap 的模型中，單筆交易對價格的影響程度取決於資金池的規模。同樣一筆買賣，資金池越大則滑價越小。BlackHoleSwap 於是在 Uniswap 既有的模型上加入「虛擬」的流動性，就像是沉水面下的冰山一樣，所以在同樣的「真實」資金量下，BlackHoleSwap 會有明顯較小的滑價，並且真實的資金水位可以降到低於零，也就是負存貨 / 負債。

下方範例為給定 100 DAI 與 100 USDC 存貨之交易對，並試圖用一倍的存貨量（100 DAI）來進行兌換之情形。在 Uniswap 中受限於乘積固定，只能兌回 50 USDC；而在 BlackHoleSwap 則受益於接近無限的虛擬庫存，將能兌回「98.01 USDC」！



底下的虛擬資金量取決於兩種幣的加總，再乘上一個槓桿倍數。

虛擬流動性  $S = x + y$ ，槓桿倍數  $A$

得到 BlackHoleSwap 公式：

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

上面的算式可以整理成

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

並且

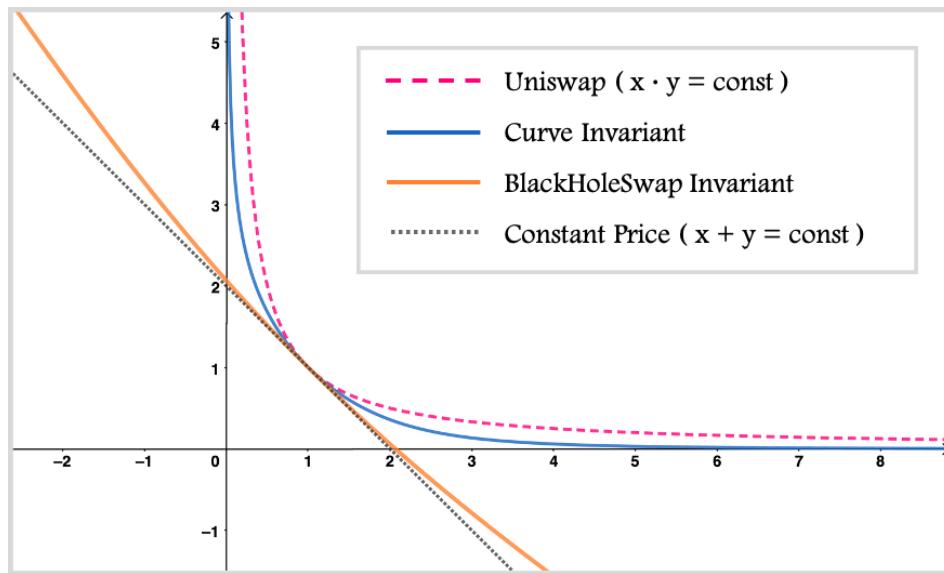
$$a = A/(A + 1), \quad 0 < a < 1$$

所以實際上 BlackHoleSwap 可以看做是對 Uniswap 做了一次線性變換，把原曲線投影到一個新的坐標系上：

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

## 參數選擇

觀察恆等公式會發現，當  $a = 0$  時 BlackHoleSwap 會退化成 Uniswap 的  $xy = K$ ，而當  $a = 1$  時則變成  $x + y = K$  的價格恆定模型。藉由調整參數  $a$ ，BlackHoleSwap（下圖橘色實線）會決定一個彎曲程度介於  $xy = K$ （粉色虛線）和  $x + y = K$ （黑色虛線）之間的曲線。

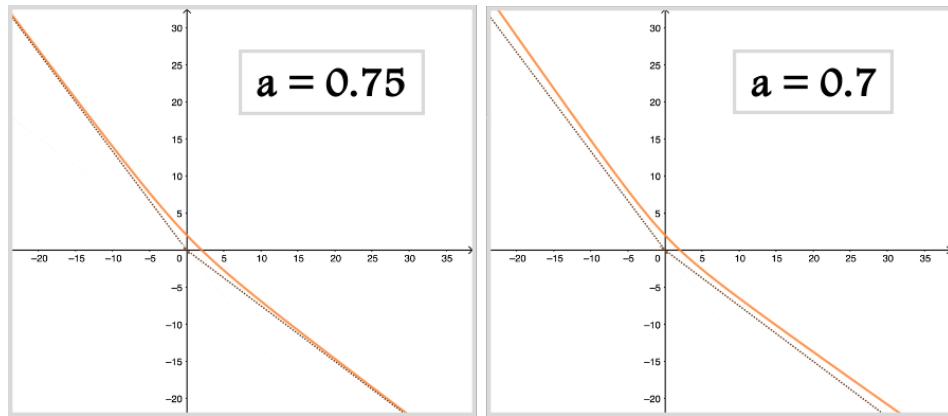


很明顯的，當  $a$  越接近 1 的時候曲線的斜率變化越小，也就是 BlackHoleSwap 的「效能」表現越好，但除了考慮效能，BlackHoleSwap 還要滿足來自外部的限制，也就是借貸平台本身的債務上限。

以 Compound Finance 為例，目前穩定幣 DAI 和 USDC 的抵押率（collateral factor）都被設定為 75%，也就是以 DAI 或 USDC 做為抵押所能借出的資金上限是 75%，否則會因為抵押品不足而借款失敗，甚至被清算，BlackHoleSwap 必須考慮到這一限制。

回到模型，因為 BlackHoleSwap 實際上是 Uniswap 的線性變換，所以其實它也繼承了一些 Uniswap 的特性。 $xy = K$  是一個雙曲線，漸進線分別是  $x$  軸和  $y$  軸，Uniswap 會無限接近於  $x = 0$  和  $y = 0$  但永不相交。同理可知 BlackHoleSwap 漸進到  $x + ay = 0$  和  $y + ax = 0$ ，而這正巧和借貸平台的規則類似。

當  $a = 0.75$ ，BlackHoleSwap 會達到理論上最有效率的狀態，恆定曲線會無限接近 75% 借貸上限，但不會真的碰到，在最為極端的情況下提供最好的交易流動性。



考慮到可能遭遇的各種情況，包括些許計算誤差，以及隨著時間負債產生的利息可能多於存款利息等，不能冒然把實際上線的 BlackHoleSwap 設定在最極端的  $a = 0.75$ ，必須要保留一些緩衝空間，否則攻擊者可以用「交易–等待–清算」的方式攻擊 BlackHoleSwap 套利。

一種緩衝的方法是將  $a$  設定成略小於 0.75 的值，這樣即便出現極端交易，曲線也不會太過靠近清算線。但  $a$  除了影響漸進線也會改變整個恆定曲線的形狀，設定成較小的  $a$  會讓 BlackHoleSwap 的表現變差。

另一種方法是設置負債率上限，不改變  $a$ ，而是在每次交易後檢查系統的負債率，並拒絕可能使負債率過高的交易。好處是不影響大部分的價格深度，但系統設定了硬上限，讓原本追求無限流動性的理念打了點折扣。

不過，畢竟實際上 BlackHoleSwap 總是不會有真正的無限流動性，最後仍舊受限借貸平台的總存貨，當 Compound 的 DAI 被借光，交易還是會失敗。所以評估過後 BlackHoleSwap 決定採用設置負債率的方式，目前將負債上限設為 62%。

## 4. 風險與損益

任何的造市商都承受一定的風險，而且通常滑價和手續費越低的造市者，因為價格波動虧損的機率/程度就越高。同樣使用 AMM，投在 Curve 的利用率高於 Uniswap 的同時，風險也較高。同理，BlackHoleSwap 也承受價格波動風險，且因為有借貸，還額外承受清算的風險。

從系統安全的角度評估，Uniswap 只對自己的程式碼漏洞曝險。而 Curve 和 BlackHoleSwap 因為深度結合借貸協議，如果遭遇底層借貸協議漏洞、oracle 失靈、抵押品擠兌等情形，上層的 AMM 同樣會受害，因此潛在的攻擊面會更廣。

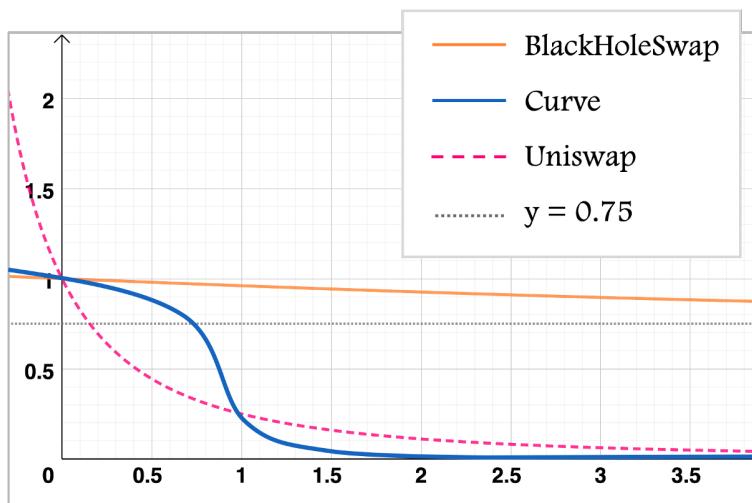
穩定幣 AMM	深度	價格波動損失	額外風險	資金利用效率
Uniswap	差	較低	無	很低
Curve	好 (price within 0.96~1.04)	較高	借貸協議 (ytoken, ctoken)	高
BlackHoleSwap	最好	較高	借貸協議 + 倉位清算風險	最高

清算風險可以靠設置負債上限檢查避免（同時也避免潛在的 flashloan 攻擊），如果需要的話，程式系統性風險也可以用保險減緩損失。然而，價格變化才是最無法規避，也是作為流動性提供者本來就該承受的風險。

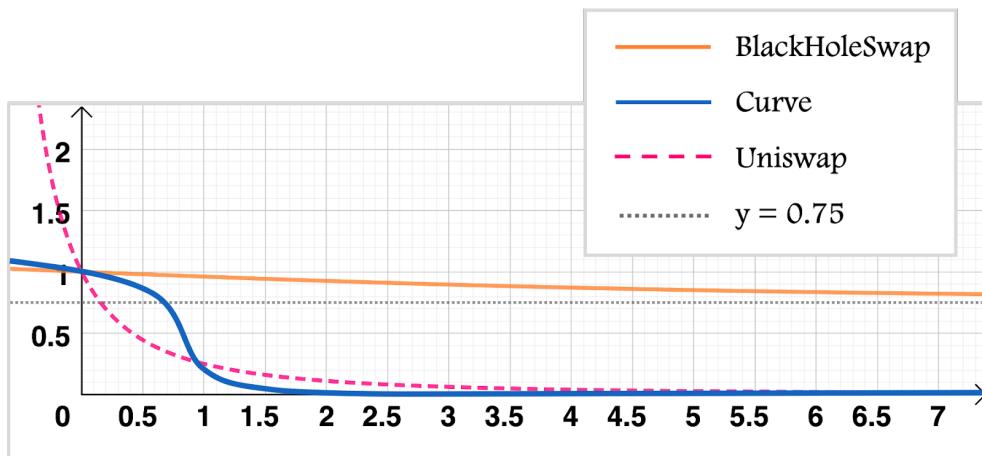
AMM 有很強的短板效應，也就是一個 AMM 的價值會否暴跌，取決於其成分資產中最弱的那一個，所以無論是 DAI 或 USDC 爆炸都會導致流動性提供者巨大虧損（遠不止於 50%）。

## 5. 效能分析

很明顯的，BlackHoleSwap 在提供穩定幣兌換上的表現遠優於 Uniswap。在 1:1 時單邊存入 1 倍初始資金可得 ~0.98 另一種貨幣。並且 BlackHoleSwap 的價格變化十分平緩，沒有 Curve 在流動性耗盡前價格驟降的現象。

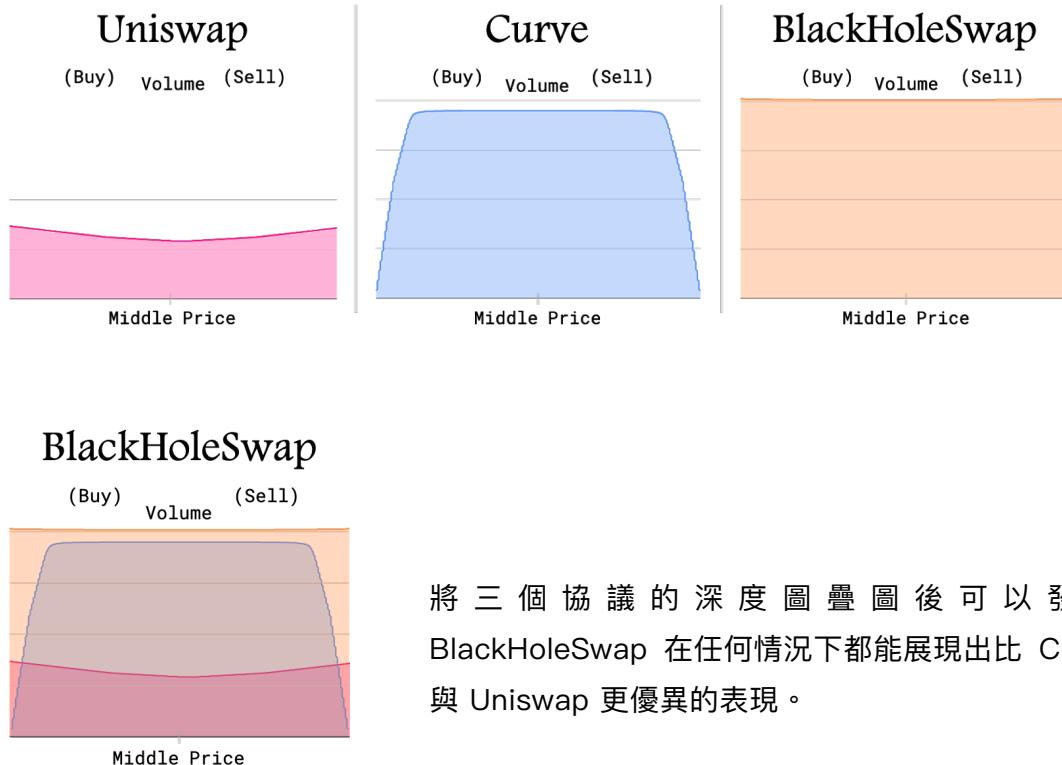


價格最後會趨近於 0.75，也就是交易的輸入用於抵押，輸出幾乎完全來自於借款。



## 深度圖

若將各個協議的深度圖（Order Book）進行比較，將如下圖所示，縱軸為存貨供應量、橫軸為價格，中間價以左為協議之購買價、以右為販賣價，著色區域面積為總供貨量。Uniswap 能提供的供應量較差，但在不同的價格區間都能提供一定量的流動性；Curve 則是將大量的流動性集中至中間價一帶，一但經過臨界價格，流動性將懸崖式崩落；BlackHoleSwap 則是在各個價位都能提供遠優於其它協議的穩定流動性。



將三個協議的深度圖疊圖後可以發現 BlackHoleSwap 在任何情況下都能展現出比 Curve 與 Uniswap 更優異的表現。

## 額外收入

BlackHoleSwap 現在選擇整合的借貸協議 Compound Finance 有「借貸挖礦」機制，發放協議代幣 Comp 級給存款人和借款人。BlackHoleSwap 在收到 Comp 之後會自動透過去中心化交易所換成穩定幣 DAI 或 USDC，直接滾入資金池，成為流動性提供者的收益。

## 6. 未來工作

### (1) 支援更多種類穩定幣

因為借貸協議的限制，BlackHoleSwap 目前僅能支援有限的穩定幣種。當 Compound Finance 或其它借貸協議支援更多穩定幣種作為抵押擔保品時，BlackHoleSwap 將會上架更多的穩定幣交易對。

### (2) 將「黑洞」應用至其它 AMM 模型

BlackHoleSwap 本質上來說是將 Uniswap 的模型進行一次線性轉換而成。因此，經過審慎地分析後，相似的線性轉換機制應也能應用至其它自動造市模型，生成 BlackHoleCurve、BlackHoleBalancer 等去中心化協議。