Uniswap 简明导论

怀菁

武汉大学

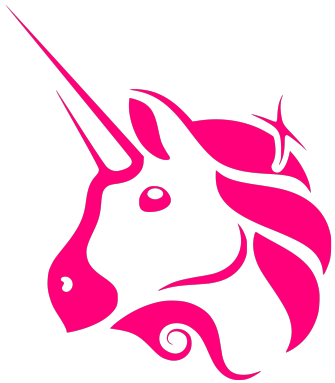
2023 年 12 月 3 日

这是什么?


1h
Compare
Indicators
WhaleFarm Token/WHALE · 1h · BSC_DEXGURU O0.1048456 H0.1178463 L0.1048456 C0.1133138 +0.0084682 (+8.08%)
Volume 33.78
260.0000000
240.0000000
220.0000000
200.0000000
180.0000000
160.0000000
140.0000000
120.0000000
100.0000000
80.0000000
60.0000000
40.0000000
20.0000000
0.1133138
-20.0000000
24
25
26
27
28
29
30
Jul
1y 1m 7d 1d 12h Default
19:02:17 (UTC)
% log

Uniswap 简介

- 一个去中心化交易协议
- V1 上线时间：2018 年 11 月 2 日
- 恒定积自动做市商
- 去中心化交易所的奠基者和领军者



中心化交易所的订单簿

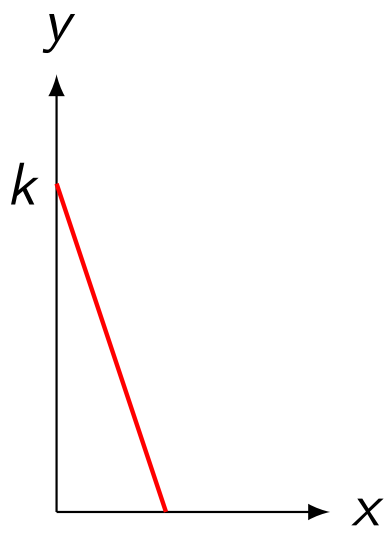

委托订单
最新成交
交易数据
信息
买
卖
1
12.07931 26,356 26,357 2.51519
2.30609 26,355 26,358 2.36092
2.77333 26,354 26,359 0.40391
3.00399 26,353 26,360 6.52676
2.83194 26,352 26,361 4.42732
1.34397 26,351 26,362 2.36782
5.21894 26,350 26,363 1.78910
6.16264 26,349 26,364 5.20883
1.12558 26,348 26,365 2.73296
1.36137 26,347 26,366 3.86532
1.19242 26,346 26,367 1.95022
2.75670 26,345 26,368 8.69570
1.32159 26,344 26,369 0.93633
8.49353 26,343 26,370 3.36002
0.79166 26,342 26,371 2.47049
更多
预警
杠杆
网格
买入
卖出

例子：可乐自动售货机

- 机器中有 x_0 瓶可乐与 y_0 枚一元硬币
- 一瓶可乐 3 元
- 交易若干次后，机器中有 x 瓶可乐与 y 枚一元硬币

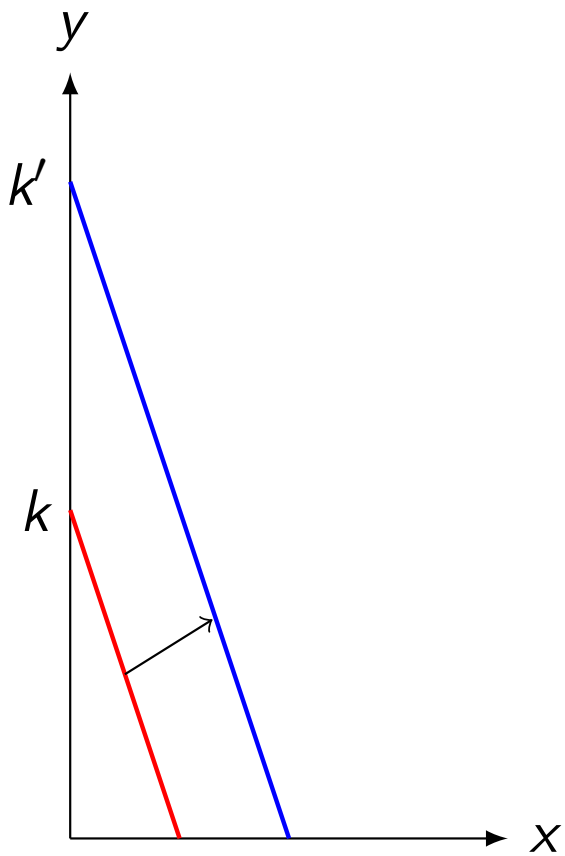
$$3x + y = 3x_0 + y_0 \tag{1}$$

设 $k = 3x_0 + y_0$ ，有 $y = -3x + k$



为可乐交易所添加流动性

向交易所中投放更多的可乐和硬币，得到 $k' > k$



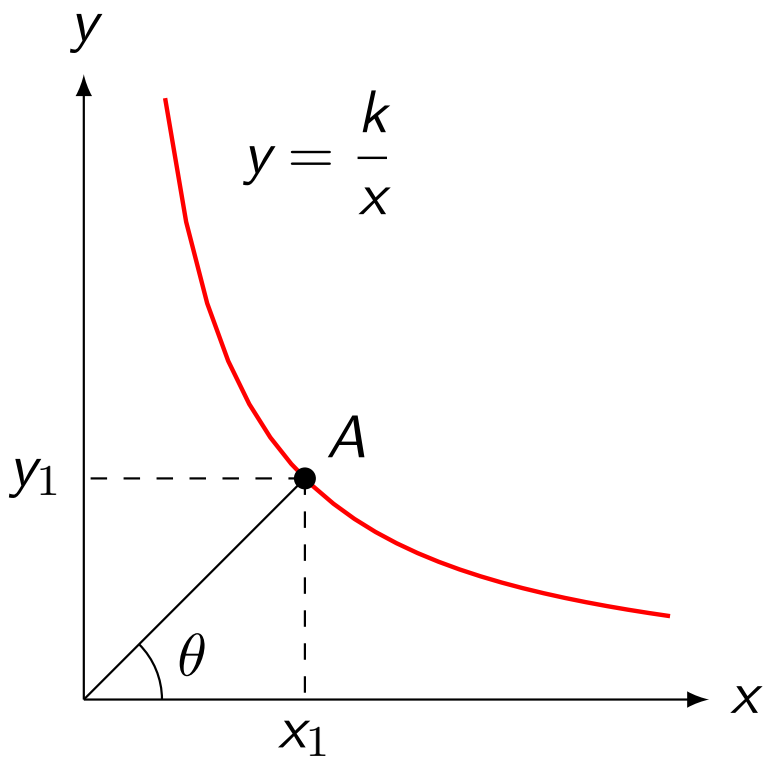
这个可乐交易所就是一个**恒定和自动做市商**（CSAMM）

Uniswap 恒定积自动做市商

- X：计价货币（Quote Currency）
- Y：基准货币（Base Currency）
- Y/X：交易对
- x_0：X 的储备量
- y_0：Y 的储备量

$$xy = k \tag{2}$$

$$p_X = \frac{y_1}{x_1} = \tan\theta \tag{3}$$



图：Y/X 交易对储备图

交易改变价格

假设交易者用 Δx 个货币 X 购买一些货币 Y

$$x' = x_0 + \Delta x$$

$$x'y' = k \tag{4}$$

$$y' = \frac{k}{x'} = \frac{k}{x_0 + \Delta x} < y_0 \tag{5}$$

交易者买到的 Y 的数量即为

$$\Delta y = y_0 - y' = y_0 - \frac{k}{x_0 + \Delta x} \tag{6}$$

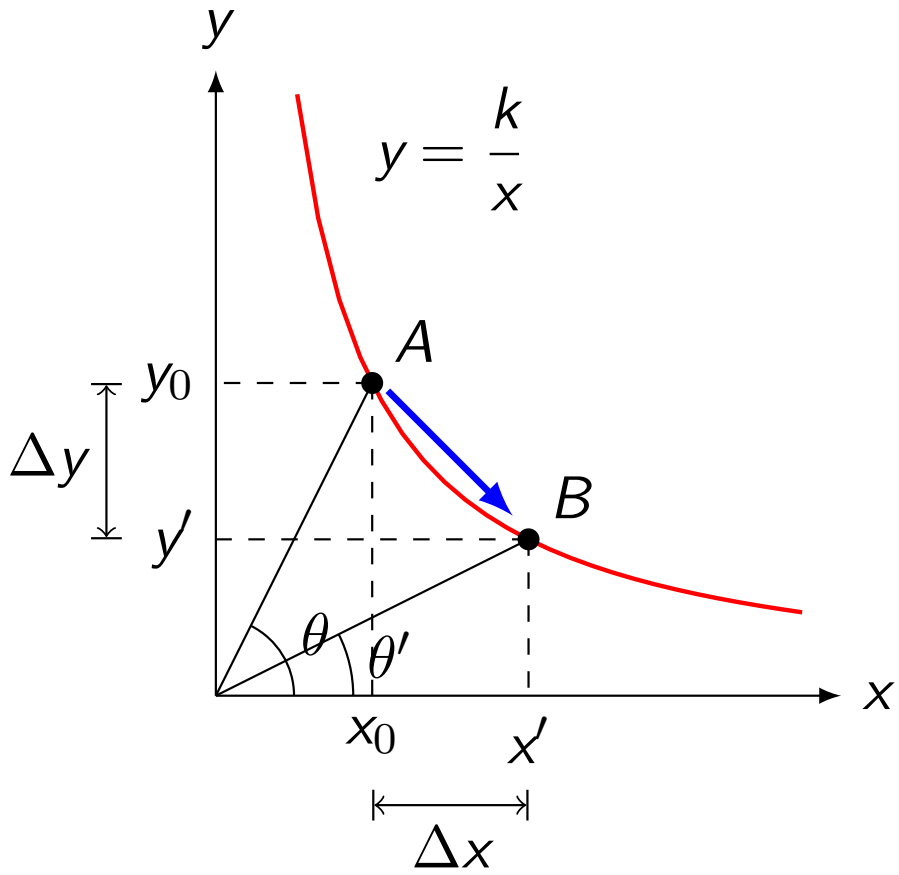


图: 交易改变了价格

添加或移除流动性

流动性提供者（Liquidity Provider）为流动性池提供资金，并赚取交易手续费。

$$x' = x_1 + x_2, y' = y_1 + y_2$$

$$k' = x'y'$$

那么新的恒定积公式就是

$$xy = k'$$

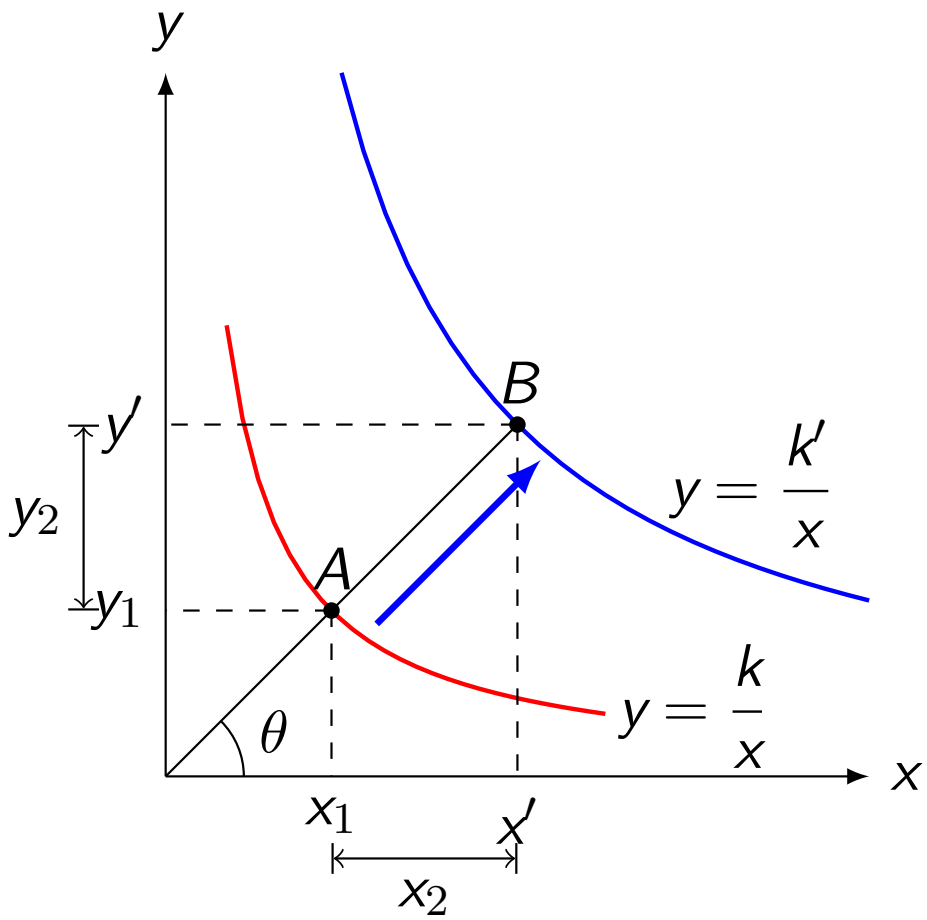


图: 添加流动性引起储备曲线缩放

添加流动性的好处

- 降低交易者的滑点（Slippage）

$$\left|\frac{\Delta x}{\Delta y}-\frac{x_0}{y_0}\right|=\left|\frac{\Delta x}{y_0}\right| \tag{7}$$

- 减弱价格推动效应

$$|p'_X-p_X|=\left|\frac{x_0y_0}{(x_0+\Delta x)^2}-\frac{y_0}{x_0}\right|=\left|\frac{2x_0y_0\Delta x-y_0(\Delta x)^2}{x_0(x_0+\Delta x)^2}\right| \tag{8}$$

收益分配的依据：流动性代币

流动性代币（Liquidity Token）是一种特殊的代币，它衡量了 LP 对流动性池的贡献。它是所有者权益的凭证，或者简单理解为流动性池的股票。

- LP 存入 X 和 Y 时，流动性池铸造一种名为“YX”的代币发送给 LP
- LP 将 YX 发送至流动性池销毁掉，就可以按份额提取出自己的 X 和 Y

对于第一位 LP，其获得的流动性代币数量为

$$s = \sqrt{x_0 y_0} \tag{9}$$

对于之后的 LP，其获得的流动性代币数量为

$$\Delta s = \frac{x_1}{x_0} s_0 = \frac{y_1}{y_0} s_0 \tag{10}$$

并使用 $s_0 \leftarrow s_0 + \Delta s$ 更新 s_0 的值

风险 1：流动性不足——三明治攻击

	价格	数量
卖 2	1.2	1
卖 1	0.9	1

订单簿中的三明治攻击：经纪商买入 -> 经纪商挂卖单 -> 交易者买入

日期	类型	价格 USD	全部的	价格 ETH	金额 BTC2I	共计 ETH	保留无翻译	其他
Oct 10 22:00:11	sell	$0.0003525	$21.01	0.0₆2239	59,608.5	0.0133	0xae...ae13	2
Oct 10 22:00:11	buy	$0.0002377	$1,573.93	0.0₆1510	6,620,244	1.00	0x9b...5f67	1
Oct 10 22:00:11	buy	$0.0001583	$9.43	0.0₆1006	59,608.5	0.0060	0xae...ae13	2

AMM 中的三明治攻击：攻击者买入 -> 交易者买入 -> 攻击者卖出

- 都是依靠自己的单边信息优势，获取无风险利润
- 提高流动性可以使这种攻击无利可图

风险 1：流动性不足——撤池跑路

撤池跑路（Rug Pull）是指 LP 突然撤出全部的流动性使交易者无法再交易的行为

锁仓可以降低 Rug Pull 风险

风险 2：无常损失

- 恒定积自动做市商存在着“劣币驱逐良币”的倾向
- 这意味着更有价值的货币将持续流出
- 而劣币的占比和绝对数额将会提高
- LP 可能因此受到财产损失

$$\begin{cases} X/USD = a_0 \\ Y/USD = b_0 \\ Y/X = \dfrac{x_0}{y_0} \\ x_0 y_0 = k \end{cases} \rightarrow \begin{cases} X/USD = a_1 \\ Y/USD = b_1 \\ Y/X = \dfrac{x_1}{y_1} \\ x_1 y_1 = k \end{cases} \tag{11}$$

$$r = \frac{B_1}{B_0} = \frac{a_1 x_1 + b_1 y_1}{a_0 x_0 + b_0 y_0} = \frac{\sqrt{a_1 b_1}}{\sqrt{a_0 b_0}} \tag{12}$$

$$r^* = \frac{B^*}{B_0} = \frac{a_1 x_0 + b_1 y_0}{a_0 x_0 + b_0 y_0} \tag{13}$$

风险 2：无常损失

无常损失（Impermanent Loss）是由于流动性池中两种代币的**相对**价格变化导致的、相较于单纯持有代币的机会损失

$$
\begin{aligned}
\delta &= r - r^* \\
&= \frac{a_1(x_1 - x_0) + b_1(y_1 - y_0)}{a_0 x_0 + b_0 y_0} \\
&= \frac{2\sqrt{a_1 b_1} - \left(a_1\sqrt{\frac{b_0}{a_0}} + b_1\sqrt{\frac{a_0}{b_0}}\right)}{2\sqrt{a_0 b_0}} \\
&\leq \frac{2\sqrt{a_1 b_1} - 2\sqrt{a_1\sqrt{\frac{b_0}{a_0}} \cdot b_1\sqrt{\frac{a_0}{b_0}}}}{2\sqrt{a_0 b_0}} \\
&= \frac{2\sqrt{a_1 b_1} - 2\sqrt{a_1 b_1}}{2\sqrt{a_0 b_0}} \\
&= 0
\end{aligned}
\tag{14}
$$

当且仅当 $a_1\sqrt{\frac{b_0}{a_0}} = b_1\sqrt{\frac{a_0}{b_0}}$

即 $\frac{a_0}{b_0} = \frac{a_1}{b_1}$ 时取等号

- 也就是说只要相对价格与初始相对价格不一致，就会产生无常损失
- 而当二者回归一致时，无常损失就为 0

风险 2：无常损失

当 $a_0 = b_0$ 时，无常损失的图像与 $z = 0$ 平面相切于 $y = x$ 直线

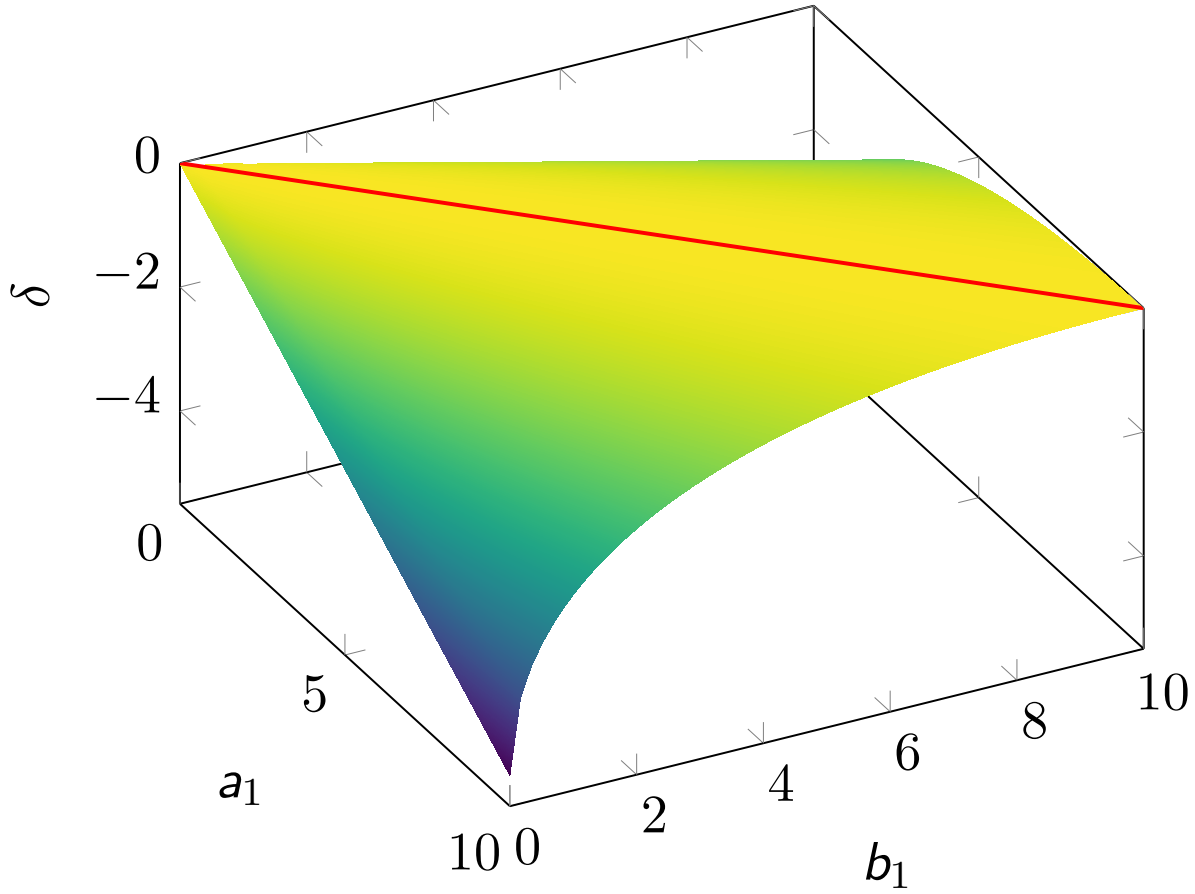


图: 无常损失 δ 图像

风险 3：诈骗、假币与洗钱犯罪

任何人都可以创建假的 USDT 、BTC 和 ETH 代币并建立流动性池

利用 Uniswap 进行洗钱犯罪难以追查

风险 4：价格预言机失灵

- 预言机（Oracle）使得链上合约可以读取链下信息，比如某个代币的价格
- 因为套利者的存在，Uniswap 可以扮演价格预言机，但早期版本容易被操纵
- V2 更新：在每一个区块开始就计算并确定报价，此后的交易改变实时价格，但不再改变报价，从而保证报价的相对稳定性

风险 5：黑客攻击

- 屎山代码，bug 连篇
- 留下后门，监守自盗
- Uniswap V2 将存放资金的“核心合约”与实现其他功能的“边缘合约”分隔开，从而最小化攻击面

新特性：集中流动性

缩小价格值域，只给某一个区间提供流动性，而不是整个正实数域

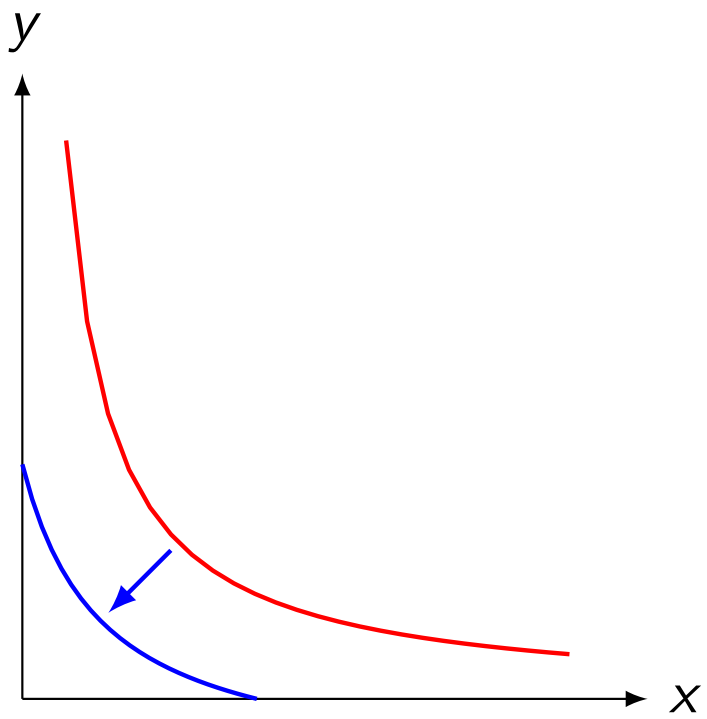
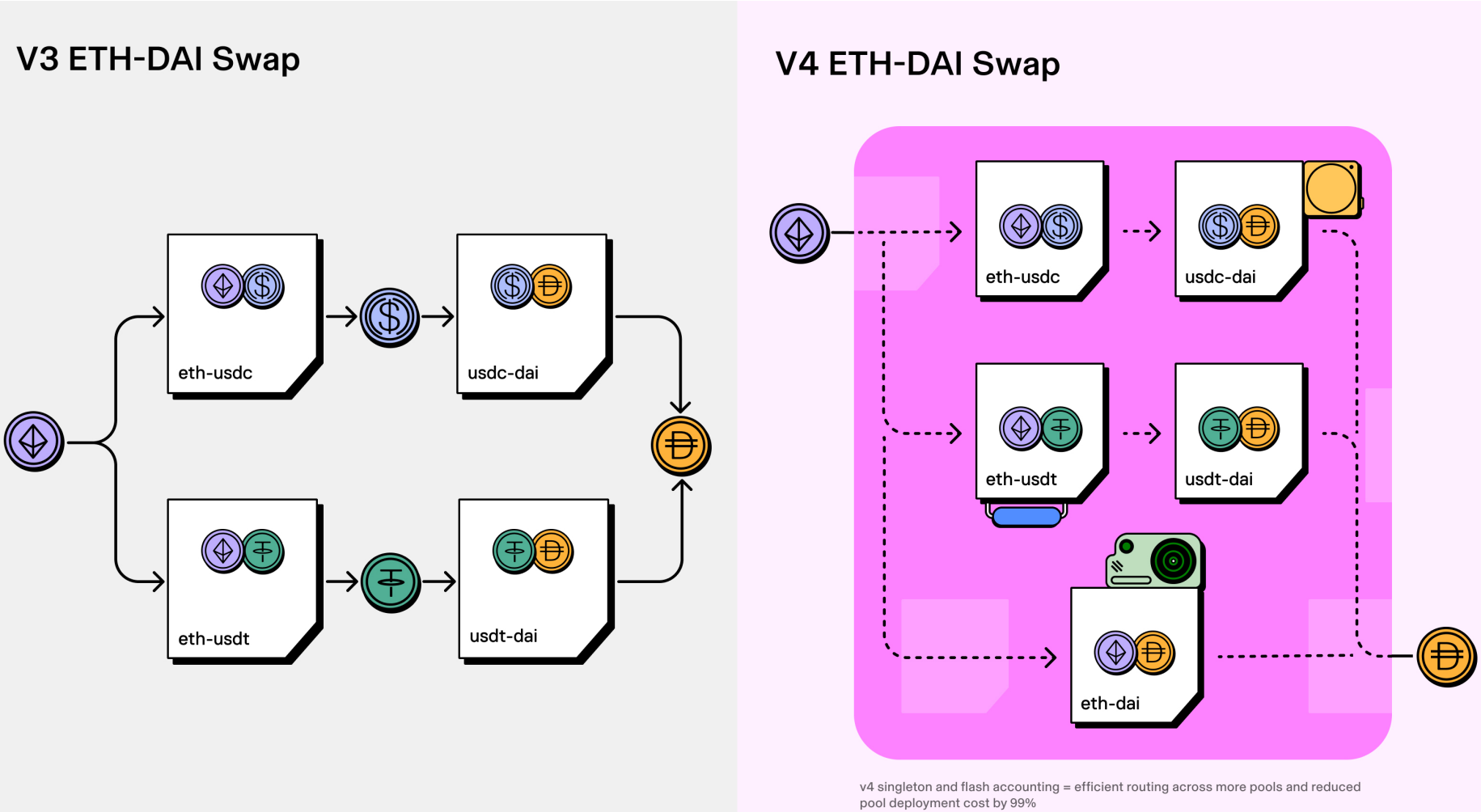


图: 集中流动性使储备曲线平移

新特性：单例和闪电记账

- 单例（Singleton）：使用一个合约管理链上所有的流动性池
- 闪电记账（Flash Accounting）：多重交换的过程只需要支付资金进出系统的两次 gas fee



新特性：挂钩

- 挂钩（Hooks）：一个与流动性池相匹配的外部合约，其中实现了当流动性池在特定时间检查是否满足特定条件，并执行相应操作
- 特定时间包括：初始化、调整持仓、交换和支付的之前和之后

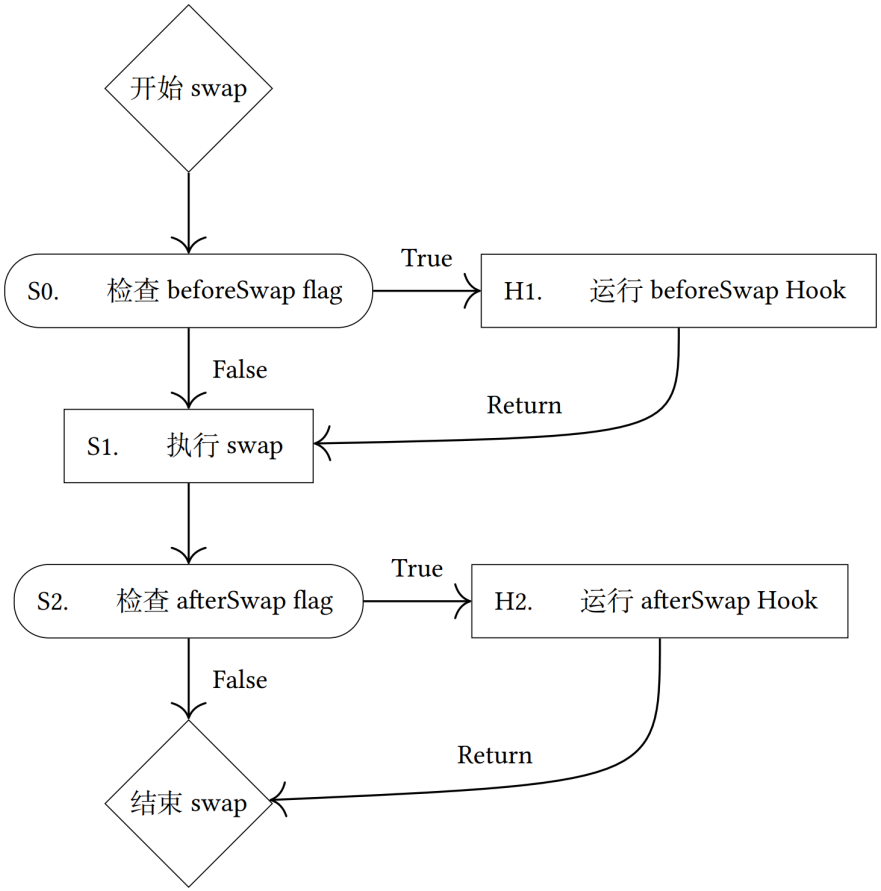


图: 挂钩示意图

结论与思考讨论

1. 了解了 Uniswap 的利弊之后，你是更愿意选择中心化交易所还是去中心化交易所？为什么？
2. 交易费过高会提升交易者的交易成本，过低又会打击 LP 的积极性。你认为什么水平的交易费才是最合适的？你是根据什么原则来确定交易费水平的？
3. 在你看来，相较于旧版的多池，单例模式是否违背了 Web3 去中心化的核心价值观？用一个合约管理所有的流动性池会造成多大的风险？这种风险相比于它带来的方便性是值得我们去承担的吗？
4. 从宏观经济角度来看，为了保持交易所的流动性，社会总是需要在流动性池中锁定一笔价值不菲的资金。在你看来，这笔资金应当被视为储蓄还是投资？假如一个实力雄厚的巨鲸（或者称之为“政府”）向流动性池注入大笔资金，会对经济系统造成什么影响？
5. 你认为还有哪些值得思考的问题？

Thanks for Listening!