

# Uniswap 简明导论

怀菁

武汉大学

2023 年 10 月 14 日

# 这是什么？



- 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



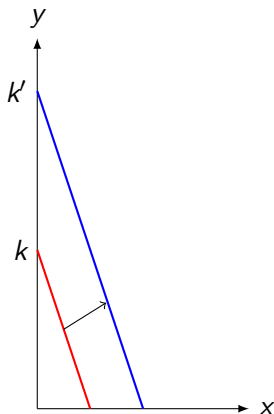
# 中心化交易所的订单簿





# 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

$$xy = k \quad (2)$$

$$p_X = \frac{y_1}{x_1} = \tan \theta \quad (3)$$

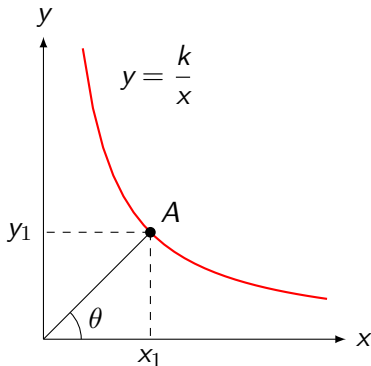


图: Y/X 交易对储备图

# 交易改变价格

假设交易者用  $\Delta x$  个货币 X 购买一些货币 Y

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

$$x'y' = k \quad (4)$$

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

交易者买到的 Y 的数量即为

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

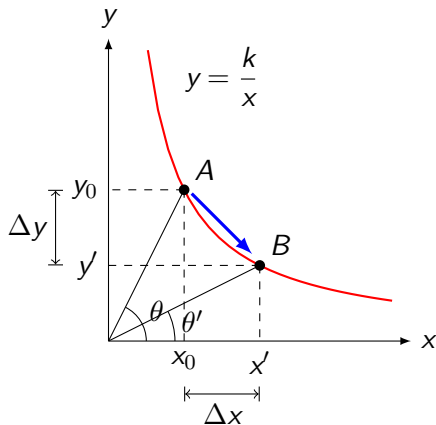


图: 交易改变了价格



# 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

$$xy = k'$$

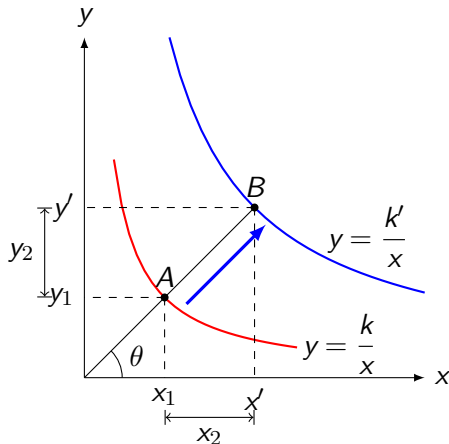


图: 添加流动性引起储备曲线缩放

# 添加流动性的好处

- 降低交易者的滑点 (Slippage)

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

- 减弱价格推动效应

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

# 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

$$s = \sqrt{x_0 y_0} \quad (9)$$

对于之后的 LP，其获得的流动性代币数量为

$$\Delta s = \frac{x_1}{x_0} s_0 = \frac{y_1}{y_0} s_0 \quad (10)$$

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 BTC21 ▾	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 红	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 红	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

$$\begin{cases} X/USD = a_0 \\ Y/USD = b_0 \\ Y/X = \frac{x_0}{y_0} \\ x_0 y_0 = k \end{cases} \rightarrow \begin{cases} X/USD = a_1 \\ Y/USD = b_1 \\ Y/X = \frac{x_1}{y_1} \\ x_1 y_1 = k \end{cases} \quad (11)$$

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

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

## 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

$$\begin{aligned}\delta &= r - r^* \\ &= \frac{a_1(x_1 - x_0) + b_1(y_1 - y_0)}{a_0x_0 + b_0y_0} \\ &= \frac{2\sqrt{a_1b_1} - \left(a_1\sqrt{\frac{b_0}{a_0}} + b_1\sqrt{\frac{a_0}{b_0}}\right)}{2\sqrt{a_0b_0}} \\ &\leq \frac{2\sqrt{a_1b_1} - 2\sqrt{a_1\sqrt{\frac{b_0}{a_0}} \cdot b_1\sqrt{\frac{a_0}{b_0}}}}{2\sqrt{a_0b_0}} \\ &= \frac{2\sqrt{a_1b_1} - 2\sqrt{a_1b_1}}{2\sqrt{a_0b_0}} \\ &= 0\end{aligned}\tag{14}$$

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

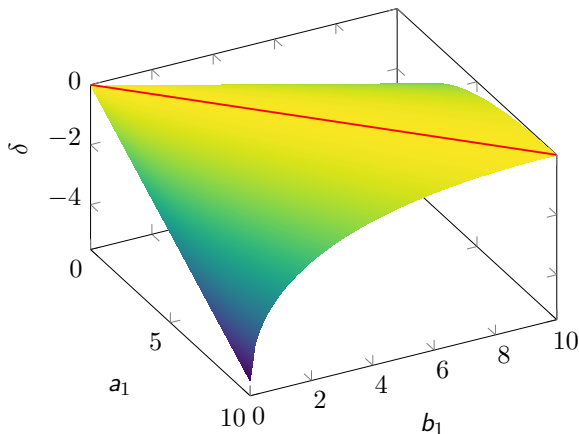


图: 无常损失  $\delta$  图像



## 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

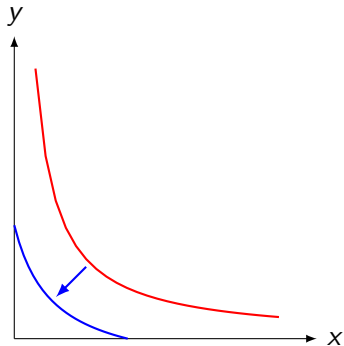
- 预言机 (Oracle) 使得链上合约可以读取链下信息，比如某个代币的价格
- 因为套利者的存在，Uniswap 可以扮演价格预言机，但早期版本容易被操纵
- V2 更新：在每一个区块开始就计算并确定报价，此后的交易改变实时价格，但不再改变报价，从而保证报价的相对稳定性

# 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

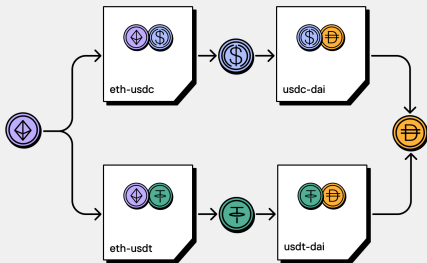


图：集中流动性使储备曲线平移

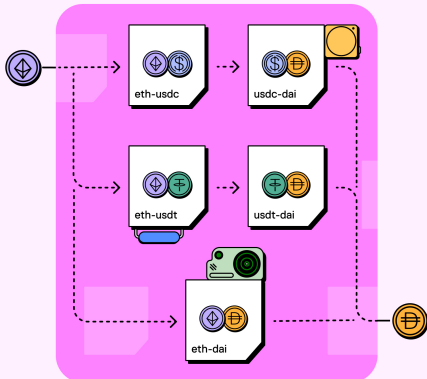
# 新特性：单例和闪电记账

- 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

V3 ETH-DAI Swap



V4 ETH-DAI Swap



v4 singleton and flash accounting = efficient routing across more pools and reduced pool deployment cost by 99%

# 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

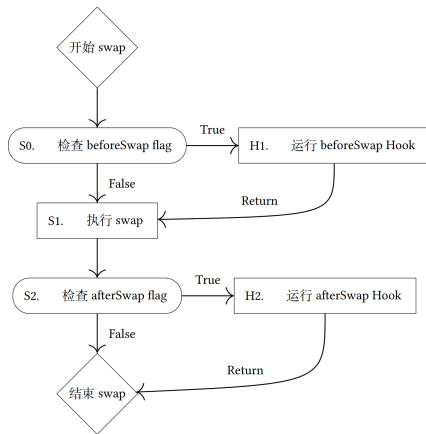


图: 挂钩示意图

# 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!*