Uniswap 简明导论

Splendor White

2023 年 10 月 10 日

1 简介

Uniswap 是以太坊区块链上的一个去中心化交易所。它既表现出与传统中心化交易所不同的特性，又是去中心化交易所的典型代表。了解其基本运行机制，是认识去中心化金融的基础。

与传统的中心化交易所不同，Uniswap 的交易不需要订单簿，而是由自动做市商根据恒定乘积公式对流动性池进行动态调整，满足交易者的交易需求。流动性提供者可以向流动性池中添加流动性，降低交易者的滑点，并按照份额赚取流动性费用。

Uniswap 是一个不断发展的交易协议。在 Uniswap V2 中，任意交易对、安全的价格预言机、闪电兑等功能得以实现。在 Uniswap V3 中，集中流动性的引入大大提高了资金利用率。在即将上线的 Uniswap V4 中，挂钩、单例、闪电记账等新元素使得合约可以更加灵活地定制化。

2 从订单簿到自动做市商

2.1 订单簿

在传统的金融交易过程中，一部分买者和卖者需要在一个公共的**订单簿**（Order Book）上给出自己的买进报价（Bid）或卖出报价（Ask），这类交易者被称为挂单者（Maker）。其他的买者和卖者可以在订单簿中找到自

已心仪的报价，并付给相应的商品或货币，从而完成交易，这类交易者被称为吃单者（Taker）。如图 1 所示。

图 1: 订单簿示意图

这种交易方式能够确定每一笔订单的成交价格和成交数量，并使得市场深度一目了然。但其流动性是不稳定的，市场深度有时大有时小。而且，由于所有的挂单信息都是公开的，市场操纵者可以根据这些信息使用一定数量的资金来将价格瞬间调整到自己想要的水平。

在订单簿模式下，如果挂单者寥寥无几，成交就会变得异常困难。有没有办法让交易者（无论是买者还是卖者）在任意时刻都能够轻松成交呢？**自动做市商**（Automatic Market Maker）实现了这一点。

2.2 自助售货机

为了理解自动做市商，我们可以先以自助售货机作为一个例子。

考虑一个 24 小时不停工作的可口可乐售货机，里面存放着若干瓶可口可乐和一些零钱。当你想要购买一瓶可乐的时候，你需要将钱放入售货机中，然后售货机就会弹出一瓶可乐。现在，让我们将这个模式推广一下——假设你用某种手段（e.g. 走私或者自制）搞来一些符合质量要求的可口可乐，来到自助售货机面前，希望将可乐卖成零钱。你需要做的就是将可口可乐放入自助售货机中，然后售货机就会将相应的零钱付给你。这样，我们就拥有了一个可口可乐交易所。

假设最开始机器中有 x_0 瓶可乐与 y_0 枚一元硬币，并约定一瓶可乐的价格是 3 元。经过若干次交易之后，机器中有 x 瓶可乐与 y 枚一元硬币。很显然，我们有下面的恒等式：

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

这意味着，**留在机器中的可乐价值与硬币价值的总和是一个定值**，我们设 $k = 3x_0 + y_0$ ，于是有

$$3x + y = k \tag{2}$$

将这个式子化为 $y = -3x + k$ ，并画出其函数图像，我们得到一个一次函数（如图 2 所示）。

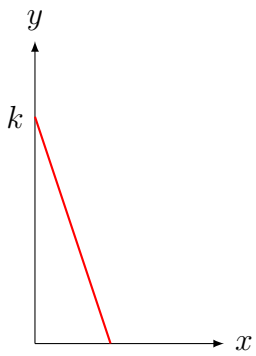

图 2: 可乐交易所储备图

然而，我们可能会遇到这样的窘境：我们一次性想要买的可乐太多了，机器里的可乐根本不够；或者我们一次性想要卖的可乐太多了，机器里的钱根本不够。这其实就是流动性问题。

传统金融中的**流动性**（Liquidity）是指资产可以迅速、容易地被买卖或兑换成现金的能力。流动性本来是每种资产的特性，例如，我们认为现金的流动性最大，存款、国债、股票、劳动力的流动性次之，而房产、工厂、机器设备的流动性相对而言就小得多，因为我们很难将这些资产变成现金。

在去中心化金融中，流动性的概念发生了一定的改变。笔者认为，Uniswap 中的流动性可以被定义为一个交易对将一定规模的某种资产以很低的成本转换为另一种资产的能力。

解决流动性问题的办法是显然的，我们只需要在机器中额外地投放更多的可乐或硬币即可。投放更多的可乐与硬币，使得机器的总价值从 k 变为 k'，其中 $k' > k$。于是恒等式 (2) 变为

$$3x + y = k' \tag{3}$$

相应的函数图像变为

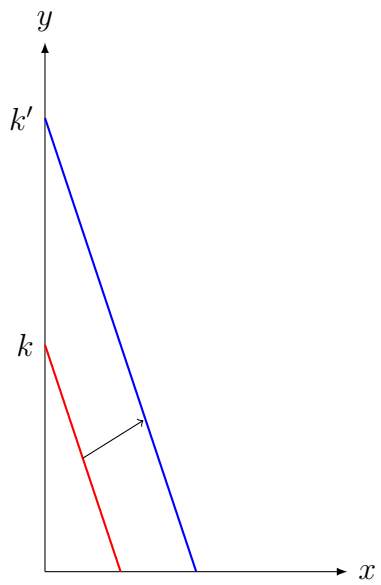

图 3: 添加流动性后的可乐交易所

通过投放可乐或硬币，自助售货机就可以完成更大规模的交易。我们将这种行为称为**添加流动性**。

这个自助售货机，或者说可口可乐交易所，其实就是用一个**恒定和自动做市商**（Constant-Sum Automatic Market Maker, CSAMM）完成了交易

过程，为买者和卖者提供了方便的交易服务。交易所的流动性越大，买者和卖者就能完成越大规模的交易。

2.3 Uniswap 的恒定积做市商

可口可乐交易所的例子非常简明，但是它的弊端十分明显——可乐的价格是不能变化的。在真正的金融市场上，资产价格应当随着供求关系的变化产生波动。

我们假设有人用货币 X 和货币 Y 一起建立了一个**交易对**（Pair），记作 X/Y ，使得任何人都可以使用一种资产交易另一种资产。在这里，我们称 X 为**基准货币**（Base Currency），称 Y 为**计价货币**（Quote Currency）。

Uniswap 为两种资产建立起一个**流动性池**（Liquidity Pool），其中储备有若干 X 和 Y。设 X 的储备数量为 x ，Y 的储备数量为 y ，这两个量是变量。

Uniswap 使用**恒定积自动做市商**（Constant-Product Automatic Market Maker, CPAMM）实现可变的价格。设建立流动性池的人向池中加入 x_0 个 X 和 y_0 个 Y ，设其乘积为 $k = x_0 y_0$ 。如果不添加或移除流动性，自动做市商控制恒定积公式

$$xy = k \tag{4}$$

恒成立，也就是说 x 与 y 的变化始终成反比例关系，保持其乘积是定值。

x 与 y 相对数量的变化反映了价格（汇率）的变化，而 xy 的变化反映了流动性大小的变化。我们将在下面的一节中详细介绍。

3 CPAMM 的经济原理

3.1 价格与储备量的关系

首先需要声明的是，在笔者看来，价格与汇率并无本质区别。通俗意义上说，价格是一种特殊的汇率，是以法币或稳定币作为计价货币的汇率。生活在传统金融和 Web2 中的人们更倾向于使用美元、人民币、USDT 等来

作为通用的计价货币，因为这些货币往往有权威背书，购买力相对稳定。这样固然会让讨论问题变得更加方便，但其实也会导致我们束手束脚。

在 Defi 中，我更希望抛弃这样一个垄断了标价权的货币，允许用各种货币作为计价货币。这样，汇率与价格便统一起来。两种货币的汇率，就是以其中一种货币为单位而表示的另一种货币的价格。

在 CPAMM 中，**基准货币的价格就是两种货币储备量之商的倒数**。体现在储备图上，价格就是储备线上某点与原点连线的斜率。

结合图 4，我们可以用数学语言表示，在状态 A 下

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

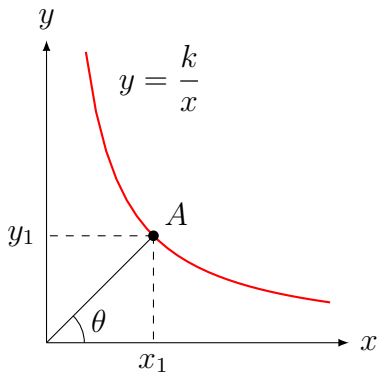

图 4: X/Y 交易对储备图

很显然，如此得到的价格的值域是 $(0, +\infty)$ ，符合实际情况。

读者很可能产生一个疑问：为什么以 Y 为单位 X 的价格能够被表达为 $\frac{y_1}{x_1}$ ？这就是 Defi 的精妙之处。对此，我有两种方式做出解答。

第一种解释是将流动性池看做整个市场的缩影。也就是说，在整个市场上流通着的 X 和 Y 数量之比，就等于流动性池中的 X 与 Y 数量之比。虽然他们数量的绝对大小不同，但比值是相等的。如果人们更加认可 X 的价值，将 X 贮藏起来而不花出去，那么就会使得流通中的 X 数量减少，其价格也就会升高。对于 Y 而言，这条规则同样适用。如果我们认为货币都是平等的，那么数量之商（无论是局部的还是整体的）就是表现人们对货币价值评价的最佳变量。

第二种解释是，CPAMM 能够比较完美地履行以 $\frac{y_1}{x_1}$ 为价格进行交易的职能。我们将在下一节中详细了解这一机制。

有些人认为，CPAMM 的运行完全是依赖于人们的共识、依赖于套利者才能够与其他中心化交易所的价格相锚定。这种观点是片面的。不可否认，套利对于维护去中心化交易所的正常报价至关重要，但这种解释其实是否定了 CPAMM 本身的内在价值，认为 Defi 只不过是完全依附于传统金融的赌场。如果我们继续深入理解 CPAMM ，便会明白，它的价值不是来源于一群信徒的幻想，而是来源于其自身的经济规律。

3.2 改变价格

现在激动人心的时刻来了。我们即将见证，CPAMM 究竟是如何在以特定价格完成交易的同时引起价格变化从而反映供求关系的。

我们假设初始状态下流动性池中有 x_0 个货币 X 和 y_0 个货币 Y 。某个交易者准备用 Δx 个货币 X 购买一些货币 Y。流动性池收到了这 Δx 个货币 X，现在总共有 $x' = x_0 + \Delta x$ 个货币 X。为了满足恒定积公式恒成立，新的 Y 储备量 y' 应该满足

$$x'y' = k \tag{5}$$

解得

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

显然有 $y' < y_0$ 。实际上，交易所会将一笔数量为

$$\Delta y = y_0 - y' = y_0 - \frac{k}{x_0 + \Delta x} \tag{7}$$

的货币 Y 发送给交易者。这样，一笔交易就完成了。

首先，让我们从交易者的角度来研究，他的这笔交易是否合他的心意。交易者卖掉了 Δx 个货币 X ，买来了 Δy 个货币 Y 。如果初状态下价格 $p_X = \frac{y_0}{x_0}$ ，这笔买卖是不是按照价格进行的呢？通过下面的计算我们可以发现，如果交易量相对于流动性池巨大的储备量而言微乎其微，那么这笔交易就是按照价格进行的。

$$\begin{aligned}\frac{\Delta x}{\Delta y} &= \frac{\Delta x}{y_0 - \frac{k}{x_0+\Delta x}} \\ &= \frac{\Delta x(x_0+\Delta x)}{y_0(x_0+\Delta x) - x_0 y_0} \\ &= \frac{x_0+\Delta x}{y_0} \\ &\approx \frac{x_0}{y_0} = p_X\end{aligned} \tag{8}$$

如果交易量较大以至于相对于流动性池储备不可忽略，交易者可能会承受多余的成本，这就是去中心化交易所中的**滑点**（Slippage）。关于滑点的细节，我们将在下一节详细介绍。

接下来让我们从交易所的角度来研究，这笔交易如何改变价格以反映供求关系的变化。交易完成后新的价格 p'_X 满足

$$\begin{aligned}p'_X = \frac{y'}{x'} &= \frac{x_0 y_0}{(x_0+\Delta x)^2} \\ &< \frac{x_0 y_0}{x_0^2} = \frac{y_0}{x_0} = p_X\end{aligned} \tag{9}$$

这意味着新的价格比旧的价格更低。实际上这不难理解。交易者卖出 X 而买入 Y，实际上是增加了对 Y 的需求与对 X 的供给。货币 X 供过于求导致价格下降，在代数上就体现为 $p'_X < p_X$。

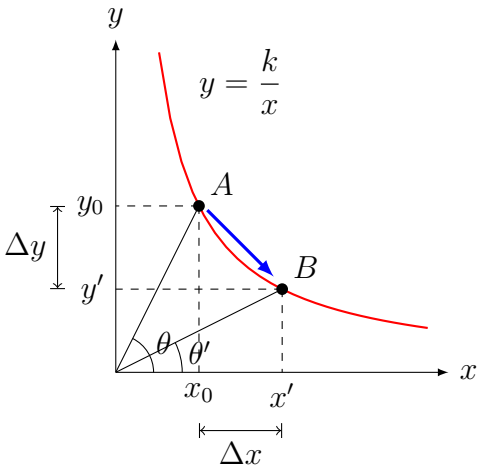

图 5: 交易改变了价格

图 5 是对这笔交易的夸张化演绎。通过几何方法，我们也可以由 $\tan\theta' < \tan\theta$ 得出价格下降了。

一次交易可能并不会对价格产生显著的影响，但是诸多交易者的合力将会共同组成一只看不见的手，推动价格朝着特定方向持续演化，直到形成新的均衡。

交易使得流动性池的状态从 A 点移动到 B 点，改变了交易对的价格，但没有改变储备曲线本身。

3.3 改变流动性

通过前面的例子，我们发现，除了 x 和 y，流动性 k 的大小也是值得研究的对象。

流动性过小有诸多危害：较高的滑点导致交易者付出更高成本，巨鲸可以很轻松地掏空流动性池引起价格剧烈变化，价格对交易过于敏感导致难以精确反映供求信息，交易者减少交易量导致流动性提供者收益下降……

为了鼓励**流动性提供者**（Liquidity Provider, LP）向流动性池中注入更多资金，Uniswap 协议为每一个交易对设定了一个交易费（通常是 0.3%），作为给 LP 的报酬。交易者向流动性池放入的资金先扣除这一笔交易费，剩余的资金再根据恒定积公式进行交易。交易费将转化为新的流动性，持续累积在流动性池中，直到 LP 决定移除流动性为止。这其实就是一种全自动的再投资。

流动性相关的知识可谓是博大精深，我们这里只讨论两个非常简单的问题：添加或移除流动性会发生什么，以及 LP 的收益是如何分配的。

当第一位 LP 向流动性池存入第一笔资金时，此交易对的价格就由这笔资金中两个货币的数量决定。显然，第一位 LP 不能随心所欲地按照任意比例存入资金。如果其中任意一种货币在市场上已经存在了一个价格，那么 LP 必须尊重这个价格并严格按照这个价格确定存入资金的比例，否则就存在套利空间。如果两种货币都没有已经确定的价格，第一位 LP 存入资金的比例就决定了开盘价。

我们假设第一位流动性提供者存入了 x_0 个货币 X 和 y_0 个货币 Y，而且这个价格并不存在套利空间，并设 $k_0 = x_0 y_0$。交易者付出交易费引起再投资，k 会缓慢地增大，但我们先忽略这一点，假设不存在交易费。

若干次交易之后，流动性池中有 x_1 个货币 X 和 y_1 个货币 Y，且依然满足 $x_1y_1 = k$。这时，第二位 LP 决定向流动性池中加入 x_2 个货币 X 和 y_2 个货币 Y。显然，他必须保证 $\frac{x_1}{y_1} = \frac{x_2}{y_2}$，否则就会存在套利空间。

我们设 $x' = x_1 + x_2, y' = y_1 + y_2$，新的恒定积可由 $k' = x'y'$ 计算得出，新的恒定积公式为

$$xy = k' \tag{10}$$

显然 $k' > k$。

公式 (10) 和公式 (4) 是同一形式、不同规模的反比例函数。在图像上，我们可以发现，新的储备曲线是由旧的储备曲线以原点为中心放缩得到的。

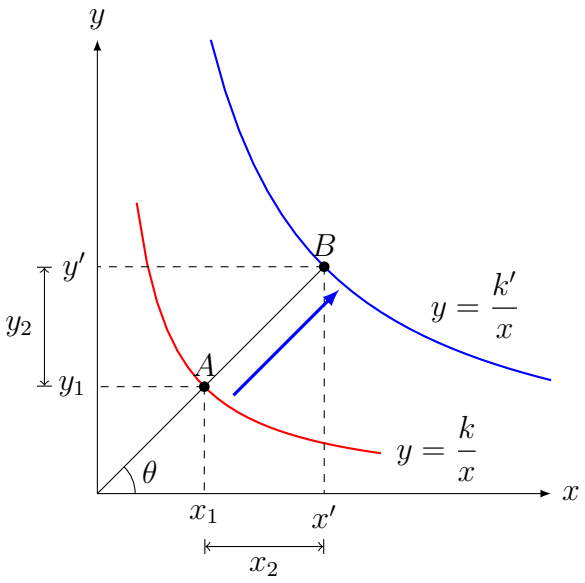

图 6: 添加流动性引起储备曲线放缩

反之，如果 LP 移除一部分流动性，那么变化方向就与上图相反。

添加或移除流动性使得流动性池的状态从 A 点移动到 B 点，使得储备曲线以原点为中心放缩，但没有改变价格。

在继续深入学习之前，我们先岔开话题，讨论一下为什么一定价格条件下对于确定规模的交易，流动性越大，滑点就会越小，交易引起的价格变化也越小。

视 Δx 为外生变量，滑点用价差 $\left|\frac{\Delta x}{\Delta y}-\frac{x_0}{y_0}\right|$ 表示，价格变化用 $|p'_X-p_X|$ 表示，于是有

$$\left|\frac{\Delta x}{\Delta y}-\frac{x_0}{y_0}\right|=\left|\frac{\Delta x}{y_0}\right| \tag{11}$$

当 y_0 增大时，这个值显然会减小。

$$|p'_X-p_X|=\left|\frac{x_0y_0}{(x_0+\Delta x)^2}-\frac{y_0}{x_0}\right|=\left|\frac{2x_0y_0\Delta x-y_0(\Delta x)^2}{x_0(x_0+\Delta x)^2}\right| \tag{12}$$

这个分式的分子是一个二次多项式，分母是一个三次多项式，当 x_0, y_0 同比例增大时，分式的值显然会减小。

除了代数证明，也可以使用几何方法证明这两个规律，请读者自行尝试。

下面让我们回到正题，了解流动性代币与收益分配的机制。

一个流动性池可能有多个 LP ，我们往往需要按他们的贡献分配收益，这样才能保证公平公正。一位 LP 提供的流动性越多，最终获得的收益就越大。

为了把这个机制量化，我们引入了**流动性代币**（Liquidity Token）。流动性代币是一种特殊的代币，它衡量了 LP 对流动性池的贡献。用传统金融的术语来解释，它可以被视为所有者权益的凭证，或者简单理解成流动性池的股票。

当 LP 向流动性池添加流动性时，交易所会铸造一定数量的流动性代币发送给 LP 。当 LP 决定移除流动性时，他便可以将一定数量的流动性代币发送给交易所并赎回自己的份额，交易所将这一部分流动性代币销毁。

对于第一位 LP ，若其存入了 x_0 个货币 X 和 y_0 个货币 Y ，Uniswap 使用公式

$$s=\sqrt{x_0y_0} \tag{13}$$

计算其初始份额，也就是流动性代币数量。

对于第二位及以后的 LP ，若流动性池中已经有 x_0 个货币 X 和 y_0 个货币 Y ，已经铸造的流动性代币总量为 s_0 ，某位 LP 存入了 x_1 个货币 X 和 y_1 个货币 Y （无套利），Uniswap 使用公式

$$\Delta s = \frac{x_1}{x_0} s_0 = \frac{y_1}{y_0} s_0 \tag{14}$$

计算本次添加流动性铸造出的流动性代币数量，并使用 $s_0 \leftarrow s_0 + \Delta s$ 更新总的份额值。

提取流动性时，某位 LP 向流动性池发送数量为 Δs 的流动性代币，自动做市商销毁这些代币，并将 Δx 个货币 X 和 Δy 个货币 Y 从流动性池中取出，发送给 LP ，其中 $\Delta x = \frac{\Delta s}{s_0} x_0, \Delta y = \frac{\Delta s}{s_0} y_0$ 。

这样的计算方式能够保证不存在无风险套利机会。无论价格怎样变化，各个 LP 的贡献总是得到了公平公正的评估，最终收益分配也是公平公正的。

4 Uniswap 的相关风险

4.1 流动性不足

现阶段，Uniswap 的流动性问题再怎么强调都不为过。前文已经提及，如果资金池的流动性不足，交易者会承受过大的滑点。这里我们再将相关危害拓展一下，探讨另外两个话题：三明治攻击和撤池跑路。

在传统金融市场中，抢先交易（Front Running）往往被认为是一种市场操纵行为。交易者向经纪商发送交易请求后，经纪商可以根据掌握的信息进行套利。下面是一个例子。

假设交易者委托经纪商以 1 美元购入 1 支股票，此时订单簿状况为

	价格	数量
卖 2	1.2	1
卖 1	0.9	1

在真实的 Defi 交易市场上，时间不是连续的，而是离散的，这是区块链的特性决定的。一笔交易往往是随着其他许多笔交易一起在同一个区块中处理。假如在一个区块中，两个交易者都针对同一个交易对发出了交易广播，那么这两笔交易的先后顺序就会影响各自交易的实际价格。如果交

易者 A 先于交易者 B 完成购买，那么价格就会被推高，交易者 B 购买时获得的实际价格就会高于期望价格，承受更大的滑点。

矿工可以在公共内存池中自由地选择若干笔交易并进行任意排序，而矿工自己也可以发送交易广播。如果矿工发现。

4.2 无常损失

4.3 诈骗与假币

4.4 价格预言机失灵

4.5 黑客攻击

监守自盗