

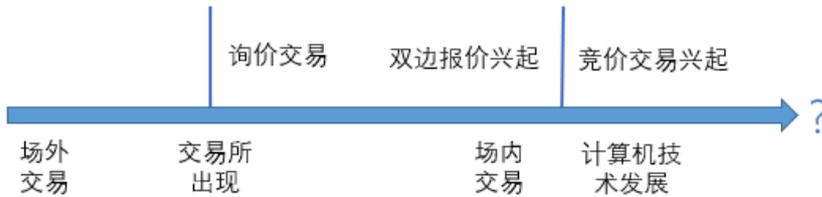
欧科云链研究院：金融市场交易的范式革命

--- 自动做市商制度 (AMM)

1900 年，英国物理学家汤姆生在皇家学会发表了一场著名的演讲。他在回顾物理学所取得的伟大成就时说，“物理大厦已经落成，所剩只是一些修饰工作，只不过出现了两朵令人不安的乌云。”汤姆生的演讲代表了 19 世纪末物理学界的主流思潮：经典物理学基础牢固，臻善臻美，往后难有作为。但汤姆生很可能没有想到的是，两朵小乌云随后带来了狂风暴雨，经典物理学大厦被瞬间颠覆，物理学由此进入了以相对论和量子力学为基础的新时代。

百年后的 2020 年，金融市场上正在发生同样的事情。交易制度一直是金融市场顺利运行的重要基础。经过 200 多年的发展，金融市场从最初的询价交易制度发展到后来的做市商交易制度，再到 20 世纪 80 年代以来电子信息技术的快速发展下兴起的竞价交易制度，金融市场呈现出丰富纷繁的交易制度。

■ 图 1. 金融市场交易制度的演变



资料来源：欧科云链研究院

很多市场人士认为，目前的金融市场交易制度已经趋近成熟，稳定于“询价、报价、竞价”三种交易制度，难以再生产新型的交易制度。但 2020 年横空出世的 DeFi（去中心化金融）项目 Uniswap，却采用一种新的交易范式：基于区块链智能合约的 AMM（Automated Market Maker，自动做市商）。

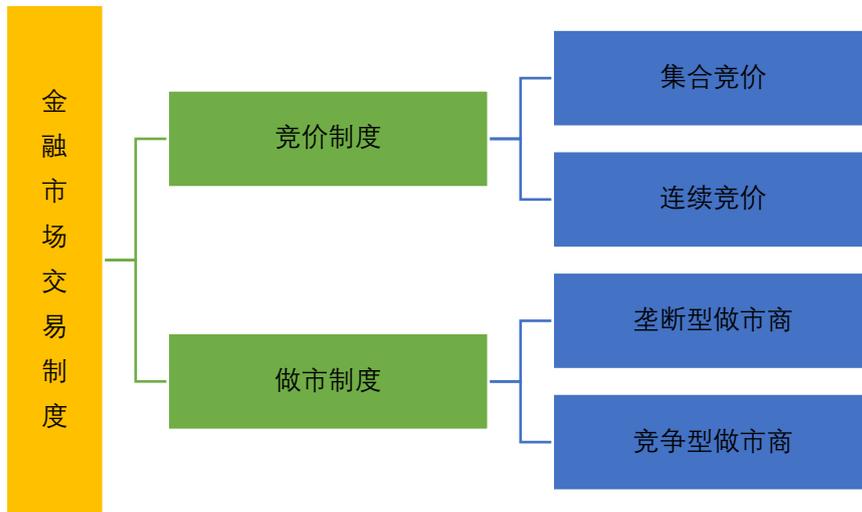
一、金融市场交易的范式革命---自动做市商 (AMM)

范式 (paradigm) 一词是由美国著名科学哲学家托马斯·库恩提出，库恩认为只有导致

科学革命，使科学获得一个全新的面貌的一套理论体系才能被称之为范式，而自动做市商（AMM）很明显属于此类。因为自动做市商制度（AMM）不仅仅只是实现了交易自动化，无人化，更重要的是它为金融市场引入了一种全新的交易方法和理念，是从“0 到 1”的创新。

想要理解 AMM 带给金融市场的变革，需要先了解现有的金融市场交易制度。经过近两百年的发展，尤其是自上世纪 70 年代的信息技术革命以来，金融市场目前有两种主要的交易制度：竞价制度和做市商制度。

■ 图 2. 金融市场现有交易制度

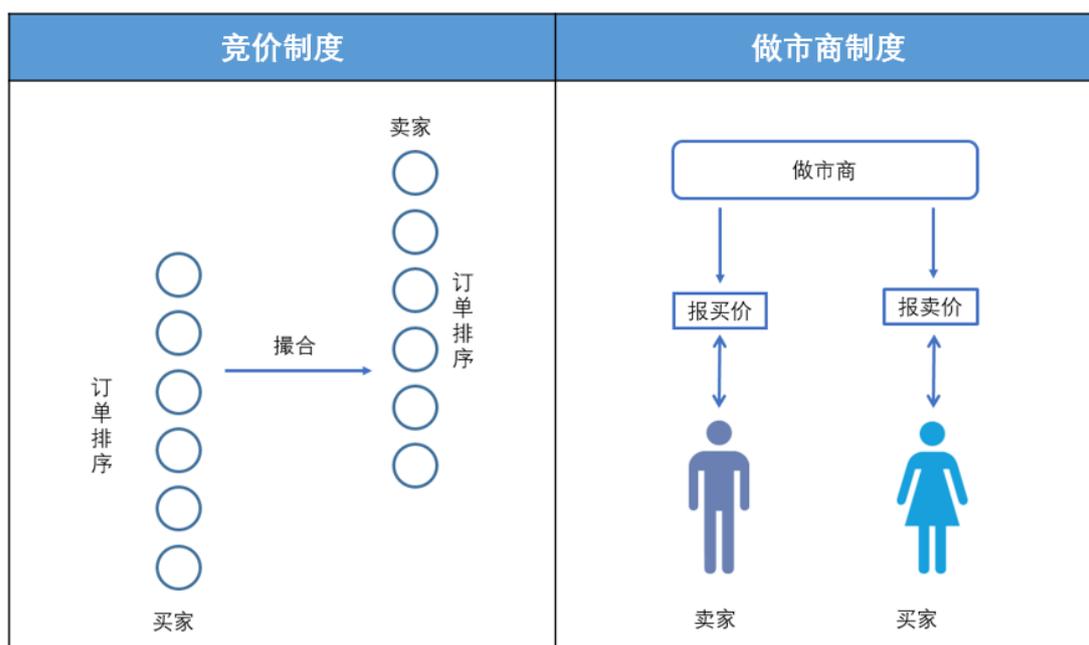


资料来源：欧科云链研究院

首先是竞价制，竞价交易是市场买卖双方直接进行交易（或委托给代理经纪商），在市场的交易中心以买卖双向价格为基准，按“价格优先”、“时间优先”等规则进行撮合达成交易的一种制度。因为价格由买方订单和卖方订单共同驱动，所以又称指令驱动制度。竞价制又分为集合竞价和连续竞价，其中在集合竞价制中，交易的买卖分时段性，是在某一规定的时间，将不同时点收到的订单集中起来进行匹配成交；而连续竞价制度，则是在各个时点连续不断地进行交易，只要存在两个相匹配的订单，交易就会发生。

其次是做市商交易，又称为双边报价交易，是指以报价商为市场的价格维护人，报价商向市场同时报出买价和卖价，市场的买家和卖家根据报价与之成交，而买家和卖家之间不直接成交的交易组织模式。该交易方式依赖做市商的报价来完成买卖，所以又称报价驱动制度。做市商制度又分为垄断型做市商制度和竞争型做市商制度，前者的由交易所指定一个券商来负责某一股票的交易，后者则是每一种股票同时由多个做市商负责。

■ 图 3. 竞价制度和做市商制度示意图



资料来源：欧科云链研究院

无论是竞价制度还是做市商制度，两者依赖订单簿（Order Book），即需要将订单挂至订单簿上，以价格作为信号进行交易。在竞价制度中的要求撮合是按最有利于交易双方的价格买卖资产；同样地，做市商制度中要求做市商必须事先报出买卖价格，而投资人在看到报价后才能下达交易委托。

■ 图 4. 竞价制度下的订单簿示意图



资料来源：欧科云链研究院

然而，以 Uniswap 为代表的去中心化交易所则采用了一种全新的交易制度---不需要订单簿，也不需要交易对手方（做市商），即可完成资产的自动交易兑换。这神奇的交易模式背后仅仅是依赖一个简洁的数学模型： $x * y = k$ ，其中 x ， y 分别代表需要交易的两种资产的数量，而 k 是一个固定的常数。因此这类自动做市商又被称为常数函数做市商（constant function market makers，简称 CFMM）。

一般而言，CFMM 中包括三类参与方，如下表所示。在这三类参与方中，最重要的角色是流动性提供者（LP），负责向 Uniswap 的智能合约中注入自己的资产，作为资产储备池，为交易提供流动性，并以此获取交易费用收益。其次是套利者，他们负责修正交易价格，保证交易价格与市场价格一致，但也会产生无常损失（Impermanent Loss），给流动性提供者带来亏损的风险。

■ 表 1. AMM 制度下的三类参与方

角色名称	功能
交易者	用一种资产交换另一种资产
流动性提供者	将自己的资产注入储备池，为交易提供流动性，获得一定费用
套利者	让资产价格保持与市场价格一致，以赚取一定利润

资料来源：欧科云链研究院

我们以 Uniswap 中资产 A 和资产 B 的交易为例。在交易开始前，我们需要向区块链的智能合约中注入 x 数量的资产 A 和 y 数量的资产 B 来作为流动性储备，即在公式 $x*y=k$ 中， x ， y 和 k 的初始值由流动性提供者（LP）确定。因为资产 A 和资产 B 之间的初始价格 $P = x / y$ ，所以当第一个流动性提供者（LP）把自己认为等价值的资产 A 和资产 B 充值到此智能合约中，就可以实现初始价格 P 的设置。

假如一个交易者想用 m 个资产 A 购买一定数量的资产 B（忽略交易手续费，在实现中，这部分交易手续费将保留在资产池中并成为流动性提供者的收益），为此他需要向 Uniswap 的智能合约发送 m 个资产 A。为了保证 k 值不变，那么智能合约需要向投资者支付 n 个资产 B，即

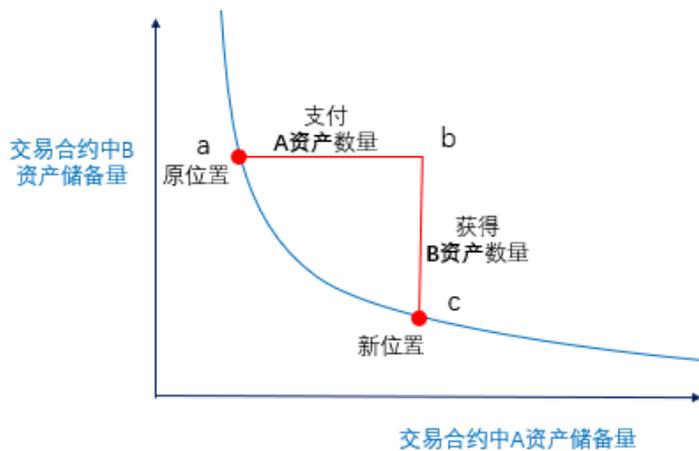
$$(x + m) * (y - n) = k \quad (1)$$

$$n = y - \frac{k}{x + m} \quad (2)$$

公式 (2) 即决定了支付给交易者的资产 B 数量 n。

从图像上看这一交易过程更为简洁：因为 k 是一个固定的常数，所以两种资产的数量 x 和 y 只能在下图中的反比例函数图像上运动。开始时 (x, y) 在图中的 a 点，当交易者向智能合约打入 A 资产时，(x, y) 的坐标来到 b 点；为了使 (x, y) 回到反比例函数图像上，必须减少 B 资产的数量，随后(x, y)运动到了新位置 C，并完成交易。

■ 图 5. AMM 交易流程示意图



资料来源：欧科云链研究院

从图像上看，在交易前合约内两种资产的数量为 (x_1, y_1) ，交易后变为 (x_2, y_2) ，那么其实际交易价格为：

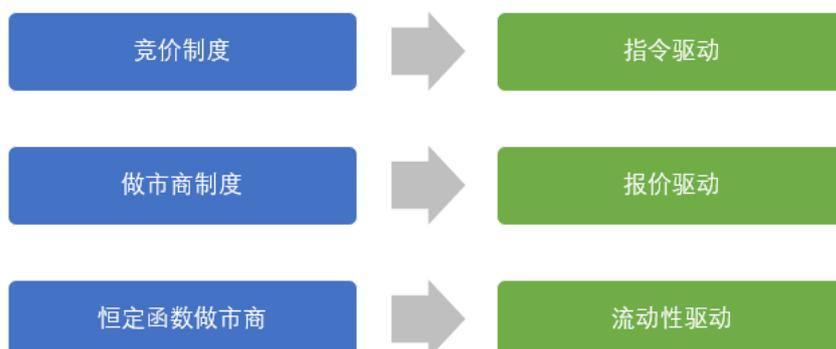
$$P = \left| \frac{y_2 - y_1}{x_2 - x_1} \right| = -\frac{\Delta y}{\Delta x}$$

当两种资产的数量都微小变动时，我们可以发现实际交易价格为原函数的导数，即：

$$P = -\frac{dy}{dx} = \frac{k}{x^2} = \frac{y}{x}$$

从上我们可以看出，自动做市商制度打破了传统的交易制度模式，不需要订单簿，也不需要做市商报价或者系统撮合，而是利用储备池中的流动性来完成资产的交易兑换；最重要的是，AMM 的交易价格也不是由做市商的报价或交易者的订单确定，而是由资产池中两种资产数量的比值确定，因此它是一种流动性驱动的交易制度。

图 6. 各交易制度的价格决定方式



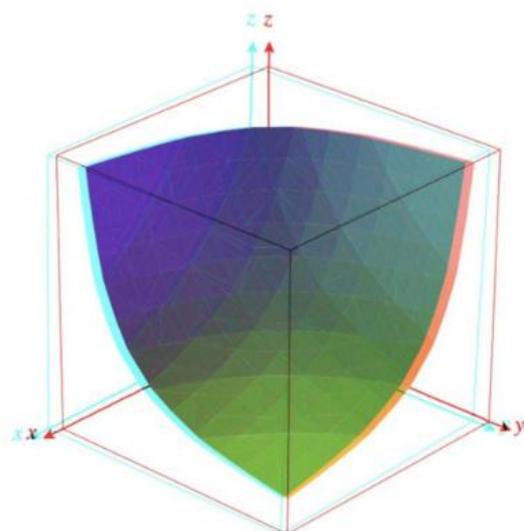
资料来源：欧科云链研究院

Uniswap 的模型设计是基于两种资产进行交易，所以反映在二维图像上是一条双曲线；另一个著名的 DeFi 项目 Balancer 则对此进行了扩展，将 CFMM 推广到超过两种资产的情况，其恒定函数模型如下：

$$\prod_{i=1}^n R_i^{W_i} = k$$

R 是每种资产的储备量，W 是每种资产的权重，k 是常数。从图像上看，Balancer 将原来的二维双曲线扩展至多维，下图即在三维下的恒定值曲面图像。

图 7. Balancer 恒定函数模型在三维下的图像



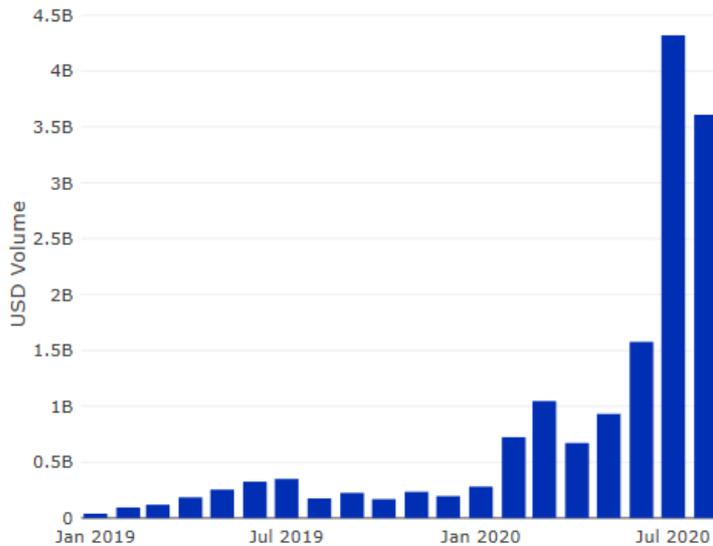
资料来源：Balancer 白皮书，欧科云链研究院

在 Balancer 的储备资产池中，尽管有多种资产，但与 Uniswap 平台一样，任意两种资产进行兑换时，如果资产数量只发生微小变动，其实际兑换价格实际上就是这两类资产的偏导数，即：

$$P_i = -\frac{\Delta R_i}{\Delta R_j} = -\frac{\partial R_i}{\partial R_j} = \frac{R_i/W_i}{R_j/W_j}$$

在金融市场交易制度日益复杂的今天，自动化做市商机制以 $x * y = k$ 这样一个简洁的模型横空出世。自 6 月至今，CFMM 类的去中心化交易所在以太坊上迅速崛起，其月均交易额从年初的不足 5 亿美元迅速上升至目前的 40 亿美元。特别是 Uniswap，其日均交易额突破 1 亿美元，超越了许多中小型交易所，达到美国最大加密资产交易平台 Coinbase 日均交易量的三分之一，这印证了中国古代的哲学智慧----大道至简。

■ 图 8. 去中心化交易所月均交易额变化



资料来源：Dune Analytics，欧科云链研究院

二、AMM 是否能取代传统交易制度？

由于近几个月来 AMM 在以太坊上的大获成功，很多人都在讨论 AMM 能否取代传统的竞价和做市商制度。正所谓“汝之蜜糖，彼之砒霜”，AMM 凭借其极富数学简约之美的交易模型在市场上大放异彩，但也造就了它的缺陷不足。在与传统交易制度竞争时，AMM 主要面临无法独立定价、无常损失和交易深度不足等问题，使得它很难取代传统的交易制度。

1. AMM 的定价问题

首先是资产交易的独立定价问题。在竞价制度中，价格优先原则是竞价市场上普遍采用的撮合原则，而且被作为首要的优先原则，即第一优先原则。它要求经纪商在接受委托进行交易时，必须按照最有利于委托人的利益买进或卖出资产，即买进资产时，较高的买进价格订单优先满足于较低的买进价格订单；卖出资产时，较低的卖出价格订单优先满足于较高的卖出价格订单。除价格优先原则外，还有时间优先，数量优先，按比例分配等原则，但在世界各大金融市场上，尽管第二乃至第三、第四等撮合原则上差别很大，但第一原则一定是价格优先原则，以此保证交易制度的价格发现功能。

■ 表 2. 全球主要证券交易所撮合原则

交易所名称	优先撮合原则
纽约证券交易所	Super DOT 系统：1.价格优先 2.时间优先、客户优先 大厅交易订单：1.价格优先 2.按比例分配
东京证券交易所	1.价格优先 2.时间优先 3.市场订单优先于限价订单
韩国证券交易所	1.价格优先 2.时间优先 3.客户优先 4.数量优先
巴黎证券交易所	1.价格优先 2.时间优先
上海证券交易所	1.价格优先 2.时间优先

资料来源：欧科云链研究院

做市商制度同样具有价格发现的功能。做市商的收益主要来源于买卖差价，在对市场进行做市时，以收益最大化为目标。这要求做市商必须充分利用市场信息，提出报价，与此同时，投资者根据做市商的报价做出投资决策，并将自己的交易信息及时反馈给做市商，随后做市商再根据手上的资产头寸和价格差异调整报价。因此，在做市商与投资者的共同推动下，市场可以发现真实的交易价格。

然而，自动化做市商制度却没有价格发现的功能。比如在某一资产的交易上，用户 A（做市商 A）挂出的是 5 美元 / 手的买单，用户 B（做市商 B）挂出的是 10 美元 / 手的买单，在竞价制度或做市商制度下，用户 B（做市商 B）先实现交易，但在 Uniswap 平台上却无法

保证用户 B 先成交。因为我们前面提到，AMM 的价格是靠流动性驱动的，交易价格由储备池的资产情况决定，而非订单价格决定，即 AMM 只能产生交易价格，却不能发现市场价格。为此，AMM 不得不引入套利者这一重要角色：一旦 AMM 平台上的价格与市场公允价格不同，就会出现套利空间，并将价格拉回正轨。

金融市场交易制度的核心是发现价格功能，无法发现价格的交易制度注定无法成为主流。因此，从未来发展看，自动做市商制度很难取代现有的竞价制度和做市商制度，但可以凭借其简洁灵活的交易特征，成为金融市场交易的补充。

2. 无常损失 (Impermanent Loss)

在上文中我们提到，由于模型设计上的缺陷，AMM 不得不引入套利机制以完善其价格机制。然而，这也带来了另一个严重后果---无常损失 (Impermanent Loss)

无常损失实际上来源于套利行为。我们前面提前，AMM 的交易价格与市场公允价格是脱轨的，为此需要套利者进来购买被低估的资产或卖出高估的资产，直到 AMM 提供的价格跟外部市场匹配。因此，套利者的利润实际上来自于流动性提供者，由于套利给流动性提供者带来损失的这一部分就被称为无常损失。

我们以如下表格说明，在 Uniswap 的一个智能合约内有资产 A 1000 份，资产 B 10 份。

- 1) 初始时刻，资产 A 的价格为 1 美元，资产 B 的价格为 100 美元，此时资产池总价值为 $1 \times 1000 + 10 \times 100 = 2000$ 美元；
- 2) T2 时刻，资产 B 的价格上升为 110 美元，此时资产池总价值变为 $1 \times 1000 + 10 \times 110 = 2100$ 美元。注意到 Uniswap 此时的兑换价格为资产 A 数量与资产 B 数量的比值，即 $P = 1000/10 = 100$ ，而在市场公允价格下，兑换价格为 $110 \text{ 美元} / 1 \text{ 美元} = 110$ ，由此出现套利空间。
- 3) T3 时刻，套利者向该智能合约注入 48.81 份资产 A，换取 0.47 份资产 B。套利结束后，资产 A 有 1048.81 份，资产 B 剩余 9.53 份，此时储备池内资产总价值为 $1048.81 \times 1 + 9.53 \times 110 = 2097.62$ 美元，相较于套利前少了 2.38 美元，这部分损失即无常损失。

表 3. 无常损失产生原理

时间	T1	T2	T3
情景	初始状态	资产 B 价格变为 110 美元	套利发生
资产 A 数量	1000	1000	1048.81
资产 A 价格	1 美元	1 美元	1 美元
资产 B 数量	10	10	9.53
资产 B 价格	100 美元	110 美元	110 美元
兑换价格	$1000/10 = 100$	$1000/10 = 100$	$1048.81/9.53 = 110$
储备池资产价值	2000 美元	2100 美元	2097.62 美元

资料来源：欧科云链研究院

流动性提供者 (LP) 之所以为 AMM 提供流动性，是因为可以获取交易费用，然而无常损失的存在，提高了流动性提供者的风险。如果无常损失超过了流动性收益，那么 LP 将不再提供流动性。因此无常损失的大小是决定 AMM 类 DEX 能否正常运营的关键。

3. 交易深度问题

交易深度是衡量市场交易优劣的重要指标之一，反映的是市场在承受大额交易时价格不出现大幅波动的能力。很多行业人士认为，只要向市场提供足够的流动性，就可以解决交易深度问题。对于以订单簿为基础的竞价制度和做市商制度确实如此，但对于 AMM 而言，其模型本身也会影响交易深度。

以 Uniswap 为例，在上文中我们提到，交易前智能合约内两种资产的数量为 (x_0, y_0) ，交易后变为 (x, y) ，那么其实际交易价格为（这里我们忽略交易费用）：

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

因为 $y = k/x$ ，所以我们带入上式并求导，即可得

$$P' = \frac{2kx - kx_0 - x^2y_0}{x^2(x - x_0)^2}$$

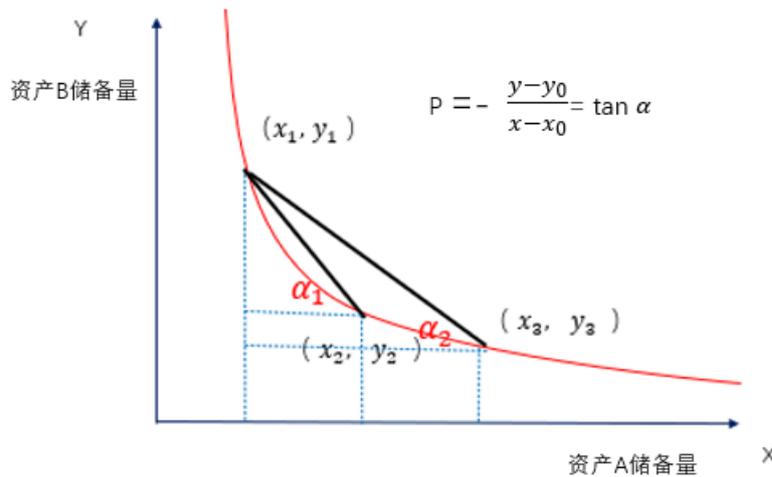
$$(x > x_0)$$

注意到 P' 的分子 $(-y_0x^2 + 2kx - kx_0)$ 是一个一元二次函数，由于

$$\Delta = (2k)^2 - 4 * (-y_0) * (-kx_0) = 4k^2 - 4ky_0x_0 = 0$$

所以 $x = x_0$ 即为一元二次方程的唯一根，并且 $-y_0 < 0$ 。当 $x > x_0$ 时， $P' < 0$ 恒成立，即价格 P 是关于 x 的一个减函数， P 将随着 x 的增大而减小。很显然， K 值（也就是 LP 的大小）并不会改变该函数性质。

■ 图 9. Uniswap 的定价图像



资料来源：欧科云链研究院

从上述分析可以看出，相较于传统交易制度，在提供相同流动性的情况下，AMM 用户向交易合约中放入越多数量的资产 A，换回的资产 B 数量越少，即交易价格越高。所以 AMM 的交易深度不仅仅取决于 LP 的大小（即 k 值），跟模型本身也有关。因此，尽管 Uniswap 简洁的交易模型为其带来了巨大优势，但同时也带来了高滑点的问题。特别是对于储备池规模较小的交易对资产，无法支持大额交易，否则将支付更高的价格。随着 AMM 的日益火热，AMM 的交易深度问题也成为用户和开发者们关注的核心问题。

三、自动做市商制度的未来发展

相较于传统交易制度，自动做市商具有自动化、低成本和高效的优势，但在定价权、无常损失和交易深度等方面存在一定的问题。然而，如果考虑到自动做市商制度从创立至今只不过几年的时间，那么以苛责的眼光要求其做到尽善尽美并不妥当。实际上，自动做市商如今已经成为区块链行业中最热门的赛道之一，出于对未来转型和战略发展的需要和市场前景的看好，许多大公司和创业都开始关注这一领域，并推动该制度的完善。

1. 无常损失的改善方案

究其本质，无常损失是由 AMM 平台价格与外部市场价格偏差产生的套利造成的。想要减少无常损失，必须要降低平台价格与外部市场价格之间的偏差。从理论上讲，这很难实现，因为 AMM 没有价格发现功能。然而我们却可以另辟蹊径---如果两种资产之间的兑换价格保持稳定，在 AMM 平台上进行交易时人们自然会以该兑换价格作为心理价格，那么价格偏差将会很小，无常损失也将很低。在区块链世界中，这类最理想的资产即稳定币，稳定币都以美元挂钩，价锚定在 1 美元，因此在稳定币之间的兑换上（如 USDT 与 DAI 之间的兑换），价格偏移将会很小，无常损失也最小。这也是 Curve 这类专注于稳定币交易的 AMM 类去中心化交易所迅速崛起的原因。

此外，行业内还有探索采用预言机提供价格的方案，以 Bancor V2 为代表。只要预言机为智能合约提供真实准确的价格，就可以降低价格偏差，减小无常损失。需要强调的是，预言机只能减小无常损失，但无法解决无常损失问题。因为价格偏差的产生是由于 AMM 无价格发现功能引起的。价格预言机捕捉的仍然是历史价格，而非市场最新价格，这是一种对结果进行事后的修正，甚至不能像订单簿模式那样看到盘口价格（市场对未来价格的预期）。

2. 交易深度的改善方案

以 Uniswap 为代表的 AMM 为例，从模型上看，由于其采用恒定乘积模型 ($x*y=k$)，导致其滑点过高，当然好处是理论上可以为交易提供无限的流动性 (x,y 永远不会等于 0)。那么什么样的模型可以实现零滑点问题呢？---恒定总和模型。以 $x+y=k$ 为例，从图像上看，其兑换价格恒定为 1（即图像的斜率恒为 1，然而这样带来的缺陷是很容易耗尽储备池的资

产。因此，一种理想的方式是构建一种混合函数，如果两种资产的价格相对稳定，就可以降低函数中的滑点值；当储备池中的资产流动性不足时，则迅速提高价格，实现理论上的无线流动性，而 Curve 构建的恒定函数模型 StableSwap 正是此类中的佼佼者，为此构造了一个复杂的函数：

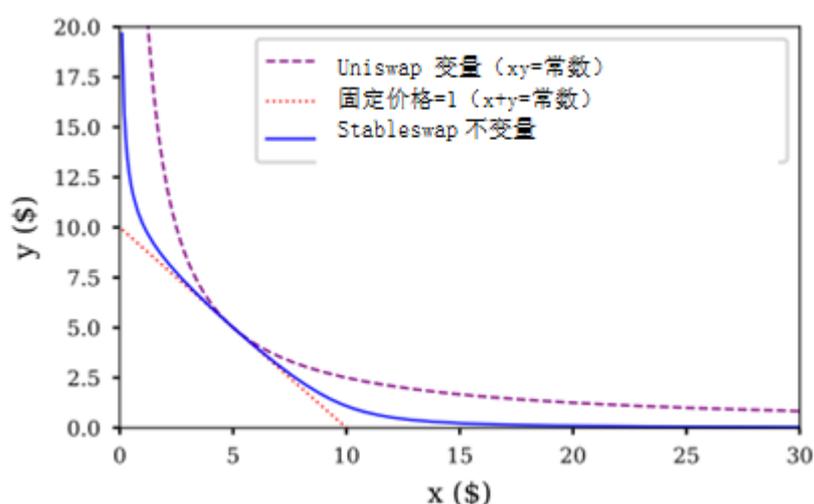
x 是每种资产的储备量， n 是资产的种类， D 是一个不变量，代表储备中的价值， A

$$An^n \sum x_i + D = ADn^n + \frac{D^{n+1}}{n^n \prod x_i}$$

是“放大系数”，即一个可调的常数，提供一种类似杠杆的作用，影响资产价格的范围，并影响流动性提供者的利润空间（即资产的波动性越高， A 也越大）。

当投资组合比较均衡时，这个函数作为一个恒定总和函数而发挥作用，当投资组合变得更不均衡时，它转换为一个恒定乘积函数，由此实现了滑点与流动性的兼顾。

■ 图 10. Stableswap 不变量与 Uniswap（常积）、固定价格不变量的比较



资料来源：Stableswap 白皮书，欧科云链研究院

四、总结

自动做市商制度是一项重大创新。尽管在交易深度、交易定价权等方面存在问题，但它具有去中介、自动化、交易快捷等优势，可在无订单簿的条件下完成交易，开创了一种全新的交易范式。目前自动化做市商仍处于发展的萌芽期，但已经展现出惊人的潜力，期待未来看到更多的进展。

作者简介：欧科云链研究院是欧科集团旗下研究机构，主要研究内容围绕区块链产业和数字货币两大领域展开，与政府、企业、高校等都有密切的合作，在业内具有一定知名度。欧科云链集团是全球领先的区块链产业集团，总部设在中国北京，在美国、欧洲、韩国、日本等 10 余个国家和地区设有分公司或办公室，旗下的欧科云链已在港交所上市。