MIP-1
MinSwap - Cardano 链上的多池去中心化交易所

由 Terrence 和 Tham CH 翻译

Long Nguyen
long@minswap.org

四月 2021

提要

这篇论文解释了 MinSwap 的动机和概念- 一个 Cardano 链上的自动造市商 (AMM) 去中心化交易所 (DEX)，支持单个流动性池的多种定价功能. 还详细阐述了交易路由、链上价格预言机和 Cardano 权益池运营商 (SPO) 的自动 babel 费用赎回.

1 简介

依照传统，订单簿中心化交易所都会得到市场制造商的支持. 做市商通常是大型贸易公司或拥有庞大的资本经纪公司、金融知识和法规遵从性. 他们促进中心化交易所的高流动性，通过交易点差赚取利润（买入价和卖出价之间的差异). 然而，去中心化交易所的兴起和 DeFi 普及了自动化做市的概念 (AMM) 允许了个体零售商可以轻松成为做市商和从交易费用中赚取利润.

在 AMM 交易所，个别做市商 - 现在称为流动性供应商 (LP) 将他们的资金集中在一起，成为一个单一的大型自动化做市商. 交易者可以基于确定性算法在这些流动性池上交易代币. 虽然方便且适用于链上智能合约，但 AMM 引入了自己的问题类别，即非永久性损失、低资本效率和抢先. 以太坊区块链上的项目正在以不同的方式解决这些问题，并进行不同的权衡. 然而，Cardano 生态系统中并没有开发这样的 DEX，更不用说优化的 AMM. 为不同的用例使用不同的 AMM 也会让不精通的用户感到困惑，并且引入了 DEX 聚合器，例如 1inch [1] 或 Matcha [6]，但他们收取额外的服务费.

2 多功能流动资金池

通过为单个流动性池利用多个定价功能，流动性提供者 (LP) 可以选择针对特定货币对进行最优化的池，从而产生最高回报/最高资本效率. 乍一看，这似乎会导致流动性碎片化。然而，LP 自然会将他们的资金流入最有效的特定货币对池中，因为该池是交易最多的. 由诸如 Yearn Finance [8] 之类的社区创建的自动化产量农业策略也将帮助 LP 将其资本重新平衡到最有效的池中. 这与拥有多个具有不同定价功能的 AMM 协议没有什么不同，但是在池和交易之间移动流动性将更快、更便宜，因为所有池都在一个平台上. 构建具有多个池功能预期的 AMM 还将导致社区中最佳想法的无缝集成，而无需进行硬分叉或重大迁移.

让我们看看可以在 MinSwap 上构建什么样的流动性池.

2.1 恒积池

UniSwap [2] 推广了恒定产品做市商的概念. 恒定乘积定价曲线适用于大多数货币对，但会导致逆相关货币对（即价格朝相反方向移动的货币对）的一些非永久性损失. 恒定产品池的定价函数非常简单:

$$xy = const$$

2.2 稳定池

Curve [3] 发现稳定货币对有更好的函数（即价格相似的货币对，主要与外部资产如 BTC 或美元挂钩). 它是具有动态 “放大系数” 的恒积函数和恒和函数的组合.

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

这有助于降低低流动性池的滑点，同时始终确保大型交易的流动性.

2.3 多资产池

Balancer [5] 将恒定产品函数的概念推广到两个以上的资产.

$$\prod x_i^{w_i} = const$$

它允许使用任意数量的任意数量资产创建一个池，而不是限制 LP 提供等量的两种资产. 这基本上意味着 LP 可以按原样提供他们的整个投资组合，并在赚取费用的同时自动重新平衡.

2.4 动态池

Kyber 将 Curve 的 “放大系数” 从稳定对扩展到其他一般对. 这个概念被称为 Dynamic Market Making (DMM) [7]. 使用 DMM, 放大系数” 是根据货币对的固有波动性进行编程的. 它还引入了更好的费用机制，根据交易量和价格波动动态调整交易费用.

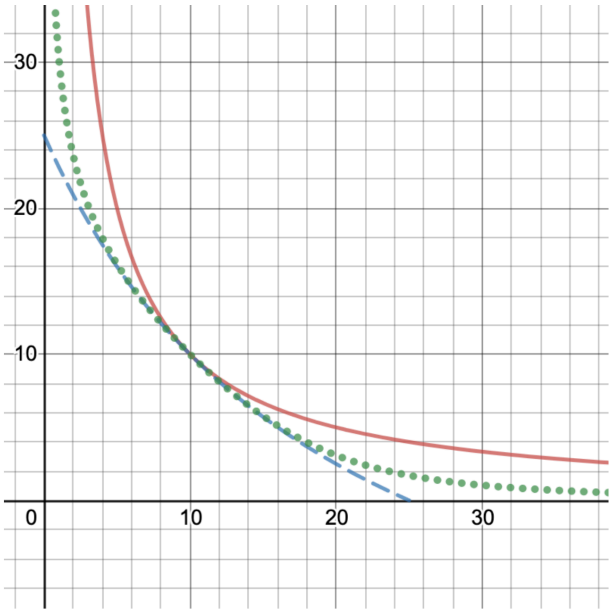

图 1: 的库存曲线（红色）、Curve（绿色）和动态定和动态定价曲线（蓝色

这四个池只是 MinSwap 功能的示例. AMM 每天都充满了更新更好的想法，最好的想法将被社区投票并集成到 MinSwap 中.

3 多池路由

对于一对具有多个池的，从代币 A 交换到代币 B 不仅仅是在 pool(A,B) 上执行常量函数. 多池路由的一个简单解决方案是找到为特定货币对产生最高回报的池. 更好的解决方案可能是将交易规模分解为更小的部分，并将它们排列到不同的池中以找到最佳回报. 多池路由算法可以完全在链上或链下执行，因为 Plutus 支持两者.

4 链上价格预言机

AMM 的一个常见用例是提供一对的链上价格，而无需查询和信任链下实体. 这是可能的，因为根据一价定律，套利机器人总是会进来将 AMM 价格移动到市场价格. 由于单个货币对存在多个矿池，货币对的价格将是该货币对所有矿池的加权平均值:

$$price(A, B) = \frac{\sum_{i=1}^{n} w_i P_i}{\sum_{i=1}^{n} w_i}$$

其中 w_i 和 P_i 分别是池 i 的大小和价格.

5 自动 babel 费用赎回

Cardano 原生资产允许用户以该确切的代币而不是 ADA 支付代币交易费用. 这个概念被称为 babel 费用 [4]. 它带来了更好的用户体验，因为他们不必总是为了促进代币交易而持有少量 ADA. 然而，原生代币的费用直接支付给权益池运营商（SPO），如果代币不受欢迎并且很少有 SPO 想要用该代币支付，这可能会导致交易缓慢. MinSwap 将通过允许 SPO 将所述代币快速交换为 ADA 来提供帮助，从而激励 SPO 处理本地代币交易.

参考

[1] *1inch*. URL: https://1inch.io/.

[2] Hayden Adams, Noah Zinsmeister, and Dan Robinson. *Uniswap v2 Core*. 2020. URL: https://uniswap.org/whitepaper.pdf.

[3] Michael Egorov. *StableSwap - efficient mechanism for Stablecoin liquidity*. 2019. URL: https://curve.fi/files/stableswap-paper.pdf.

[4] Prof. Aggelos Kiayias. *Babel fees - denominating transaction costs in native tokens*. URL: https://iohk.io/en/blog/posts/2021/02/25/babel-fees/.

[5] Fernando Martinelli and Nikolai Mushegian. *A non-custodial portfolio manager, liquidity provider, and price sensor*. 2019. URL: https://balancer.finance/whitepaper/.

[6] *Matcha*. URL: https://matcha.xyz/.

[7] Andrew Nguyen, Loi Luu, and Ming Ng. *Dynamic Automated Market Making*. 2021. URL: https://files.kyber.network/DMM-Feb21.pdf.

[8] *Yearn Finance*. URL: https://yearn.finance/.

免责声明

本文仅供一般参考之用. 它不构成投资建议，也不构成买卖任何投资的建议或招揽，不应用于评估做出任何投资决定的价值. 不应依赖它提供会计、法律或税务建议或投资建议. 本文反映了作者的当前观点，并不代表 Minswap Labs 或其附属公司，也不一定反映 Minswap Labs、其附属公司或与其相关的个人的意见. 此处反映的意见如有更改，恕不更新.