arXiv:2301.08558v1 [cs.GT] 20 Jan 2023

关于恒定乘积自动做市商

Th´eodore Conrad
École Normale Supérieure
Guillaume M´erou´e
École Normale Supérieure de Lyon
Arthur Vinciguerra
École Normale Supérieure de Lyon

2022年9月

摘要

恒定乘积做市函数由 Hayden Adams 于2017年首次提出，用于创建以太坊上的去中心化交易所 Uniswap。这使用户能够以任意汇率交换资产。后来又出现了 Balancer 和 Curve 等变体。本文分析了支配这类协议的数学原理。我们表明，将一笔交易拆分成多笔较小的交易，不会影响最终汇率。我们还表明，当无人将费用再投入时，该协议更安全、盈利能力也更强。

1 引言

2008年10月，中本聪发布了比特币白皮书 [8]：第一种加密货币，一种无人能够控制的去中心化货币。自中本聪发表这篇革命性论文以来，人们为实现各种事物的去中心化付出了大量努力。2014年，Vitalik Buterin 发布了 [3] 他自己的区块链白皮书：以太坊是首个实现智能合约的区块链。智能合约是在区块链上运行的一段代码。这项技术突破促成了首个去中心化金融（DeFi）协议 MakerDAO 的诞生 [4]。MakerDAO 让用户能够使用加密货币创建抵押债务头寸，即存入加密货币以借入资金。此后，DeFi协议的数量急剧增长，DeFi智能合约中的总锁仓价值在 [1] 2021年12月达到历史最高的2500亿美元。本文聚焦于一种特定类型的DeFi协议：去中心化交易所。首个去中心化交易所协议 Uniswap [2], 由 Hayden Adams 于2017年提出，并于2018年在以太坊区块链上发布。Uniswap 是一种自动做市商（AMM）：用户可以将加密货币锁定在智能合约中，作为做市所需的流动性。Uniswap 采用恒定乘积做市模型，我们将在后文讨论。该模型通常表现良好，但对于汇率稳定的代币交易对而言并非最优。为此，Michael Egorov 创建了另一种协议 Curve [5], ，采用另一种做市模型，专注于稳定币交易对。

Beaker 的测试网版本采用 Uniswap v2 [6] 模型，并进行了两项改动：费用不会自动复投到资金池中，用户也可以按照给定的价差进行交易。本文将深入解析这一协议背后的数学原理，并探讨与之交互时可能遇到的各种问题。

目录

1 引言 2

2 恒定乘积自动做市商的数学 4

2.1 一些有用的关系.62.2 交换过程中的流动性池演化.72.3 无常损失.102.4 投资组合随时间的相对演变.122.5 投资回报率.13

3 结论 15

4 图 16

2 恒定乘积自动做市商的数学

本节将探讨固定乘积模型背后的数学原理。在该模型中，人们会建立包含两种资产的资金池，任何个人（称为流动性提供者）都可以向其中提供流动性。这些资金池充当做市商，以任意给定的汇率提供流动性。更复杂的模型允许每个人在给定的价格区间内提供流动性 [7]。

在本文余下部分，我们考虑一个由代币$\mathbf{X}$ 和$\mathbf{Y}$组成的资金池。令x （分别为 y）表示资金池中代币$\mathbf{X}$ （分别为$\mathbf{Y}$）的数量，并令 r 表示该资金池的汇率。

我们首先选择资金池流动性和汇率的定义。这些定义决定了资金池将如何做市。

模型的核心是两个方程。第一个方程指出，代币数量的乘积应为常数，通常称为固定乘积方程。从数学上说，这意味着几何平均数应始终保持不变。我们将这个几何平均数称为流动性。

定义 2.1。资金池的流动性 L 由以下方程定义：

$$L = \sqrt{xy}.$$

因此，固定乘积假设意味着流动性在一次交易期间保持不变。

公理 2.1. L 是交易的不变量。

接下来，我们必须决定资金池将如何形成市场，也就是如何选择汇率。一个自然的想法是选择 $r = -\frac{\partial x}{\partial y}$。事实上， r是向资金池中添加无穷小量的代币$\mathbf{X}$时，我们收到的代币数量 $\mathbf{Y}$。为简单起见，我们将前一步计算的结果作为 r 的定义。

定义 2.2. 我们将资金池的汇率设为：

$$r = \frac{x}{y}.$$

现在我们已经定义了这些概念，可以定义资金池的价值了。

定义 2.3（资金池的价值）。 资金池的价值 V由以下方程定义：

$$V = p_x x + p_y y,$$

其中， p_x 和 p_y 分别是代币 $\mathbf{X}$ 和 $\mathbf{Y}$的市场价格（单位为每个代币对应的美元金额）。

为简化论述，我们对资金池的汇率作出最后一个假设。

公理 2.2（套利假设）。 我们假设资金池的汇率始终等于市场的汇率：

$$\frac{p_y}{p_x} = \frac{x}{y}.$$

实际上，当资金池的汇率与市场汇率不一致时，套利者可以通过恢复两者的一致来赚取少量利润。因此，这一假设在实践中成立。

在接下来的小节中，我们将介绍资金池变量之间的各种关系，并说明这些变量在发生交易时如何变化。随后，我们将探讨无常损失的概念，它体现了流动性提供者面临的风险；最后，我们将评估流动性提供者投资组合的变化。

2.1 一些有用的关系

在本小节中，我们将探讨涉及 x, y, L, r 和 V的各种关系。

引理 2.1 （依赖于 r）。 对于 $r \in]0, +\infty[$ 和 $L \in [0, +\infty[$:

$$x = L\sqrt{r}$$
$$y = \frac{L}{\sqrt{r}}.$$

证明。 根据 L 和 r的定义即可直接得出。 □

引理 2.2 （涉及 V）。 我们有以下关系 :

$$x = \frac{1}{2}\frac{V}{p_x}$$
$$y = \frac{1}{2}\frac{V}{p_y}.$$

证明。 根据 V 的定义和套利假设，我们得到:

$$\begin{aligned} V &= p_x x + p_y y \\ &= p_x x + p_x x \\ &= 2p_x x \end{aligned}$$

对 y也可以进行同样的处理。 □

引理 2.3 (L 的表达式**)**。 池的流动性与其价值以及$\mathbf{X}$ 和$\mathbf{Y}$ 的价格之间存在如下关系 :

$$L = \frac{1}{2}\frac{V}{\sqrt{p_y p_x}}.$$

证明。 这由 $L^2 = xy$ 得出。 □

这 3 个表达式给出了确定 x、 y、 r、 L 和 V 的不同方法。

2.2 资金池通过交换的演变

在本小节中，我们尝试描述资金池进行交易时 x、 y、 r 和 V 的变化。为简化记号，我们将交换前**X** 代币（分别为**Y**代币）的数量称为 x （分别为 y），将交换后**X** 代币（分别为**Y**代币）的数量称为 x' （分别为 y'）。类似地，我们定义 r 和 r'。

定理 2.4 （交换后的变量状态）。 交换后，我们有以下方程：

$$\begin{aligned} x'y' &= xy \\ r' &= r\left(\frac{y}{y'}\right)^2 \end{aligned}$$

证明。 第一个方程直接由 $x'y' = L^2 = xy$ 得出。第二个方程也很容易得出：

$$\begin{aligned} r' &= \frac{x'}{y'} \\ &= \frac{1}{y'}\frac{xy}{y'} \\ &= \frac{(ry)y}{(y')^2} \\ &= r\left(\frac{y}{y'}\right)^2 \end{aligned}$$

□

在描述对交易过程建模的方程之前，我们先给出最后一个定义。

定义 2.4。 交易的价差 σ 定义为交易过程中的相对汇率变化

$$\sigma = \left|\frac{r'-r}{r}\right|.$$

推论 2.4.1 （针对 $\mathbf{Y}$ 的交换方程）。 假设某用户想用 n 枚 $\mathbf{Y}$ 代币换取一些 $\mathbf{X}$ 代币，且最大价差为 σ，那么该用户将收到数量为 m 的 $\mathbf{X}$ 代币，其数量由以下方程给出：

$$m = \frac{x\alpha}{y+\alpha}, \quad with\ \alpha = \min\left(n, y\left(\frac{1}{\sqrt{1-\sigma}} - 1\right)\right)$$

证明。 根据价差的定义，我们对可交易的代币**Y** 最大数量q 有所限制。当价差达到限制时，我们有：

$$\begin{aligned} \sigma &= \frac{r-r'}{r} \\ \sigma &= 1 - \left(\frac{y}{y'}\right)^2. \end{aligned}$$

设 q_σ 为价差为 σ时可交易的代币 y 的最大数量。将 $y' = y + q_\sigma$ 代入前一个方程，得：

$$1 - \sigma = \left(\frac{y}{y + q_\sigma}\right)^2$$

最终得到关于 q_σ 的以下方程：

$$q_\sigma = y\left(\frac{1}{\sqrt{1-\sigma}} - 1\right).$$

因此，用户交换的**X** 代币最大数量 α 为

$$\alpha = \min\left(n, y\left(\frac{1}{\sqrt{1-\sigma}} - 1\right)\right).$$

因此，我们有 $y' = y + \alpha$，并且可以得出用户将收到的代币数量 m：

$$\begin{aligned} m &= x - x' \\ &= x - \frac{xy}{y'} \\ &= x\left(1 - \frac{y}{y'}\right) \\ &= \frac{x\alpha}{y + \alpha} \end{aligned}$$

□

推论 2.4.2 （X交换方程）。假设用户想用n 个**X** 代币交易一些**Y** 代币，且最大价差为 σ，那么用户将收到数量为 m 的**Y** 代币，其数量由以下方程给出：

$$m = \frac{y\alpha}{x + \alpha}, \quad with\ \alpha = \min\left(n, x\left(\sqrt{1+\sigma} - 1\right)\right)$$

证明。 由于 $r' > r$，此情况下价差的表达式为：

$$\begin{aligned} \sigma &= \frac{r'}{r} - 1 \\ &= \left(\frac{x'}{x}\right)^2 - 1 \end{aligned}$$

设 q_σ 为价差为 σ时可交易的代币最大数量 x 。将 $x' = x + q_\sigma$ 代入上一个方程，得到：

$$1 + \sigma = \left(1 + \frac{q_\sigma}{x}\right)^2$$

and

$$q_\sigma = x\left(\sqrt{1+\sigma} - 1\right).$$

证明的其余部分与前一个证明类似。 □

推论 2.4.3 (交换的实际汇率**)**。 假设用户想用 n 代币$\mathbf{Y}$ 交换一些$\mathbf{X}$代币，那么用户实际获得的汇率为

$$r = \frac{x}{y+n}.$$

证明。 当不存在最大价差时，前面的方程变为

$$m = \frac{xn}{y+n}.$$

根据定义，我们有 $r = \frac{m}{n}$ 。因此：

$$r = \frac{x}{y+n}.$$

□

有人可能会问，将一笔交易拆分成 k 笔较小的交易，是否能换回更多代币。下述定理说明事实并非如此。

定理 2.5。 设 k 为正整数，且 m_i 为第 i^{th} 笔交易$(1 \leq i \leq k)$收到的代币数量，则：

$$m = \sum_{i=1}^{k} m_i.$$

证明。 设 k 为正整数， x_i （分别为 y_i）表示进行 i^{th} 次交易（$1 \leq i \leq k$）后资金池中的$\mathbf{X}$（分别为$\mathbf{Y}$）代币数量，其中 x （分别为 y）是资金池中代币的初始数量。设 n_i 为第 i^{th} 次交易中交易的$\mathbf{Y}$ 代币数量。我们有以下关系：

$$y_i = y_{i-1} + n_i \text{ and } y_0 = y$$

在这种情况下，我们允许任意价差，即 $\sigma \to 1$。我们可以计算总和：

$$\begin{aligned}
\sum_{i=1}^{k} m_i &= \sum_{i=1}^{k} \frac{x_{i-1} n_i}{y_{i-1} + n_i} \quad \text{using the swap equation with } n_i \text{ and } \sigma \to 1 \\
&= \sum_{i=1}^{k} \frac{xy}{y_{i-1}} \frac{n_i}{y_{i-1} + n_i} \quad \text{using } x_{i-1} y_{i-1} = x_{i-2} y_{i-2} = \cdots = xy \\
&= xy \sum_{i=1}^{k} \left(\frac{1}{y_{i-1}} - \frac{1}{y_{i-1} + n_i} \right) \\
&= xy \sum_{i=1}^{k} \left(\frac{1}{y_{i-1}} - \frac{1}{y_i} \right) \\
&= xy \left(\frac{1}{y} - \frac{1}{y_k} \right) \quad \text{by telescoping the sum} \\
&= x - \frac{xy}{y_k} \\
&= x - x_k \quad \text{using } xy = x_k y_k \\
&= m.
\end{aligned}$$

□

2.3 无常损失

人们常常忽视资金池提供者可能面临的无常损失 。它代表提供者通过提供流动性所承担的风险。因此，资金池收取的费用 f 不仅是对提供者所提供服务的奖励，也是对他们愿意承担风险的补偿。那么，什么是无常损失? 无常损失是投资于资金池的投资组合价值与未投资时的价值之间的相对差异。之所以称为无常 损失，是因为这种损失取决于代币 $\mathbf{X}$ 和 $\mathbf{Y}$当前的汇率。因此，损失可能会波动，只有当提供者从资金池中撤出流动性时才会实现。在本节中， x和 y 表示用户最初持有的代币数量， x' 和 y'则表示这些代币投入资金池、并经历汇率 r的一些波动后的数量。

定义 2.5（无常损失）。 设 V_p 为投资于资金池时投资组合的价值， V_n 为未投资于资金池时投资组合的价值。那么，无常损失定义为：

$$\Lambda = \frac{V_p - V_n}{V_n}$$

定理 2.6。 设 δ_x 和 δ_y 分别为$\mathbf{X}$ 和$\mathbf{Y}$的相对价格变化，则无常损失为：

$$\Lambda = 2\frac{\sqrt{\delta_y \delta_x}}{\delta_x + \delta_y} - 1,$$

其中 $\delta_x = \frac{p'_x}{p_x}$ 和 $\delta_y = \frac{p'_y}{p_y}$。

证明。 在这种情况下， V_p 和 V_n 由以下方程定义：

$$\begin{aligned} V_n &= xp'_x + yp'_y \\ V_p &= x'p'_x + y'p'_y. \end{aligned}$$

根据我们的池模型，我们有：

$$L^2 = \begin{cases} \frac{1}{r}x^2 \\ \frac{1}{r'}(x')^2 \end{cases} \tag{1}$$

设 r' 为资金池的最终汇率。我们有：

$$x' = \sqrt{\frac{\delta_y}{\delta_x}}x \quad \text{because } \frac{r'}{r} = \frac{\delta_y}{\delta_x}.$$

and

$$\begin{aligned} V_p &= x'p'_x + y'p'_y \\ &= 2x'p'_x \quad \text{from the fixed product assumption} \\ &= 2p'_x\sqrt{\frac{\delta_y}{\delta_x}}x \\ &= 2p_x x\sqrt{\delta_y\delta_x} \quad \text{using } p'_x = \delta_x p_x. \end{aligned}$$

接下来，我们得到一个仅涉及 x的 V_n 表达式：

$$\begin{aligned} V_n &= xp'_x + yp'_y \\ &= xp'_x + \frac{xp_x}{p_y}p'_y \\ &= xp'_x + \delta_y x p_x \\ &= xp_x\left(\delta_x + \delta_y\right). \end{aligned}$$

计算差值可得：

$$\begin{aligned} V_p - V_n &= 2p_x x\sqrt{\delta_y\delta_x} - xp_x\left(\delta_x + \delta_y\right) \\ &= p_x x\left(2\sqrt{\delta_y\delta_x} - \left(\delta_x + \delta_y\right)\right). \end{aligned}$$

最后可以用后者计算无常损失：

$$\begin{aligned} \Lambda &= \frac{V_p - V_n}{V_n} \\ &= \frac{p_x x\left(2\sqrt{\delta_y\delta_x} - \left(\delta_x + \delta_y\right)\right)}{xp_x\left(\delta_x + \delta_y\right)} \\ &= 2\frac{\sqrt{\delta_y\delta_x}}{\delta_x + \delta_y} - 1 \end{aligned}$$

□

在图（1）中，我们绘制了 Λ 仅当其中一种代币的价格发生变化时的情况。为了更清楚地了解其中的变化，我们还在图（2）中绘制了相对投资组合比较。

这些图表具有误导性，因为它们给人的印象是，不提供流动性总是更有利。这是因为无常损失的计算没有考虑应计费用。

2.4 投资组合随时间的相对演变

如上一节所述，无常损失没有考虑应计费用，因此可能会产生误导。在提供流动性之前，了解哪些情形更有利，以及自己愿意承担哪些风险非常重要。本节将探讨提供或不提供流动性时，投资组合如何演变，以及费用处理方式对其产生的影响。交易手续费有两种处理方式：

1. 自动将费用重新注入流动性中（例如 Uniswap v2）；
2. 收取费用并单独存放（例如 Beaker）；

本节后续将分别把它们称为手续费模型 (1) 和 (2)。

由于交换发生的时间无法预测，我们考虑在给定流动性增长率 α （每年百分比）的情况下的演变，并为简便起见，假设增长是线性的（即交换以相同的频率、相同的数额发生）。

定理 2.7 （手续费模型 (1) 的相对演变）。设 δ_x 和 δ_y 分别为$\mathbf{X}$ 和$\mathbf{Y}$ 的相对价格变化， t 为经过的年数。那么，在手续费模型 *(1)* 中，流动性提供者投资组合的相对演变 $\Delta_1(t) = {}^{V_p(t)}\!/_{V(t)}$ 为：

$$\Delta_1(t) = \sqrt{\delta_y \delta_x}\,(1+\alpha t)\,.$$

证明。 我们首先计算价格不变时资金池中应有的$\mathbf{X}$ 代币数量 $x(t)$。在流动性按 α演变的情况下进行复利时，池的流动性每年将增长 α 。因此，我们有：

$$L(t) = L(0)\,(1+\alpha t)\,.$$

当资金池的比率不变时，两种代币会以相同的比例增长，因此：

$$x(t) = x(0)\,(1+\alpha t)\,.$$

由于 L 不依赖于 r，我们可以复用无常损失证明中的 $x' = \sqrt{\frac{\delta_y}{\delta_x}}\,x$ 及其余部分。由此可得：

$$V_p(t) = 2p_x x\sqrt{\delta_y \delta_x}\,(1+\alpha t)\,.$$

除以投资组合的初始价值 $V = 2xp_x$ ，证明结束。 □

注释。 有人可能会认为，采用自动复利后，投资组合的价值应该呈指数增长。事实上，只有在假设资金池的交易量与池的流动性以相同速率增长时，这一说法才成立。然而，没有理由认为这一假设一定成立。一些交易所在计算资金池的预期年化收益率时，暗中采用了这一错误假设。

定理 2.8 （手续费模型 (2) 下的相对演变）。 设 δ_x 和 δ_y 分别为 $\mathbf{X}$ 和 $\mathbf{Y}$ 的相对价格变化， t 为经过的年数。那么，在手续费模型 *(2)* 中，流动性提供者的投资组合相对演变 $\Delta_2(t) = {}^{V'(t)}\!/_{V(t)}$ 为：

$$\Delta_2(t) = \sqrt{\delta_y \delta_x} + \alpha t \frac{\delta_x + \delta_y}{2}.$$

证明。 在手续费模型 (2) 中，应计费用单独存储，不进行复利计算。根据我们对费用累积的假设，单独存储中累积的代币数量 $x_{out}(t)$为：

$$x_{out}(t) = x(0)\alpha t.$$

因此，投资组合的最终价值为：

$$\begin{aligned} V'(t) &= V_p(t) + V_{out}(t) \\ &= 2p_x x\sqrt{\delta_y \delta_x} + p'_x x_{out}(t) + p'_y y_{out}(t) \quad \text{re-using result from IL.} \end{aligned}$$

因此我们得到：

$$\begin{aligned} \Delta_2(t) &= \frac{V'(t)}{V(t)} \\ &= \sqrt{\delta_y \delta_x} + \frac{p'_x x_{out}(t) + p'_y y_{out}(t)}{2p_x x} \\ &= \sqrt{\delta_y \delta_x} + \left(\frac{\delta_x}{2} + \frac{p'_y y}{2p_y y}\right)\alpha t \quad \text{using } p_x x = p_y y \\ &= \sqrt{\delta_y \delta_x} + \alpha t \frac{\delta_x + \delta_y}{2}. \end{aligned}$$

□

图 (3) 比较了流动性增长 $\alpha = 20\%$ 时两种手续费模型的表现。该图表明，手续费模型 (2) 比手续费模型 (1) 更安全，也更有利可图。直观而言，复利计算的奖励也容易遭受无常损失。不过，这里有个问题：在手续费模型 (2) 中，如果有些人定期将奖励复投，而另一些人不这样做，会发生什么？

2.5 投资回报率

在上一节末尾，我们提出了一个重要问题。为了回答这个问题，我们首先要计算复利用户的投资回报率

以及不将费用复利的用户的投资回报率。我们先计算将奖励复利的用户的流动性变化。

定理 2.9。令 L_c（分别为 L_{nc}）表示复利（分别为不复利）其奖励的人所拥有的池的流动性，令 L_0 为池的初始流动性。那么， L_c 满足以下微分方程：

$$\frac{\mathrm{d}L_c}{\mathrm{d}t} = \alpha L_0 \frac{L_c}{L_c + L_{nc}}.$$

证明。根据定义， L_{nc} 为常数。在时间 t产生的费用总额为：

$$f(t) = \alpha L_0 t.$$

令 $\mathcal{P}(t) = \frac{L_c(t)}{L_c(t)+L_{nc}}$ 表示复利用户拥有的池占比，那么 L_c 的增长等于费用增长与 $\mathcal{P}(t)$ 的乘积：

$$\begin{aligned}\frac{\mathrm{d}L_c}{\mathrm{d}t}(t) &= \frac{\mathrm{d}f}{\mathrm{d}t}\mathcal{P}(t) \\ &= \alpha L_0 \frac{L_c(t)}{L_c(t) + L_{nc}}\end{aligned}$$

□

定义 2.6（复利用户的投资回报率）。对于复利用户，我们将投资回报率定义为以下比值

$$\rho_c(t) = \frac{L_c(t)}{L_c(0)}.$$

定义 2.7（非复利用户的投资回报率）。对于非复利用户，我们将投资回报率定义为以下比值

$$\rho_{nc}(t) = 1 + \frac{f}{L_{nc}},$$

其中， f 是这些用户的应计费用总额。

由于前一个微分方程的解没有简单的表达式，因此使用了方程求解器。图中绘制了最坏情况（99% 的用户进行复利）4。图示表明，进行复利的用户投资回报率为 20.02%，其他用户的投资回报率为 18.20%，而非预期的初始投资回报率 20%。

注释。用户不进行复利只会损失 1.8% 的投资回报率，因此他们很可能不会在意。

由此，现在可以比较复投费用与不复投费用的用户的投资组合演变。图（5）展示了这项比较。新的比较表明，当相对价格变化不大时，复投的用户可以获得轻微的对冲效果。不过，正如前一条注释所指出的，为了获得少量溢价而定期复利奖励似乎并不值得。因此，投资 Beaker 池的用户应预期其投资组合会如（3）所述发生变化。

3 结论

总而言之，我们的分析表明，投资于使用恒定乘积做市函数的流动性池，归根结底就是押注两种代币的价格走势。我们还证明，无人复投费用时，协议会更安全，也更有利可图。

4 图

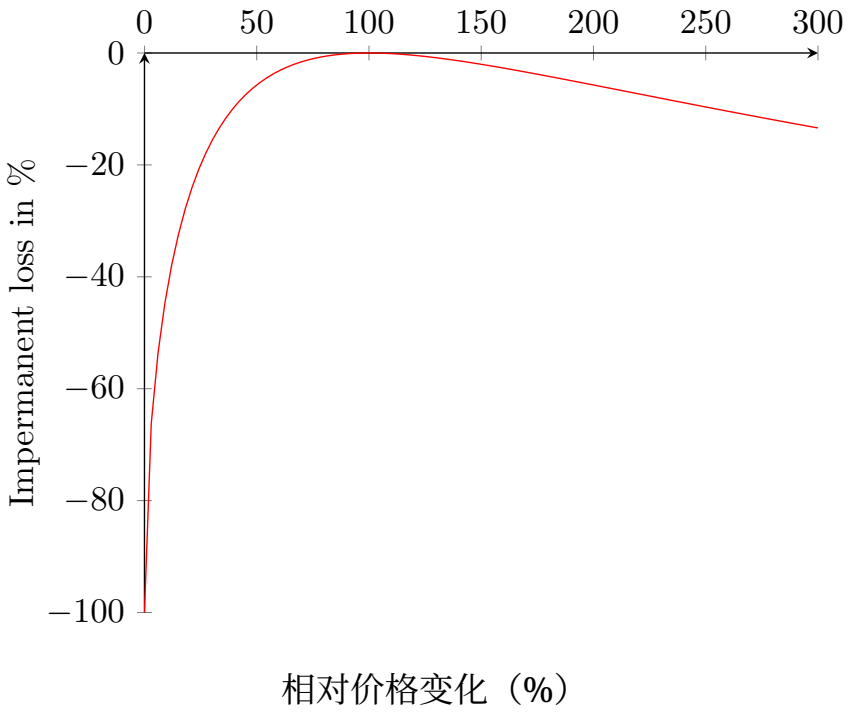

图1：仅一枚币的价格发生变化时的无常损失

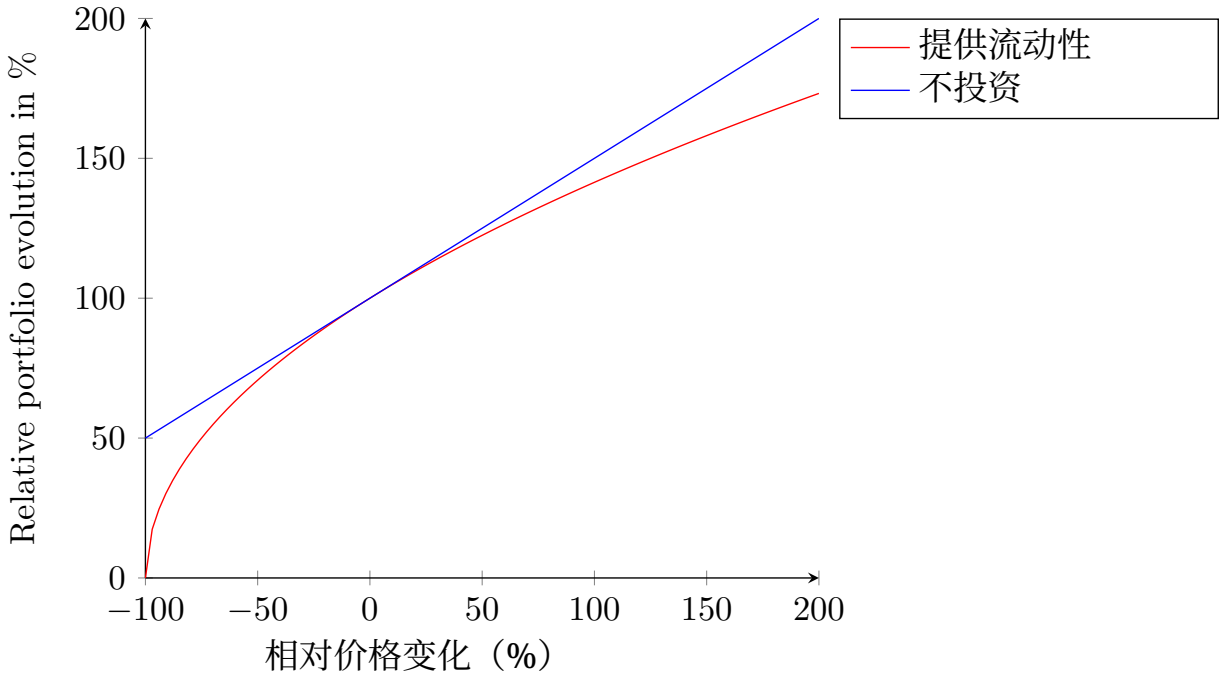

图2：一枚币的相对价格变化时，投资组合的相对演变

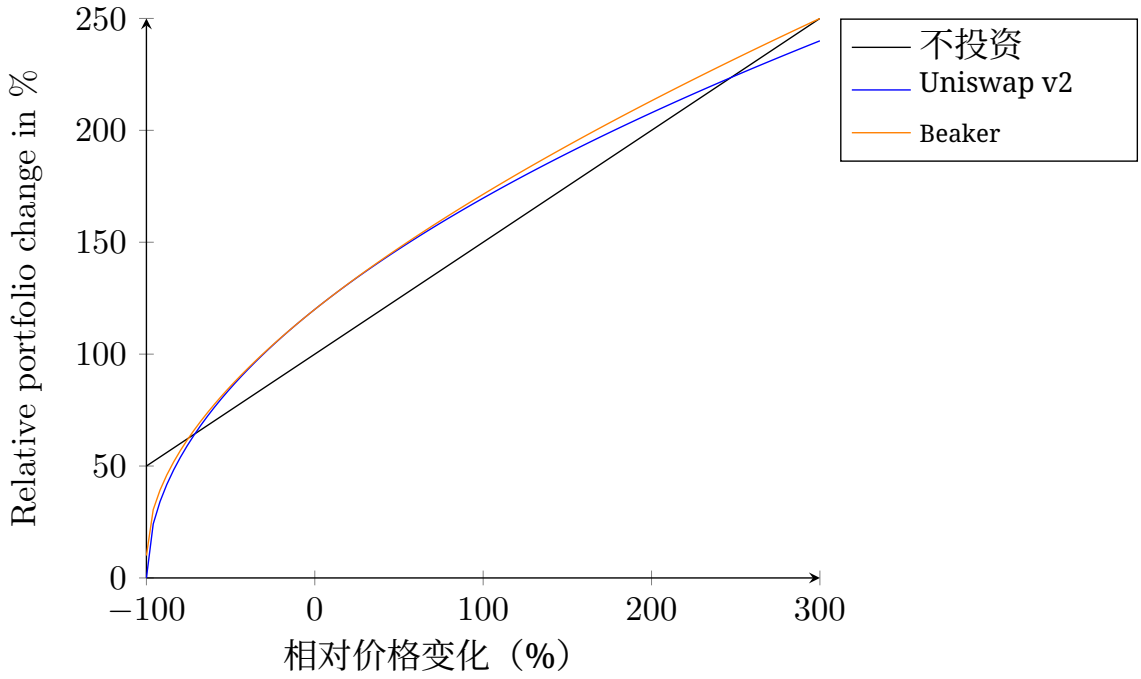

图3：一年后，在年利率为 20% 的情况下，一枚币的价格发生变化时，相对投资组合变化随资金池模型的变化

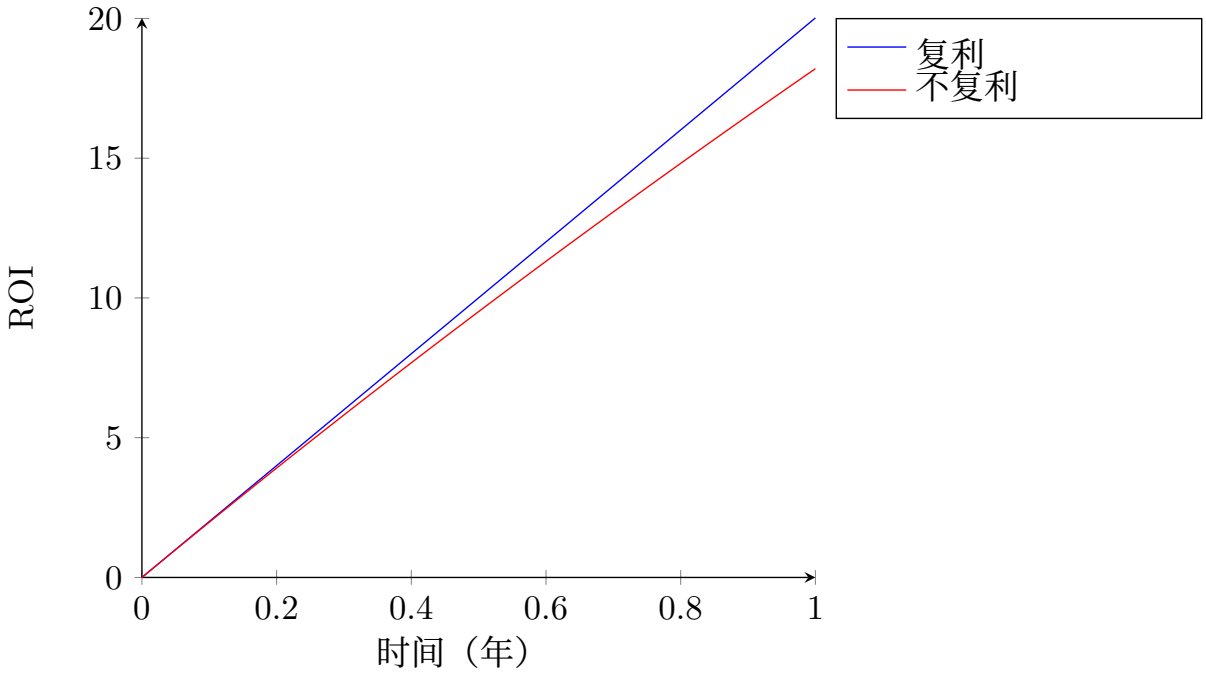

图 4：在初始年利率为 20% 的情况下，99% 的用户将其奖励再投资时的投资回报率对比

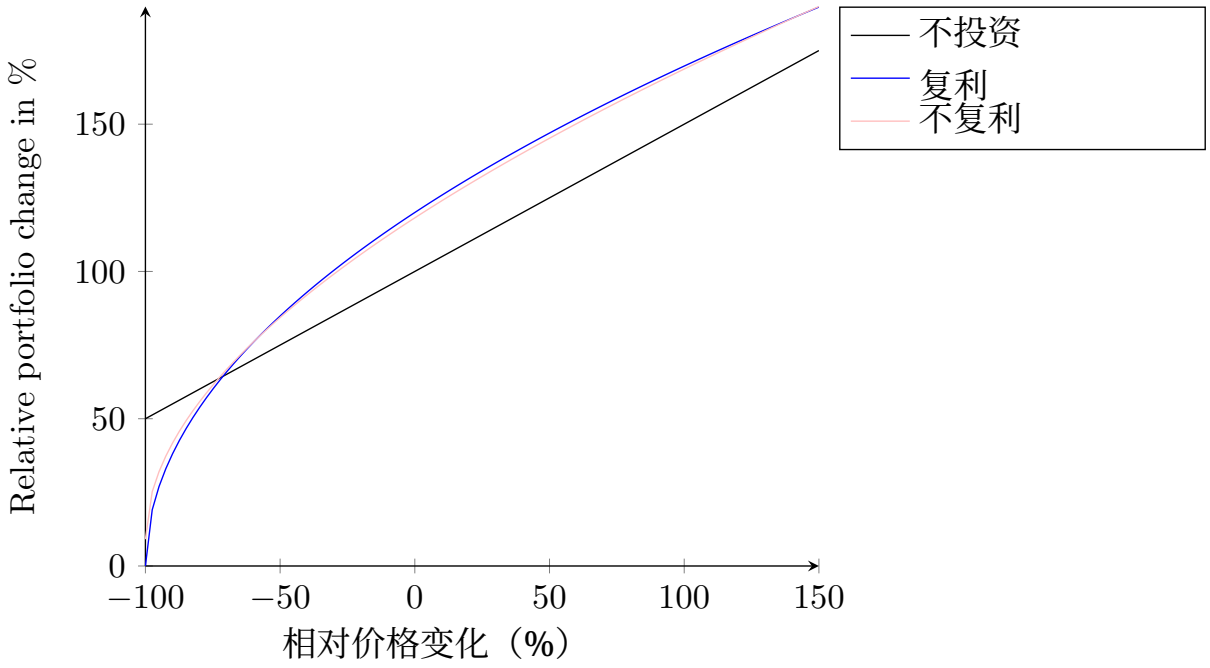

图5：一枚币的价格发生变化且初始年利率为 20% 时，一年后根据复利费用计算的校正后的相对投资组合变化

参考资料

[1] DeFi 总锁仓量追踪器。 https://defillama.com/。[2] Hayden Adams。Uniswap v1。 https://docs.uniswap.org/protocol/V1/introduction。[3]Vitalik Buterin。以太坊白皮书。https://ethereum.org/en/whitepaper/。[4]Rune Christensen。MakerDAO 白皮书。 https://makerdao.com/en/whitepaper/#abstract。[5] Michael Egorov。Curve 稳定交换池白皮书。https://curve.fi/files/stableswap-paper.pdf。[6] Dan Robinson、Hayden Adams、Noah Zinsmeister。Uniswap v2 核心白皮书。https://uniswap.org/whitepaper.pdf。[7] Moody Salem、Hayden Adams、Noah Zinsmeister。Uniswap v3 核心白皮书。https://uniswap.org/whitepaper-v3.pdf。[8] 中本聪。比特币白皮书。https://bitcoin.org/bitcoin.pdf。