Uniswap 简明导论

怀菁

2023 年 10 月 4 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）。

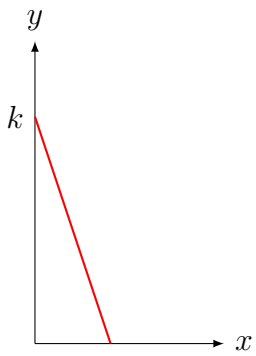

图 2: 可乐交易所

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

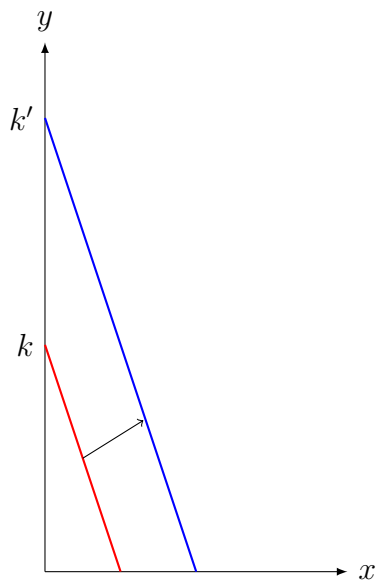

图 3: 添加流动性后的可乐交易所

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。

我们假设武汉大学发行了一种代码为 WHU 的加密货币，并将其与比特币 BTC 一起建立了一个**交易对**（Pair），记作 WHU/BTC ，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 WHU 为**基准货币**（Base Currency），称 BTC 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 WHU 和 BTC。设 WHU 的储备数量为 x ，BTC 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 WHU 和 y_0 个 BTC ，设其乘积为 $k = x_0 y_0$ 。如果不添加或提取流动性，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。

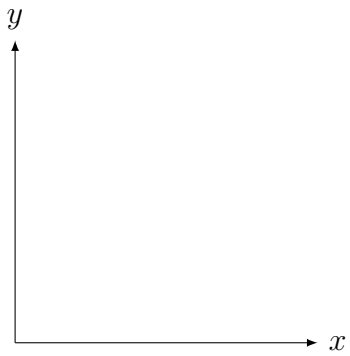

图 4: 添加流动性后的可乐交易所