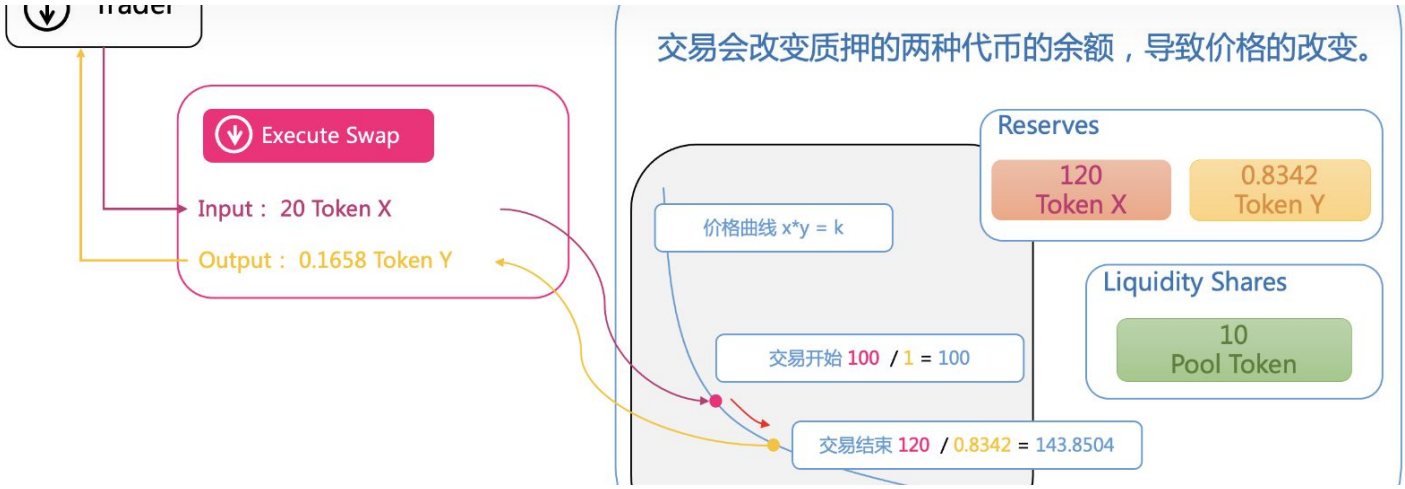


Uniswap深度科普

JasonW
喜欢思考，博而不专的铲屎官

一、Uniswap是什么

首先要搞清楚一下相关的名词都是什么意思：

- **Uniswap Labs**：负责开发Uniswap协议、网络接口的公司。
- **The Uniswap Protocol**：一个实现自动化做市商的智能合约全家桶，促进点对点做市和以太坊上ERC-20 token的交易的协议（即Uniswap核心技术，后续工作原理介绍也都是针对协议内容的解释）。
- **The Uniswap Interface**：为了方便使用Uniswap protocol而开发的网络接口，是与Uniswap protocol交互的众多方式之一（也可以直接与智能合约交互）。
- **Uniswap Governance**：一个Uniswap Protocol的民主治理系统（社区式治理方式，论坛模式）。

按官网上的介绍，Uniswap协议是一个用来在以太坊区块链上交易加密货币（ERC-20代币）的点对合约系统。这个协议通过一个持久化、不可更改的智能合约集合来实现，旨在优先考虑抗审查性、安全性、自我监管，以及在没有任何可能有选择地限制访问的可信中介的情况下运行。简单点说就是通过智能合约实现了一个去中心化的ERC-20代币的自动交易系统。

二、Uniswap的发展历程

Uniswap诞生至今也不过两年多的时间，但是却创造了很多令人惊叹的记录：

- 2018年11月2日，Uniswap公开宣布上线并部署到以太坊主网，推出第一个版本Uniswap v1，但这个v1版本只能算是一个新型去中心化交易方式的概念验证，可实用性并不强。
- 2020年1月31日，经过1年多的沉淀，Uniswap锁仓金额突破5000万美元，成为DeFi龙头。
- 2020年5月19日，Uniswap v2版本上线，增加了自由组合交易对、价格预言机、闪贷、最优化交易路径等功能，对v1版本进行了全面的技术升级。
- 2020年7月27日，Uniswap 24小时交易额突破1亿美元，DeFi在2020年迎来爆发式增长。
- 2020年8月7日，Uniswap官方宣布已完成1100万美元的A轮融资，由Andreessen Horowitz领投。
- 2020年8月31日，Uniswap锁仓金额突破10亿美元。
- 2020年9月1日，Uniswap总交易量超过100亿美元。
- 2020年9月3日，Uniswap锁仓金额突破20亿美元，距离10亿美元仅仅过了3天，可见市场之火爆。

流动性预言机等技术升级，核心是提升资本效率，具体实现可关注另一篇文章**Uniswap v3 设计详解**。有一点需要注意的是v1和v2版本都遵循的是GPL开源协议，但是v3使用的是Business Source License 1.1（有效时限GPL-2.0或更高版本的许可证）。该许可证将v3源代码在商业环境或生产环境中的使用期限限制为两年，届时它将永久转换为GPL许可证。

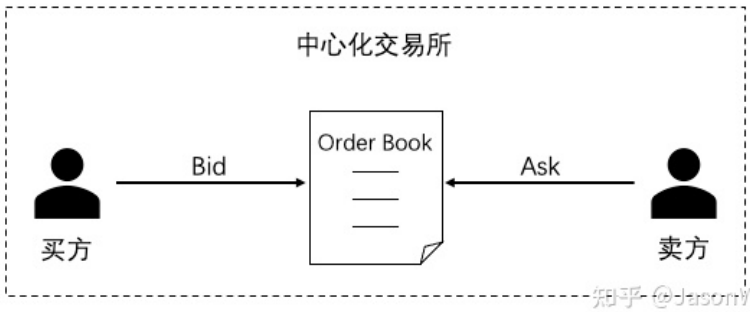
三、Uniswap中的自动化做市商（Automated Market Maker，AMM）

在开始介绍Uniswap之前，先来说说中心化的交易所是怎么交易的

在传统中心化交易所中，你以一个价格发出买单，系统会在order book寻找合适的卖单进行撮合成交，如果当前没有合适的对手单，则将新的订单暂存到order book中等待合适的对手单出现。这个order book以中心系统的形式保存了所有买单、买单的信息，如下图所示：

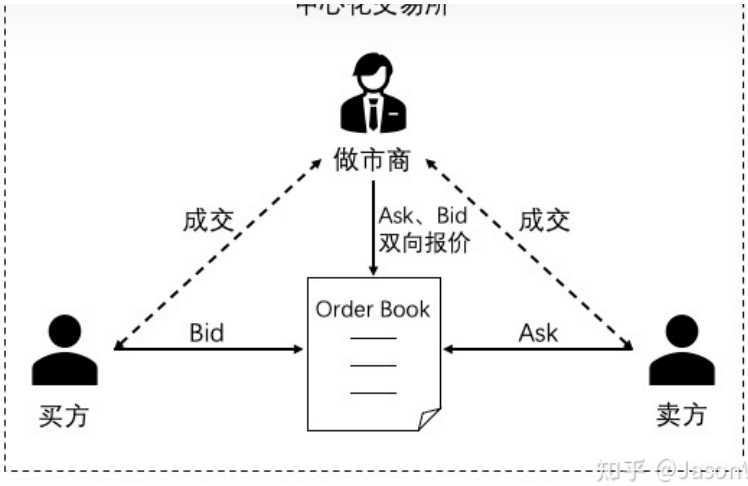
		Ask Price	Ask Size
		103	40
		102	23
		101	10
20	99		
15	98		
35	97		
Bid Size	Bid Price		

Order Book



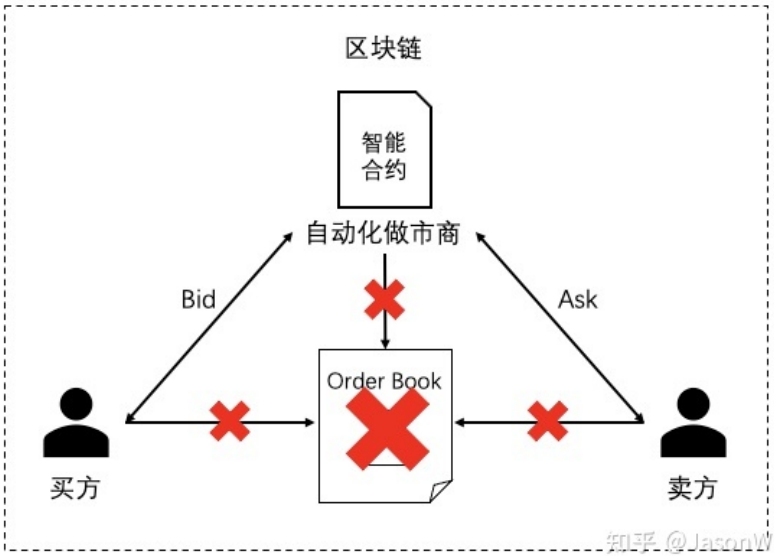
在这种中心化交易平台上，每笔交易的撮合并不需要通过区块链，而是在中心化系统中实现，保证了交易的高并发和低时延，但如果平台上的买卖双方不够活跃，用户发出的买单或者卖单无法快速找到交易对手方进行撮合，就会出现长时间的挂单，交易效率低下，这时就出现了做市商。

做市商是指在传统证券市场上，由具备一定实力和信誉的独立证券经营法人作为特许交易商，不断向公众投资者报出某些特定证券的买卖价格（即双向报价），并在该价位上接受公众投资者的买卖要求，以其自有资金和证券与投资者进行证券交易。买卖双方不需等待交易对手出现，只要有做市商出面承担交易对手方既可达成交易。



做市商通过做市制度来维持市场的流动性，满足公众投资者的投资需求。做市商通过买卖报价的适当差额来补偿所提供服务的成本费用，并实现一定的利润，但是在中心化平台中，买方/卖方并不确定做市商是否真的在区块链上有实际的资产（账户中的余额只是中心化数据库中的一个数字），而且用户的资产都保存在中心化交易所的钱包里，自己没有绝对的控制权，而中心化交易所也没接受任何监管机构的监管，很容易发生监守自盗的事件。

基于以上种种弊端，Uniswap提出了一种通过智能合约实现**自动化做市商（Automated Market Maker，AMM）**来与用户进行交易的去中心化交易协议，用户资产完全由自己控制，而智能合约中锁定的做市资产也是公开可查，是一种更安全透明的交易方式。



四、Uniswap技术原理

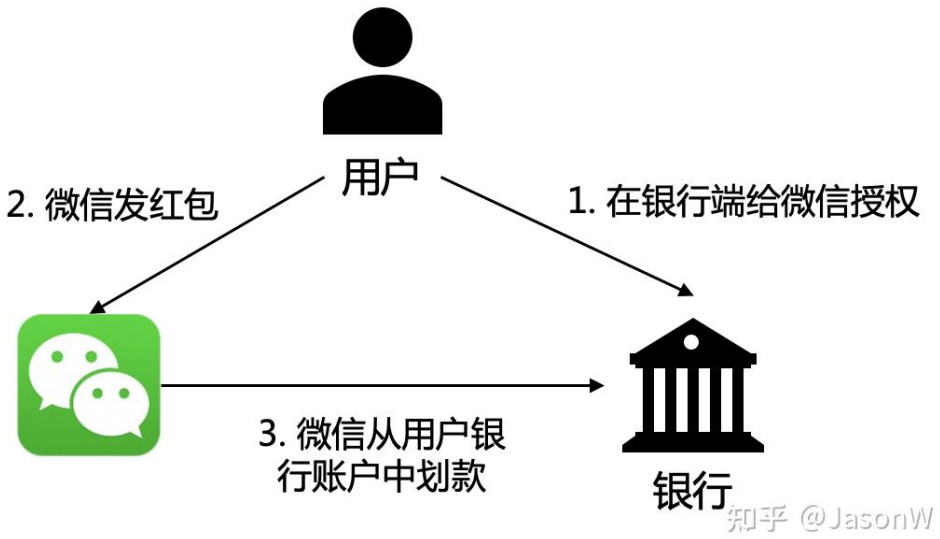
由于v1版本主要是概念验证，因此不做过多介绍，主要就v2版本来深度解析一下Uniswap的技术原理，关于v3版本的更新，会再单独解析。

AMM要实现能自动跟买方/卖方完成交易，需要满足几个特性：

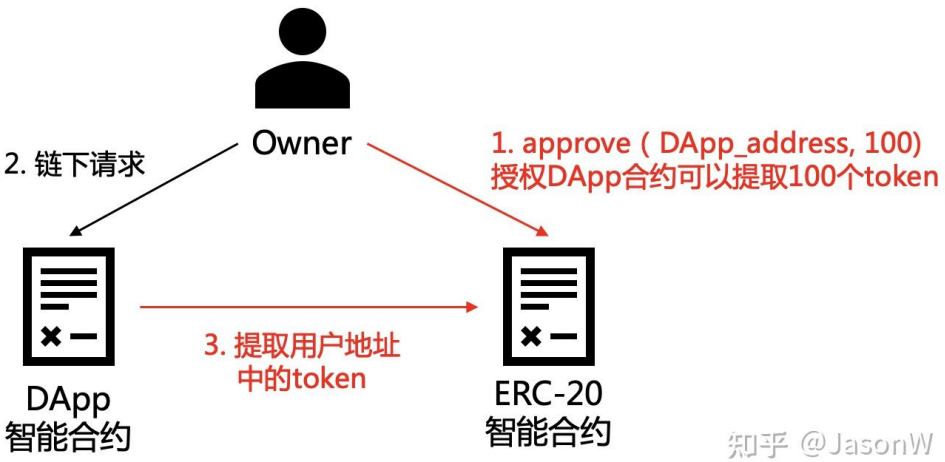
1. AMM要持有资产，由于要做双向报价，所以要持有两种资产；
2. AMM资产池要能充值/提现；
3. AMM可以根据市场情况自动调整价格；
4. AMM要能通过交易赚取利润；

由于Uniswap是部署在以太坊上的，而且支持的是同质化代币之间的交易，因此可交易的资产是符合ERC-20标准的Token.

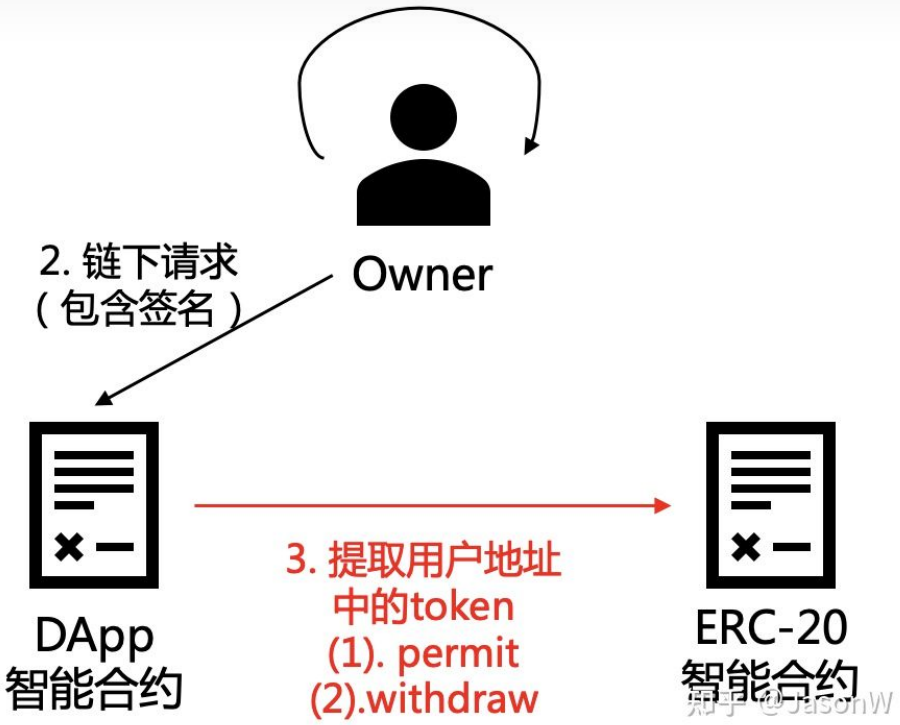
我们在开发去中心化应用时，通常是通过智能合约来执行交易，当我们需要从一个用户的地址中转移一部分token到另外一个地址时，需要地址拥有者授权，就像是你用微信发红包，直接关联到银行卡的话，就需要你先授权微信可以从你的银行账户里划款一样，用户要先给银行一个指令，告诉银行可以给微信授权一个额度，然后微信才能去用户在银行的账户中划款，如下图所示：



如果在区块链上实现一个去中心化的微信应用，分别用智能合约来实现微信（DApp）和银行（ERC-20）的功能，那么用户就要发起至少两次链上交易，如下图中红色部分所示，第1步owner授权DApp可以从他的地址提取100个token，第3步DApp智能合约执行交易从ERC-20合约中owner的地址余额提取不多于100个的token，也就是要消耗两次gas手续费，极大地提升了链上交易的成本。



为了降低成本，减少链上交易次数，可以通过链下签名授权的方式来实现第1步的授权，首先owner在链下进行对某个DApp授权操作的签名，一起发给DApp的智能合约，在DApp智能合约中发起的ERC-20的执行交易中，先验证授权签名（permit），然后再调用提取函数（withdraw）进行owner账户下的token提取，这样整个交易流程就只有一个链上交易，只需要消耗1次gas。



作为Uniswap核心合约之一，UniswapV2ERC20合约定义了Uniswap中所有交易资产的标准。

UniswapV2Pair：

有了资产之后就到了最核心的交易部分了，Uniswap提供了一个UniswapV2Pair的智能合约来交易任意两种ERC-20代币，pairs交易对主要提供三个功能：

1. 流动性追踪，追踪交易池中的代币余额，并且提供流动性代币；
2. 自动做市，根据特定算法自动计算出来的价格来撮合交易；
3. 去中心化预言机，暴露相关数据给外部使用；

接下来分别详细介绍一下这几个功能：

流动性追踪

首先我们也是要先了解几个重要概念：

- **流动性：**指的是pair合约里的两种ERC-20代币的总和，如果同时质押两种代币，则称为增加（提供）流动性
- **流动性池（Pool）**：所有流动性汇集成的池子，即AMM的资产池，Uniswap协议通过流动性池提供个人对合约的交易撮合
- **流动性提供者（Liquidity Provider/LP）**：向流动性池中提供流动性的人
- **流动性代币（Pool Token也叫做Liquidity Token）**：UniswapV2Pair本身也是一种ERC-20合约，它的代币用来代表流动性供给，即为流动性代币，在LP提供流动性时自动增发（mint）代币给LP，提取流动性时燃烧（burn）LP的代币
- **流动性池份额（Liquidity Pool Share/LPS）**：计算出来代表所占有的流通的流动型代币的份额值，用来记录每个LP的流动性贡献比例

在初始化一个pair合约之后，其中两种代币的初始值都是0，为了使流动性池可以开始促成交易，必须有流动性提供者（LP）质押一定量的两种代币来启动流动性池，第一个LP就是设定这个流动性池初始价格的人，并且获得流动性池份额（LPS）。

的调整遵循如下公式：

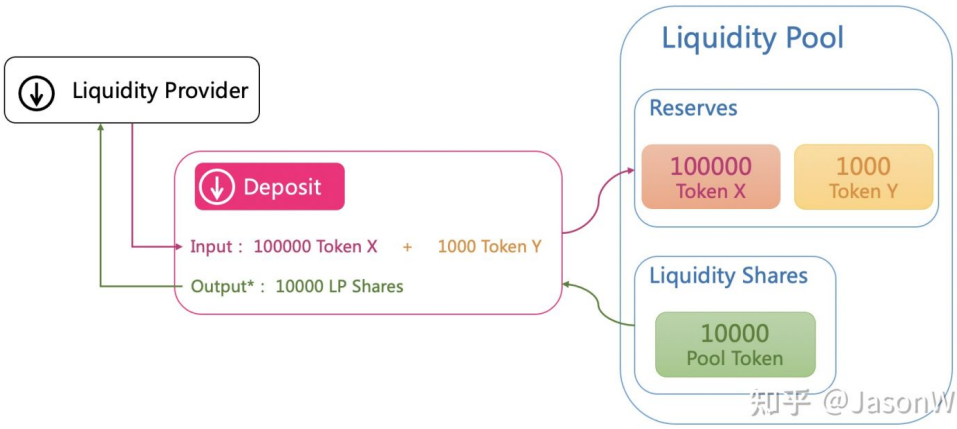
$$x \times y = k, \quad k\text{为常数}$$

x和y代表两种代币的数量，具体在交易中这个公式发挥的作用会在后文详细介绍。

如果第一个LP初始化质押的两种代币量分别为x_0和y_0，则获得的流动性池份额（Liquidity Pool Share/LPS）为s_0：

$$s_0 = \sqrt{x_0 \times y_0}$$

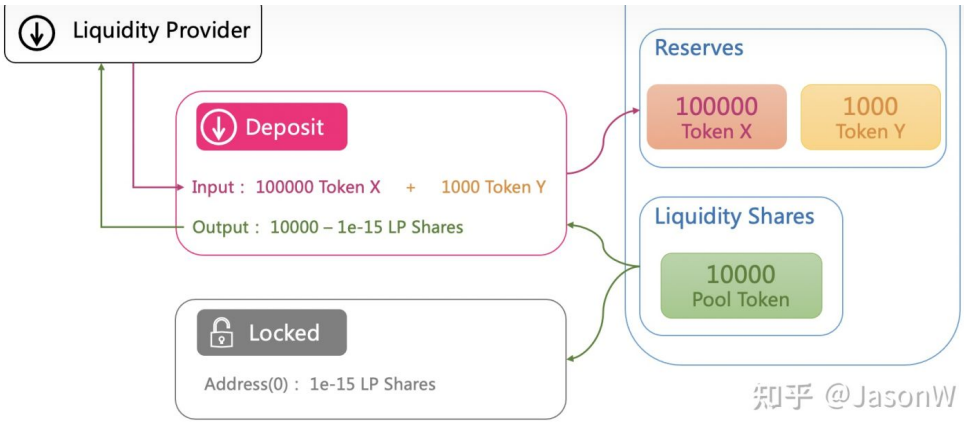
使用几何平均数计算的好处是可以使LPS在任何时候都不受质押的两种代币的比例影响，因为两种代币在流动性池中的比例可能与市场价格不符。如下图所示，假设初始质押量为x_0 = 100,000，y_0 = 1,000，则s_0 = 10,000，在LP质押完X和Y代币之后会收到10,000LPS，此时s_current也同样是10,000，相当于第一个LP持有100%的LPS（除去锁定到零地址的LPS），Liquidity Pool中当前Y相对于X的价格为 1 Y = 100000 / 1000 X = 100 X，例如X是USDT，Y是ETH的话，那么 1 ETH = 100 USDT。



*：Output数据在第一次质押中实际会做一些调整，这部分的介绍在Uniswap白皮书中比较简略，但其实蕴含的内容和机制还是较多较复杂，接下来深入挖掘一下。

按照LPS初始值的计算公式，一个LPS的价值不会低于Pair中两种质押代币的几何平均数，而且随着交易手续费的积累或者"捐赠"会使LPS的价值升高，因为交易手续费在流动性池中积累，针对这部分手续费并不会产生新的LPS，效果就是池子变大了，但是LPS总量没变，两者的比值即LPS的价值就升高了。

Pair智能合约对应的LPS是有18位小数的（以太坊中最大的小数位数），理论上有一种情况是LPS的最小量（即1e-18 LPS）价值非常大，导致后续小流动性提供者很难再提供流动性了，因为提供流动性的成本太高了，例如1e-18 LPS = $100的话，因为这个是最小单位了，所以要增加流动性就至少质押$100美金才能获得LPS，而且随着LPS增值，流动性成本越来越高，不利于维持交易的流动性。在Uniswap白皮书中把这种极端情况认为是一种可能的人为攻击，为了提高这种攻击的成本，在新创建流动性池的时候，设置了一个最小流动性值MINIMUM_LIQUIDITY=1e-15，即LPS最小单位的1000倍，任何流动性池在启用之初都要在零地址中锁定1e-15的LPS，所以上面流动性池初始化的图修订后为：

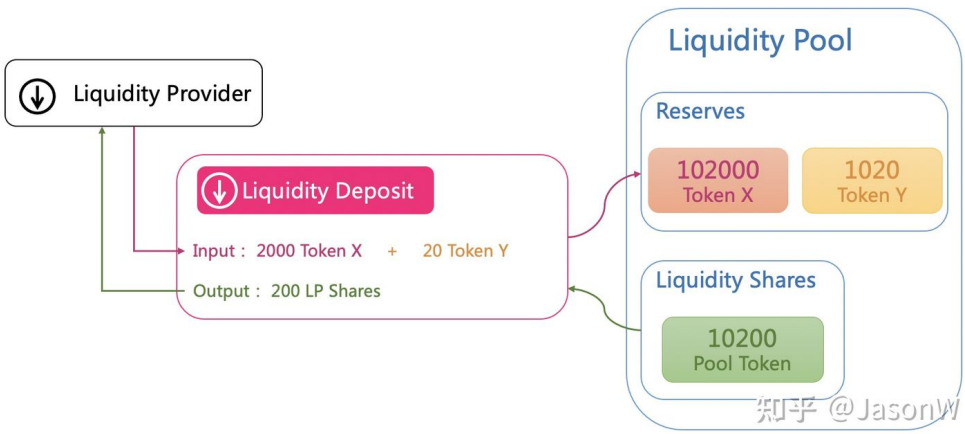


在这种机制之下，如果人为把LPS价值提升到1e-18 = $100的话，就需要在零地址中锁定价值$100 * 1e3 = $100000 的LPS，这样就极大地提升了攻击成本，而且在通常情况下，1e-15的LPS的价值是很小的，甚至可以忽略，所以修订图中第一次质押后获得的LPS虽然要减少1e-15LPS，但约等于10000不变。当然也会有极端情况，例如Pair中质押的两种代币都没有小数，而且单价很高，那么1e-15LPS的价值还是可以感知到的，不过这种类型的代币也不太适合用Uniswap协议来交易。

接下来如果有LP继续添加流动性，则按新增的流动性等比例增发LPS，假设当前Pool中X的量为x_current，Y的量为y_current，存量LPS为s_current，新增加的流动性中的X为x_add，Y为y_add（通常情况下x_current/y_current = x_add/y_add，即等比例增加流动性），则新增发的LPS为s_add：

$$s_{add} = \min(\frac{x_{add}}{x_{current}}, \frac{y_{add}}{y_{current}}) \times s_{current}$$

如下图所示，增加2000 X和20 Y之后，获取200 LPS，此时LPS都在各个LP自己的地址里，他们可以自由转账，流动性池里只是记录了目前LPS总量的值。通常情况下，LP会按照目前流动性池里的X和Y的比例来增加流动性，获取LPS，Uniswap也提供了周边辅助性智能合约来完成增加流动性的操作，如果新质押的X和Y比例与流动性池中不一样，会按照少的代币量等比例质押，另一种多出来的不会去质押，避免损失，如果是直接去操作Pair合约，需要自己校验，否则还是按少的代币量计算LPS，但另一种多出来的就不会返还了，当是捐赠了。



如果是减少流动性，例如减少LPS为s_remove，存量X为x_current，Y为y_current，LPS为s_current，则LP可以提出去的两种代币量分别为x_withdraw和y_withdraw：

$$x_{withdraw} = \frac{s_{remove}}{s_{current}} \times x_{current}, \quad y_{withdraw} = \frac{s_{remove}}{s_{current}} \times y_{current}$$

自动做市

Uniswap的流动性池是通过一个**恒定乘积公式**来计算价格的，以x和y来代表流动性池中两种ERC-20代币（假设为X和Y）的数量，则：

$$x \times y = k, \quad k\text{为常数}$$

如果我们想要用X从流动性池中交换Y，假设输入X的量为deltaX，交易换回的Y为deltaY，在交易池中的资产足够的前期下，满足：

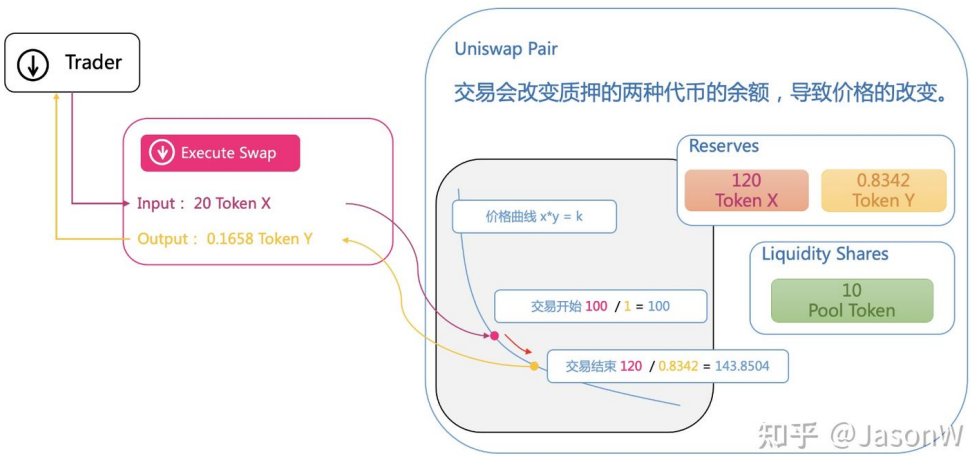
$$(x + \Delta x) \times (y - \Delta y) = k$$

$$\Delta y = y - \frac{k}{x + \Delta x} = \frac{\Delta x \times y}{x + \Delta x}$$

也就是说交易前后，流动性池中两种代币的乘积是恒定不变的，基于此，如果交易的量相对于流动池中的量很小的话，那么交易价格就近似为当前两种代币的比：

$$price_y = \frac{\Delta x}{\Delta y} \approx \frac{x}{y}$$

在实际交易过程中，还会有0.3%的交易手续费，扣除方式是先扣掉手续费，再利用乘积公式进行计算，由于最终兑换出来的交易数量是跟交易量有关的，因此实际交易价格并不等于当前两种代币的比例，而且同一个区块里可能会有多笔交易，同一区块里前面的交易对后续的交易也都会有一定的影响，我们来看一下单笔交易的过程：



如上图所示，原流动性池中两种代币余额为100 X和1 Y，可认为Y相对X的价格为1 Y = 100 X，此时要通过流动性池交易20个X，如果按照当前价格全量交易的话，应该换回 20 / 100 = 0.2 个Y，再减去0.3%的手续费，最后返回0.1994个Y，但实际返回了0.1658个Y，我们来逐步分析一下：

1. 输入20个X，先扣除0.3%的手续费，即实际交易量为19.94个X；
2. 按照x*y=k（k=1*100=100）的公式进行计算：

3. Uniswap pair会给交易者地址返回0.1658个Y，此交易平均交易价格为 1 Y = 20 / 0.1658 X = 120.6273 X，比交易开始时的100要高20%多，主要是因为交易量20个X相对于流动性池的比例较大（20%），相当于大额交易，对价格会产生较大影响，直观的感觉就是市场上有人大量买入Y，从而导致Y的价格上涨，此笔交易之后，交易池中Y相对于X的价格变为了143.8504；

4. 更新流动性池中的余额，虽然交易的时候扣掉了0.3%的手续费，但实际上这个手续费依然会放到流动性池中，作为流动性提供者的收益，因此X更新后的余额还是100 + 20 = 120，Y的余额是1 - 0.1658 = 0.8342，Liquidity Shares的值不变。随着交易手续费的积累，整个流动性池的总价值在上涨，LPS的总量不变，则LPS的单位价值上涨。

以上基本介绍了Uniswap协议中的最核心设计原理，涉及到了流动性池和AMM机制等，除了基础核心部分，Uniswap还提供了一些高级功能，同时也带来了一些很有挑战性的问题，包括上文提到的手续费的收取、滑点损失、无偿损失等LP收益相关问题等等，都是很值得深入挖掘和探讨的。

编辑于 2022-01-20 10:22

DeFi Uniswap

推荐阅读

不懂必看 I 科普系列之二： 什么是以太坊?

SMT大侠 发表于区块链干货...

区块链课程：uniswap简介

为吸引注意力，先看一个数据： 从2020年3月1日到3月25日，Uniswap上的总交易规模大约2.06亿美元，这期间流动性提供商大约捕获了60多万美元的费用价值。其中3月12日和3月13日交易量都超...

ustcs... 发表于区块链技术...

科普 | 区块链？以太坊？智能合约?

依然范儿特... 发表于代码改变世...

4 条评论 切换为时间排序

写下你的评论...

ofhjffhhfghjbvv 2021-08-14

不错哦

赞

Eason Zhang 01-20

好文，支持

赞

王界乔 01-04

进的非常清楚了！想问个问题：为什么通过交易手续费的积累，整个流动性池的总价值就会上

在uniswap v2版本中，交易手续费是放回到流动性池中的，例如用价值100U的X换取价值100U的Y，如果没有手续费，流动性池的总市值是不变的，有交易手续费，相当于流动性池获得了100U的X但给出去的Y会比100U的价值少，多出来的手续费就留在流动性池中了，所以流动性池中的总价值是增长的，而此时LPS的总量是没变的，LPS总价值是跟流动性池中的价值对应，所以单位价值上涨。

赞