

学习uniswap基本知识

一、CEX和DEX

1.1 概念

CEX (Centralized Exchange) :

中心化交易所是被中央机构所控制的交易所，交易所负责保管用户资金，用户之间的货币买卖交易通过由交易所撮合，比如：

[Coinbase](#)：首个在纳斯达克上市的中心化加密货币交易所

[Binance](#)：全网交易量最大的中心化交易所，提供多达 100 种加密货币交易

[Kraken](#)：一家位于美国的加密货币中心化交易所，同时提供银行服务

DEX (Decentralized Exchange):

去中心化交易所是一种运行在区块链上的分散式交易所（不存在中心权力），在这个交易所中没人会负责资金保管，用户之间进行点对点的加密货币交易，比如：

- [Uniswap](#)：ETH 主网上的 DEX，它的出现让 Token 之间的交换更方便，用户可以自由添加 Token 对

1.2 优缺点对比

CEX 的优点

- 交易流程简单，成交速度快，可以迅速响应市场变化
- 交易自由，金融衍生品丰富
- 交易量大，流动性高
- 存在法币与加密货币之间的交易
- 一般具有全平台 APP

CEX 的缺点

- 钱包密钥不归用户所有，资产由交易所保管，交易所跑路风险
- 受法律约束，需要提供个人信息进行账户验证
- 交易所网络波动（拔网线）、黑客攻击会影响交易甚至造成资产损失

DEX 的优点

- 不受中心化控制与监管
- 匿名化交易，不需要提供任何个人信息
- 运行于区块链网络，网络难以被黑客攻击，交易能够稳定执行（智能合约仍有被攻击的风险）

DEX 的缺点

- 交易速度慢，每笔交易需要由矿工完成验证和打包，难以迅速响应市场变化，存在 Slippage (滑点) 问题
- 交易手续费 (Gas Fee) 收当时网络情况影响，网络拥挤的时候手续费高
- 流动性由用户提供，低流动性会影响交易对的价格
- 购买金融衍生品需要去特定平台
- 大部分 DEX 都是在单链上运行，跨链交易受限

参考：

[What Are Centralized Exchanges?](#)

[What Is a Decentralized Exchange \(DEX\)?](#)

[CEX vs. DEX — here are the differences](#)

1.3 一些其他DEX

PancakeSwap 是一家基于币安智能链BSC上的去中心化交易所。该交易所采用自动做市商 ("AMM") 机制，允许在币安智能链进行代币交易。此外，还可以通过收益农场赚取CAKE，通过盯盘赚取CAKE，通过糖浆池赚取更多的代币。

官网：<https://pancakeswap.finance/>

Curve 是一个去中心化交易所 (DEX)，专注在提供高效的稳定币兑换服务。Curve团队在2019年12月开始投入Curve的开发，1个月后产品正式上线，真正推动Curve被大众所了解是在2020年8月推出Curve的原生代币CRV。Curve是DeFi最大的去中心化交易所，主要是针对“类似资产”之间的低滑点交易进行了优化，总锁定价值排行第一，其在以太坊和Polygon的日交易量达数亿美元。

官网：<https://curve.fi/>

Balancer 是一种AMM（自动化做市商）协议，它允许任何人向现有的Balancer资金池提供流动性，也允许任何人自己创建一个流动性池。此外，每个Balancer资金池都是一个自平衡指数基

金，在传统的指数基金中，投资者必须为再平衡服务支付费用，但在Balancer资金池中，流动性提供者实际上可以得到回报，可以说Balancer是Uniswap与Set协议的一个结合体。

官网：<https://balancer.fi>

1inch 主要由 DEX 聚合器和流动性协议（原 Mooniswap）组成。作为 DEX 聚合器，1inch 主要运用 Pathfinder 作为路由算法，旨在为用户寻找最优的 swap 路径。1inch 自称是最大流动性、最低滑点、最佳汇率的 DeFi 聚合器，目前已支持 7 条链，包括 Ethereum、BSC、Polygon、Avalanche、Gnosis、Optimistic 和 Arbitrum。

官网：<https://1inch.io/>

ParaSwap 是一个流动性聚合器，兼容以太坊、BSC智能链、Polygon MATIC等区块链。ParaSwap从不同来源获得 流动性，因此用户可以最佳比率交换资产并支付最少的费用。ParaSwap类似于1inch。

官网：<https://www.paraswap.io/>

SushiSwap 是 Uniswap分叉的一个自动做市DEX，Sushiswap 增加了代币经济激励，也就是将其交易费用的一部分分配给 Sushiswap 代币 SUSHI 的持有人。SushiSwap通过智能合约实现了自动价格确定机制，消除了托管/破产风险，现已在Polygon MATIC上提供，以利用Polygon二层网络的低费用和快速处理的优势。Sushiswap的平台币是SUSHI，它的交易手续费和uniswap一样也是0.3%。它将这0.3%的手续费分成2个部分，其中0.25%提供给LP，方法和Uniswap一样；剩下的0.05%将用于回购SUSHI代币，即用这部分钱购买SUSHI代币持有者手里的SUSHI代币。这意味着，SUSHI的价值与Sushiswap平台交易量是挂钩的。在Sushiswap上，交易量越大，SUSHI捕获的价值就越高。

官网：<https://www.sushi.com/>

1.4 TVL Rankings

网址：<https://defillama.com/chain/Ethereum>

TVL Rankings									
All Ethereum Terra BSC Avalanche Fantom Solana Tron Polygon Cronos Waves Arbitrum Others									
Name	Chains	1d Change	7d Change	1m Change	TVL	Mcap/TVL			
1 Curve (CRV)		+0.43%	+13.65%	+17.01%	\$17.94b	0.05188			
2 MakerDAO (MKR)		+1.11%	+6.27%	+9.15%	\$16.75b	0.10886			
3 Convex Finance (CVX)		+0.17%	+1.23%	+1.98%	\$12.74b	0.102			
4 AAVE (AAVE)		+3.02%	+12.81%	+19.86%	\$8.96b	0.25443			
5 Lido (LDO)		+3.92%	+21.41%	+68.94%	\$8.74b	0.06936			
6 Uniswap (UNI)		-1.47%	+0.87%		\$7.14b	0.69507			
7 Compound (COMP)		+1.50%	+2.57%	-0.16%	\$7.01b	0.11276			
8 Instadapp (INST)		0%			\$5.09b	0.00368			
9 Yearn Finance (YFI)		-0.65%	+1.45%	-3.39%	\$2.75b	0.27741			
10 Balancer (BAL)		+1.62%	+2.64%	-3.51%	\$2.68b	0.05248			
11 SushiSwap (SUSHI)		+0.99%	+6.40%		\$2.64b	0.26317			
12 Abracadabra (SPELL)		+1.21%	+3.54%	+2.04%	\$2.39b	0.16905			

二、Uniswap

关于什么是 Uniswap，先看一下 Uniswap 白皮书中的定义：

Uniswap is a protocol for automated token exchange on Ethereum. It is designed around ease-of-use, gas efficiency, censorship resistance, and zero rent extraction.

Uniswap 是一个基于以太坊的自动代币交换协议，它的设计目标是：易用性、gas 高利用率、抗审查性和零抽租。

- ease-of-use（易用性）：Token A 换 Token B，在 Uniswap 也只要发出一笔交易就能完成兑换，在其它交易所中可能需要发两笔交易：第一笔将 Token A 换成某种媒介货币，如 ETH，DAI 等，然后再发第二笔交易换成 Token B。
- gas efficiency（gas 高利用率）：在 Uniswap 上消耗的 gas 量是以太坊上的几家主流去中心化交易所中最低的，也就代表在 Uniswap 交易要付的矿工费最少。

Exchange	Uniswap	EtherDelta	Bancor	Radar Relay (0x)	IDEX	Airswap
ETH to ERC20	46,000	108,000	440,000	113,000*	143,000	90,000
ERC20 to ETH	60,000	93,000	403,000	113,000*	143,000	120,000*
ERC20 to ERC20	88,000	no	538,000	113,000	no	no

区块链大杂烩

*wrapped ETH

- censorship resistance (抗审查性)：抗审查性体现在 Uniswap 上架新 Token 没有门槛，任何人都能在 Uniswap 上架任何 Token。这在去中心化交易所中很少见，虽然大多数的去中心化交易所不会像中心化交易所那样向你收取上市费，但还是需要提交上市申请，通过审查后运营团队才会让你的 Token 可以在他们的交易所上交易。下面是各去中心化交易所上市规则的详情：
 - KyberSwap上市规则：<https://developer.kyber.network/docs/Reserves-ListingProcess/>
 - EtherDelta上市规则：<https://steemit.com/cryptocurrency/@mindsey69/new-etherdelta-coin-listing-rules>
 - IDEX上市规则：<https://medium.com/@forrestwhaling/idx-token-listing-guidelines-eae00785fdd2>
 - Uniswap上市规则：<https://uniswap.org/docs/v1/frontend-integration/token-listing/>
- zero rent extraction (零抽租)：在 Uniswap 协议设计中，开发团队不会从交易中抽取费用，交易中的所有费用都归还给流动性提供者。

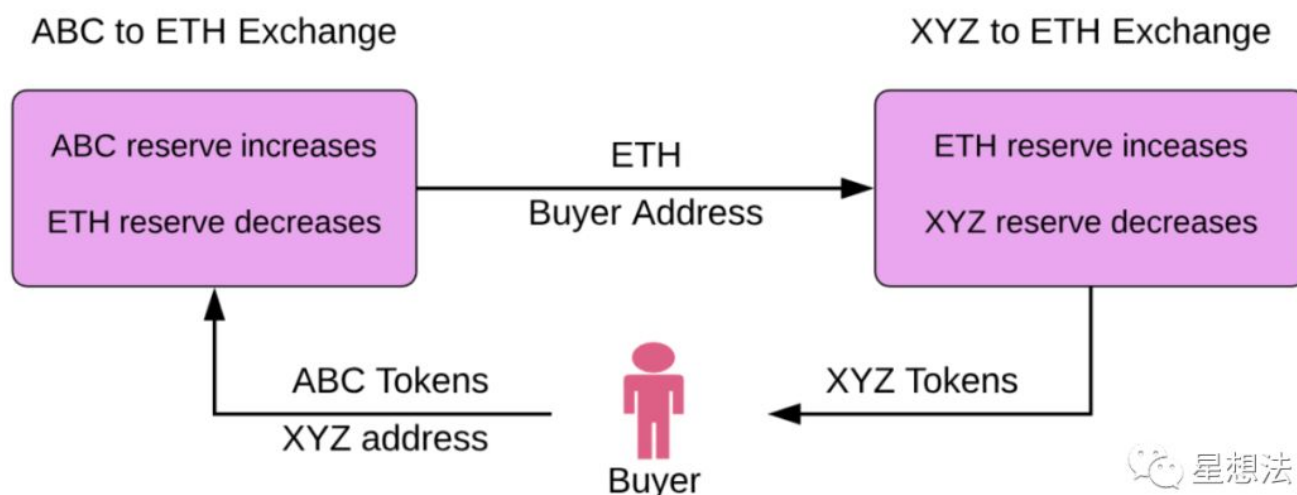
Uniswap 采用流动池加恒定乘法公式这种自动化做市商 (AMM) 模式实现了资产的交换。自动化做市商模式方式不需要买卖双方进行挂单，也不要买卖双方的订单重叠，可以进行自由买卖。

- 流动池：使用流动池来提供买卖双方交易，做市商只要把资金放入流动池即可
- 恒定乘法公式：按照流动池中 Token 的数量，自动计算买卖价格

2.1 自动化做市商 (Automated Market Maker, AMM)

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。

每个 Uniswap 智能合约或配对都管理一个由两个ERC-20代币储备组成的流动资金池，在多种代币都能和ETH交易的前提下，代币和代币之间交易如下图所示：



两个Exchange，一个提供了ABC和ETH的交易，一个提供了XYZ和ETH的交易。通过Uniswap协议，一个用户可以先通过ABC to ETH Exchange将ABC转成ETH，接着再通过XYZ to ETH Exchange将ETH转换成XYZ。整个过程Uniswap自动完成，从用户的角度来看，ABC代币直接转换成了XYZ代币。整个代币ABC转换XYZ过程都是自动化完成。

2.2 流动池

变量说明

x x 交易对中token0的存量 y y 交易对中token1的存量 Δ 一般表示增量 Δx 交易对新增的token0[用户输入或输出] Δy 交易对新增的token1[用户输入或输出] Δlp 交易对新增的lp token[用户输入或输出]

流动池就是锁定在智能合约中所有的代币以及资金的总称，流动是资金转为代币，或代币转为资金的意思。

流动性相关概念：

- **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

2.2.1 流动性池初始化

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）。

流动性池中两种代币的相对价格是通过池子中两种代币的数量比来决定的，直观的理解就是两种代币的总价值是相同的，每次交易完之后由于两种代币的数量会发生变化，相对价格也会变化，价格的调整遵循如下公式：

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

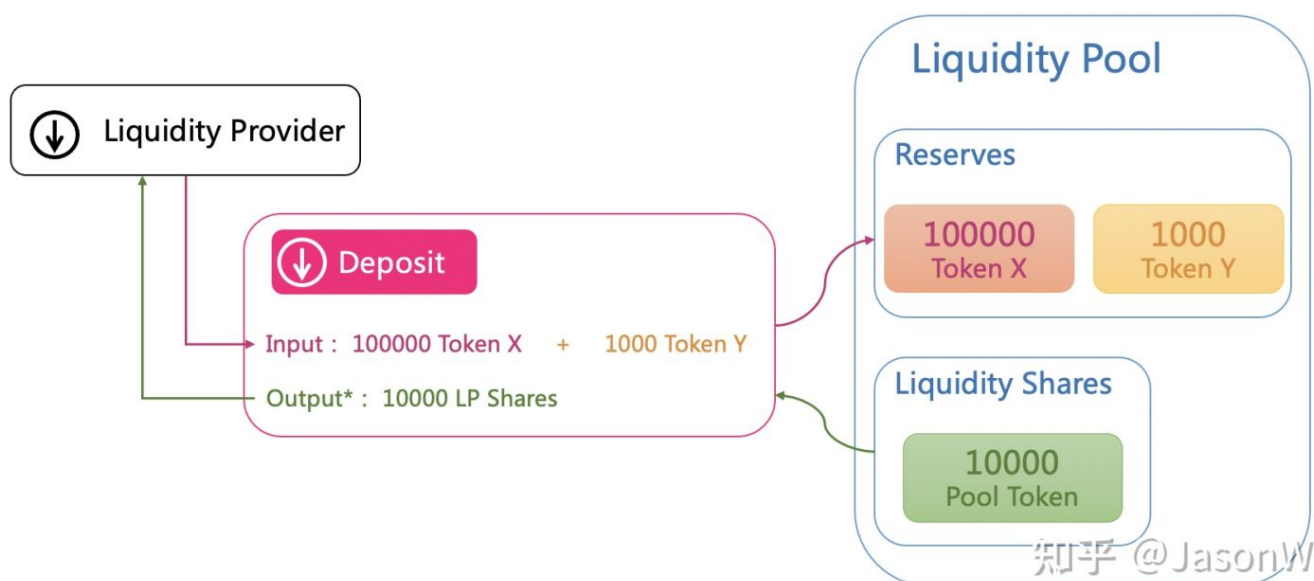
x和y代表两种代币的数量，具体在 **2.3 章节恒定乘积公式** 描述。

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。

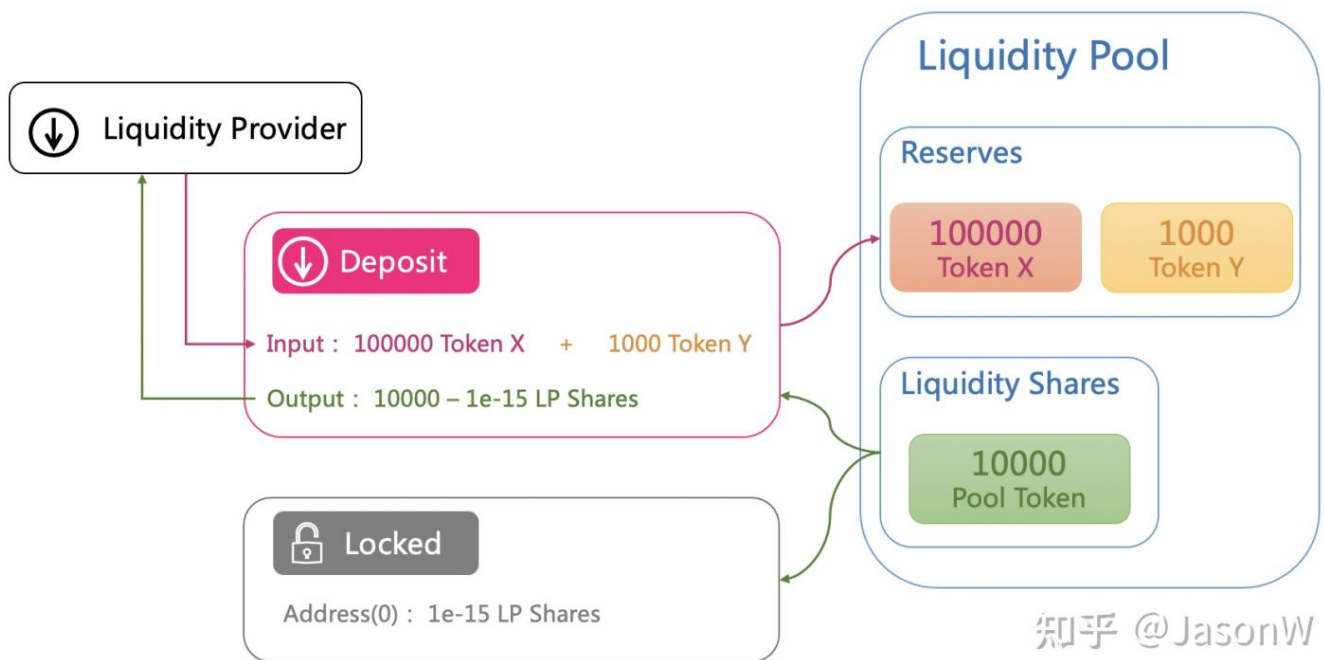
如下图所示，假设初始质押量为x_0 = 100,000，y_0 = 1,000，则s_0 = 10,000，在LP质押完X和Y代币之后会收到10,000LPS，此时s_current也同样是10,000，相当于第一个LP持有100%的LPS（除去锁定到零地址的LPS），Liquidity Pool中当前Y相对于X的价格为 $1 Y = 100000 / 1000 X = 100 X$ ，例如X是USDT，Y是ETH的话，那么 1 ETH = 100 USDT。



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：



知乎 @JasonW

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 $1e-15$ LPS，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 $1e-15$ LPS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。

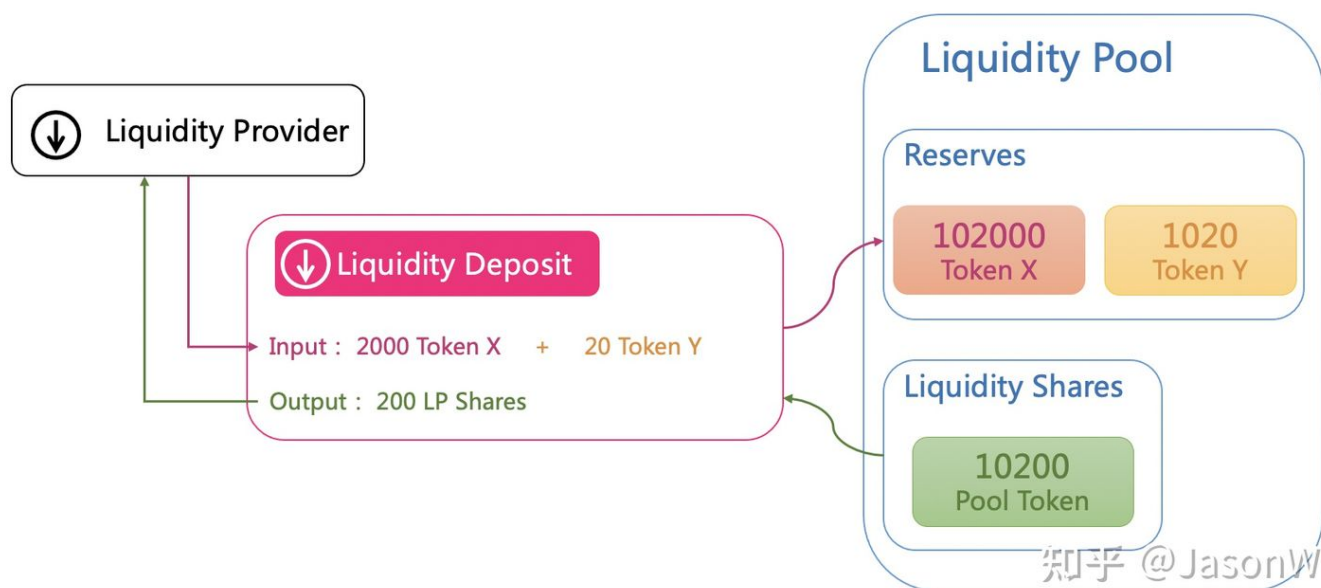
2.2.2 添加流动性

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} ：

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

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。



2.2.3 减少流动性

减少流动性就是把用户lp所占总lp比例的token0和token1返还给用户。

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 $y_{withdraw}$ ：

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

整个流动性相关还会涉及到协议手续费的问题，默认是不收取的，此处暂不讨论。

2.3.4 流动性总结

流动性有如下特点：

- 用户通过给交易对中注入token0和token1来增加交易对的深度
- 如果是交易对第一次添加流动性，用户可以注入任意比例的token0和token1来订制token0和token1的价格
- 否者则需要按照交易对中现有的比例来注入token0和token1，如果不是按照比例添加则会在增加深度的同时修改token0和token1的价格

2.3 恒定乘积公式

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 Δx ，交易换回的Y为 Δy ，在交易池中的资产足够的前期下，满足：

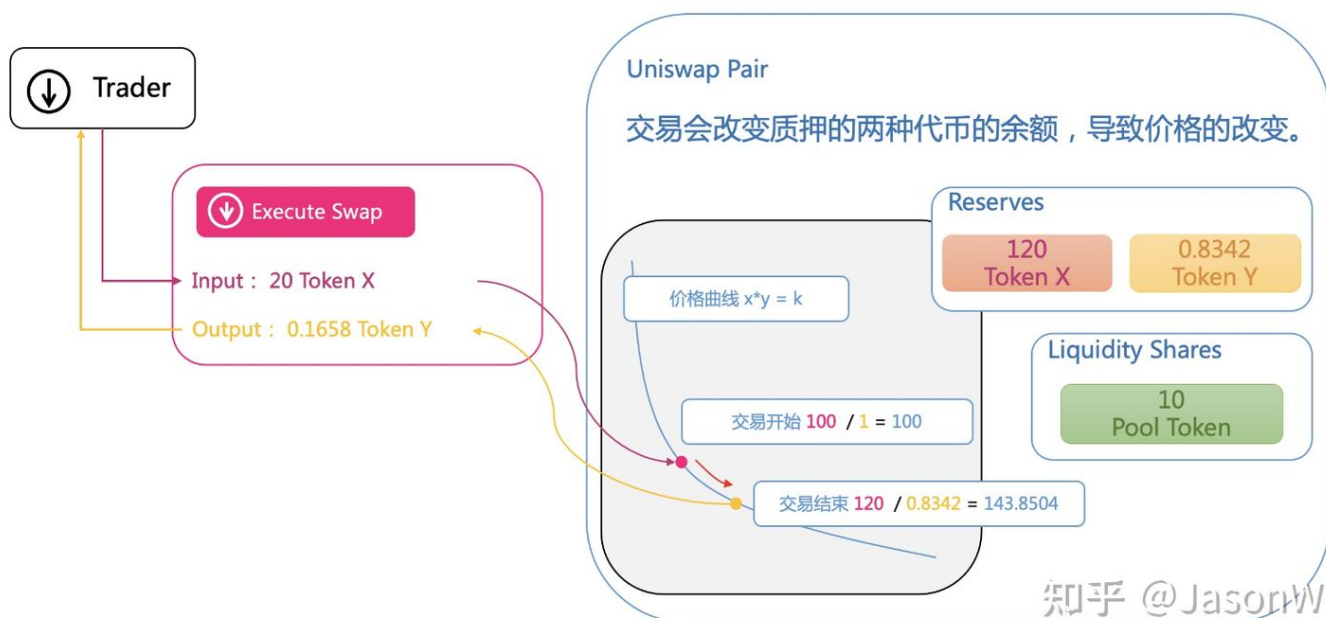
$$(x + \Delta x) \times (y - \Delta y) = k$$

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

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：

$$(100 + 19.94) \times (1 - \Delta y) = 100$$

$$\Delta y \approx 0.1658$$

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。

恒定乘积算法有如下特点：

- **根据交易情况反映价格。** 当有人用A代币兑换B代币（即买入B）时，B的价格就会上涨，反过来（卖出B）则B价格下跌，符合一般交易价格规律。
- **流动性保持。** 无论流动池的资金规模如何，该算法均能提供流动性。
- **不适合大额的交易兑换。** 我们发现在进行大额交易兑换的时候，价格变化很大，且不是线性的。当然，这个大额是相对于流动池的规模来判别的。

2.3.1 交易价格计算

交易价格的计算分成两种：一种是给定X的数量，计算能买到的Y的数量（Input）；一种是给定Y的数量，计算需要的X数量（Output）。

getInputPrice的计算公式如下：

Definition 5. Let ρ be the trade fee. $\text{getInputPrice}_{\text{spec}}$ takes as input $\Delta x > 0$, x , and y , and outputs Δy such that:

$$\text{getInputPrice}_{\text{spec}}(\Delta x)(x, y) = \Delta y = \frac{\alpha\gamma}{1 + \alpha\gamma}y$$

where $\alpha = \frac{\Delta x}{x}$ and $\gamma = 1 - \rho$. Also, we have:

$$x' = x + \Delta x = (1 + \alpha)x$$

$$y' = y - \Delta y = \frac{1}{1 + \alpha\gamma}y$$

星想法

也就是说，Delta X的代币能换取Delta Y的其他代币。此时，Y代币的价格为：

$$\frac{\Delta x}{\Delta y} = \frac{\Delta x}{\frac{\alpha\gamma}{1 + \alpha\gamma}y} = \frac{1 + \alpha\gamma}{\gamma} \frac{x}{y}$$

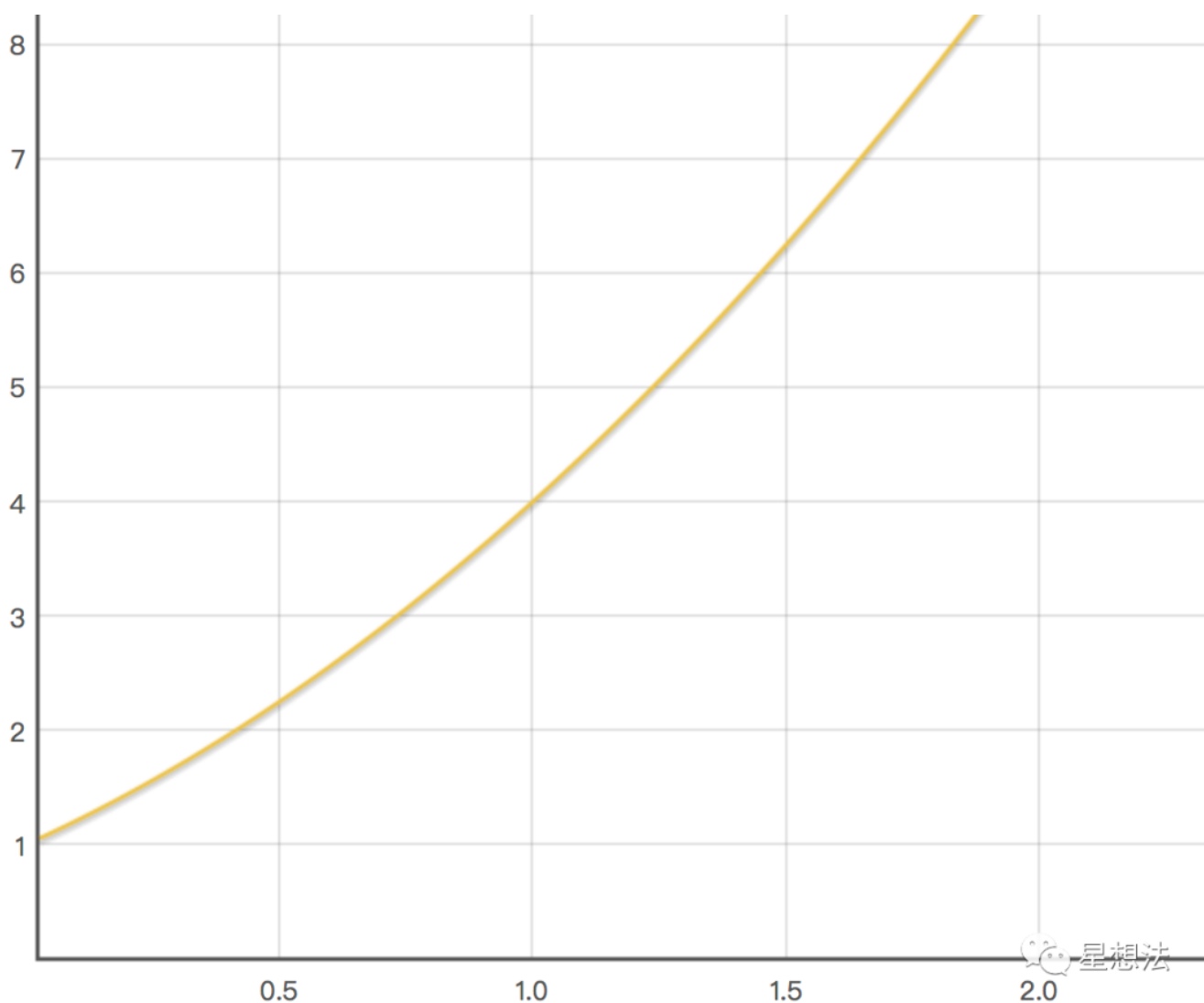
星想法

简单的说，买入越多X，alpha越大，价格也越高。如果alpha为1的话（用当前流动性中X总额相等的X代币买入），也只能买差不多流动性中的一半的Y代币。如果把x/y视作当前Exchange的价格的话，一次买入后，价格变化为：

$$\frac{x'}{y'} = \frac{(1+\alpha)x}{\frac{1}{1+\alpha\gamma}y} = (1+\alpha)(1+\alpha\gamma)\frac{x}{y}$$

星想法

下面是兑换后价格随着 δ 的增加而变化的函数图像：



星想法

getOutputPrice的计算公式如下：

Definition 7. Let ρ be the trade fee. $getOutputPrice_{spec}$ takes as input $0 < \Delta y < y$, x , and y , and outputs Δx such that:

$$getOutputPrice_{spec}(\Delta y)(x, y) = \Delta x = \frac{\beta}{1-\beta} \cdot \frac{1}{\gamma} \cdot x$$

where $\beta = \frac{\Delta y}{y} < 1$ and $\gamma = 1 - \rho$. Also, we have:

$$x' = x + \Delta x = \frac{1 + \beta(\frac{1}{\gamma} - 1)}{1 - \beta} \cdot x$$

$$y' = y - \Delta y = (1 - \beta)y$$

星想法

也就是说，Delta Y的代币能换取Delta X的X代币。此时，Y代币的价格为：

$$\frac{\Delta x}{\Delta y} = \frac{\frac{\beta}{1-\beta} \frac{1}{\gamma} x}{\Delta y} = \frac{1}{(1-\beta)\gamma} \frac{x}{y}$$

星想法

简单的说，买入越多Y，beta越大，价格也越高。如果beta为1/2的话（买入当前流动性中一半的Y代币），大约需要当前流动性中等量的X代币。getInputPrice和getOutputPrice分别从两种代币角度计算价格，具体的价格是一致的。

2.3.2 恒定乘积的总结

在满足 $k = xy$ 的场景下：

- 添加流动性注入的token0和token1会使k变大
- 移除流动性取走的token0和token1会使k变小
- 交易如果不收取手续费，k值不变
- 在收取手续费的情况下，交易会使得k增大

2.4 滑点

什么是滑点，滑点一般指预设成交价位与真实成交价位的偏差。由于在uniswap的交易不是指定价格成交的限价单模式，每个用户的交易都会影响市场的价格，并且影响市场的价格和交易数量

有关。为了避免该用户的交易在广播到区块链前有交易量很大的用户进行交易进而对市场的价格有较大的影响，该项目设计了滑点保护机制来避免用户损失。一般来讲交易额越大，滑点越大，交易者的损失就越大。

公式分析

根据恒定乘积，当用 dx 个 x 兑换 dy 个 y 时（忽略手续费），有：

$$\begin{cases} xy = k \\ (x + dx)(y - dy) = k \end{cases}$$

可得，兑换量：

$$dy = \frac{y \cdot dx}{x + dx} \quad (1)$$

则在实际兑换中， y 相对 x 的单价为：

$$dx/dy = \frac{x + dx}{y}$$

而兑换前，池中的 y 单价为 x/y ，那么 y 单价的滑点就产生了：

$$Slippage_{yPrice} = dx/dy - x/y = \frac{dx}{y}$$

交易量 dx 越大，产生的滑点就越大，偏离实际价位就越大，而池中的资金储备越多、交易深度越大，则能尽量减少滑点的溢价，使用户的交易损耗降低。


实际计算

Uniswap在实际计算交易滑点时，是通过百分比来显示的：

Swap

From


4

 ETH

↓

To (estimated)

19.0735

 AAVE

Price

0.209714 ETH per AAVE

Connect Wallet

Minimum received

18.97 AAVE

Price Impact

0.04%

Liquidity Provider Fee

0.012 ETH

View pair analytics

Uniswap源码中对滑点的计算是在 `uniswap-v2-sdk/src/entities/trade.ts` 文件中的 `computePriceImpact` 函数中实现的

```

/**
 * Returns the percent difference between the mid price and the execution price,
 i.e. price impact.
 * @param midPrice mid price before the trade
 * @param inputAmount the input amount of the trade
 * @param outputAmount the output amount of the trade
 */
function computePriceImpact(midPrice: Price, inputAmount: CurrencyAmount,
outputAmount: CurrencyAmount): Percent {
  const exactQuote = midPrice.raw.multiply(inputAmount.raw)
  // calculate slippage := (exactQuote - outputAmount) / exactQuote
  const slippage = exactQuote.subtract(outputAmount.raw).divide(exactQuote)
  return new Percent(slippage.numerator, slippage.denominator)
}

```

按照函数中的逻辑，滑点百分比计算公式如下：

$$PriceImpact = \frac{midPrice \cdot dx - dy}{midPrice \cdot dx} \quad (2)$$

这里的 `midPrice` 从代码上看不出是x对y的价格还是y对x的价格，但按照公式的计算逻辑，当 `midPrice` 代表x对y的价格时，`midPrice · dx` 就代表理论应得y的数量，那么这个公式就是按照滑点差值/理论应得量的方式计算的

为验证这一点，来到Uniswap界面断点调试，以ETH兑换AAVE为例

The image shows a composite view of the Uniswap interface and its source code. On the left, the Uniswap Swap interface is visible, showing a swap from 4 ETH to 214.274 AAVE. The price is listed as 0.210011 ETH per AAVE. A red arrow points from this price to the code. In the center, the source code for the `computePriceImpact` function is shown, with a red box highlighting the calculation of `exactQuote` and `slippage`. On the right, the debugger's 'Scope' panel shows the state of variables, with a red box highlighting the `midPrice` object. At the bottom, the console shows the state of the `temp1` object, with a red box highlighting the `numerator` and `denominator` values.

Key data points from the interface and code:

- Swap: From 4 ETH, To (estimated) 214.274 AAVE, Price 0.210011 ETH per AAVE.
- Code: `const exactQuote = midPrice.raw.multiply(inputAmount.raw)`
- Debugger Scope: `midPrice` object with `baseCurrency` 'ETH' and `quoteCurrency` 'AAVE'.
- Console: `temp1` object with `numerator` [1786478792, -798442239, 2314, sign: false] and `denominator` [257326518, 1857195416, 482, sign: false].

可以看到 `midPrice` 实际采用的确实就是前面猜测的x对y的价格，并且是不同于界面中Price所显示实际兑换价的理论价

那么化简公式 (2)：

$$PriceImpact = \frac{y/x \cdot dx - dy}{y/x \cdot dx} = 1 - \frac{dy \cdot x}{y \cdot dx}$$

将前面推导的公式 (1)，代入上式可得：

$$PriceImpact = \frac{dx}{x + dx} \quad (3)$$

那么滑点百分比即是兑换量占用于兑换的资产储备量的百分比

当然，这里总结出的滑点计算还只是通过AMM机制所算出的理论滑点，实际上滑点还会受很多因素影响，比如网络延时、区块确认等等。

2.5 套利

套利交易者是Uniswap生态系统中一个不可或缺的组成部分。这些交易员擅长发现多个交易平台之间的价格差异，并利用它们来获取利润。例如，如果BTC在Kraken上的交易价格是3.55万美元，Binance的价格是3.45万美元，你可以在Binance上购买BTC，然后在Kraken上出售，从而轻松获利。如果交易量大，就有可能以相对低的风险获得可观的利润。

套利交易者在Uniswap上所做的是找到高于或低于其平均价格的Token交易——这是由于大量交易在pool中造成失衡并降低或提高价格的结果——并相应地买卖它们。

2.6 做市商的收益和风险

做市商的收益来源于两个部分，一个部分是交易者的手续费，另一部分是做市挖矿。做市挖矿也是后来uni上线以后才推出的，把做市的LP token抵押挖uni。而做市商的风险来源于无常损失

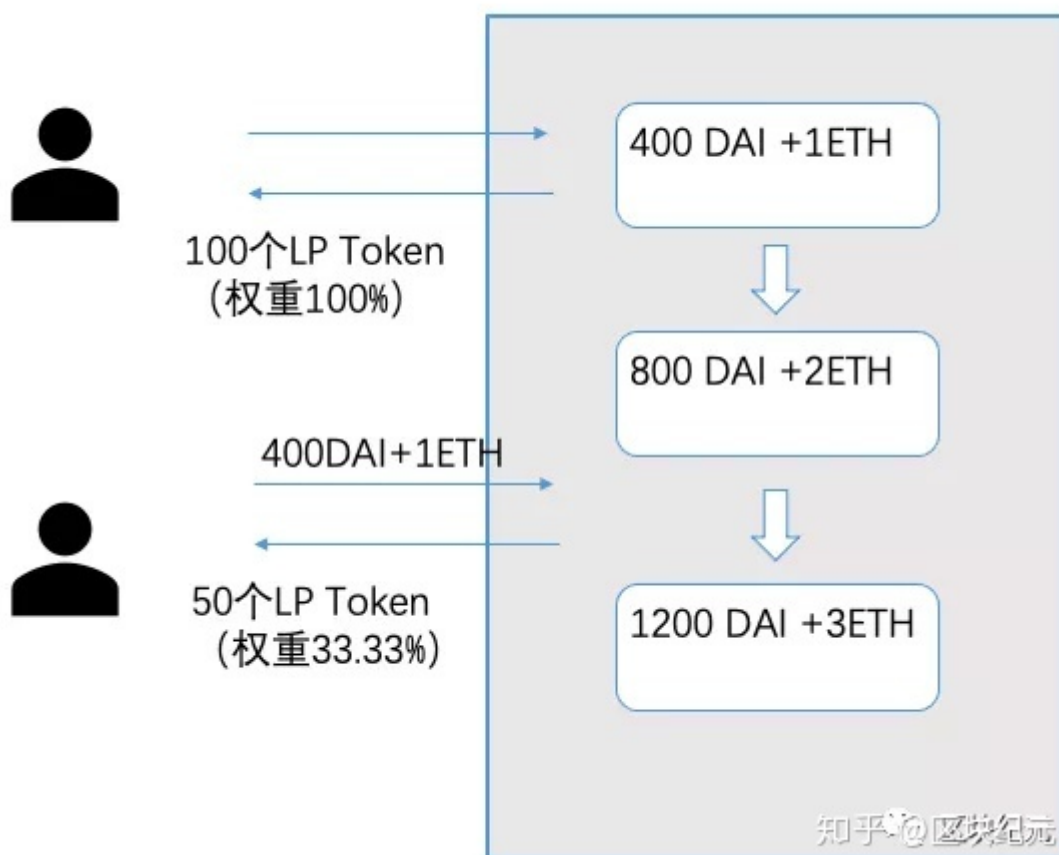
2.6.1 收益部分（手续费+uni）

- 手续费获取的操作步骤：

做市商提供流动性（DAI和ETH），根据数量的权重获得特定数量的LP token

交易者进行兑换，每次兑换都给池子里支付本金的0.3%手续费（如果支付DAI购买ETH，就收DAI的0.3%做手续费，反之亦然）

退出做市，根据LP token占整个池子LP token的比例和池中2个币种数量的比例赎回DAI和ETH



举例：

第一个做市商往池子里加入400个DAI和1个ETH，获得100个LP token，权重为100%

交易者进行兑换，为池子中贡献了400个DAI和1个ETH的手续费。池子中变成800个DAI和2个ETH。如果第一个做市商退出做市，会获得池中100%的DAI和ETH

第二个做市商往池子里加入400个DAI和1个ETH，池子中变成1200个DAI和3个ETH。由于第二个市商贡献的比例为 $400/1200=33.33\%$ ，所以获得的LP token占整个LP token的33.33%。有以下关系 $LP\ token / (100 + LP\ token) = 33.33\%$ ，得出LP token=50

若2个做市商退出做市，且此时池子中变成 1500个DAI和1.5个ETH。第一个市商获得 $1500 \times 66.67\% = 1000$ 个DAI 和 $1.5 \times 66.67\% = 1$ 个ETH。第二个市商获得 $1500 \times 33.33\% = 500$ 个DAI 和 $1.5 \times 33.33\% = 0.5$ 个ETH

注：虽然两个做市商投资的成本是一样的，但是在第二个做市商做市之前，第一个做市商获得了手续费的收入。

- uni的收益

根据debank的数据，目前uni的挖矿年化在13%~25%之间



(uni的价格走势，数据来源：非小号)

2.6.2 风险部分（无常损失）

为了更好的理解无常损失，先来感性地了解一下为什么会出现无常损失。假设一个池子中只有一个市商，添加了400个DAI和1个ETH的流动性。几分钟后，eth的价格上涨到500DAI/ETH，但是池子里还是400，于是就有用户过来用400的价格购买ETH，直到池子中DAI的数量/ETH的数量等于500，套利结束。那么对于做市商来说，价值500DAI的ETH，却在400~500之间的价格出售了，这就导致了做市商的亏损

当做市商赎回token的时候，会根据交易池里两个币种的比例进行赎回。由于赎回的token数量和比例和添加流动性时的不一样，导致参与做市和不做市最后的美金价值的不一致的。（注：这里只考虑无常损失，没有考虑手续费收益）

无常损失=（持币不做市的token价值-做市商以后的token价值）/持币不做市的token价值

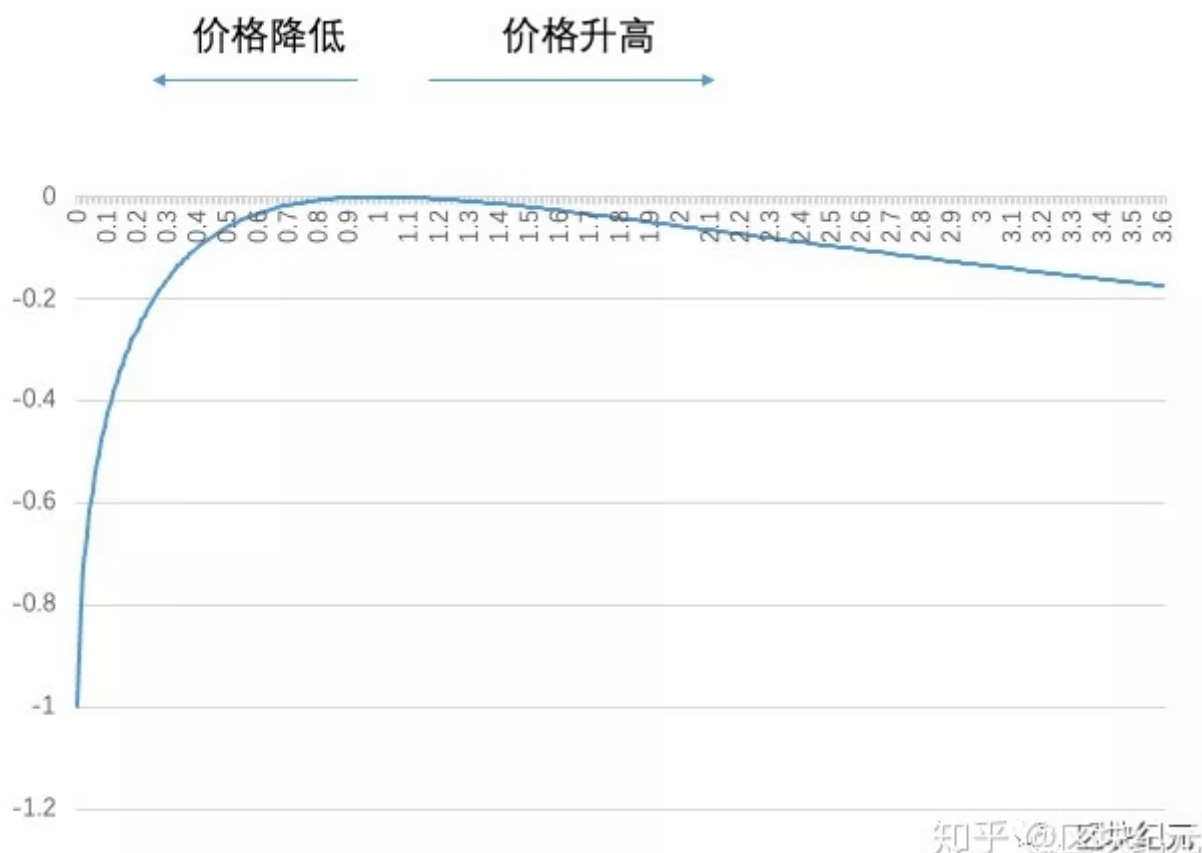
$$\text{无常损失} = \frac{\text{参与做市的价值}}{\text{持币但不做市的价值}} - 1$$

$$= \frac{X' + Y'P'}{X + YP'} - 1$$

$$= \frac{2\sqrt{\gamma}}{1 + \sqrt{\gamma}} - 1$$

$\gamma = \frac{P'}{P}$ ，为价格的变化 知乎 @区块链纪元

以 γ 为横轴，无常损失为纵轴，可得出曲线如下图所示。无论价格是升高还是降低，都会存在无常损失。只有价格不变不存在无常损失。并且当价格降低的时候我们可以发现，亏损的程度呈指数型上升，本金甚至有归零的风险。对于价格波动越是剧烈的token，越是要谨慎参与做市。



另：无常损失参考案例

	DAI	ETH	Price (DAI/ETH)		
添加时数量	400	1	400	做市	不做市
Price变成1600	800	0.5	1600	$800 + 0.5 \times 1600 = 1600$	$400 + 1 \times 1600 = 2000$
Price变成100	200	2	100	$200 + 2 \times 100 = 400$	$400 + 2 \times 100 = 600$

三、uniswap其他知识

3.1 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，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。
- 2020年9月17日，Uniswap宣布其协议治理代币UNI已在以太坊主网上发布，针对每一个之前使用过Uniswap protocol的区块链地址空投400个UNI，UNI的持有者有对平台新的发展及改变的提议的投票权。
- 2021年5月5日，Uniswap v3版本上线，提供了集中流动性、多重收费层次、高级价格预言机、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。

3.2 uniswap的发展壮大的原因

3.2.1 几乎零门槛发币

为了提供更加多样的代币兑换和更好的流动性，用户是可以免费建立流动池的，这也就意味着无需上币费用即可上币，上币成本为0也就意味着作恶成本极大降低。由此也造成了大量“空气币”割韭菜的现象。

3.2.2 滑点

因为很多 shit coin 的池子流动很小，所以交易兑换时滑点相当大。只要短时间有一批人涌入，很容易买飞，就造成一种价格翻了十多倍的景象

3.2.3 数据公开透明

uniswap上面有多少资产，成交量多少，都在区块链上，可以公开查询，一目了然。

3.2.4 匿名性

uniswap是区块链公链的，这恰恰满足了一些特别用户匿名需求。

3.2.5 开源共享共治社区

uniswap刚开始并没有发行自己的治理代币。秉承着谁为社区做贡献谁收益的原则，把所有交易手续费收益分给做市商。在发行治理代币的时候，直接给使用过uniswap的用户空投价值约1w人民币的uni，零成本地邀请交易者和做市商参与社区的治理。

附录

[去中心化交易](#)

[uniswap是什么？](#)

[一文彻底了解无常损失](#)

[Uniswap v3 设计详解](#)

[UniswapV2公式推导](#)