



uniswap - V3技术白皮书导读



Star.Li

4 人赞同了该文章

uniswap V3一公布就引发广泛关注。相对V2来说，逻辑和代码都复杂一些。V3的核心是通过盘口区间提供流动性（集中式流动性），解决LP提供流动性时的资金利用率的问题。什么是资金利用率？V3如何推导区间流动性的计算公式？如何理解流动性？如何计算swap费用？本文先从V3技术白皮书详细分析开始。

先给出一些uniswap官方有关V3的资料：

- V3官方介绍

[uniswap.org/blog/uniswap...](https://uniswap.org/blog/uniswap-v3)

- 技术白皮书

[uniswap.org/whitepaper-...](https://uniswap.org/whitepaper-v3)

- 智能合约代码

[github.com/Uniswap/unis...](https://github.com/Uniswap/uniswap-v3-core)

[github.com/Uniswap/unis...](https://github.com/Uniswap/uniswap-v3-core)

推荐先认真查看技术白皮书，再看智能合约代码，最后再对照官方介绍。理解了技术白皮书，代码非常容易理解。在技术白皮书的第一章总结了uniswap V3的技术特点，最核心的概念是"Concentrated Liquidity"（集中式流动性）。

1 资金利用率

先看看uniswap V2的资金利用率：

▲ 赞同 4 ▼

● 4 条评论

↗ 分享

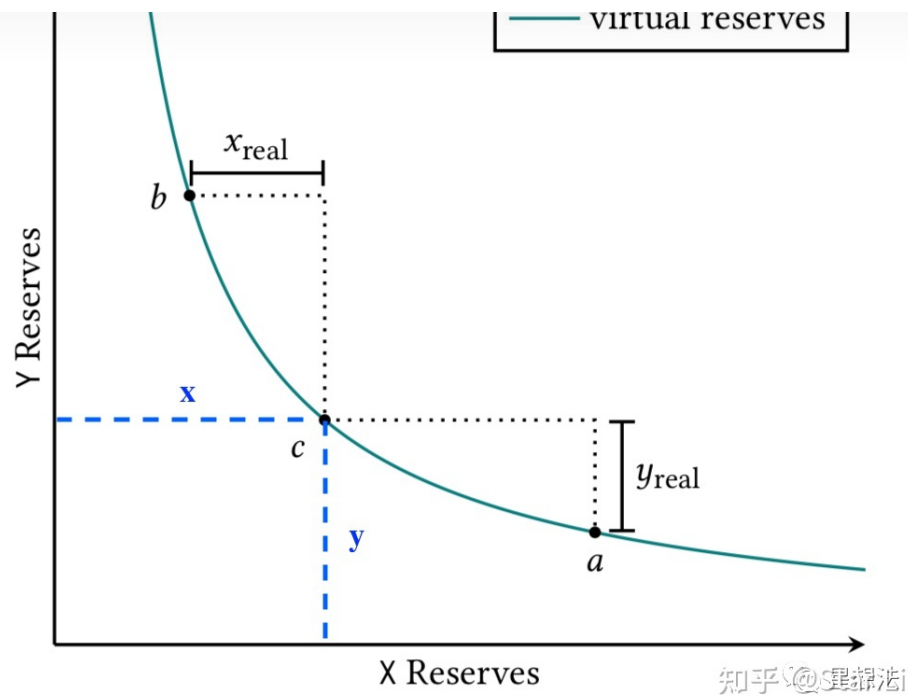
♥ 喜欢

★ 收藏

📄 申请转载

...



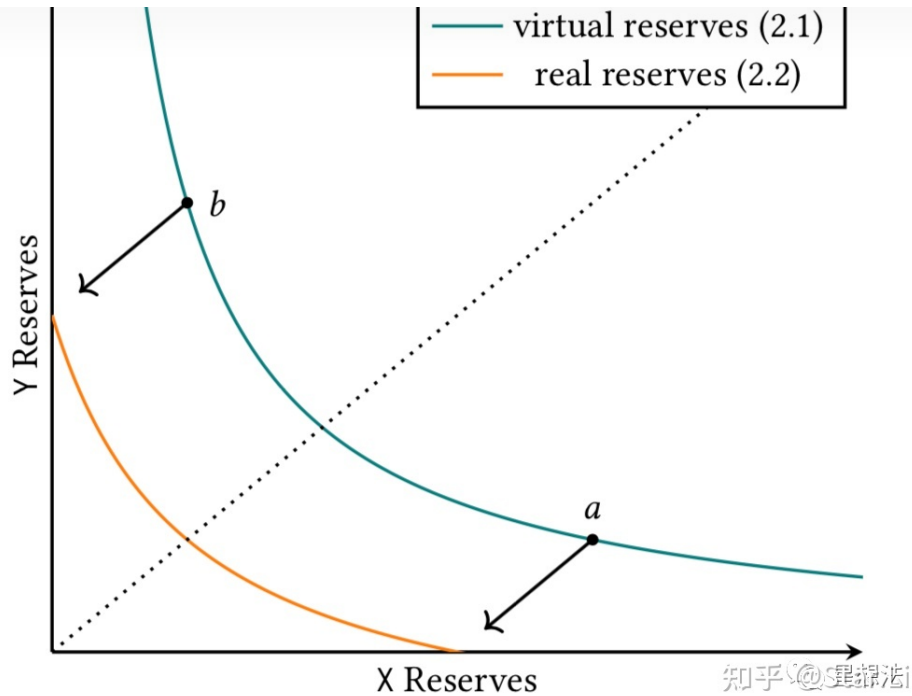


上图资金池中的 x/y 的量变化曲线。资金池中的当前价格在 c 点，并且假设会在 a 价格点和 b 价格点之间波动。从 c 点向 a 点滑动，消耗最大 y_{real} ，从 c 点向 b 点滑动，消耗最大为 x_{real} 。也就是说，当前价格 c 点，在 a 点和 b 点之间震荡的话，最大只需要消耗 x_{real} 和 y_{real} 。理论上只要提供 x_{real} 和 y_{real} 就足够了。而事实上，如上图所示，在价格 c 点，分别提供了大于 x_{real} 和 y_{real} 的 x 和 y 。明显可以看出， $x-x_{real}$ 和 $y-y_{real}$ 的资金在这种情况下是永远用不上的，也就称为闲置资金。

在这种情况下，资金利用率为 x_{real}/x 或者 y_{real}/y 。如果价格波动非常小的话，资金利用率是非常低的。uniswap V3就是尝试解决资金利用率低的问题。想法比较简单，所有资金可以只添加到某个区间，只添加到有可能价格波动到的区间范围。如何在某个区间添加流动性并提供swap功能是uniswap V3的重点。先从Virtual Reserves说起。

2 虚拟资金池 (Virtual Reserves)

uniswap的交易采用的乘积固定模型($x*y=k$)。所谓的虚拟资金池(Virtual Reserves)，是指还在乘积固定曲线上，只提供某个区间流动性的资金池：



图中的墨绿色的曲线就是虚拟资金池满足的乘积固定曲线。事实上需要的资金的曲线如图中的橘黄色。橘黄色的曲线公式如下图：

$$\left(x + \frac{L}{\sqrt{p_b}}\right)(y + L\sqrt{p_a}) = L^2 \quad (2.2)$$

你可以想象成虚拟资金曲线在x/y轴进行平移，使得a/b点和x/y轴重合。也就是用一定量的资金就能达到“虚拟”的交易曲线的效果。

如何计算在某个区间提供虚拟资金池，先要从深入理解流动性开始。

3 流动性 (Liquidity - L)

乘积固定的交易模型，满足资金池中的两种代币金额满足： $x*y = K$ 。如果设定 $K=L^2$ 的话， $x*y = L^2$ 。L就是我们说的流动性。由乘积固定的交易模型得出如下的公式：

$$L = \sqrt{xy} \quad (6.3)$$

$$\sqrt{P} = \sqrt{\frac{y}{x}} \quad (6.4)$$

在已知L和 \sqrt{P} 的情况下，也能推导出资金需求量x和y。

$$y = L \cdot \sqrt{P}$$

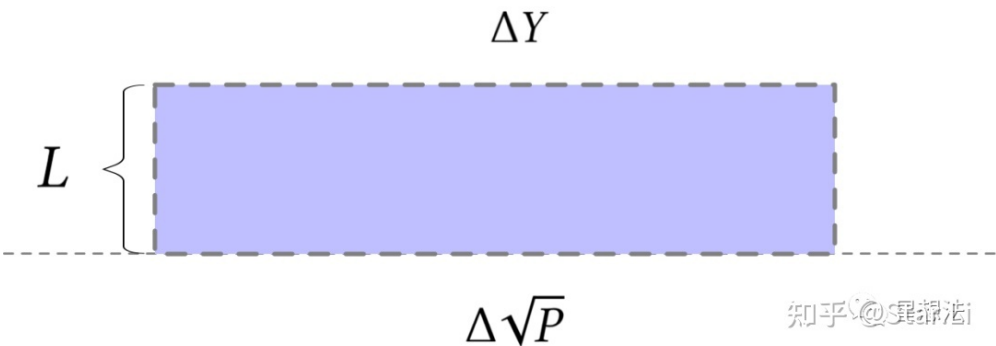
知乎@星想法 (6.6)

通过公式6.6，在流动性不变的情况下（不添加删除流动性），流动性可以看成是单位“价格波动”的y资金量的变化。“价格波动”打上引号是因为事实上是sqrt(P)的变化。

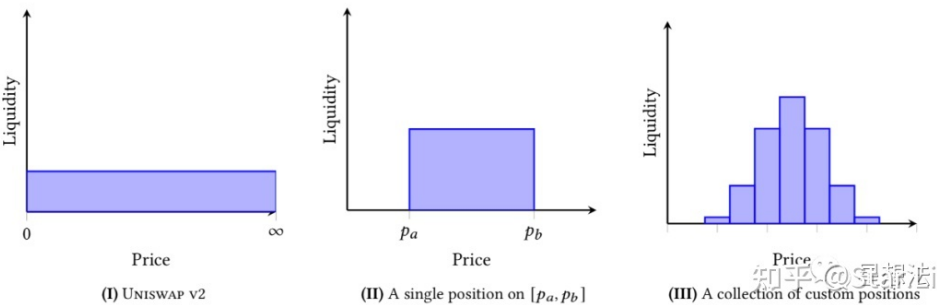
$$L = \frac{\Delta Y}{\Delta \sqrt{P}}$$

星想法 (6.7)

这个是uniswap V3核心公式（6.7），用相对值（资金和价格相对值）来计算流动性。所谓的流动性，就是单位“价格变化”的资金量。在一定的交易量的情况下，如果流动性好，价格变化就小，流动性不够的话，价格波动就大。



特别注意的是，一个区间上的流动性和V2的普适的流动性不同。一个区间上的流动性，重点在“区间上”。不同区间的流动性没有可比性。V2的流动性和区间上的流动性的区别如下图：



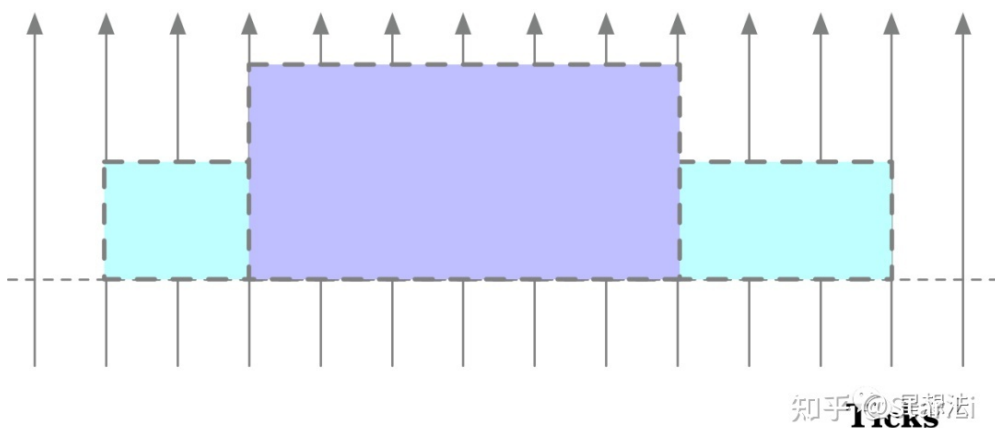
V2的流动性是“普适”的，在所有价格点上流动性相同。V3的流动性是由一系列不同区间上的流动性组成。相对来说，在当前价格左右的流动性比较高。流动性提供者LP只有提供了可供交易的流动性才能获取交易费。为了获取更多的交易费，为了提高资金的利用率，流动性提供者会将资金提供在合理的价格波动范围内。也就是说，在某个区间swap交易产生的手续费，只有该区间流动性提供者才能获取手续费。为了计算每个区间获取的手续费，引入了Tick的概念和计算方法。

4 Tick

uniswap V3引入了Tick的概念。交易费用实时结算并单独记录，并不混入流动资金中。虽然整个区间和区间的流动性没有可比性，但是，在具体的某个价格点上（一个价格片上），流动性是可比較的。uniswap V3将整个价格范围(负无穷到正无穷)分成一个个的Tick（价格点）：

$$p(i) = 1.0001^i \quad (6.1)$$

后一个价格点的价格是前一个价格点价格基础上浮动万分之一。



每个Tick也有一个唯一的序号。区间（Position）可以由两个Tick表示。逻辑上交易手续费可以一个个的Tick计算，并在每一个Tick上根据流动性的占比进行交易分配。先看看一个Tick范围的swap的计算。

5Tick内的SWAP

假设有一个很小的量的y，需要swap为x。通过6.13的公式，可以计算出因为y的变化导致的价格变化。

$$\Delta \sqrt{P} = \frac{\Delta y}{L} \quad (6.13)$$

再利用6.15的公式可以算出换取的x的量。

$$\Delta \frac{1}{\sqrt{P}} = \frac{\Delta x}{L} \quad (6.15)$$

在同一交易池中只支持一种费率。也就是说，在一个交易池中支持不同的价格区间，但是都是同样的费率。如果需要添加同样交易对的不同交易费的交易池，必须创建新的交易池。

接下来，深入讲解一下 添加/删除流动性以及交易费用的计算逻辑。

6 添加/删除流动性

V3的添加/删除流动性是当前价格情况下在某个区间添加或者删除流动性。所有的流动性添加/删除流动性采用如下的公式：

$$\Delta Y = \begin{cases} 0 & i_c < i_l \\ \Delta L \cdot (\sqrt{P} - \sqrt{p(i_l)}) & i_l \leq i_c < i_u \\ \Delta L \cdot (\sqrt{p(i_u)} - \sqrt{p(i_l)}) & i_c \geq i_u \end{cases} \quad (6.29)$$

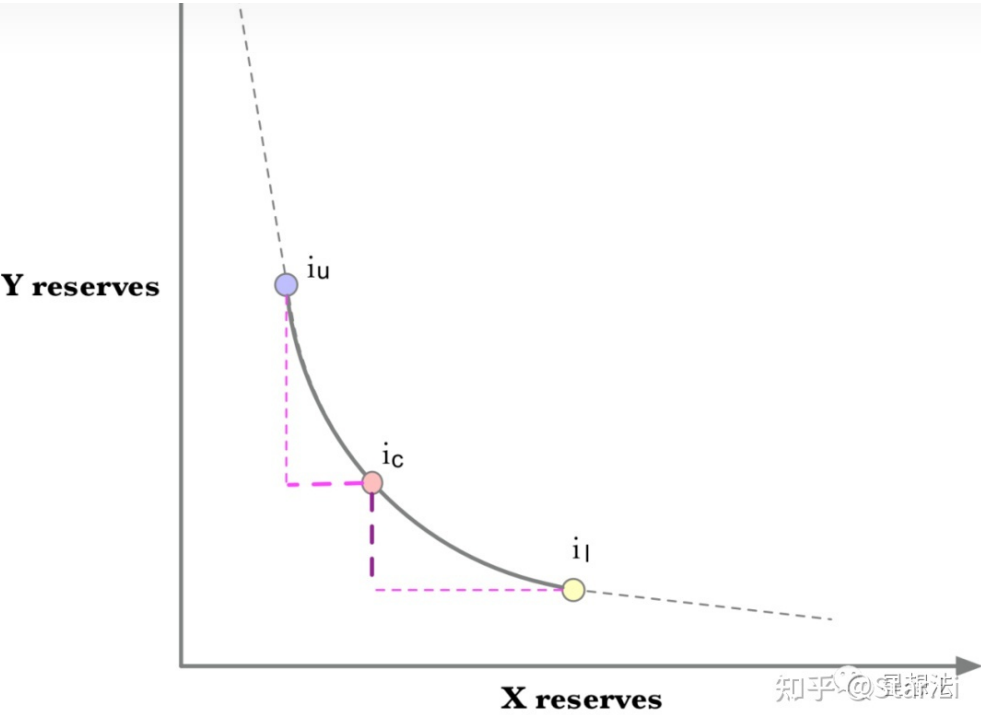
$$\Delta X = \begin{cases} \Delta L \cdot (\frac{1}{\sqrt{p(i_l)}} - \frac{1}{\sqrt{p(i_u)}}) & i_c < i_l \\ \Delta L \cdot (\frac{1}{\sqrt{P}} - \frac{1}{\sqrt{p(i_u)}}) & i_l \leq i_c < i_u \\ 0 & i_c \geq i_u \end{cases} \quad (6.30)$$

知乎@墨菲法

注意，价格变化并不是指区间的大小，而是在某个区间上提供流动性，相对当前价格，“需要相应资金变化”对应的价格变化。

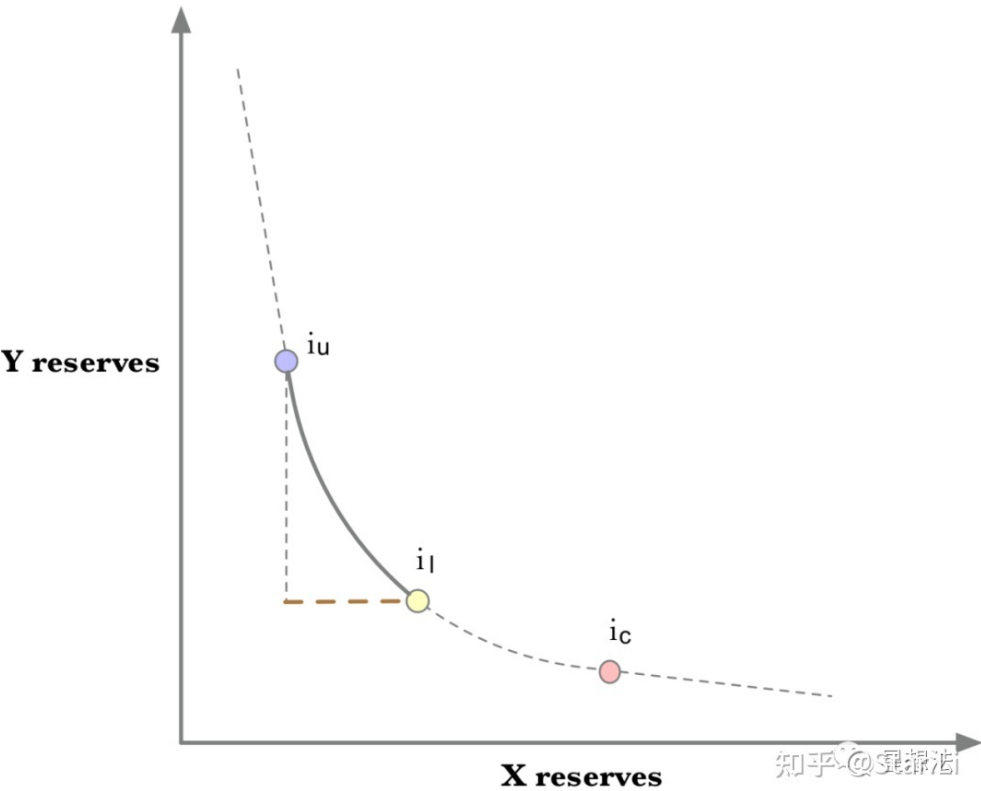
分为三种情况，想要添加的流动性区间和当前价格的关系。

- 当前价格处于流动性价格区间 ($i_l \leq i_c < i_u$)



因为价格在区间范围内，如果价格滑动到 i_l ，则需要提供y资金。如果价格滑动到 i_u ，则需要提供相应的x资金。所以，对于 ΔY 来说的，价格变化为 $\sqrt{P} - \sqrt{P(i_l)}$ ；对于 ΔX 来说，价格变化为 $1/\sqrt{P} - 1/\sqrt{P(i_u)}$ 。

- 当前价格低于流动性价格区间



因为当前价格远低于 i_l ，即使从当前价格向 i_u 滑动，也只需要x的资金，不需要y的资金。所以，在来说，价格变化

和第一种情况类似，不重复分析了。

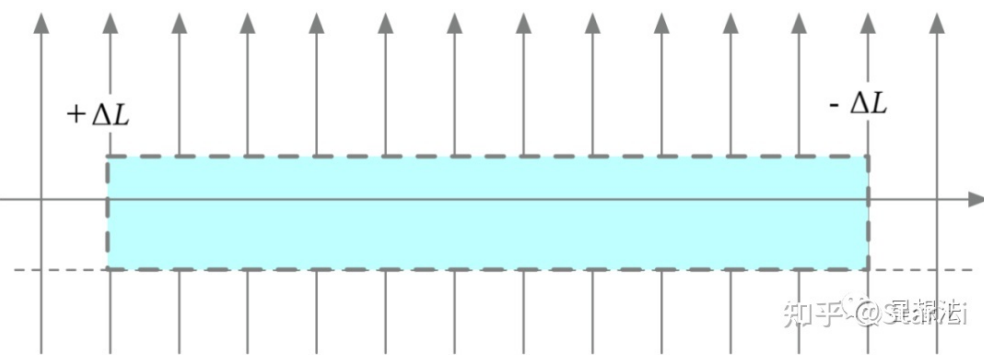
7 Swap交易费用

uniswap最复杂的逻辑是计算交易费用并分配。在添加和删除流动性之前需要将相应的交易费用提取。

• Tick上的总流动性

在某个Tick上可以存在多个区间。在计算交易费用时，需要平摊这些费用给所有在这个Tick上多个区间的总的流动性。在每个区间的边界的Tick上记录下delta_L（所有以这个Tick为边界的区间的流动性总和）。

存在一个全局状态：liquidity，保存当前价格对应Tick的流动性总和。当价格波动，穿过某个Tick时，会进行流动性的增加或者减少（取决于价格波动方向）。举例来说，价格从左到右穿过区间，当穿过区间的第一个Tick时，流动性需要增加，穿出最后一个Tick时，流动性需要减少，中间的Tick都没有流动性的增加和减少（delta_L为0）。



• 区间（Position）上的交易费用率

计算一个区间上的交易费用率，采用总的费用率减去区间外的费用率的方法。在一个区间的边界Tick上记录feeGrowthOutside。所谓的feeGrowthOutside，就是“另外”一个方向上总的费用率。另外的一个方向是相对穿过当前Tick的方向而言。当价格从左到右穿过一个Tick，feeGrowthOutside指的是Tick左边所有区间的费用率。简单的说，就是价格要去方向的相反方向所有区间的费用率。feeGrowthOutside用fo表示。因为fo是一个Tick的两个方向的总的费用率，两个方向的费用率的总和肯定是等于fg（全局的费用率）。所以当穿过一个Tick时，这个Tick上的fo要进行翻转：

$$f_o(i) := f_g - f_o(i)$$

(6.20)

当一个区间创建时，区间边界上Tick的fo需要初始化：

$$f_o := \begin{cases} f_g & i_c \geq i \\ 0 & i_c < i \end{cases}$$

(6.21)

到，所以，可以简单的假想为所有的费用发生在Tick价格之下，也就是 $f_o=f_g$ 。如果Tick的价格大于当前价格，价格还没有穿过Tick，因为假设了之前所有发生的费用发生在Tick价格之下，Tick之上是没有费用的，所以 $f_o=0$ 。在理解了这些逻辑的基础上，在swap的过程中，随着价格的波动，一个区间上，超过最高Tick的费用率以及低于最低Tick的费用率可以用如下的方式计算：

$$f_a(i) = \begin{cases} f_g - f_o(i) & i_c \geq i \\ f_o(i) & i_c < i \end{cases} \quad (6.17)$$

$$f_b(i) = \begin{cases} f_o(i) & i_c \geq i \\ f_g - f_o(i) & i_c < i \end{cases} \quad (6.18)$$

知乎@星想法

以低于最低Tick的费用率的计算为例，如果 $i_c > i$ （当前的价格是高于最低Tick的），低于Tick的所有费用率就是 f_o （定义如此）。如果 $i_c < i$ 的情况下， f_o 记录的是高于Tick的所有费用率，所以需要翻转，即 $f_g - f_o$ 。在获取了一个区间外的所有费用的情况下，计算本区间的费用率：

$$f_{i_l, i_u}(0) = f_g - f_b(i_l) - f_a(i_u) \quad (6.19)$$

获取的费用率的基础上，用费用率乘以区间的流动性可以计算出该区间收取的费用。

总结：

uniswap V3版本核心思想是流动性集中。流动性提供者可以在某个区间提供流动性，提高资金使用率。在某个区间获取的交易费，由所有在该区间的流动性提供者均分。uniswap V3设计了区间粒度-Tick，并且推导了流动性添加/删除以及费用计算的过程。在之基础上，uniswap V3也更新了价格预言机的实现。

欢迎关注“星想法”，交流区块链和零知识证明技术。

发布于 2021-04-18 10:15

智能合约

Uniswap

区块链技术

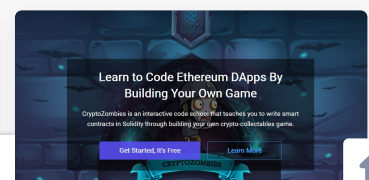
推荐阅读

「教程」用Solidity开始编写你的第一个智能合约

本文翻译自：Gerald Nash《Build

区块链游戏项目（战舰游戏）基于layer2区块链技术，使用以...

本文首发在本人博客



▲ 赞同 4 ▼

● 4 条评论

↗ 分享

♥ 喜欢

★ 收藏

📄 申请转载

...

管井
译
T
le

4 条评论

切换为时间排序

写下你的评论...



 breakpoint2021-05-21

去中心化交易所这个模型流动性挖矿巨坑，就是给别人送钱

 赞

 知乎用户 回复 breakpoint2021-12-11

给别人送钱的意思是？

 赞

 Star.Li (作者)2021-05-16

中心化交易所，交易快，费用低，有客服。但是，有中心化问题，资金有潜在隐患。

 赞

 royslg2021-05-05

感觉好复杂。向作者请教一个问题，通过去中心化交易所交易相比 中心化交易所何优势和好处？

 赞