

UniSwap V3协议浅析(上)

2021-07-21 阅读 201

文章前言

本篇文章主要对Uniswap V3协议的新特性、工作原理、项目构成、源码实现等部分进行详细解读。

协议简介

Uniswap v1版本于2018年11月面世，其本质上是一个运行在以太坊区块链上的基于"恒定乘积"算法的"自动化流动性"协议，我们可以将其看做是一个建立在以太坊上的去中心化数字货币交易所(DEX)，在该交易所上的所有交易(代币互换)都由智能合约来执行且免信任。

Uniswap v2版本于2020年5月面世，相较于Uniswap v1最主要的变化是在原先只支持ERC-20/ETH流动性池的基础之上增加了对ERC-20/ERC-20流动性池的支持，任意ERC-20之间都可以直接进行币币交易。

Uniswap v2版本于2021年5月面世，相较于Uniswap v2最主要的变化是引入了集中流动性(Concentrated Liquidity)概念，实现了资本效率的最大化，一方面使得LP可以赚取更多的回报，另一方面提高了交易的执行力，Uniswap V3还改进了Oracles以提供灵活的费率以及范围订单功能。

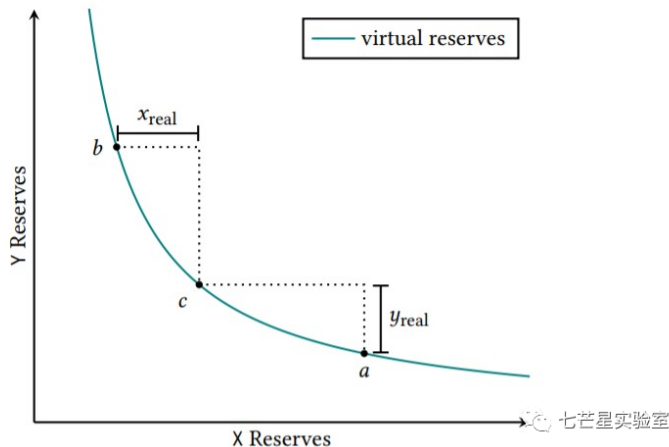
协议变化

下面我们对UniSwap v3协议中的主要变化做以简单的介绍：

集中流动性

在早期版本中，流动性沿Curve曲线均匀分布，其中 x 和 y 分别是两个资产X和Y的储备，而 k 是一个常数，换句话说，早期版本旨在提供整个价格范围为 $(0, +\infty)$ 的流动性，这很容易实现并且可以有效地聚合流动性，但这意味着池中持有的大部分资产永远不会被触及，例如，v2版本中的DAI/USDC对仅保留约0.50%的资本用于在0.99美元和1.01美元之间进行交易，这是LP期望看到最多交易量并因此赚取最多费用的价格范围。

考虑到这一点，允许LP将其流动性集中在比 $(0, +\infty)$ 更小的价格范围内似乎是合理的，在Uniswap V3中将流动性集中在一个有限范围内称为头寸，一个头寸只需要保持足够的储备(reserve)来支持其范围内的交易，它可以像一个恒定的产品池一样在该范围内拥有更多的储备(我们将其称之为虚拟资金)。



具体而言，一个头寸只需要持有足够的资产X来覆盖价格变动到其上界，因为向上的价格变动对应于X储备的耗尽，相似地，它只需要持有足够的资产Y来覆盖价格向其下界的变动，上图描述了区间 $[x_{real}, x_{real}]$ 上的头寸和当前价格 $p \in [y_{real}, y_{real}]$ 的这种关系。 x_{real} 和 y_{real}

作者介绍



Al1ex

安全研究员

关注

专栏

文章	阅读量	获赞	作者排名
123	31K	315	1966

精选专题

腾讯云原生专题

云原生技术干货，业务实践落地。

活动推荐

一键订阅《云荐大咖》...

获取官方推荐精品内容，学技术不迷路！

立即查看

腾讯云自媒体分享计划

入驻云加社区，共享百万资源包。

立即入驻

运营活动



目录

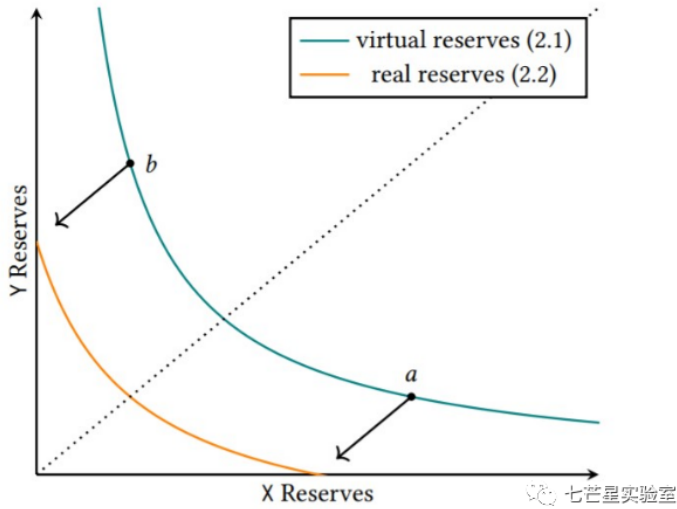
- 文章前言
- 协议简介
- 协议变化
- 源码分析

表示头寸的实际储备，而当价格超出仓位范围时，仓位的流动性不再活跃，也不再赚取费用，那时它的流动性完全由单一资产组成，因为另一资产的储备肯定已经完全耗尽，如果价格重新进入该范围，流动性将再次活跃，提供的流动性数量可以用 $\sqrt{?}$ 来衡量，它等于 $\sqrt{?}$ ，头寸的实际储备由曲线描述：

$$\left(x + \frac{L}{\sqrt{pb}}\right)(y + L\sqrt{pa}) = L^2 \tag{2.2}$$

七芒星实验室

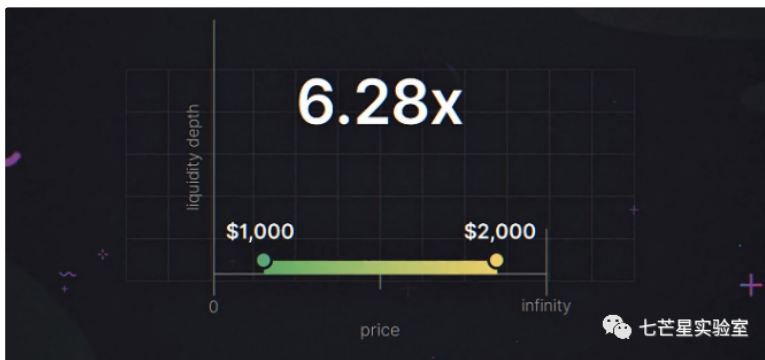
函数式2.2对应的曲线图如下，此曲线是公式 $X*Y=K$ (2.1)的平移，因此位置正好在其范围内：

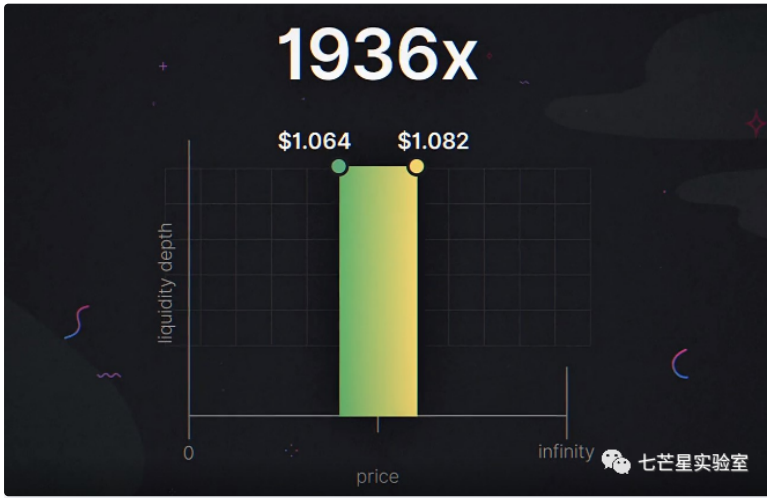


流动性提供者可以根据自己的价格范围自由创建任意数量的头寸，通过这种方式LP可以在价格空间上近似任何所需的流动性分布，此外这是一种让市场决定流动性分配的机制，理性的LP可以通过将其流动性集中在当前价格附近的狭窄范围内，并在价格变动时添加或移除代币以保持其流动性活跃，从而降低资本成本。

资本效率改变

通过集中流动性，LP可以在指定的价格区间内提供与 $v2$ 相同的流动性深度，同时将远低于 $v2$ 的资本风险，节省下来的资本可以对外持有，投资于不同的资产，存放在DeFi的其他地方，或者用于增加指定价格区间内的风险敞口，赚取更多的交易费用。





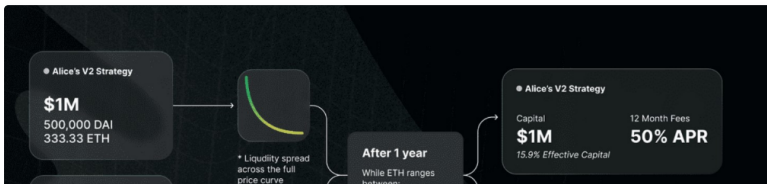
现在我们假设：

Alice和Bob都想在Uniswap v3上的ETH/DAI池中提供流动性，他们每人有100万美元，目前ETH的价格是1500DAI。

Alice决定在整个价格范围内部署她的资本(就像她在Uniswap v2中一样)，于是她存入50万DAI和333.33ETH(共值100万美元)

Bob则建立了一个集中的仓位，只在1000到2250的价格范围内存款，他存入了91751DAI和61.17ETH，总价值约18.35万美元，他自己保留了另外的81.65万美元，按照自己的喜好进行投资。

此时Alice投入的资金是Bob的5.44倍，但只要ETH/DAI价格保持在1000到2250的区间内，则他们赚取的费用是一样的：



[展开阅读全文](#)

举报

点赞 1

分享

0 条评论

我来说两句

[登录](#) 后参与评论

相关文章

[UniSwap V3协议浅析\(下\)](#)

NoDelegateCall合约的主要功能是提供一个修饰器来阻止对使用修饰器修饰过的函数进行delegatecall调用, 合约代码...

Altex

Uniswap V3 介绍

Uniswap v1 于 2018 年 11 月推出, 主要是验证自动做市商 (AMM) 的概念, 是一种任何人都可以将资产汇集到资金池做市策略的去中心化交易所。

Tiny熊

Instadapp 治理已经启动!

我们在三年前构建了 Instadapp, 以使 DeFi 更易于访问和使用。从那时起, Instadapp 已成为 DeFi 基础设施的关键任...

公众号---人生代码

剖析DeFi交易产品之Uniswap: V2上篇

在 DeFi 赛道中, DEX 无疑是最核心的一块, 而 Uniswap 又是整个 DEX 领域中的龙头, 如 SushiSwap、PancakeSwap 等都是 F...

Keegan小钢

Uniswap V3 路径编码的进一步优化

前几天群里有讨论 Uniswap V3[2] 中询价的处理, 简单翻了下代码, 发现与 Uniswap V2[3] 相比, V3 变化真的很大~

Tiny熊

使用TheGraph 获取Uniswap数据(c#)

Uniswap 是一个建立在以太坊上的去中心化协议, 用户可以交换 ERC-20 代币, 不需要买家和卖家创造需求。它是最受欢迎的去中心化交易所(DEX), 在撰写本...

Tiny熊

协议分析|HTTP协议浅析

HTTP和HTTPS Cookie、Session HTTP请求方法 (Get/Post) 一次HTTP请求的过程 一次请...

Ms08067安全实验室

协议分析|HTTP协议浅析

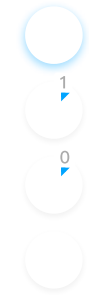
HTTP和HTTPS Cookie、Session HTTP请求方法 (Get/Post) 一次HTTP请求的过程 一次请...

谢公子

Defi? Uniswap 项目漏洞教程新骗局

昨晚突然看到群里的一个消息, 揭秘uniswap-defi项目漏洞-割韭菜新手法, 心想还有这事? 而且还是中英文介绍。

Seebug漏洞平台



Uniswap.py – Python对接Uniswap专用开发包

Uniswap.py 开发包适用于为Python应用快速增加对Uniswap协议的支持能力。即支持使用自有部署以太坊区块链节点的应用场景，也支持使用第三方节点的...

用户5687508

JavaScript对接Uniswap开发教程

Uniswap.js 开发包适用于为Web前端或Node.js应用快速增加对Uniswap协议的支持能力。即支持使用自有部署以太坊区块链节点的应用场景，也支持使...

用户5687508

5个最流行的Polygon区块链DEX协议【DeFi】

Polygon区块链的生态发展非常迅速，每天至少有一个DeFi/NFT项目加入Polygon区块链。MATIC 的价格也在过去几个月中迅速增长。然而，以太坊不断...

用户5687508

爬虫 | 浅析HTTP协议

爬虫就是模拟浏览器向服务器发送请求，然后获得相应的过程。而在这种通信过程中，HTTP协议起到至关重要的作用...

buguse

浅析 HTTPS 和 SSL/TLS 协议

1.ssl协议：通过认证、数字签名确保完整性；使用加密确保私密性；确保客户端和服务端之间的通讯安全 2.tls协议：...

一个会写诗的程序员

10 大趋势带你预见 DeFi 2020!

本文是加密货币研究平台 Messair 近日发布的《Crypto Theses for 2020》报告的节选部分，将探讨 DeFi...

区块链大本营

浅谈TCP IP协议栈(四)IP协议解析

通过之前的网络层基础知识，IP地址以及路由器的简介，大家应该对于TCP/IP有一个大致的了解，在脑海里应该对于网络的几个基础概念有个大概的了解，简单点说整个...

233333

[ffffff0x] 工控协议:S7COMM协议分析(上)

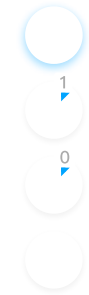
在上一篇文章中，我们通过模拟器环境实现了S7-300的启停实验。本次文章，我们将详细介绍S7comm协议的S7Com...

r0fus0d

基于Flash Loan的套利软件开发教程【一】

套利 (Arbitrage)、智能合约开发 (Contract Coding) 和乐观转账 (Optimistic Transfer) 共同创造了一个令人印象深刻的新工具...

用户5687508



浅析 HLS 流媒体协议

在最近工作中接触到了视频点播和直播业务，也了解到了一些流媒体的后端技术，这段时间希望将了解到的一些知识总结下来，这篇文章主要介绍 HLS 流媒体协议 的基础...

高楼Zee

[更多文章](#)



1



0



社区

活动

资源

关于

云+社区

专栏文章

阅读清单

互动问答

技术沙龙

技术快讯

团队主页

开发者手册

腾讯云TI平台

原创分享计划

自媒体分享计划

邀请作者入驻

自荐上首页

在线直播

生态合作计划

技术周刊

社区标签

开发者实验室

视频介绍

社区规范

免责声明

联系我们

友情链接



扫码关注云+社区
领取腾讯云代金券

热门产品

域名注册

云服务器

区块链服务

消息队列

网络加速

云数据库

域名解析

云存储

视频直播

热门推荐

人脸识别

腾讯会议

企业云

CDN 加速

视频通话

图像分析

MySQL 数据库

SSL 证书

语音识别

更多推荐

数据安全

负载均衡

短信

文字识别

云点播

商标注册

小程序开发

网站监控

数据迁移