链上一站式交易服务平台

OneSwap Team

2020.09.06

目录

摘要

区块链承载的数字资产的流动性提供和价值发现的功能，一直以来都是由中心化交易所提供的。然而在数字资产大爆炸的背景之下， 中心化交易所奉行的审核制上币越来越力不从心，无法满足长尾市场的交易需求。

长尾代币的交易和流动性需求， 催生了去中心化交易所 DEX， 而 DeFi 领域自动化做市商的兴起带来了 DEX 的爆发。但是繁荣之下，用户体验差、交易方式受限等问题仍亟待解决。

OneSwap 在 DEX 的无需许可上币和自动化做市的基础上， 引入限价单的支持， 并通过自带的 OneSwap Wallet 改善用户交互方式， 提供一站式交易体验。作为通用链上一站式交易服务平台，OneSwap 可以部署在任意支持智能合约的区块链平台。

一、数字资产的价值流动

由比特币催生的区块链行业本质上是金融行业，而交易所是区块链行业重要的基础设施，发挥着流动性提供和价值发现的作用。经过十多年的发展， 区块链上承载的数字资产的种类和数量迎来爆炸式的增长： 从最初单一的比特币发展成为包含数字货币、稳定币、应用代币在内的上万种数字资产。

一直以来作为交易所主要解决方案的中心化交易所（CEX）奉行的审核制上币在应对数字资产大爆发时显得力不从心。此外， 中心化交易所也因为违约风险高、 安全隐患大、 规则不透明等问题饱受诟病。中心化交易所的审核制上币与中心化信任机制， 与区块链领域的去中心化和去信任等核心理念背道而驰。

以子之矛攻子之盾，区块链行业从业者一直在努力通过区块链的方式解决中心化交易所的问题。依托区块链技术构建的去中心化交易所（DEX）通过无需许可上币和交易的方式， 来解决数字资产大爆发所催生的长尾市场的交易需求。

一个自然的思路是构建 DEX 专用公链， 如 BitShares、 CoinEx Chain 等。虽然 CoinEx Chain 在交易处理速度和交易确认时间等方面提供了近乎中心化交易所的体验， 但是在跨链技术进一步成熟之前， CoinEx Chain 等 DEX 公链尚无法以去中心化和去信任的方式连接和聚合更多的数字资产。在当下以及可预见的未来， CEX 仍然会是最好的跨链交易方案， 而 DEX 与 CEX 将互为补充。

以太坊通过智能合约技术带来的可编程资产的理念，带来了数字资产种类和数量的爆炸式增长，也催生了对 DEX 的强烈需求。智能合约技术也为构建 DEX 以重构数字资产交易市场、解决长尾市场的交易需求提供了新的思路。另外， 考虑到受制于低交易处理速度、 高交易费用的以太坊发展现状，以 CoinEx Chain 为代表的 DEX 公链仍有很大的发展空间。

二、基于智能合约的DEX平台

囿于以太坊的交易处理速度与交易费规则， 以太坊上涌现的基于订单簿的 DEX 合约如 Dex.top、 IDEX 等大多采用链下撮合、 链上结算的技术路线。由于用户体验与资金流动性等问题，基于订单簿的 DEX 的交易量一直较小，无法匹敌中心化交易所。

最近以 Uniswap、 Balancer 等为代表的自动做市商 （Automated Market Maker，AMM）异军突起， 开启了分布式金融（Decentralized Finance， DeFi）的发展热潮， 也为基于合约的 DEX 平台构建提供了崭新的思路。这些 DeFi 项目一方面利用资金池盘活了用户手中的闲置数字资产， 解决了资金流动性问题； 另一方面则通过恒定函数做市商（Constant Function Market Maker， CFMM）的方式以简洁的逻辑快速处理用户的交易请求。虽然 AMM 项目目前仍面临着暂时性亏损（Impermanent Loss）、低资金利率等问题，但是资金池中锁定的数字资产总价值和日交易量的持续增长， 宣告了 AMM 的可行性以及用户对于 AMM 的认可。甚至出现了诸如 Kyber、 1Inch.Exchange 等在繁荣的 DeFi 世界为用户自动发现最优交易路径服务的项目。

尽管 AMM 模型中的明星项目 Uniswap 的日交易量已经突破了 1 亿美金， 但是由于目前自动做市商中不存在订单簿， 用户在 AMM 项目中无法像在中心化交易所一样进行限价单交易（Limited Order）， 只能按照 AMM 在交易当时给出的市价进行交易。然而来自中心化交易所的实际运营经验显示， 中心化交易所中普通用户的成交量主要是通过限价单完成的， 也即限价单已然成为用户交易活动中不可或缺的部分。订单簿功能缺失， 也会导致 CFMM 模型在处理大额交易时，出现较大的滑点，挫败用户交易的积极性。

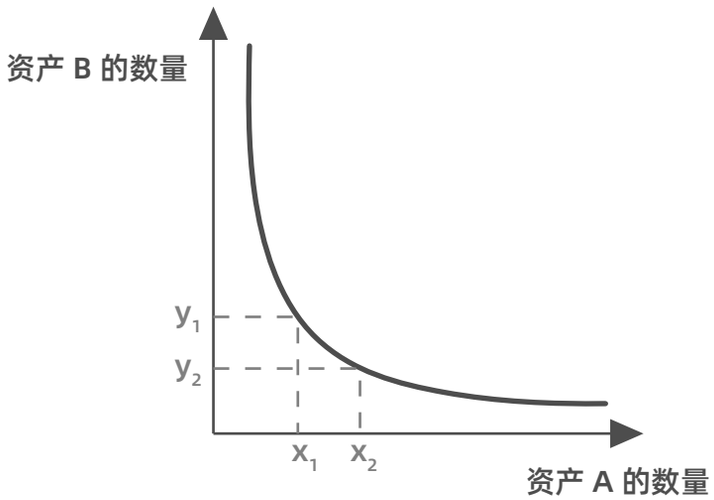
三、链上一站式交易服务平台OneSwap

链上一站式交易服务平台 OneSwap 在 DEX 无许可上币的基础之上， 充分借鉴 AMM 项目的成功经验， 在 CFMM 模型的基础之上引入链上订单簿来改善 AMM 用户的交易体验。CFMM 模型和链上订单簿的组合， 不仅为用户提供了熟悉的限价单交易方式， 也进一步增强了数字货币资产的流动性。OneSwap 致力于以 DEX 的方式， 在保障安全和去中心化的前提下， 解决长尾代币的交易与流动性问题。另外， 借助平台自带的 OneSwap Wallet 中精心设计的交互界面以及一键发币等工具，OneSwap 致力于为用户提供一站式交易体验。

在充分考察当前 AMM 项目中的各种 CFMM 模型的基础之上， OneSwap 选用了 Uniswap 项目中的恒定乘积做市商（Constant Product Market Maker， CPMM）模型。在仅涉及两种代币的交易场景中 CPMM 比恒定总和做市商 （Constant Sum Market Maker，CSMM）、 恒定平均值做市商（Constant Mean Market Maker， CMMM）等模型更简洁也更通用。

OneSwap 支持所有符合特定标准的代币之间的交易， 创建市场无需许可也不收取任何上币费用。在 CPMM 模型下， 可以预期的是每个理性的流动性提供者在创建关于两种资产的资金池时， 会根据当时的市场价注入适当数量的两种资产作为资金池。例如， 当 ETH 和 USDT 的市场价比例为 1： 350 时，为资金池注入的 ETH 和 USDT 数量之间也会维持该比例，例如 10ETH： 3500USDT。 OneSwap 用户可以利用手中闲置的数字货币资产为 OneSwap 的交易对资金池注入流动性， 成为流动性提供者并赚取交易手续费。 OneSwap 中的每个资金池都有相应的权益代币， 为资金池注入流动性的用户会收到相应的权益代币， 作为取回资金的权益证明。

每个资金池在响应兑换交易请求时，会维持资金池中两种代币数量 x 和 y 的乘积为常数：x * y = k。如果在一笔兑换交易前后资金池中两种代币的数量分别为 x1、 y1 和 x2、 y2， 则 CPMM 保证： x1 * y1 = x2 * y2。值得提及的是， 这种相等的情况仅发生在不收取任何交易手续费的情形下， 当收取交易手续费时， CPMM 模型中 k 会随着交易费的累积不断增大。另外 k 的绝对值也会随着流动性的注入和流出不断变动。

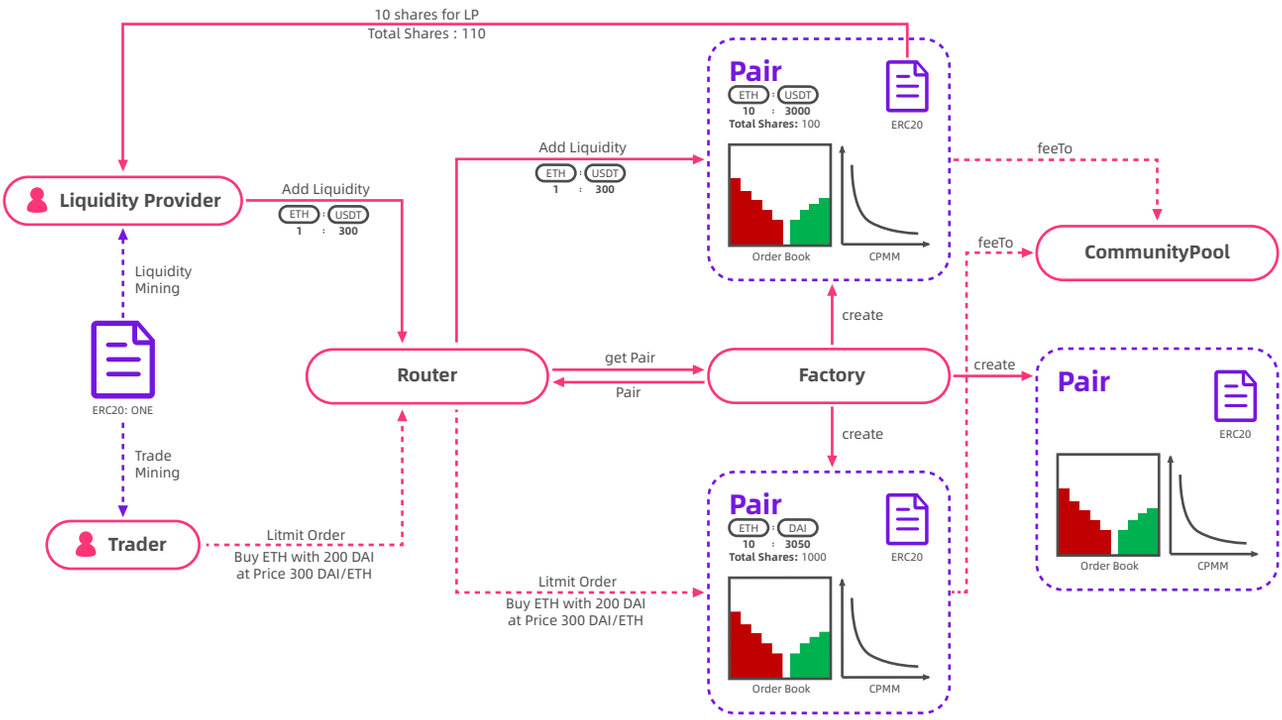


OneSwap 的用户既可以发起市价单交易也可以发起限价单交易。处理市价单时， Pair 合约会对比订单簿最优价格与 AMM 价格， 并尝试以最优价格响应交易请求。对于无法成交的市价单部分，通过 CPMM 模型及时处理，并且根据 CPMM 的价格波动及时处理满足条件的限价单交易，未成交的订单则暂时保存至链上订单簿等待后续处理。

OneSwap 是通用的一站式交易服务平台， 可以在任意支持智能合约的区块链上实现并部署， OneSwap 团队计划首先在以太坊上实现并部署， 为了便于链上治理和激励社区发展，以太坊上的 OneSwap 会发行治理代币，用于流动性挖矿、交易挖矿以及链上治理投票。

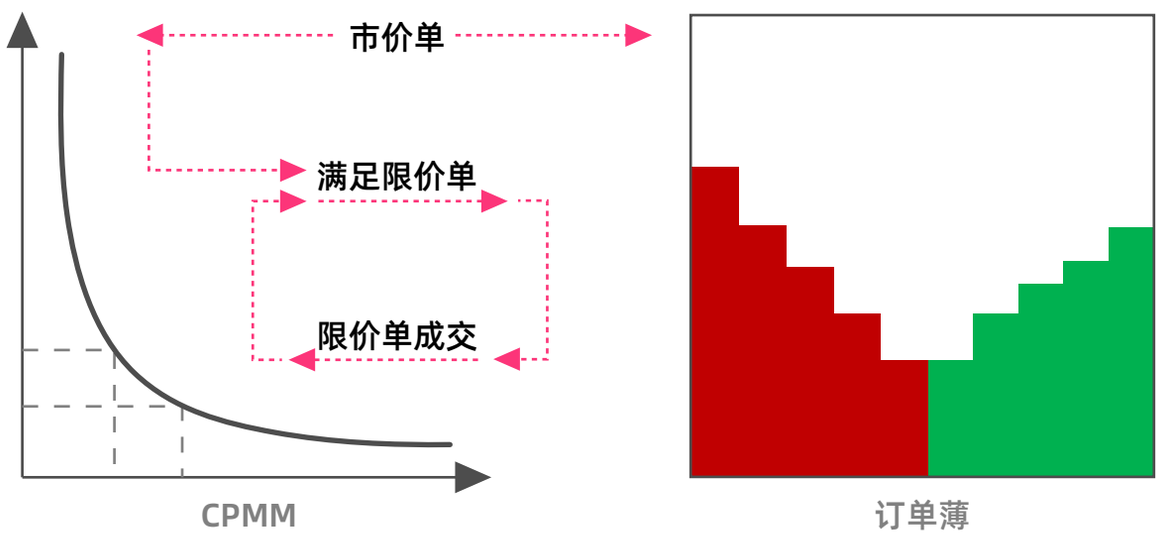
四、OneSwap的架构设计

部署在每个区块链平台上的的 OneSwap 都会包含一系列的资金池，OneSwap 中用交易对 Pair 合约指代这些资金池。每个 Pair 合约都有三个组成部分： 1） 链上订单簿： 存储无法成交的限价单交易； 2）CPMM 模型： 恒定乘积做市商， 为 Pair 合约提供流动性； 3）权益代币： 记录流动性提供者权益的代币。以太坊上的 OneSwap 架构在下图中展示，其中权益代币为符合 ERC20 标准的代币。



流动性提供者向 Pair 合约的资金池中注入数字资产时，Pair 合约按照当前的资金池总量、已经发放的权益代币总量以及本次注入的资金量， 为流动性提供者铸造新的权益代币。当流动性提供者想要取回自己的资金时， Pair 合约按照提供的权益代币数量和权益代币总量的比例，将资金池中相应比例的资金返还给流动性提供者并销毁相应的权益代币。

每个 Pair 合约都是由工厂 Factory 合约按需创建的， 而为了方便用户使用， OneSwap 还提供了路由 Router 合约来作为用户和 Pair 合约之间沟通的桥梁。所有用户的交易都发给 Router 合约。每当有用户为全新的交易对注入资金时， Router 合约会指示 Factory 合约为该交易对生成新的 Pair 合约。OneSwap 支持用户指定交易的兑换路径， 用户将兑换路径发给 Router 合约， Router 会根据 Factory 合约中存储的 Pair 合约地址， 按照用户提供的路径完成相应数字资产的兑换。



如前所述， 每个 Pair 合约同时支持市价单与限价单。处理市价单时， Pair 合约会对比订单簿最优价格与 AMM 价格， 并尝试以最优价格响应交易请求。由于每次交易都会造成 CPMM 的价格波动， 每当价格波动到待成交的限价单的价格时， Pair 合约都会尝试处理订单簿中的限价单。无法立刻成交的限价单，则暂时保存在 Pair 合约的订单簿中。

链上订单簿总会引发关于 Gas 费消耗过大的担忧， 尤其是在当前以太坊网络交易拥堵造成 Gas 价格居高不下的前提之下。通过对 Pair 合约的深度优化， OneSwap 可以将交易的 Gas 费消耗控制在与 Uniswap V2 一样的水准， 并且在特定情形下 OneSwap 交易所需的 Gas 费更少。这部分是因为 OneSwap 开发团队为 Pair 合约精心组织了数据结构， 部分也是因为 OneSwap 中没有实现 Uniswap V2 额外提供的闪兑（Flash Swap）和链上价格预言机（On-chain Price Oracle）的功能。这些功能在增强了 Uniswap 的功能之外， 也导致了更多的 Gas 消耗。

五、OneSwap 的激励与治理

为了支持链上治理， 以太坊上部署的 OneSwap 会发行名为 ONES 的 ERC20 治理代币，ONES 代币支持转让所有权以及黑名单机制。ONES 代币总量恒定， 总量为 1 亿个。代币分配及流通方式如下，其中初始流通的 ONES 占总量 11%。

分配项	比例	主要用途	初始流通	解锁方式与周期
创世挖矿奖励	5%	用于奖励创世挖矿的参与者	5%	全解锁
远期挖矿奖励	45%	代币的主要分发方式，用于日后推出的新的流动性挖矿计划，社区建设与推广、项目合作等。远期挖矿的释放由社区投票决定，包括释放时间，挖矿市场，释放的份额等	0%	由社区投票按需解锁
项目运维	25%	用于确保网络安全及维护项目功能	2.5%	4年半分9次解锁，每半年解锁2.5%
战略投资机构	15%	分发给项目长期战略投资机构	1.5%	4年半分9次解锁，每半年解锁1.5%
团队激励	5%	分发给核心团队及未来员工	1%	2年分4次解锁，每半年解锁1%
早期投资者	5%	分发给项目早期投资人、早期流动性支持者	1%	2年分4次解锁，每半年解锁1%

远期挖矿奖励部分主要用于支持流动性挖矿和交易挖矿、 社区建设与发展， 推广宣传活动费用， 项目合作等， 这部分花费遵循链上治理流程； 项目运维部分用于 OneSwap 的合约、 Dapp、 钱包等应用的开发测试、 安全审计、 网络维护等； 而创世挖矿部分用于在 OneSwap 上线初期激励用户参与流动性挖矿和交易挖矿， 为资金池注入流动性的用户以及与资金池进行交易的用户，都有机会收到 ONES 代币作为激励。

链上治理通过发起提案并进行社区投票的方式进行， 拥有足够数量 ONES 代币（超过代币总量的 1%）的用户可以发起提案， 而任何持有 ONES 的用户可以针对提案投出赞同票或者反对票。投票周期为三天，遵循一币一票的计票规则，在投票周期结束之后，收到的赞成票多于反对票的提案获得通过。

投票过程由治理合约统一管理， 对于投票通过的提案， 治理合约在链上自动执行相应操作。OneSwap 目前支持四种类型的提案： 纯文本提案、社区基金花费提案、交易手续费率修改提案以及 Pair 合约升级提案，其中纯文本提案仅用来发起社区民意调查。

为了增强 OneSwap 项目的透明度和可信度， 用做远期挖矿奖励部分的 ONES 代币由治理合约代管， 而需要按照时间线性解锁的 ONES 代币则由锁仓合约管理。ONES 代币创建完成之后， 将初始流通的 11% 的代币按照前述的比例分别转入归属方地址， 将 45% 的代币转入治理合约，并将 44% 的代币转入锁仓合约。

为了申请资金支持， 需要发起社区建设花费提案， 并在提案中明确申请的代币数量。ONES 代币持有人根据申请方陈述的资金用途投票决定是否同意资助。投票周期结束后， 如果提案获得通过，申请人可以从治理合约获得 ONES 代币。

OneSwap 按照成交金额对 Taker 收取固定比例的交易手续费， 而 Maker 无需缴纳交易手续费。 Pair 合约中所产生的交易费分成两部分处置： 60% 直接归属于流动性提供者，40% 用于 ONES 代币的回购和销毁。ONES 代币的回购和销毁通过代币回购合约自动完成，也因此 ONES 是通缩代币。

为了跟随市场变动， OneSwap 支持在一定区间内修改交易手续费率。可以通过发起交易手续费率修改提案来修改交易手续费率， 具体的数值包含在提案中。提案投票通过后， 治理合约根据提案内容更新 OneSwap 的交易手续费率。

得益于 OneSwap 合约实现中代理模式的采纳， 不仅在创建 OneSwap 交易对时能够节省大量 Gas， 更使得升级 Pair 合约的逻辑成为可能。通过发起 Pair 合约升级提案， 遵循链上治理流程，提案投票通过之后，治理合约可以升级 Pair 合约的逻辑。

六、OneSwap的开发计划

OneSwap 团队计划率先在以太坊上实现和部署 OneSwap， 并随后在 TRON 上部署。OneSwap 团队会持续关注智能合约公链的发展， 并适时在成熟的智能合约平台上部署 OneSwap。

OneSwap 所有合约代码均会交由顶级安全机构审核以保证合约代码的安全性。在完善的机制设计和安全的合约之外，良好的用户体验也是任何 DeFi 项目成功运营的关键因素。为了提升用户体验， OneSwap 团队围绕钱包支持、 交互设计、 代币管理和交易服务等方面进行努力。

为了降低用户的接入门槛， OneSwap 自带钱包支持。通过 OneSwap Wallet 钱包用户可以快速接入 OneSwap， 而无需依赖任何第三方工具。通过丰富行情数据的展示以及简洁明了的交易界面设计， OneSwap Wallet 致力于为用户提供更好的交易体验。 OneSwap Wallet 还支持 C2C 法币交易，致力于为用户提供一站式交易服务。

为了降低代币发行的技术门槛， OneSwap Wallet 内置一键发币工具。借助该工具， 用户只需要填写要发行的代币名字、总量、是否支持增发、燃烧、冻结等选项，即可完成链上完成代币合约的创建。

在基本功能支持之外， OneSwap 团队会密切跟踪 DeFi 领域的进展， 并及时在 OneSwap Wallet 中支持额外的 DeFi 协议。依托 OneSwap Wallet，OneSwap 平台致力于成为未来 DeFi 世界的入口。