PairX：单币配对质押挖矿协议

PairX.finance 白皮书 v3.0

2020 年 12 月 14 日

目录

摘要

PairX 是一个基于智能合约的去中心化单币配对挖矿平台，使用户能够在高收益 AMM 市场上获得奖励。PairX 基于以太坊开发，帮助用户实现单币种质押，智能合约自动配对成为 LP，参与流动性挖矿并分享收益。同时通过二次分配降低用户可能的无常损失，提高资本利用率，为 DeFi 行业带来更多流动性和交易深度。

项目背景

DeFi 行业在链上锁定的资产已经超过 160 亿美元，并且正呈现加速度发展。锁仓资产主要由几部分构成：（1）借贷平台，支持有限几种资产质押；（2）AMM 平台，几乎支持所有资产成为做市商，但是通常要求两种资产配对成为 LP；（3）衍生品平台，支持有限几种资产质押；（4）智能资管平台，支持有限几种资产质押。

实际上，DeFi 用户手里持有的大量单币资产一直处于被动等待升值状态，没办法参与 AMM 平台锁仓获取更多收益，因为参与 AMM 平台挖矿需要额外的 ETH 或者稳定币或者其他资产进行配对才能成为 LP，这就限制了这些资产被有效利用来为 DeFi 提供更多的流动性和交易深度。

比如某些用户长期持有 AMPL，而有的用户则长期持有 ETH，各自并不愿意（或者有能力）用多余的资本去配对参与 AMPL 官网的流动性挖矿。如何让这两个群体实现单币质押挖矿，进而获得更多收益呢？

显而易见，让有需求的投资者配对质押即可。PairX 就是为了解决这一问题而来。

解决方案

目前高收益的流动性挖矿主要是为 AMM 提供流动性，成为自动做市商。比如先在 uinswap 上双币 50 比 50 配对成为 LP，再将取得的 LP 令牌质押在项目官网，获得项目的代币空投奖励。以 AMPL 为例，用户需要以同等价值的 AMPL/ETH 配对加入 uinswap V2 流动池，获得 uni V2 代币，再将 uni V2 代币质押到 ampleforth 官网，即可以获得 AMPL 奖励。这一激励措施导致 1000 多万美元的 AMPL/ETH 交易对被锁定在 uinswap 中提供流动性。而在 balancer 平台，AMPL 还提供 AMPL-USDC 交易对的流动性奖励。所以让各自持有单币种的用户能够高效配对参与挖矿，就可以捕获单纯持币之外更多的收益。

1、合并存款

在第一个版本中，我们将根据市场动态有选择的开放可支持的币种。合并存款是指将所有用户已存款的代币放在一个单独的池中，一旦挖矿期结束，用户就可以从中提取存款。

PairX 为每一个支持的币种创建一个池子，用户将单币存入该池子，获得该池子的份额代币；两种可配对的池子按照同等价值存入 AMM 流动池，生成的 LP 代币自动质押到项目官网。

为了简化分析，我们假设有两个池子（α 和 β），每个池子各有 1 名参与者（甲和乙），并且假设两个池子的资产总值正好可以配对参与挖矿（如果某池子有富余，富余部分虽然无法参加挖矿，但是会参与利润分配）。按照 uniswap 的恒定乘积公式：

$$(R_\alpha - \Delta_\alpha)(R_\beta + \gamma\Delta_\beta) = k.$$

其中 R 代表资产的数量，α 及 β 代表资产种类，γ 代表手续费，Δ代表交易的资产，k 是一个恒定常数。

在挖矿结束的时候，由于币价变动，返回 PairX 的资产数发生了变化，一种资产的数量变多为（Rβ+γΔβ），另一种资产的数量变少为（Rα-Δα），所以用户在做资产赎回的时候，PairX 需要对资产进行再分配，甲的资产仍然为 Rβ 个 β，乙的资产则为（Rα-Δα）个 α 以及 γΔβ 个 β，系统会自动将 γΔβ 个 β 卖出换回 α。对于乙来说，可能要承担部分无常损失。

用一个具体实例来进行说明。假设 A 为甲的单币资产（10 个），B 为乙的的单币资产（500 个），甲乙分别将这两种资产存入 PairX 后，PairX 在 UniSwap 上代币 A/B 池中按照 1A = 50B 的价格存入了这 10 个 A 和 500 个 B。而这个池中一共有 100 个 A 和 5000 个 B，PairX 的 LP 份额占 10%。

交易前			
代币	数量	价格	价值
A	100	50	5000
B	5000	1	5000

由 AMM 的固定乘积公式可知，K=100*5000=500,000
当市场价格波动至 1A=100B 时，在 AMM 的固定乘积公式中，K 为定值，保持不变。假设在稳定后池总 A 总数数量变成 X，B 的数量变成 Y，为方便讨论此处忽略掉手续费，那么：
X*Y=K=500,000
100X=Y

解出 X,Y，得到：

交易后			
代币	数量	价格	价值

A	70.71	100	7071
B	7071	1	7071

价格波动后，由于 PairX 的 LP 份额占据池中的 10%，PairX 的持有代币价值为 7.071A+707.1B，而用户提供的初始资产为：甲方 10A（价值 500），乙方 500B（价值 500），所以赎回时的资产分配调整为：甲方 7.071A+207.1B，乙方 500B。智能合约自动将 207.1B 以现价卖出可以换回 2.071A，则甲方最终可以赎回 9.14A（价值 941），需要承受 10A-9.14A=0.86A 的无常损失。乙方完整赎回 500B（价值 500），无任何数量损失。挖矿奖励则平均分配给甲和乙。

在这个实例中，因为 A 相对于 B 的价格上涨，虽然甲方承受了一些无常损失，但是总价值相对之前提升了许多，再加上挖矿奖励，从投资决策上来说，完全可以承受这些无常损失。

在后续的改进方案中，PairX 将对挖矿奖励部分进行再平衡，用部分挖矿奖励弥补无常损失后再按照资本比例分配给参与者，降低可能的无常损失。

2、排队机制

参与 AMM 流动池质押要求两种资产价值等比，所以我们设计配对池有一个最低资本量（以减少手续费支出，同时可以满足任意资金量的挖矿需求），两种资产都达到最低资本量就配对注入 AMM 流动池。当其中一种资产提前达到最低资本量，则新加入的用户需要排队，充值资产进入排队池。当排队的资金超过最低资本量的 3 倍时，将暂停接受存款。以防止一种资产量过大，而另一种资产不足。

3、自选池和策略池

自选池是指平台将所有支持的挖矿项目列出来交给用户自己判断选择，比如用户想参与 AMPL/ETH 的流动性挖矿，只需要选择存入 AMPL 或者 ETH。

策略池，也叫保管库（Vaults），遵循独特的策略，旨在最大程度地提高所存放资产的收益并最大程度地降低无常损失风险。存入该池的用户可以获得无损挖矿保障。该功能将在下一个版本中推出。

4、挖矿周期

挖矿时间如果过短，可能造成收益无法覆盖无常损失的情况。并且当某个用户临时撤出本金，也会导致配对的代币撤出而产生闲置。为了提高收益，降低损失，PairX 设定的挖矿周期为两周（有些项目为 30 天），系统锁定流动性并将其部署到 AMM 平台。在某个周期结束时，清算并计算所赚取的

收益，并根据其存入资产占比将其分配给存款人。在挖矿期结束后，会生成 PAIR 代币，奖励给参与者，并且可以使用与赎回收益相同的比例计算来赎回 PAIR 代币。

5、无产损失补偿（IL 保险）

在配对挖矿结束时，因币价波动，只有一方可能会出现无常损失，这种风险当且仅当配对代币相对己方代币价格大幅下跌时才会发生。为了降低参与门槛，我们引入无常损失补偿机制。一般通过三种途径对于可能发生的无常损失进行补偿，第一种机制是将挖矿收益中更大比例分配给发生无常损失一方（损失方与配对方分配比例为 6:4）；第二种机制是用平台代币奖励来降低损失；第三种机制是合作的项目方以项目代币补贴参与者的无常损失。

在以后的版本中，PairX 将通过内置无常损失保险为 LP 创建风险对冲管理选项。

经济模型

PAIR 代币是一个多年发行计划，第一年计划发行总量为 900,000 PAIR。 其中 65％将分配给 PAIR 社区成员。在最初的 12 个月内，通过流动性挖矿和无常损失补偿的方式分配给社区参与者。

第一年之后每年都会铸造 100,000 PAIR，并逐年减半。其中 90％用于流动性挖矿和无常损失补偿，10％归属 PairX 的管理金库。

并且挖矿奖励的 10％以及 LP 的手续费将自动进入管理金库，作为平台收益。平台收益用于支付开发团队持续迭代的费用以及回购平台代币。

PAIR 持有者有权改变协议的未来。在协议启动后不久，将启用专用的快照以启动社区治理。治理流程的工作原理是让用户使用其持有的 PAIR 令牌对各种建议进行表决，这些建议包括从协议参数到使用存储在金库中的资本资产用于创建新激励，资本化以及用户增长等。

结论

PairX 的目标是为代币长期持有者提供单边流动性挖矿机会，为整个 DeFi 行业带来更多的流动性和资产交易深度。激活存量资产的资本效率对于加密市场的健康和成功至关重要。PairX 的使命是促进 DeFi 行业的繁荣，建构面向未来的开放金融基础设施。从数字货币交易对开始，然后发展到加密证券，NFT。PairX 资产增长的唯一限制是以太坊链上资产的可用性。

参考文献：

[1] Uniswap v2 Core
https://uniswap.org/whitepaper.pdf

[2] Constant Function Market Makers: DeFi's "Zero to One" Innovation
https://medium.com/bollinger-investment-group/constant-function-market-makers-defis-zero-to-one-innovation-968f77022159

[3] Bonding Curves In Depth: Intuition & Parametrization
https://blog.relevant.community/bonding-curves-in-depth-intuition-parametrization-d3905a681e0a

[4] Bancor's Smart Tokens vs Token Bonding Curves by Simon de la Rouviere
https://medium.com/@simondlr/bancors-smart-tokens-vs-token-bonding-curves-a4f0cdfd3388

[5] Let's run on-chain decentralized exchanges the way we run prediction markets by Vitalik Buterin
https://www.reddit.com/r/ethereum/comments/55m04x/lets_run_onchain_decentralized_exchanges_the_way/