LeverPool Protocol (LEV)

一、项目简介

LeverPool Protocol 是一个旨在通过配资杠杆形式引入增量用户和增量资产的去中心化 DeFi 聚合挖矿协议。在社区治理和去中心化的基础上，LeverPool Protocol 能够让用户以零手续费挖矿，并且可以引入真实世界中的资产和信用来配资挖矿资金杠杆，实现小投入也能参与挖矿并获得可观的回报，解决用户“手续费占比太高、挖矿资金不够用”的痛点，从而让用户充分享受 DeFi 世界红利。

在技术层面，LeverPool Protocol 采用 hub-zone 等 Layer2 扩容方案，提供高效、完备、可伸缩的清算机制；结合 Oracle 智能化滑动平均价格机制，对抗恶意插针等攻击行为，确保用户资金安全；提供丰富的可插拔的策略适配接口，为用户带来灵活的配资方案，最大化潜在收益。

二、核心功能介绍

1、零手续费聚合挖矿

基于智能算法的聚合挖矿模型，实现提升资金使用效率和降低操作手续费的双重目标优化，并给予用户出入金手续费的 100%代币补贴，从而大大降低小资金体量用户的 DeFi 挖矿进入门槛。

2、杠杆挖矿配资模式

追求流动性挖矿代币本位高激励的 DeFi 矿工受限于手中有限的数字资产，无法充分享受 DeFi 红利，而另一方面追求低风险和相对于法币本位稳定收益率的投资者不愿参与

到 DeFi 挖矿中，同样也无法享受 DeFi 红利。为此，我们在 LeverPool 提供杠杆挖矿配资模式，将矿工分为杠杆使用者 A 和杠杆提供者 B，前者放大数字资产挖矿杠杆获取超额收益，后者获得法币本位的稳定收益并获得资金优先保护。例如面对 APY 为 100%收益的矿池，A 可以使用 1 万 USDT 并杠杆放大为 5 万 USDT 参与到挖矿中，并向提供 4 万 USDT 杠杆资金的 B 支法币本位 APY 为 30%的杠杆利息。LeverPool 通过智能合约模块组控制挖矿资金的流向，回流资金优先支付 B 的本金和利息。在这种情况下，假设挖矿 APY 不变，那么 A 的 ROE 将提升到 380%，而 B 将获得相对法币的稳定收益。

3、引入合成资产上链和信用协同的利率和杠杆率自动调节市场

在上述 LeverPool 配资模型中，杠杆使用者可以利用杠杆实现超额收益，而杠杆的利率和比例将由市场化机制和智能合约实现。与此同时，DeFi 世界当前只能使用链上数字货币和资产进行挖矿和交易，使得 DeFi 挖矿的无风险收益远高于真实世界的的优势无法充分发挥，为了进一步引入真实世界中的资产和信任，LeverPool Protocol 采用类似 Synthetix 的合成资产机制和资产上链模型，杠杆使用者可以将真实资产抵押到链上，通过预言机实现价格联通，该链下真实资产将帮助杠杆使用者带来更低利率和更高比例的杠杆提供者，起到增信和劣后的作用。与此同时，LeverPool 也将以真实世界信用为基底的区块链地址信用协同关系，通过多方安全计算将信用体系引入链上数字世界，从而为杠杆使用者提供增信和更优的杠杆使用方案，并设立信用协同保险池降低杠杆提供者的资金风险。

三、核心功能实现

1. 核心流程

根据逻辑流程，LeverPool 系统由 Pool，Vault，Controller，Strategy，Farm 五个模块构成，它们的交互关系如图 1 所示。

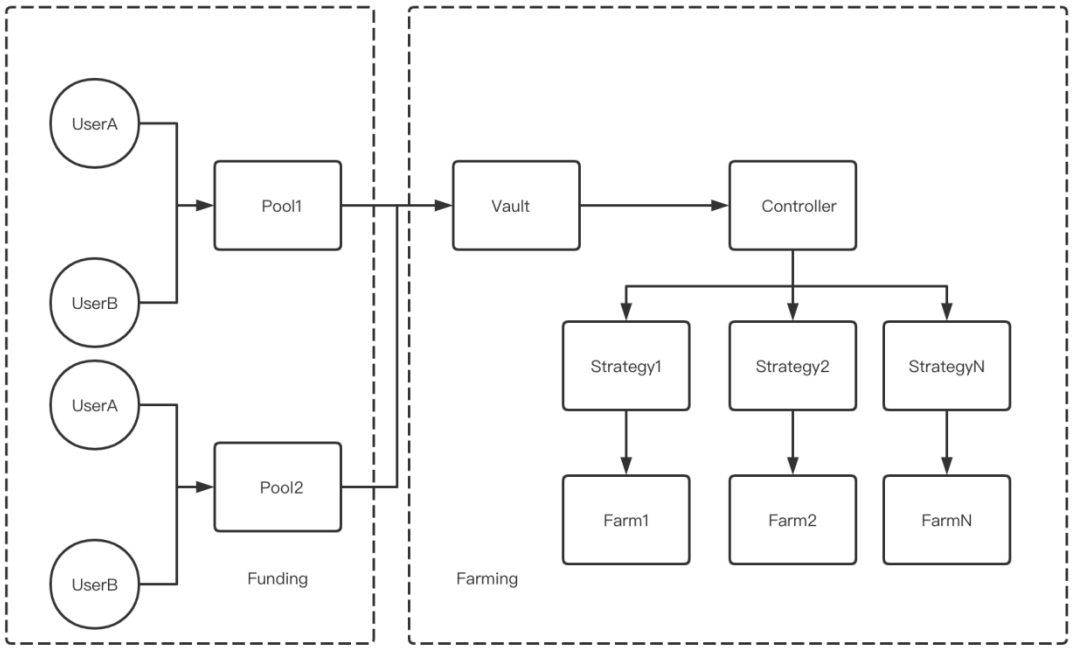

图1： LeverPool 各个模块关系示意图

图 1 中箭头的方向代表用户资金进行挖矿的流动方向，而用户获得收益的资金流动方向与图中箭头相反。下面我们依次介绍每个模块的逻辑功能，值得注意的是，所有的模块均是 Ethereum 上的智能合约，资金的流动是合约之间的函数调用。

LeverPool 系统在逻辑层级上分成两个模块，分别是用户入金与配资的 Funding 模块；以及智能化挖矿 LeverPool 模块。前者依托后者运行，而后者是一个功能完善的子模块，可以作为独立的非用户配资模式的流动性挖矿系统独立运行。

对于 Funding 模块，其目的是满足两部分人不同需求，两部分人分别用 杠杆使用者 UserA 与 杠杆提供者 UserB 表示。对于 UserA，其追求的是高风险高收益，例如 APY 100% 以上，但是缺乏足够的本金；而对于 UserB，其有足够的本金，但是追求的是相对较高的稳定收益，例如 APY 30%。具体而言，Funding 模块的功能由一系列智能合约 Pool 实现，每个 Pool 是一个独立的资金池，包含如下功能：

a. 配资： 对于每个智能合约 Pool，其规定了接受资金种类，例如 ETH，对于 UserB 的保底收益，例如 APY 30% 以及杠杆比例，例如 300%。在此数值设置下，UserA 可以以 1：3 的比例由 Pool 进行配资。如果 UserA 通过配资，即借 UserB 的钱，经流动性挖矿获得了超过 APY 100% 的收益，那么 UserA 需要将配资部分收益的 30% 分给 UserB。对于每个 Pool，UserA 会发布配资需求，UserB 可以根据需求将资金存储到 Pool 中，当然，UserB 也可以在没有足够需求的情况下将资金存储在 Pool 中，以备后续优先使用。

b. 清算：除了上述配资流程中对于收益的结算， Pool 还需要维护由于资产价值变化所造成的平仓清算等操作。UserA 通过配资会进而转投到 Vaunt 合约当中（关于 Vaunt 的介绍见后文），在 Vaunt 中用户可能需要将资产进行转换，例如当前 Vaunt 当中收益率最高的币种为 YFI，而 Pool 的资金为 ETH，那么 UserA 可以首先通过一步转化将 ETH 转换为 YFI 存入到 Vaunt 中。而 ETH 与 YFI 的相对价格变化会影响 UserB 的本金安全。Pool 通过引入场外价格的预言机来进行判断，周期性判断是否触发平仓操作来保护 UserB 的资金安全。

对于 Farming 模块，总体而言，智能可约的关系可以概括为资金池 Vault 收集资金通过控制器 Controller 采用不同的策略 Strategy 将资金投到不同的流动性挖矿场景 Farm 中赚取收益。其资金的出入口为 Vaunt 智能合约，这是智能化自动挖矿的一系列

不同资产，例如 ETH 与 YFI ，的聚合资金池，其汇集资金并且在挖矿结束后进行收益结算。总体而言。 作为 LeverPool 系统的核心特色， Vault 在用户进行投资的时候，额外维护用户的邀请关系（例如用户可以通过制定一个地址作为自己的邀请者），进而在收益结算的时候进行一定比例或者数量的邀请分红。

当用户资金汇集到一个阈值后，Vaunt 会将将资金投入到具体的流动性挖矿挖矿场景 Farm 当中，这由控制器 Controller 进行统一管理。具体而言，Controller 首先代持用户的资金，其有一个可以被信任的挖矿策略 Strategy 的池子，每经过一段时间，Controller 会通过智能化算法与预言机模型，选择当前市场上收益率最高的策略进行投资。例如，假设当对市场 YFI 流动性挖矿收益最高的方式是投资到 Compound DeFi 当中，那么在更新节点之后，Controller 将会选择将 YFI 投入到 Compound 的 Strategy 来对 YFI 进行投资管理。 从上述表述中，可以看到 Strategy 主要完成两个功能：

a. 具体指定某种资产的挖矿链路。

b. 对流动性挖矿场景合约，即 Farm 合约的对接功能。

相比现有 DeFi 产品只能使用链上资产和信息，LeverPool 采用 Synthetix 类似的机制来合成资产，引入增量用户和资金进入 DeFi 生态。但是与 Synthetix 不同的是，LeverPool 用户在发布资产时可以选择合适的信用或资产进行抵押并参与到聚合挖矿当中。例如假设用户寻求发布 N 所住宅资产，代币数量为 M， 这里的信用可以是一份具有法律效用的数字合约，约定当用户攒足 M/N 份代币即可兑换一所住宅。那么，以此为抵押（具体实现方式是将此数字合约放置于合成资产合约当中），用户即可在不需要代币抵押的前提下进行资产发布，进而进行流动性（交易）挖矿。

2. 扩容方案

随着系统用户以及管理的资金增加，单一的区块链底层（例如 Ethereum）会逐渐承载不住频繁的交易，为此，LeverPool Protocol 采用 Layer2 结构的扩容方案来优化清算逻辑。

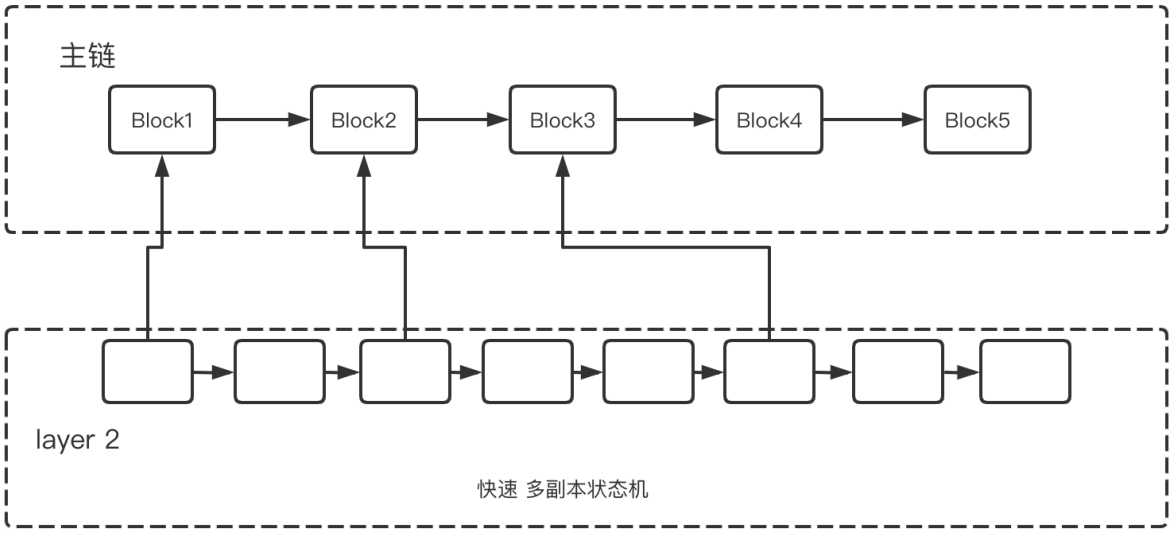

图 2. 主链与 Layer2 之间的逻辑关系图

Layer2 本身是是完整的功能系统，其与主链相对独立（可以为第三方），并且速度更快，采用预先指定的通讯协议进行信息交流，如图 2 所示。Layer2 主要包括两个重要的模块：

a. 逻辑计算模块：根据不同的数据、流程完成任务，其抽象为一个函数(s, p, h) = f(x), 其中 x 为数据，可以由主链、本地存储单元以及外界指令提供; s 为计算结果(最终状态)；p 为计算过程的表示（例如中间随机数的选取等等）；h 为计算过程 p 的哈希值，用于验证计算过程。

b. 存储单元：用于存储中间结果以及计算过程。其提供验证功能 g(p, h), 其中 p 为计算过程，h 为由此计算过程产生的唯一哈希值。

layer2 首先从主链、本地存储单元以及外界获取数据 x；之后完成逻辑计算(s,p,h) = f(x) 并将计算验证过程 p 存储在本地存储单元；最后将最终结果 s 以及计算哈希 h 提交到主链完成同步，由此即完成了一个功能循环。对于主链上数据的真实性，我们可以提供主链数据的哈希值，调用 layer2 中的验证模块 g(p,h) 进行验证。

在 LeverPool Protocol 的清算逻辑中，Layer2 不断地进行复杂的当前持仓用户的清算条件检查，例如在判断是否需要对用户进行强制平仓操作，Layer2 根据主链的数据以及外部预言机数据进行条件检查，如果检查结果为需要平仓，则将平仓指令以及计算验证信息提交到主链进行实际的操作。

3. 鲁棒性增强

a. 持久化 Oracle 投票机制 persistent voted oracle（PVO）： LeverPool 对于安全性要求极高，尤其是其清算模块需要引入外部 Oracle 数据，为了增强外部数据的可信度，项目引入持久化 Orcale 投票机制（PVO），具体而言：

PVO 可以被视为一种按需使用的 POS+PBFT 共识机制的子链，其主要功能为记录主链调用外界信息的情况，采用“投票验真”的逻辑。具体而言，对于一个主链上的智能合约 S，其依次通过 PVO 提供的 api 调用了外界数据 d_1,...,d_n, 那么主链在出块的同时，也同时提交一个包含调用外界数据信息的 PVO 块。对于 POV 块，每个超级节点 j 会对其数据进行验真：

对于每个数据 d_i, 这里要求 d_i 是来源于多个不同的 Orcale 提供的数据综合。PVO 子链以 PVO 块中记录的相同的调用方式尝试获取数据 d'_ij，这里 j 表示不同的 Orcale 数据来源，如果：

a. $d_i = d'_{ij}$, 那么标记数据 d_i 为可复现数据；

b. $d_i \neq d'_{ij}$, 那么标记数据 d_i 为不可复现数据；

对于每个 d_i 都有超过 2/3 的超级节点标记为可复现数据，那么此区块为可复现区块；否则为不可复现区块。两种情况下，数据都通过 pbft 的共识机制永久存储。只要当 PVO 子链标记区块为可复现区块时，才代表 Orcale 提供的数据为可信的，可以供后续使用。这样的设计一方面保证了少量不诚实的 Orcale 数据或者少量不诚实的节点并不能污染数据。

*b. 智能滑动窗口平均报价：*市场恶意的插针攻击行为会给正常用户造成资金损失，并且由此引发的强制平仓行为可能会对系统造成很大的不稳定性、因此，在计算不同 Token 的价格时，系统采用智能的滑动窗口平均策略，即当前 Token 的价格是由过去一段时间 dt 的平均价格给出的，这里的 dt 是根据 Token 的价格变化剧烈程度所决定，若 Token 价格变化剧烈，则 dt 较大，反之较小，针对不同 Token 的 dt 随着价格变动剧烈程度而改变的函数关系由 DAO 给出。

四、发展规划

2020 Q1-Q2

产品模型设计，基础架构建设；

2020 Q3

LeverPool 测试版本--矿池挖矿 demo 测试

2020 Q4

LeverPool alpha 1.0 正式上线--杠杆功能和流动性矿池上线

2021 Q1-Q2

LeverPool beta1.0--信用借贷机制设计与开发

2021 Q3-Q4

LeverPool beta2.0--合成资产上链及抵押借贷开发

五、治理模式

LeverPool Protocol 在经过初期测试和代码设计后，将会上线使用推广。度过初期开发者委员会推动产品、社区冷启动后，LeverPool 的治理将完全进入 DAO 阶段。该协议受 LEV 的约束，任何改进将由 LEV 的持有者投票决定。该治理系统可以控制的部分权力列举如下：

- 设立新的挖矿矿池并选择合适的挖矿协议
- 更新预言机地址和杠杆资金利率和比例
- 更改收益后端抽成比例和方法方式
- 设立新的 DAO community

六、代币模型

代币分发将采取去中心化模式的社区推动模式，依托智能合约自动分发，总计 1000 万枚。其中：

- 私募：100 万枚，占比 10%。将在产品上线后分 100 天线性解锁。

- 天使矿池：100 万枚，占比 10%。项目初期将以天使矿池的方式启动，天使矿池将置入 100 万枚 LEV 和社区捐赠的 USDT 提供早期流动性。
- 流动性挖矿：800 万枚，占比 80%。项目将对天使矿池、收益机枪池、杠杆矿池、资产上链矿池的用户进行流动性挖矿奖励，在根据社区投票分批进行。