火锅基金

HOTPOT FUND WHITE PAPER

V2白皮书

HotPot Fund V2–White Paper

目录

一、概要

本文档是火锅基金 V2 的技术白皮书，文档中全面阐述了火锅基金智能合约背后的设计思路。

随着 Uniswap V3 的发布，火锅基金也做了相应的升级。火锅基金 V1 全部是投资 Uniswap V2 流动池，与 V1 类似，V2 全部是投资 Uniswap V3 流动池。同时火锅基金 V2 对功能进行了一些升级：任何有流动池投资经验的人，都可以通过火锅基金的平台创建基金；基金投资不再受基金本币的限制，可以投资任何由受信(Verified Token)代币组成的交易对；基金治理代币 HPT 的销毁机制更加灵活。

二、介绍

在去中心化金融(DeFi，Decentralized Finance)领域，由自动做市协议(AMM)驱动的去中心化交易所(DEX)，通过汇聚流动性，以算法为交易者完成交易提供服务。目前，以 Uniswap 为代表的去中心化交易所，已经成为区块链技术最重要的用例之一。

去中心化交易所是通过汇聚流动性来为交易提供服务，理论上任何人都可以成为流动性提供者(Liquidity Provider)，但实际上要高效地提供流动性，需要专业知识、深入的数据分析和相应的自动化工具。火锅基金的初衷，是通过汇聚用户资金，由专业的基金团队进行管理，在代码开源、操作透明、用户资金安全的前提下，创造有价值的流动性收益。

首先，我们简单地回顾一下火锅基金 V1，在 V1 中，我们实现了以下功能：

（1）通过以太坊区块链上的一套智能合约，汇聚用户资金投资 Uniswap V2 流动池；

（2）每支基金由一种基金本币进行结算，用户存入和提取、资产核算都是基于基金本币；

（3）用户随时可以存入和提取，用户资金始终由用户自身钱包控制；

（4）基金经理统一完成投资操作，基金经理可以投资、撤资、调整交易对。基金经理的投资操作是受限的：只能投资包含基金本币的交易对，且交易对中的另一种代币必须是受信代币，基金经理可以投资多个交易对，但无权将资金池中的资金挪作任何其它用途；

（5）用户收益的 20%，用于在 Uniswap 购买并销毁项目治理代币，以体现治理代币价值。

随着 Uniswap V3 的发布，其对自动做市协议(AMM)进行了大幅度的升级，核心是引入了聚焦流动性(Concentrated Liquidity)的概念，大幅度优化了资金效率，使得流动性提供方式发生了很大改变。

Uniswap V3 的聚焦流动性，可以理解为将以前 x * y = k 的反比例函数，做了类似于微积分的改造。同时，用价格的对数作为价格刻度(几何平均价格)，能更好地均匀分布价格。

同时，Uniswap V3 提高了流动性提供的难度，为了获得更高的资金利用率，流动性提供者需要频繁调整投资头寸(Position)，对于小额投资者而言，流动性收益或许还不足以覆盖投资所需开销的 Gas 费用，而且，缺乏深入数据分析和相应自动化工具的弱点，对散户投资者显得尤为突出。

在本文档中，我们全面介绍了火锅基金 V2，一种投资 Uniswap V3 流动池的基金，它使得具备专业知识和工具的基金经理，可以通过汇聚用户资金，高效地利用用户资金创造流动性收益。

在和火锅基金 V1 保持相同关键特性的同时，V2 提供了一些新的特性：

1.头寸(Position)管理：Uniswap V3 的聚焦流动性改变了流动性投资的方式，火锅基金作为投资 Uniswap 流动性的基金，在管理交易对之外，还需要进一步管理投资头寸。不同于火锅基金 V1 只需要管理交易对，在 V2 中，基金经理需要更精细地管理投资头寸，并根据价格

波动情况，及时调整投资头寸，从而提高资金效率。

2.工厂化：每一支基金都是通过工厂合约创建的，任何人都可以使用火锅基金的工厂合约，创建投资 Uniswap V3 流动性的基金。

3.投资不再受基金本币限制：火锅基金 V1 限制只能投资包含基金本币的交易对，V2 不再有此限制。为此，基金经理需要为除基金本币之外，投资交易对中的每种代币设置交易路径(Swap Path)，且交易路径中的每一种代币都必须是受信的。

4.用户收益的 20%依然用于基金分成，但方式有所改变：10%的收益，以基金本币形式支付给基金经理，以覆盖基金经理的成本；10%的收益，用于购买和销毁项目治理代币，以体现代币价值。购买、销毁的路径可以由治理账户设置，实现各种基金本币到 HPT 的购买、销毁操作，从而具备更加灵活的销毁机制。购买路径全部都需要经由 Uniswap V3 WETH9/HPT(手续费率 0.3%)交易对。

三、资产核算

火锅基金 V2 依然都是用基金本币进行资产核算，用户存取也都是以基金本币的形式。

火锅基金 V2 依然用 ERC20 token 来计算和管理用户的基金份额。当用户存入时，铸造份额代币；当用户提取时，销毁份额代币。基金份额可以转让，也可以出售。关于基金份额计算和转让的细节，请参阅 V1 白皮书。

火锅基金 V2 不再管理空投或挖矿的 UNI 资产。

3.1 总资产

火锅基金 V1 的资产是由多个投资交易对组成，每个交易对的资产核算方式很简单：流

动性对应的基金本币数量 * 2 即可得到。这是由火锅基金 V1 和 Uniswap V2 的特性决定的：V1 基金中必须含有基金本币，Uniswap V2 交易对中的两种代币等值。

火锅基金 V2 的资产是由多个交易对的多个头寸组成，基金总资产(Total Assets)由所有头寸资产求和而得：

$$Total\ Assets = \sum_{i=0}^{n} Assets_i$$

总资产核算需要遍历所有头寸，所以火锅基金智能合约中使用二维动态数组管理头寸。

3.2 头寸资产

Uniswap V3 的手续费不再自动叠加进流动性资产，而是以 token 的形式单独存储。所以，每个头寸的资产，是由流动性资产和手续费两部分组成。

3.2.1 流动性资产

流动性资产也不再是 Uniswap V2 的等值分布，而是跟头寸的流动性数量、价格刻度区间、当前价格这几个要素相关：

- 当前价格在头寸的价格刻度区间之下 ($i_c < i_l$)，资产全部是 token0 (记作 X);
- 当前价格在头寸的价格刻度区间之上 ($i_c \geq i_u$)，资产全部是 token1 (记作 Y);
- 当前价格在头寸的价格刻度区间之内($i_l \leq i_c < i_u$)，流动性资产由 X 和 Y 组成，其计算规则可以理解为：价格从当前价格上涨到价格刻度上届，能够卖出的 X (涨过价格刻度上届之后，资产全部换成了 Y)；以及价格从当前价格下跌到价格刻度下届，能够卖出的 Y (跌破价格刻度下届之后，资产全部换成了 X)。

下面的计算公式来源于 Uniswap V3 白皮书：

$$\Delta Y = \begin{cases} 0 & i_c < i_l \\ \Delta L \cdot (\sqrt{P} - \sqrt{p(i_l)}) & i_l \le i_c < i_u \\ \Delta L \cdot (\sqrt{p(i_u)} - \sqrt{p(i_l)}) & i_c \ge i_u \end{cases} \tag{3.1}$$

$$\Delta X = \begin{cases} \Delta L \cdot (\frac{1}{\sqrt{p(i_l)}} - \frac{1}{\sqrt{p(i_u)}}) & i_c < i_l \\ \Delta L \cdot (\frac{1}{\sqrt{P}} - \frac{1}{\sqrt{p(i_u)}}) & i_l \le i_c < i_u \\ 0 & i_c \ge i_u \end{cases} \tag{3.2}$$

3.2.2 手续费

Uniswap V3 的手续费，以 token 的形式单独存储，不再自动增加到流动性中。每个头寸都记录了该头寸已结算的手续费 (tokensOwed)，但该变量只是记录了已结算的手续费，并不能完整地反应头寸资产。对于头寸资产而言，只有当头寸提取手续费（触发 burn 或 collect 函数) 时，才会进行结算。也就是说，每个头寸的手续费除了已结算的之外，还有一部分是在交易过程中已经产生、但尚未结算到头寸的手续费。基金和普通流动性提供者是不一样的，需要核算完整的资产，所以需要核算尚未结算的手续费。

手续费的计算涉及到以下一些变量。由于要分别记录 token0 和 token1 的手续费，所以下列的每个变量实际都会有两个。由于记录的都是单位流动性所获得的手续费，其值是一个浮点数，所以实际存储和计算时全部做了左移 128 位的处理。

- 全局手续费变量 (feeGrowthGlobal)：记录在整个合约生命周期内，每单位虚拟流动性 (L) 获得的手续费总金额，它是一个累进值。
- 价格刻度上的手续费变量 (feeGrowthOutside)：用于保存给定价格刻度内累积的手续费，当越过该价格刻度时更新。

- 当前价格：决定了头寸的价格区间当前是否能获得手续费收益。
- 头寸上最后一次更新的手续费变量 (feeGrowthInsideLast)：用于保存该头寸最后一次提取时的手续费，作为下一次提取时计算的依据。当提取该头寸手续费的时候更新。
- 头寸上已结算的手续费 (tokensOwed)：提取时更新。

计算头寸所有手续费的逻辑是：

第 1 步: 计算该头寸尚未结算的手续费 feeGrowthInside (f_{i_l,i_u})。

第 2 步: 减去该头寸最后一次更新的手续费 feeGrowthInsideLast。

第 3 步: 加上该头寸已结算的手续费 tokensOwed。

取决于当前价格在区间内还是区间外——也即，当前刻度下标 i_c 大于或等于 i ，可以用下列公式计算每单位流动性，在刻度 i 之上(f_a)以及之下(f_b)，所获得的手续费：

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

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

然后用下面的公式计算头寸尚未结算的手续费 feeGrowthInside(f_{i_l,i_u})，在两个刻度 (刻度下界 i_l 和刻度上届 i_u) 之间，累积手续费的总金额：

$$f_{i_l,i_u} = f_g - f_b(i_l) - f_a(i_u)$$

上述公式的推导过程，可以参阅 Uniswap V3 白皮书。

3.2.3 换算为基金本币资产

手续费和流动性资产的核算结果是 token0 和 token1 数量，还需要转化为以基金本币

衡量的资产。根据设置的代币交易路径，可以得到每种代币和基金本币之间的兑换价格，然后将 token0 和 token1 资产换算为基金本币资产。

因为价格是可以被改变的，任何需要依赖兑换价格进行资产核算的场景，都必须慎重考虑价格的获取方式，在 Defi 领域，因为价格被操控而出现的安全事故不胜枚举。尤其是通过闪贷的方式，攻击者可以在一笔交易中，贷出大量的资产操控价格，大大地降低了攻击成本。通过闪贷操控价格，对 Defi 项目进行攻击，是目前常见的攻击方式。

火锅基金 V2 使用 Uniswap V3 的价格预言机，获取用于资产核算的兑换价格。

Uniswap V3 中提供了新的价格预言机，相比 V2 的预言机机制做了升级。V2 预言机机制需要外部调用者自行记录两次观察点的数据，才能获取到预言机价格，所以它无法被其它需要即时核算的智能合约使用；升级之后，其它智能合约可以从 V3 预言机，获取两个或多个观察点之间的预言机价格。具体内容请参阅 Uniswap V3 白皮书。

使用 Uniswap V3 预言机之后，火锅基金用于资产核算的兑换价格，是本次交易所在的区块之前，最近一次交易的价格。即便攻击者通过闪贷方式操控了当前价格，也无法改变当前资产核算的结果，从而大幅度提高了攻击的难度。

资产核算的计算过程中没有考虑实际交易时的滑点和手续费，但这是合理的，当前基金资产本来就不应该考虑交易过程中的滑点和手续费。

3.2.4 不使用 Uniswap V3 外围头寸管理合约

Uniswap V3 核心合约没有实现头寸资产的代币化，而是在外围合约中实现。不同于 Uniswap V2 用 ERC20 代币代表流动性份额，在 Uniswap V3 外围合约中，使用 ERC721 (即

NFT) 代币来代表每一个头寸。

外围合约中的头寸管理合约，没有实现对未结算手续费的核算。所以，火锅基金没有使用外围合约来管理头寸。不使用外围合约管理头寸，意味着火锅基金所持有的 Uniswap V3 头寸资产，在 Uniswap V3 Graph 查询中不可见。

四、基金经理

火锅基金 V2 的智能合约做了工厂化改造，现在，任何有流动池投资经验的人或机构，都可以在火锅基金上创建和管理基金，成为一位基金经理。

4.1 创建基金

只需要指定一种基金本币，给基金起一个名字，再做简短的介绍（名字长度不能超过 8 字节，介绍长度不能超过 24 字节），就可以创建一支基金。

4.2 设置交易路径

基金经理首先需要为要投资的交易对中的两种代币，分别设置交易路径，除非该代币就是基金本币。每种代币的交易路径都包含购买路径 (Buy Path) 和销售路径 (Sell Path)。

火锅基金 V1 的交易路径中还包含 Curve 流动池，尤其是稳定币之间的交易，Curve 的滑点比 Uniswap V2 更低。由于 Uniswap V3 大幅度优化了资金效率，交易滑点也得到了优化，所以火锅基金 V2 的所有内置交易全部在 Uniswap V3 中完成，不再依赖其它项目。

基金经理不能随意修改交易路径，如果要修改交易路径，则所有包含目标代币的流动池，

都必须先清空所有的头寸。这是为了防止基金经理监守自盗，通过修改交易路径盗取用户的资产。

4.3 投资操作

基金经理的投资操作有 4 种：init (初始化头寸), add (投资), sub (撤资), move (调整）。初始化头寸时，可以投资也可以不投，投资时需要指定投入的本币数量。撤资和调整时不是给定流动性数量，而是指定要撤资或调整的流动性比例。由于 Uniswap V3 的手续费没有自动复投，投资时给了一个选项，可以选择是否复投已产生和已结算的手续费。

4.3.1 计算投资分布

投资或调整时，都需要计算投资的两种 token 的分布。

投资时，投资的币种包括 3 种：基金本币，收集的 token0 和 token1 手续费。

在计算投资分布时，我们首先将投资额中的基金本币和 token1，全部用当前价格换算成等值的 token0 数量，记作A 。

然后，再用 token0 的总量(A)，结合头寸的价格区间和当前价格，计算 token0 和 token1 的分布。

已知 token0 的总数量(A)，当前价格为：$P = \frac{y}{x}$，头寸的价格下届为P_l ，价格上届为 P_u ,需要计算出 token0 的数量 Δx和 token1 的数量Δy 。

当前价格在头寸的价格区间之下时，投入的资产全部是 token0：

$$\begin{cases} \Delta x = A & (P \le P_l) \\ \Delta y = 0 & (P \le P_l) \end{cases} \tag{4.1}$$

当前价格在头寸的价格区间之上时，投入的资产全部是 token1：

$$\begin{cases} \Delta x = 0 & (P \geq P_u) \\ \Delta y = A & (P \geq P_u) \end{cases} \tag{4.2}$$

当前价格在头寸的价格区间之内时，投入的资产部分是 token0，部分是 token1。我们假定 token0 到 token1 之间的兑换都能以当前价格完成，同样不考虑交易滑点和手续费。可以得到公式：

$$\Delta x + \frac{\Delta y}{P} = A \tag{4.3}$$

根据公式 (3.1) 和 (3.2)，可以得到：

$$\frac{\Delta x}{\Delta y} = \frac{\frac{1}{\sqrt{P}} - \frac{1}{\sqrt{P_u}}}{\sqrt{P} - \sqrt{P_l}} \tag{4.4}$$

由公式 (4.3) 和 (4.4) 可以得到需要的 token0 数量，token1 的数量可以由 token0 的数量计算得到，得到的计算公式为：

$$\Delta x = \frac{A}{1 + \frac{\sqrt{P_u}\cdot(\sqrt{P}-\sqrt{P_l})}{\sqrt{P}\cdot(\sqrt{P_u}-\sqrt{P})}} \qquad (P_l < P < P_u) \tag{4.5}$$

$$\Delta y = (A - \Delta x)\cdot P \qquad (P_l < P < P_u) \tag{4.6}$$

在得到投资分布的 token0 和 token1 数量之后，分别将基金本币、手续费兑换成相应数量的 token0, token1。用当前价格换算的方式，没有考虑实际兑换时的交易滑点和手续费，所以最终可能会产生一些 token0 或 token1 的残余，最后需要将残余的 token0 或 token1 兑换回基金本币。

基金经理只需要给定投资本币数量，火锅基金 V2 在一笔交易中完成相应的计算、兑换和投资，能有效地节省基金经理的 Gas 消耗。

4.4 收益

用户在提取时，其收益的 10%，以基金本币的形式支付给基金经理，以覆盖基金经理的成本。

WETH9 基金做了特殊处理：用户在 WETH9 基金提取时，提取到的是 ETH；而基金经理收到的分成是 WETH9，没有兑换成 ETH。

五、治理

火锅基金 V2 依然有治理账户，治理账户只有两种权限：设置受信代币和设置销毁路径。治理账户初期由项目组控制，后续应该考虑交给社区。

5.1 设置受信代币（Verifiled Tokens）

基金经理的投资范围被限制在受信代币之内，以规避潜在的安全风险。

5.2 设置销毁路径（Harvest Path）

用户在提取时，其收益的 10%，以基金本币的形式支付给控制器合约，这部分分成归 HPT 代币持有者所有。控制器合约提供一个公共的销毁 (harvest) 函数，任何人都可以调用该函数从 Uniswap V3 中购买和销毁 HPT 代币。

火锅基金 V1 在 Uniswap V2 中建立了多个交易对，用于购买和销毁 HPT 代币。在火锅基金 V2 中，只在 Uniswap V3 建立一个交易对：WETH-HPT，手续费率 0.3%。所有的基金本币，都需要设置销毁路径，以将基金分成体现到 HPT 代币价值中。

六、免责声明

本文档是一份技术白皮书，仅作为一般用途使用。本文档不构成对投资的任何建议，也不含对购买或出售的任何推荐，它不应被用于做出任何投资行为的决定参考。本文档阐述了火锅基金团队当前的技术设计思路，如果这些设计思路发生变化，恕不另行通知。

参考资料

- 火锅基金 V1 白皮书（EN / CN）
- Uniswap V3 白皮书（EN / CN）
- HotpotFunds V2 代码
- Uniswap V3 代码（core / pheriphery）

火锅基金

由专业的Uniswap V3做市商为您管理投资