Synallage.Exchange

以主动做市商算法驱动的去中心化全业务链聚合交易平台

分布实验室

Anton Li(anton@synallage.exchange)

Version 0.8 Feb 2021*[Updated Apr 1, 2021]*

摘要

本文介绍了下一代去中心化交易所 Synallage，采用 PMM 算法提供更强大的流动性和更小的滑点，并率先将 PMM 算法应用到永续合约和合成资产交易中，通过实现低 GAS 费的限价单及量化功能，使去中心化交易所的资金效率大大提高，除此之外，在此篇中我们将讨论 PMM 的核心算法和数学原理、永续合约核心概念及原理、限价单概念及原理、合成资产概念及原理等 。

1、简介

Synallage 是去中心化交易所，它利用主动做市商算法（PMM）为每个人提供纯链上和可履行合约的流动性。Synallage 接受流动性提供者的资产。它在市场价格附近收集资金以提供足够的流动性。为了最大程度地降低有限合伙人的交易对手风险，Synallage 会动态调整市场价格，以鼓励套利者介入并稳定有限合伙人的投资组合。与其他链上流动性解决方案相比，Synallage 具有多个优势：资金利用率高，滑点低，单一风险敞口，减少了永久损失。

作为交易者，您可以看到以下功能：提供了全业务链交易范围，包括现货交易(币币交易、杠杆交易并提供了链外撮合限价单)，衍生品（永续合约、欧式期权），合成资产（大宗商品、股票、外汇等），此外每个交易者都享有足够的流动性，类似于集中交易；也支持各种策略的量化接口，实现了比中心化交易所更强大功能，套利者可以从 Synallage 与其他交易所之间的价格差异中获利;智能合约可以原生使用 Synallage 流动性来完成链上交易，例如清算和拍卖

作为流动性提供者（LP），您可以看到以下功能：没有最低存款要求和对资产类型的限制；Synallage 为每笔交易收取费用，并最终将其作为奖励分发给 LP。有限合伙人可以使用自己的代币创建交易对；有限合伙人可以通过存放已经拥有的代币来获得流动性，而无需承担价格风险。

Synallage 还提供 SmartTrade - 这是一种去中心化的流动性聚合器服务，可以寻找并智能路由到各种流动性来源，以报出任意两个代币之间的最优价格。此外，Synallage 还消除了建立新资产流动性池的各种限制，可自由定义和实时调整资产比例，流动性深度，手续费率等。最大限度的降低了新资产发行的门槛。

基于此，Synallage 开发了众筹建池（一个无需许可、机会均等的流动性发放机制）以及面向专业链上做市商的可定制化灵活技术解决方案。

2、PMM 协议

2.1 我们的优势

2.1.1 概述：

Synallage 由 DODO[1]提出的 Pro-active Market Maker（PMM）的突破性算法提供支持（向雷明达先生及 DODO 团队致敬）。PMM 利用价格预言来检索资产的准确市场价格作为输入。然后，它旨在为每种资产提供接近市场价格的充足流动性。结果是，当远离市场价格时，流动性迅速下降。随着市场价格的变化，AMM 被动地依靠套利交易来改变价格。另一方面，PMM 会主动向同一方向移动价格曲线，以确保市场价格附近的区间保持平坦。这确保了持续提供足够的流动性。

PMM 在几个重要方面优于 AMM 解决方案。

1、 资金利用率高

PMM 像 AMM 一样，在从零到正无穷大的价格范围内提供流动性，但是 PMM 价格曲线在预言价（市场价格）附近的区域明显平坦。也就是说，大多数资金是在市场价格附近收集的，这使得交易更加活跃，频繁，从而提高了资金利用率。

2、单一风险敞口

在上面的价格曲线中，每条价格曲线均由两部分组成：左侧的出价方和右侧的要价方。这两个部分可能具有不同的深度或流动性，从而导致所谓的买入价差[2]。在 PMM 中，要价流动性仅由池中基本令牌的数量确定，而投标

流动性仅由池中报价令牌的数量确定。它允许基本池和报价池具有不同的大小，从而允许流动性提供者存放任意数量的报价或基本令牌，而不是两者（例如 Uniswap）。流动性提供者将其现有资产存入，仅此而已。

3、减少无偿损失
但是，永久性损失又如何呢？也就是说，PMM 如何确保流动性提供者在提取代币时得到他们所存放的东西呢？答案是通过鼓励套利交易。当个体交易者购买基础代币时，PMM 会稍微提高价格，以使套利者出售基础代币更加有利可图。在 PMM 中，套利交易可确保池中的代币数量始终大致等于流动性提供者存入的代币数量。该方案有效地减轻了流动性提供者的无常损失，使流动性供应成为低风险事务。

Synallage 作为一家 DEX，也应用了去中心化流动性聚合器，可以实现同一网络上两个任意代币之间的交易。它能智能地从流动性来源中找到最佳的订单路由，为交易者提供最佳的价格和最低的滑点。既是 DEX 又是聚合器。即有自己的流动性资金池，也支持全市场任意代币的兑换

此外 Synallage 将 PMM 算法进一步扩大到永续合约与杠杆交易中去，同时基于零知识证明开发了链下撮合限价单功能，让 CEX 功能引入 DEX 的同时大大减少了 GAS 的花销，基于此，实现了链上网格交易、合约网格等量化策略此外，还引入了链上欧式期权、合成资产（大宗商品、股票、外汇、特色标的等）功能，来达到出圈的目的，做到了甚至远高于中心化交易所业务覆盖，设计了更适合中心化交易所客户使用习惯的 UI 和业务逻辑，让中心化交易所使用者可以零成本迁移到 DEFI 世界中来，避免 DEFI 领域肉眼可见的“内卷”。

2.1.2 下一代流动性解决方案：

流动性是 DeFi 世界中最重要的资源，因为它是所有 DeFi 项目的基础要素。如今，有两种主要的分散式流动性提供方法：

算法做市商（例如 Uniswap）

基于订单簿的订单匹配（例如 dYdX）

然而，它们都存在缺陷。
与集中交易相比，算法做市商无法为主流资产提供足够的流动性。此外，对于小众的长尾资产，AMM 只能提供非常基本的流动性支持。

基于订单簿的订单匹配依赖于人类做市商来反映集中交易所的流动性。有效的做市商价格昂贵，几乎没有 DEX 团队能够负担得起。此外，由于涉及的人为因素，这种流动性很难用智能合约来填补，这极大地限制了 DeFi 从业人员的用例数量

PMM 也是算法做市商算法，但与其他方法相比，它在缓解方面有根本不同消除它们的劣势并扩大其优势。 PMM 为所有资产提供足够的，可履行合同的链上流动性，从而使 DeFi 用户能够利用可组合性。此外，Synallage 可以支持专业做市商在链上高效作市。任何项目方和做市商或个人，均可以通过调节市场中间价、流动性深度和盘口价差等参数，来实现完整高效灵活的作市策略。并且这些流动性还可以在链上与其他智能合约共享。

2.2 核心概念

2.2.1 基础和报价代币：

Base 和 quote 是两个被反复提到的概念，有两个方法可以区分他们：

在交易对中，base 是连字符前边的代币，quote 是后边的。

在交易中，价格往往是表示多少个 quote token 可以买 1 个 base token 。

比如，在 ETH - USDC 交易对中， ETH 是 base token , quote token。

2.2.2 PMM 参数：

PMM 算法中有 4 个参数：

B_0：base token 回归目标值 - 做市商总充值

Q_0：quote token 回归目标值 - 做市商总充值

B：base token 资产 - 当前资产池 base token 中的数量

Q：quote token 资产 - 当前资产池中 quote token 中的数量

2.2.3 PMM 定价公式：

PMM 的价格曲线对应的公式为：$P_{margin=iR}$

R是由以下公式确定：

如果 $B < B_0$，则 $R = 1 - K + \left(\frac{B_0}{B}\right)^2 K$

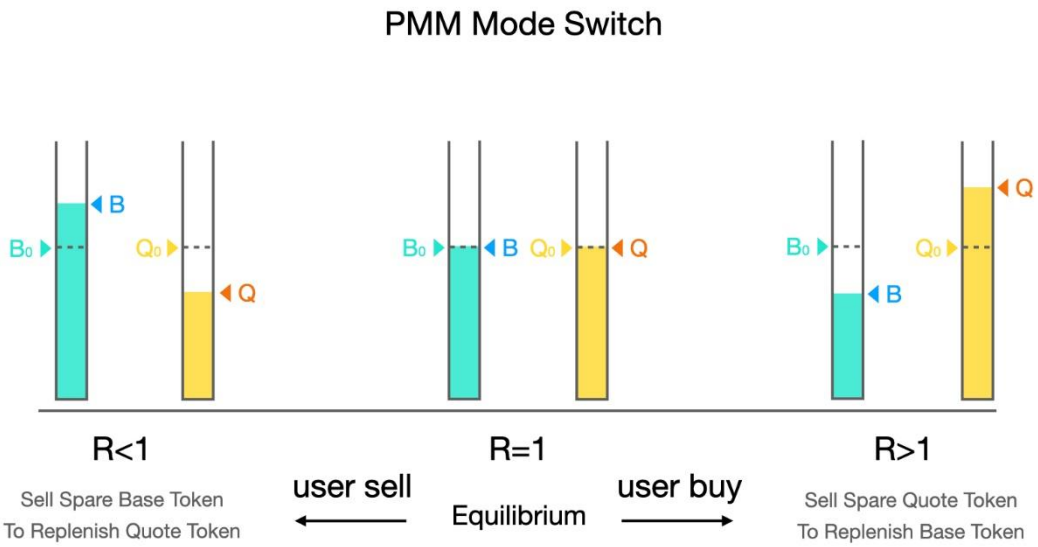
如果 $Q < Q_0$，则 $R = \frac{1}{1-K+\left(\frac{Q_0}{Q}\right)^2 K}$

其他情况R=1

i 是由预言机提供的市价，k 是一个 0 到 1 范围内的参数。

2.2.4 PMM 中的三种状态：

在任意时间， PMM 算法不外乎三种状态，base token 和 quote token 一样；base token 短缺；quote token 短缺。



在最初没有任何交易的时候，资产池处于平衡的状态。base token 和 quote token 位于回归目标。

$B = B_0$ and $Q = Q_0$

当交易者售出 base token 时，base token 资产池的余额高于回归目标；相反 quote token 资产池余额低于回归目标；在这种情况下，PMM 将会尝试出售多出的 base token，让资产池回归到平衡状态。

同理，当交易者购入 base token 时，quote token 资产池中的余额会高于回归目标；base token 余额低于回归目标。PMM 将会尝试出售多出的 quote token,让资产池回归平衡状态。
参数 R 会在回归过程起到非常关键的作用。资产池越偏离平衡状态，R 就越偏离 1。当 PMM 给出的价格与市价存在差价时，套利者就可以来搬砖帮助资产池回到平衡状态。

2.2.5 流动性付费：

每笔交易将会被收取少量的手续费，这笔手续费就是流动性付费，会按照资产比例分给做市商。换句话来说，交易者交手续费，做市商参与分成。

举个例子，在 ETH－USDC 交易市场，用户买入 ETH，需要交少量 ETH 作为手续费，这部分 ETH 将会分给做市商。当用户卖出 ETH 时，需要交少量 USDC 作为手续费，这部分 USDC 将会被分给做市商。

注意：在资产池中，base token 和 quote token 收益率是不同的。

2.2.6 运营手续费：

运营手续费同样是由交易者缴纳，分给运营者，有可能是开发团队，创始团队，DAO。
目前，运营手续费为 0.1%。

2.2.7 提现手续费：

从资产池中提取资金，将会影响其他做市商的收益。将会对提取资金收取手续费，并分给剩余做市商。
在做市商提取 b 个 base token 后，B_1下降 b，B_0下降幅度更大。这笔提取会让所有的做市商遭受亏损，这是因为这笔提取让价格曲线变的更加陡，多余的 quote token 买不回同样多的 base token。

PMM 算法要求在这种情况下，提取需要支付一定的手续费。手续费等于这笔引起的做市商的亏损总和。这笔手续费将会被分配给还未提取的做市商。

考虑到下面我们提到的充值奖励，如果做市商在充值后立即提取，提取的手续费会大于充值奖励，从而杜绝了无风险套利。

值得注意的是，只有当系统严重偏离平衡状态并且充值或提取的数量很大时，PMM 才会发放充值奖励或收取提取手续费。一般情况，交易者不用关注这两部分。当然，我们也非常欢迎交易者在系统偏离平衡状态时充值赚取奖励，等系统平衡后提取避免被收取手续费。

注意：通常提取手续费为 0 或者小于 0.01%；仅当某种资产严重短缺，做市商尝试提取该种资产时，提现手续费会大幅提高。提现手续费的设计是为了保护那些长期帮助我们健康发展的做市商。

2.2.8 充值奖励：

资产短缺时，向资产池充值的做市商会获得奖励。
当资产处于短缺的状态时，充值或提取会影响价格曲线。这就要求我们要谨慎地处理充值和提取来保证资产池的可持续性和公平性。我们来分析下当 base token 短缺时，做市商要提取代币会发生什么。

根据 B_0 的推导公式，得出：$$B_0 = B_1 + B_1 \cdot \frac{\sqrt{1+\frac{4K\Delta Q}{B_1 i}}-1}{2K}$$

当做市商存入 b 个 base token 时，B_1上涨 b，B_0上涨幅度更大。这就意味着这笔充值会让所有充入 base token 的做市商获利，这是因为这笔充值会让价格曲线变平滑，同样数量的 ΔQ可以购买更多的 base token.
这种情况下，做市商一旦充入资金，做市商就会盈利，这被称为充值奖励，奖励主要是由让系统偏离平衡状态的交易者支付的。
注意：充值奖励并不是无风险的套利交易机会。

3、PMM Perpetual 协议

3.1 概览

3.1.1 简介：

PMM Perpetual 协议是 Synallage 基于 PMM 的分散式永久交换协议。永久掉期是最流行的衍生工具之一，没有到期日，支持保证金交易，并且其价格与指数价格挂钩。

该协议的目标是允许任何人在任何永久性市场中创建和交易。首先，任何人都可以使用基础资产的价格来创建自己的永久市场，并选择任何 ERC20 作为抵押。其次，使用文章上述的 PMM 模型提供流动性，解决了流动性问题-任何人都可以通过将资产存入池中来为 PMM 提供流动性，并获得合理的市场获利。最后，任何人都可以未经许可进行永久掉期交易。交易者的资产以非托管方式存在于智能合约中，交易过程完全在链上进行。

我们认为，未经许可是此协议的关键功能，它可以使整个社区都能够为生态系统做出贡献-任何人都可以创建链上或链外合成资产的永久市场。随着社区的发展，将创建更多样的永续市场，并产生交易量。

3.1.2 市场参与者：

市场上有以下角色：
1、PMM 池
PMM 池扮演中央交易对手的角色，为永久掉期提供流动性。像普通交易者一样，具有独立的保证金账户，并且能够持有头寸。
2、中央操作员
中央操作员是永久掉期的创建者和管理者。

- 如何成为管理者：
    - 创建永久掉期并设置初始参数（例如保证金率，PMM 风险参数等）。永久掉期的 PMM 具有一组风险参数。通过调整这些参数，操作员可以更改 PMM 的做市风险，市场深度，滑点和价差等。
    - 付费（或提供）Oracle 服务。该协议定义了一个 Oracle 接口，以便当前可用的 Oracle 可以应用在该协议中。操作员也可以将自己的 Oracle 数据提供给永久交换。
    - 操作员可以设置风险参数的范围，并在此范围内调整风险参数。
    - 操作员可以启动治理过程以更改风险参数的范围。
    - 运营商可以将其角色转移到其他地址，并选择退出其运营商角色。没有运营商的永久性市场将由 LP 管辖。
- 收益：
    - 通过收取自己设定的管理费从每笔交易中获利。
    - 奖励分配给一些表现良好的潜在资源池
    - 发起治理提案
- 风险：无

操作员必须每 10 天检查一次。如果操作员在这 10 天内未能办理登机手续，将被解雇。

3、流动性提供者

- 如何成为 LP：
  - 在 PMM 池中存入抵押品
- 收益：
  - 固定比例的交易费
  - 从点差和滑点中获利
  - 交易商支付的资金
  - 清算罚款
  - LP 可以参与治理
- 风险性
  - 当 PMM 持仓时，存在风险敞口。如果此时指数价格发生变化，则 PMM 可能会亏损。此损失将由所有 LP 分担。

当 PMM 有头寸时，将尝试通过以下方法降低 LP 的风险：

- 从交易对手处获得资金支付。
- 增加 PMM 的最佳卖价和最佳买入价之间的价差。
- 更改 PMM 提供的价格，这会阻止交易者增加 PMM 的头寸，并鼓励交易者降低头寸。例如，当 PMM 持有多头头寸时，它将同时降低买价和卖价。但是买入价的降幅大于卖价的降幅。

4、交易者

交易员是市场中最主要的参与方。交易员通过与 PMM 交易开仓、平仓，实现盈亏。交易员总是吃单方（Taker）。在本协议中，交易员无法绕过 PMM 相互成交，所有的交易必须通过 PMM 达成。交易员在交易过程中，需要向 PMM 支付交易手续。交易员根据资金费率规则支付(或接受)资金费用

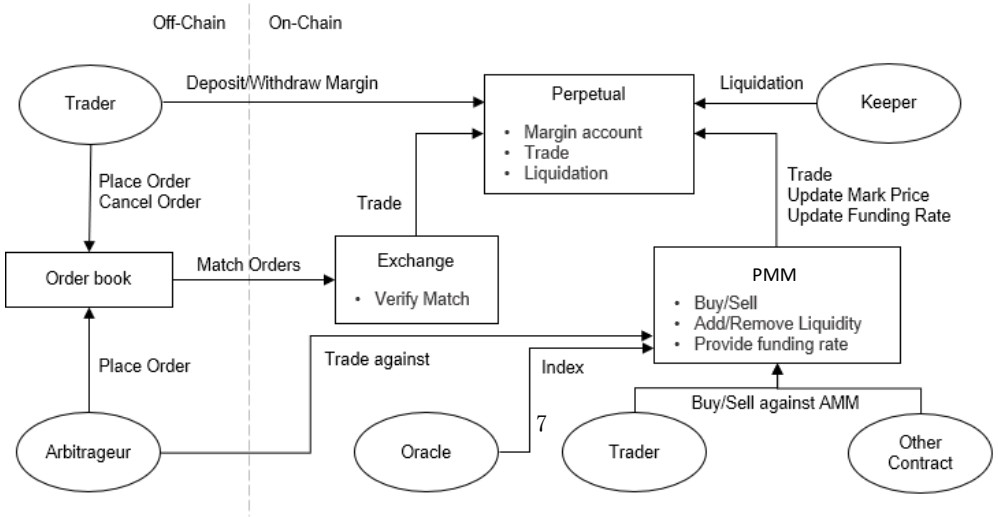
5、清算人

Keeper 是一类辅助角色。任何人都可以成为 Keeper 对保证金不足账户进行强制平仓。

6、委托人

委托人是一个特殊角色。每个保证金账户可能都有一个委托人。委托人可以在帐户上进行交易（直接针对 PMM 或通过经纪人进行交易），但不能从帐户中提取资金。委托人的目标是分离热钱包和冷钱包，并实现交易策略的保管。

3.1.2 混合架构：



PMM Perpetual 协议主要由三个部分组成：永续，PMM 和交易所。

- 永续：存储保证金帐户的数据，包括抵押品和头寸
- PMM：实现类似于中心化交易所合约的界面，以便用户直接与合同进行交互。
- 交易所：为订单簿交易实现“匹配”界面

上图显示了这种混合体系结构：

3.2 永续合约保证金账户模型

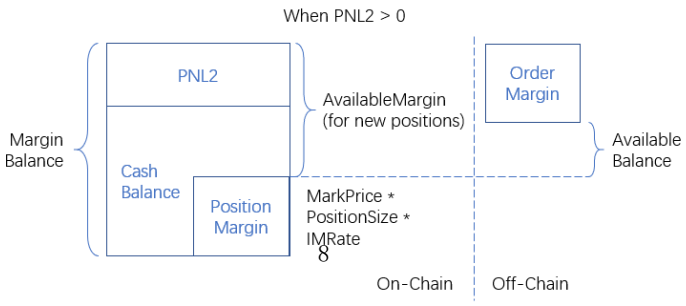
3.2.1 链上部分：

Term	Definition
CashBalance	Deposited collateral
MarginBalance	CashBalance + PNL2
PositionMargin	MarkPrice * PositionSize * IMRate
MaintenanceMargin	MarkPrice * PositionSize * MMRate
AvailableMargin	The balance that can open new positions = MarginBalance - PositionMargin
IsSafe	MarginBalance >= MaintenanceMargin
PNL1	Long position: (MarkPrice - AvgEntryPrice) * PositionSize Short position: (AvgEntryPrice - MarkPrice) * PositionSize
PNL2	PNL1 - SocialLoss - FundingLoss

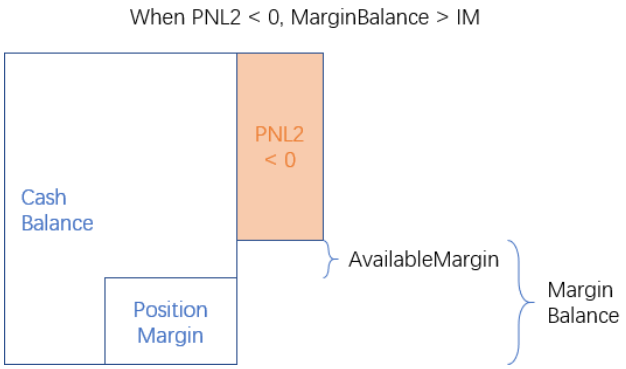
3.2.2 链下部分：

Term	Definition
OrderMargin	MarkPrice * OrderSize * IMRate
AvailableBalance	AvailableMargin - OrderMargin

示例 1：PNL2 >= 0



示例 2：PNL2 < 0



3.3 永续合约交易模型

3.3.1 资金费率：

和传统的永续合约类似，资金费用是使得本协议的永续合约价格锚定指数的重要手段。

本协议的设计中，由于交易都必须经过 PMM 达成，所以如果 PMM 没有头寸时，可以认为市场的多空需求是平衡的。此时 PMM 会给出一个在指数（Index）附近的买入(bid)/卖出(ask)报价，即可以认为此时市场价是锚定指数的价格。

当 PMM 持有某个方向的头寸时，PMM 给出的报价也会向相应方向偏移。当 PMM 持多头时，PMM 报价会向低于 index 的方向偏移，反之 PMM 报价会向高于 index 的方向偏移。此时，可以认为市场的多空需求不平衡，市场价格也相对指数发生的偏移。这种情况下，协议会向与 PMM 持仓相反的头寸征收资金费用支付给与 PMM 持仓相同的头寸（包括 PMM）。资金费率与 PMM 持仓量正相关。即 PMM 持有的头寸越多，市场价偏离约严重，此时也会收取更高的资金费用。

当出现资金费用时，一方面可以阻止更多交易员成为 PMM 的对手方，防止价格进一步的偏离。另一方面，高资金费率也会吸引更多的 LP 添加流动性或进入与 PMM 相同的头寸，赚取资金费用。根据 PMM 的设计，向 PMM 添加流动性或与 PMM 交易减少 PMM 的持仓都会减少价格偏离的程度。上述两方面的作用，会使得市场价格回归指数。

3.3.2 保证金与盈亏：

由于本协议的无需许可的特点，任何人都可以创建风险程度各不相同的永续合约。为了防止风险在不同的永续合约之间随意传递，本协议使用隔离保证金机制（Isolated Margin）。在隔离保证金机制下，交易员每个永续合约内都有一个独立的保证金账户，该保证金账户的盈亏不会影响其他合约的保证金账户。

当交易员以 P_entry，的价格做多或做空 ΔN 个合约时，ΔN>0 意味着该交易员做多，而 ΔN<0 意味着该交易员做空。

当开仓时，保证金账户的余额须不小于初始保证金：

$P_{mark} \cdot |N| \cdot R_{im}$

P_mark 是 Oracle 提供的标价。P_mark 通常等于指数价格 P_index，或者是指数价格 P_index 的时间加权平均价格。R_im 是永续合约的初始保证金率。

头寸盈亏的计算如下：

$(P_{mark}-P_{entry}) \cdot \Delta N$

用户可以在任何时间提取永续仓位的盈利。也就是说，此合约中的“PNL”永远指的是已实现的盈亏。并且持仓亏损也是由实时的保证金账户余额推演而来的。

交易员可以平仓价格/止损价格 P_exit 平仓，其平仓后 PNL 为：

$(P_{exit}-P_{entry}) \cdot N$

交易员务必确保保证金账户余额不小于维持保证金 M_mm：

$P_{mark} \cdot |N| \cdot R_{mm}$

如果保证金账户余额无法达到维持保证金的数额，则该仓位将会被强平。

最后，每个永续合约都有一个“Keeper Gas Reward”参数。当头寸被强制平仓时，Keeper 可以获得该参数规定的奖励用于支付 Gas。所以，本协议要求，只要保证金账户的头寸不为 0（无论头寸的价值如何），保证金账户至少要有可以支付“Keeper Gas Reward”的保证金余额，否则头寸也会被强制平仓。

3.3.3 强制平仓：

当保证金账户内的保证金余额低于头寸的维持保证金时，头寸将被强制平仓。任何人都可以作为 Keeper 对保证金不足的头寸发起强制平仓。Keeper 可以选择两种强制平仓方式之一：

- 通过 PMM 强制平仓：被强制平仓的头寸将通过 PMM 平仓。这也意味着头寸被转移给了 PMM。强制平仓罚金将进入资金池。Keeper 可以获得“Keeper Gas Reward”数量的资金作为清算奖励。
- 由 Keeper 强制平仓：被强制平仓的头寸将被转移给 Keeper。这种模式下，Keeper 承担了头寸风险，也将获得强制平仓罚金。

3.3.4 交割：

虽然是永续合约，但是在遇到极端行情下，依旧会出现流动性匮乏情况。如果在强制平仓时由于 PMM 的流动性不足或者清算不及时出现清算损失（Liquidation Loss）时，PMM 中的保险基金会首先用于支付清算损失。如果 PMM 的保险基金也不足以偿付损失时，合约会进入交割状态。永续合约会以最后的指数价格进行交割。合约中剩余的资产会按持有头寸的交易员的保证金余额的比例进行分配。也就是说，清算损失是由所有的持有头寸的交易员根据其保证金余额规模共同承担的。这也意味着，如果交易员没有头寸，则不会承担任何清算损失。我们认为，在极端行情下尽快交割合约并使得交易员可以提取出自己的保证金可以保护各方利益，也是一种变相的市场熔断机制。交易员可以在市场情绪稳定后，重新创建永续合约继续交易。

另外，当 Oracle 超过 24 小时不更新数据时，合约也会进入交割状态。

合约的交割分为两个阶段，第一阶段称之为紧急状态（Emergency），在这一状态时，永续合约 Oracle 不再更新。此时，Keeper 对永续合约的所有保证金账户发起复查操作。Keeper 将获得等于“Keeper Gas Reward”的奖励。在复查操作中，会以交割价计算保证金账户的保证金余额。 当所有的保证金账户复查完毕，交割进入第二阶段称之为清算完成状态（Cleared）。在此阶段，交易员可以提取出剩余的保证金。

3.3.5 保险基金：

每个永续合约都附带 1 个保险基金用于赔付系统的清算损失。

任何人都可以向保险基金内捐献资金。我们鼓励 Operator 向一级保险基金中捐献初始资金，并在合约持续运营的过程中补充持续资金。

当账户的维持保证金不足而被清算时，将收取一定的清算罚金。清算罚金中一定比例（由 PMM 参数确定）的资金归属保险基金，剩余罚金归属清算人（PMM 或 Keeper）。 每个保险基金设置一个基金规模上限。当保险基金达到上限时，新增的资金会进入 PMM 的流动性资金池。LP 可以通过治理的方式调大保险基金的规模上限，但不能下调。

3.3.6 PMM 参数及治理：

PMM 的参数分为可修改参数和不可修改参数。Operator 与 LP 可以通过投票的方式调整可修改参数。PMM 有 5 个风险参数，每个风险参数都有一个有效范围。Operator 可以根据市场情况在有效范围内自由调节风险参数。如果需要修改风险参数的有效范围，则需要通过 PMM 内的投票治理。

Operator 可以发起治理提案。如果永续合约没有 Operator，也可以由不低于 1%份额的 LP 发起治理提案。每个治理提案需要由 LP 投票通过后执行。投票率（Vote Quorum）不得低于 LP 总份额的 10%。只有在提案发起前存在的 LP 代币具有投票权。每个提案的投票时间为 72 小时，决议通过后需要经过 48 小时的时间锁后方能生效。LP 在投票时需要质押 LP 代币。如果提案通过，投赞成票的 LP 代币将在提案执行后 72 小时解锁，投反对票的 LP 代币将在投票结束立刻解锁；如果提案没有通过，则参与投票的所有 LP 代币将在投票结束后立刻解锁。LP 发起提案时，该 LP 自动质押 LP 代币并投赞成票。

PMM 参数	含义	可修改/不可修改
底层资产	一个标识合约底层资产的字符串	不可修改
抵押物代币地址	抵押物 ERC20 代币地址	不可修改
Operator 地址	Operator 的地址	Operator 可以修改
Oracle 适配器地址	兼容 PMM Oracle 标准的适配器合约地址	不可修改
初始保证金率	初始保证金率，决定了开仓的最大杠杆	LP 治理修改，只能减小
维持保证金率	维持保证金率，决定了头寸被强制平仓时的杠杆；必须小于初始保证金	LP 治理修改，只能减少
金库费率	交易手续费中进入 DAO 金库的费率	由 DAO 治理修改
Operator 费率	交易手续费中归属 Operator 的费率，不大于 1%	LP 治理修改
LP 费率	交易手续费中归属 LP 的费率，不大于 1%	LP 治理修改
推荐返点 Referral Rebate 费率	从 Operator 和 LP 费中给予 Referral 的返点比例	LP 治理修改
强平罚金费率	强制平仓罚金费率。罚金=头寸价值*罚金费率。不大于维持保证金率。	LP 治理修改
保险基金费率	罚金中归属保险基金的比例	LP 治理修改
保险基金最大值	保险基金规模上限	LP 治理修改，只能增大
Keeper Gas Reward	当 Keeper 执行强制平仓或在交割阶段复查账户时，获得的固定数量的奖励，用于支付 Keeper 的 Gas 费用。	LP 治理修改
PMM 做市风险参数	一组控制 PMM 做市商风险的参数	Operator 可在范围内调整

值得注意的是，每个 PMM 都有一组做市商风险参数，这些参数决定了以下做市特征：盘口价差（Spread）、滑点（Slippage）、PMM 最大持仓规模、PMM 持仓量与资金费率的关系。每个风险参数都有一个有效范围。Operator 可以不经过治理流程直接在有效范围内修改风险参数。通过这种方式，LP 可以授权 Operator 根据市场情况及时调整风险参数，这在永续合约上线运营初期是很有必要的。当合约运营一段时间、风险参数趋于稳定后，LP 可以通过治理减少风险参数的有效范围（甚至固定风险参数），从而提高 PMM 的去中心化程度。

除了修改 PMM 的参数的提案外，还有 2 个特殊的提案，通过这些提案需要的投票率不得低于 LP 总份额的 20%：

- 使永续合约进入交割状态；
- 设置新的 Operator。只有当合约没有 Operator 时，LP 可以发起提案设置新的 Operator；

3.4 限价单与止损单

3.4.1 概述：

直接与 PMM 进行交易类似通过传统订单簿的市价单交易。在永续合约交易场景下，人们往往喜欢通过限价单等待交易机会、控制成交价格。另外，止损单也是一类高杠杆交易时重要的工具。为此，我们提供了去中心化且有效控制 GAS 费的限价单和止损单功能。该系统由两个合同组成：OrderBook 和 Settlement。

3.4.2 OrderBook：

OrderBook 部署在 kovan 和 rinkeby 测试网上。

OrderBook 保留用户已提交的限价单。任何人都可以致电 createOrder()创建一个限价单，其中包含要卖出的数量和最低价格。他/她需要批准 Settlement 合同出售的金额。
为了减少用户的 GAS 费，不将 OrderBook 部署在主网上。kovan testnet 上的一个用于生产。

3.4.3 Settlement：

Settlement 部署在以太坊主网上，kovan 和 rinkeby 测试网上。
Settlement 负责将令牌交换为订单。任何人都可以致电 fillOrder()填写提交的订单。我们称这个呼叫者为“ relayer”。中继器需要使用适当的参数来调用它，以满足订单中设置的最低价格要求。如果呼叫成功，则费用将转移到中继器。
订单的制造商可以取消它 cancelOrder()上 Settlement。
可能仅填充一定数量的令牌，而不是全部。在大多数情况下，提交的订单将驻留在上 OrderBook，其金额将由不同块中的不同调用者填写。

3.4.3 中继器[3]：

Settlement 是围绕 Router02 的包装合约。该合约中的每个功能在中都有一个 Settlement 带有额外参数的重复版本 args。如果 args 不为空，则用于填写订单；如果不为空，则用于填写订单。

因此，用户可以选择是否成为中继器。如果他/她决定这样做，则调用任何交换功能 Settlement 将使他们受益。否则，他/她就可以直接调用功能，Router02 而无需支付任何费用。

3.4.4 费用：

对于每次 fillOrder()通话，将收取所售金额的 0.2%的费用。收取 20%的费用给 VIP 代币持有者，其余的给中继器。费用在调换之前扣除。

假设 *Alice* 创建了一个订单，以最低价格 500 DAI 卖出 1 ETH。ETH 的当前价格为 400 DAI，因此无法立即执行此订单。当市场价格上涨到 500 DAI 时，*鲍勃（Bob*）试图以中继员的身份填补该订单的全部金额。
如果呼叫成功，则传输的令牌数量为：

- 限价订单费用：1 ETH x 0.2%x 80%= 0.0016 ETH（给 *Bob* ;中继器）
- 限价订单费用分割：1 ETH x 0.2%x 20%= 0.0004 ETH（给 VIP 代币持有者）
- 手续费：（1 ETH - 0.002 ETH）x 0.3%= 0.002994 ETH（给流动性提供者）

- ETH 售出数量：1 ETH - 0.002 ETH - 0.002994 ETH = 0.995006 ETH（进入流动资金池）
- DAI 买入量：0.995006 ETH x 500 DAI = 497.503 DAI（给 *Alice*）

4、*Pratt & Whitney* 协议

4.1 概览

4.1.1 简介：

Pratt & Whitney 是基于 UMA 的去中心化合成资产发行协议，代表“普惠”。我们的共同信念是，金融市场应该是自由，开放和公平的。自由开放的市场创造的经济自由使每个人都有平等的机会追求繁荣和建立金融独立。

我们的目标是使任何人都能通过 *Pratt & Whitney* 协议无缝安全地获得或转移任何形式的风险，以使每个人都能够参与可普遍访问的金融系统。

合成资产可以在无需持有某种实际资产的情况下，提供对这种资产的交易。合成资产有一系列优势，包括减少在不同资产之间切换时的摩擦（例如，从 Apple 股票到合成黄金），扩大某些资产的可触及性，使任何人可以在任何时间交易任何资产，例如外汇、股票、大宗商品、贵金属等而无需审查、开户、出入金等复杂操作，达到普惠的目的。

4.1.2 特色产品-KPI：

关键绩效指标（KPI）选项是合成令牌，如果项目的 KPI 在给定的到期日期之前达到预定目标，它将获得更多奖励。每个 KPI 期权持有人都有提高 KPI 的动力，因为他们的期权将价值更高。这旨在使个人令牌持有者的利益与协议的集体利益保持一致。

使用 *Pratt & Whitney* 的到期多方（EMP）合同模板和 Optimistic Oracle，任何项目都可以创建自己的 KPI Option 令牌。这些可以由任何已批准的 ERC-20 令牌支持，并且可以针对项目想要改进的任何 KPI 进行估价！

在 *Pratt & Whitney* 上启动 KPI 期权合约的过程非常简单。不需要链上的价格提要或智能合约开发。这是启动自己的过程所需要遵循的典型过程。

1. 您应该提交两个 *Pratt & Whitney* 改进建议。第一种应将您的治理令牌添加为受支持的抵押品类型。第二个应该定义一种方法，用于说明 Pratt & Whitney Optimistic Oracle 如何定价您的 KPI 期权。
2. 这些提议通过 Pratt & Whitney 治理批准后，您就可以启动即将到期的 KPI 期权合同！通过遵循 EMP 部署教程，可以在几分钟内完成此操作。
3. 启动即将到期的合同后，您将可以通过将抵押物锁定在合同中来铸造 KPI 令牌。铸造后，您可以以任何方式和任何人将这些 KPI 令牌空投。
4. 合同到期后，可以根据您的 KPI 进度确定可兑换 KPI 期权的金额。另外，您的项目可以决定“过渡”到新的 KPI 选项中，以尝试加重 KPI 的增长。

4.2 运作方式

4.2.1 引入 DVM：

Pratt & Whitney 提供无价的金融合同。无价金融合同是精明的合同，在发生纠纷时仅需要链上价格即可。经济担保和网络激励措施可确保网络参与者在大多数情况下都能诚实行事，但如果发生恶意参与者或临时市场事件，则可引发争议，以称为 Pratt & Whitney 的争议解决系统，即数据验证机制（DVM）。DVM 是 Pratt & Whitney

提供的 oracle 服务的名称。DVM 不提供链上价格供稿。相反，它仅用于解决清算纠纷并在到期时结算合成代币合同。

4.2.2 合成方式：

1、Pratt & Whitney 上有五个主要的网络参与者

1. 代币赞助商
2. 清算人
3. 纠纷
4. 数据验证机制（DVM）
5. 代币持有人

2、如何在 Pratt & Whitney 中保护合成资产

代币发起人是将抵押品锁定在智能合约中以铸造合成代币的人。代币发起人有责任确保其头寸始终保持超额抵押，否则其头寸将被清算。

智能合约中抵押品的价值由强大的清算人网络在链下进行连续监控。清算人通过参考链下价格信息来持续监控头寸是否得到了适当的抵押。清算可以配置为自动搜索要清算的头寸（通过清算机器人），或者由持有合成资产和要清算头寸的抵押货币的任何人手动进行。清算人会受到奖励，以奖励他们发现和清算欠抵押品头寸。如果清算人自动清算头寸，清算完成之前将有 2 个小时的延迟。

在 2 小时的延误期间，将鼓励争议方使用 Pratt & Whitney 的无价金融合同来监督合同。与清算人类似，争议者可以采用争议机器人的形式，也可以手动执行。争议者参考自己的链下价格供稿来确定清算是否有效。如果无效，则争议机器人将对清算提出争议，该清算将称为 Pratt & Whitney 的 Oracle，即数据验证机制（DVM）。清算头寸将待定，直到 DVM 解决（48 小时后）。希望收到高于 48 小时价格的合同，可以使用 Pratt & Whitney 的 Optimistic Oracle。

DVM 将通过建议代币持有人投票以在给定的时间戳上获取资产价格来解决纠纷。代币持有人将参考链下价格供稿，以向 DVM 报告价格信息。DVM 将汇总代币持有人的票并报告链上资产的价格。

如果争议方是正确的，则 DVM 将奖励争议方和代币保荐人所影响的头寸。如果清算人是正确的，则 DVM 将奖励清算人，对争议方进行处罚，代币保荐人将损失其头寸中的资金。

4.2.3 无价合约：

如今，分散的预言机解决方案由 API 组成，这些 API 反复在链上提交价格数据以管理 DeFi 合同。解决方案也无法对 API 报告的不正确价格提出异议。这使得合同容易受到腐败，操纵，快速贷款攻击和临时市场事件的影响。无价金融合约是仅在发生纠纷时才需要在链上写下价格的合同（这种情况很少发生）。无价合约减少了对 Oracle 的依赖，使 Pratt & Whitney 上的合约不易受到攻击。

无价合约的设计旨在激励那些造币的人（称为代币发起人），以确保他们的头寸得到适当数量的抵押品的支持。提取头寸涉及铸造合成令牌，可以将其偿还以关闭头寸并退还抵押品。除非被确认为抵押品不足，否则假定仓位是有偿付能力的。代币保荐人有责任确保其仓位始终得到所需数量的抵押品的支持。

确保对头寸进行适当抵押的关键机制是清算和纠纷流程，该流程奖励对未抵押头寸的清算。任何人都可以通过抵押清算人债券并参考自己的链下价格供给来确定资产的价格，从而开始清算。清算将持续 2 个小时，直到清算活跃期结束为止为止，以便有争议者有机会对清算提出异议（如果需要）。大多数清算和纠纷是由机器人监视 Pratt & Whitney 上的合同自动启动的。

4.2.4 预言机系统：

Pratt & Whitney 的预言机系统由两个核心组件组成：

1. 乐观预言机[4]
2. 数据验证机制（DVM）

Pratt & Whitney 的乐观预言机使合同可以快速请求和接收价格信息。乐观预言机充当发起价格请求的合同与 Pratt & Whitney 的争议解决系统（称为数据验证机制（DVM））之间的通用升级游戏。除非有争议，否则乐观预言机提出的价格不会发送到 DVM。这使合同能够在任何预定的时间长度内获取价格信息，而无需将资产的价格写在链上。

如果发生争议，则将请求发送到 DVM。所有基于 Pratt & Whitney 的合同都使用 DVM 作为解决争议的支持。Pratt & Whitney 代币持有人在给定时间对资产价格进行投票后 48 小时，将解决发送到 DVM 的争议。Pratt & Whitney 上的合约不需要使用乐观预言机，除非它要求资产价格快于 48 小时。

4.2.4.1 乐观预言机：

1. 请求者在给定时间询问资产价格。请求者提交以下信息以请求价格：

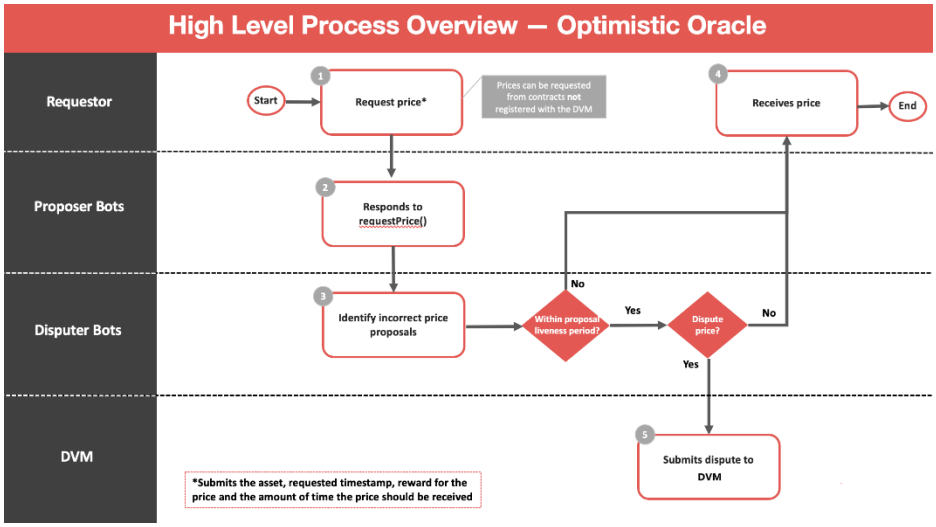
   资产

   时间戳记

   收到价格的时间

   奖励金额

   注意-要求价格的合约不需要在 Pratt & Whitney *的 DVM 中注册*
2. 投标者通过引用链下价格供稿来提交资产价格，从而对价格请求做出响应。作为他们工作的回报，他们将收到由请求者设置的预定义提案奖励。要提议价格，提议者必须放下提议保证金。如果他们提出的价格信息有争议并且被认为不正确，则提议者将失去其担保。
3. 争议者可以通过引用其自己的脱链价格供稿来反驳投标人在投标有效期内提交的价格。提案有效期是在请求者收到资产价格之前可以对提案进行争议的预定时间。
4. 如果争议方未在投标有效期内反驳投标人提交的价格，则将价格发送给请求者。
5. 如果提案有争议，则价格将提交给 Pratt & Whitney 的 DVM，并在 48 小时后解决。



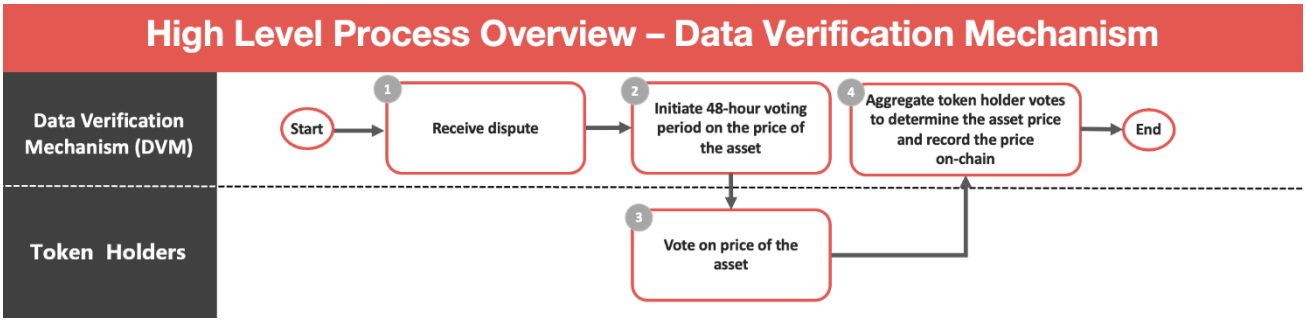
-4.2.4.2 DVM:

数据验证机制（DVM）是基于协议构建的合同的争议解决服务。争议通过渠道发生：

- 来自乐观预言机的争议
- 合同清算争议
- 发生争议时，价格请求将提交给 DVM，DVM 提议对代币持有人进行投票，以报告特定时间戳记下的资产价格。
- 投票将在 48 小时后结束，从而导致争端解决。
- 令牌持有者将参考价格标识符来确定如何通过链外价格供稿计算资产价格，以及如何在协议的 Voter dApp 中记录资产价格。
- DVM 将汇总令牌持有者的投票，以确定给定时间戳记下资产的最终价格。如果 DVM 返回的价格表明争议方是正确的，则提案人或清算人（取决于争议的来源）将失去所抵押的保证金，并获得争议方的奖励。如果 DVM 认为提案人或清算人是正确的，则争议方将失去其争议保证书，清算人或提案人将获得奖励。

DVM 具有强大的功能，因为它包含了人为判断的要素，以确保当动荡的（有时是可操纵的）市场出现问题时，可以安全，正确地管理合同。

协议的预言机系统的构建具有经济保证，包括破坏 DVM 的成本，以确保破坏预言机的成本（即获得 51%或更多的代币）要比破坏预言机的收益（即窃取资金）多在有关协议的合约中）。



4.3 合成代币

4.3.1 合成资产类型:

合成令牌是抵押支持的令牌，其价值根据令牌的参考索引而波动。合成代币融合了预测市场，期货市场和抵押贷款的特征。

合成令牌的一些示例包括：

- 综合的现实世界资产（例如：黄金或茅台股价）
- 合成跨链密码资产
- 各种不可交易索引的跟踪令牌

关于合成代币的一些最具创意的想法属于最后一类。例如：

- 跟踪 DeFi 项目未来使用情况的令牌（例如，锁定在 Uniswap 中的资产）
- 跟踪 Chrome 扩展程序下载次数的令牌（例如 Metamask）
- 在 r / WallStreetBets 上跟踪交易想法成功的代币

通过更改无价合成令牌的价格标识符，您可以创建行为类似于其他衍生产品的令牌化版本（如期权）的合成令牌。

4.3.2 合成资产发起人：

在合成代币的生命周期内，令牌发起人（创建新的合成令牌的人）可能希望在其头寸中存入更多抵押品，以避免清算。如果仓位对他们有利，则保荐人也可能希望提取过多的抵押品。

代币赞助商可以随时存入额外的抵押品。
代币保荐人可以通过以下两种方式之一提取过多的抵押品：“快速”提取或“缓慢”提取。

1、快速提款
“快速”提款允许代币发起人立即从其仓位中提取多余的抵押品，只要所得仓位的抵押品至少等于全球抵押品担保率（GCR）。要求提款导致抵押品至少与 GCR 一样高，这提供了一些保证，即只要尚未清算 GCR 以下抵押品的其他代币保荐人，则该代币保荐人在提款后就不应清算。

2、 缓慢提款
如果代币保荐人希望从其仓位中撤回抵押品，这会使他的抵押品低于全球抵押品率 GCR，那么他可以通过“缓慢”撤资来做到这一点。由于提取此数量的抵押品可能会损害可替代合成代币的偿付能力，因此这种“缓慢的，分为两部分的提取过程”允许其他代币持有人做出标记，以说明代币发起人是否会破产。

在“缓慢的”提款中，分为两个部分：代币发起人向合同提交提款请求，指出他希望提款的抵押物数量和请求的时间戳。
在此期间，任何代币持有人如果认为撤回提款请求中指示的金额会使代币发起人在清算时的抵押品低于“抵押要求”，则可以清算代币赞助商的头寸。如果在没有代币持有人清算代币保荐人的情况下经过了“退出活跃期”，代币保荐人可以从其头寸中提取抵押品，直至所请求的金额。

4.3.3 清算和争议：

在任何时候，清算人机器人都可以根据其所引用的链下价格供求来清算代币赞助商的头寸，以帮助确定头寸是否得到了适当的抵押。清算会立即发生，而无需提取 oracle。任何人都可以在“清算活跃期”内对清算提出异议。

为了清算代币保荐人的头寸，清算人机器人向合同提交合成代币以发布清算保证金。清算保证金是在启动合成合同之前预先定义的，用于以下方面：

1. 为了证明清算人，即代币保荐人的头寸应该被清算。
2. 指出要清算的头寸规模
3. 关闭代币赞助商的位置
4. 如果清算有争议，则承担调用 DVM 的费用

如果清算无异议，清算保证金将退还给清算人。如果有争议的清算人发现其无效，清算人将损失与代币相对应的抵押品的一部分。
以下是解决清算的三种方式：

1. 在清算期间，没有人对清算提出异议。清算期限结束后，代币保荐人存入的抵押品将与清算人在清算中提交的合成代币数量成比例返还给清算人。例如，假设代币赞助商已存入 150 个 DAI 抵押品以创建 100 个合成代币，然后将其出售给市场。后来，清算人提交了 30 个合成代币以清算代币保荐人。如果没有人对清算提出异议，清算人将获得代币保荐人担保物的 30％或 45 DAI。
2. 在清算期间，有人对清算提出异议。为此，争议者必须发布保证金。提出争议后，将向 DVM 提出价格请求。该价格请求将在清算时返回价格标识符的值，该价格标识符将确定代币保荐人是否抵押不足并解决“争议”。

如果 DVM 返回的价格表明在清算时代币保荐人的抵押品不足：

争议者将失去联系。

清算人将获得代币保荐人头寸的所有抵押品。

代币保荐人不会收到他们先前存入该仓位的任何抵押品。

如果 DVM 返回的价格表明代币保荐人在清算时没有抵押不足：

争议者将收回他们的争议保证金和争议奖励。

清算人将获得抵押品均等：（i）由 DVM 确定的清算时代币的价值减去（ii）支付给争议者的争议奖励，减去（iii）支付给原始人的不当清算奖励代币赞助商。

代币保荐人将获得剩余的抵押品和不当清算的奖励。

下表总结了这些支出：

	代币发起人	清算人	争议者
清算无异议	0	代币发起人的抵押品+清算人债券	0
代币发起人过度抵押	代币发起人的抵押品-代币价值+不当清算奖励	代币的价值-争议奖励-清算奖励不当	争议保证金+争议奖励
代币发起人抵押不足	0	代币发起人的抵押品+争议债券+清算人债券	0

4、Borrow 协议

4.1 概览

4.1.1 简介：

Compound 和 Aave 之类的平台允许用户将资产作为抵押品存入，并以此借入其他资产。这些协议吸引了数十亿美元，但它们受到一些主要限制。消除这些限制可能会看到更大的采用率。Borrow 协议旨在做到这一点。
我们通过以下功能来解决这些问题：

- 单独的借贷对。任何人都可以创建一个配对，这取决于用户他们认为足够安全的配对。风险只限于当时。
- 灵活的预言机，包括链上和链下。
- 流动利率基于特定的目标利用率范围，例如 70-80％。
- 针对低 GAS 优化的合同。
- 所提供的资产可用于紧急贷款，从而为供应商提供额外的收入。

4.1.2 借贷对：

当前的解决方案允许用户提供各种抵押资产并借用另一组资产。如果其中一项资产的价格下跌速度超过清算人的反应速度，则每个用户和每项资产都会受到此影响。因此，平台的风险基于平台上列出的最高风险资产的风险级别。随着每增加一个额外资产，这种风险就会增加，导致大多数平台上资产的选择非常有限。

通过隔离借贷对，任何人都可以创建一个新对，类似于任何人都可以创建 Uniswap 对。一些借贷市场将非常稳定和安全，而如果其中包括流动性很强且流动性较低的资产，则其他市场不那么重要。由于这些是孤立的池，因此风险仅限于单个池，而利率将反映该风险。较高的风险池将吸引更少的供应商，从而推高利率。

4.1.3 做空任何代币：

这将允许为任何令牌创建成千上万对借贷对，从而可以在多种令牌上做空保证金。需求很高，但目前不适用于大多数令牌。

假设有一个新令牌叫做 XXX。我们想做空这是因为我们认为它被高估了，因为它的价格是如此的高。我们（或其他人）创建了一个 ETH-XXX 贷款池，抵押率为 80％。

我们提供了价值 1000 美元的 ETH，并借来了价值 750 美元的 XXX。我们出售 ETH 的 XXX 并将 ETH 供回池中。现在我们有：

供应：1750 美元的以太币，借款：750 美元的 XXX

我们额外借了 500 美元的 XXX 并将其出售给 ETH。我们重新提供以太坊，并具有：

供应：2250 美元以太币，借款：1250 美元的 XXX

我们可以再重复几次该过程，或者我们可以使用一次简单的快速借贷就可以在一次交易中完成此操作。根据抵押率，我们可以利用 2-4 倍或更多的杠杆，具体取决于我们的风险状况。

现在，我们不仅可以做空这一全新的代币（目前通常无法实现），而且我们甚至可以利用该做空的手段。这将导致关联的交换池上的大量事务。

4.1.4 灵活的预言机：

创建池后，可以选择一个 oracle。我将提供 2 个基本的 oracle，但是系统可以扩展，任何人都可以将连接器写入 oracle。提供的基本预言机是：

UNISWAP

COMPOUND

任何人都可以创建一个新 oracle。

4.1.5 弹性利率：

理想情况下，您宁愿选择高但不太高的借贷比率（例如 75％左右）。当前的平台试图通过使利率随着利用率的提高而上升来实现这一目标。但是，最小和最大利率是固定的。因此，这些平台并未针对理想的利用进行优化。在非常低或很高的需求期间，必须手动调整速率以校正利用率。当利用率达到 100％时，将不再可能取款。在多个平台上已发生此问题。

每个池将优化利率以达到理想的利用率。如果池未得到充分利用，则随着时间的流逝，利率将不断下降，直到达到 0％或直到有足够的供应量/借款人到达为止。当利用率过高时，利率将开始攀升，直到恢复到理想的利用率为止。

4.1.6 重要参数设定：

Parameter	Value
Collaterization Rate	75%
Collaterization Rate (open)	77%
Target utilization	70%-80%
Minimum Interest Rate	approx 0.25% APR
Maximum Interest Rate	approx 1000% APR

Liquidation Bonus	12%
Protocol Fee	10.0%
Borrow Opening Fee	0.05%

5、新资产发行

5.1 什么是众筹建池

DEX 上的流动性发行主要有 3 种方式

1. 联合曲线发行：随着买盘资金进场，按照固定价格曲线，推高交易价格。第一个买家一定能拿到最低价格，大家都想吃第一口肉，由此产生了科学家抢跑问题和抢跑者投机问题。——低成本的代币被用来投机而没有分发到真正的投资人手里。
2. AMM+二池挖矿：AMM 要求买盘与卖盘双边等比例配资。大部分项目方难以支付高昂的买盘流动性，但是又不想放弃卖盘流动性的深度，于是发明了二池挖矿，通过释放项目代币给 Yeild Farmers，让挖矿的人来提供买盘流动性。这种方式本质是用代币的持续通胀为流动性支付租金，租来的流动性没有忠诚度，「挖卖提」导致了持续的二级市场抛压。
3. 拍卖：拍卖是一个只能买不能卖的市场，它既没有流动性溢价，也不够灵活。

也就是说，目前在 DEX 上发行流动性面临着科学家抢跑、买盘成本高、流动性缺乏等问题。我们一直在思考，如何提供一种新的流动性发行方式，对项目方来说，成本低、流动性足够；对交易者来说，起跑公平。参考股票市场的「集合竞价」，我们设计了 众筹建池 这一全新的流动性发行新方式。

众筹建池基本流程如下：

1. 项目方提供一定量的代币，指定代币单价与发行额度。在指定时间内，任何人都可以充值进行认购
2. 根据用户充值的资金量分配代币额度。 若发生超募，同样按照用户充值的资金分配代币额度，并且超募的资金，将会返还给用户
3. 众筹期结束后，公开池自动在 Synallage 平台建立，众筹价格作为开盘价立即开启现货交易市场

同时，我们针对众筹建池引入了项目方预存结算机制，为公开池增加了流动性保护机制，以及支持灵活的手续费配置

5.2 预存结算费用

我们知道，智能合约是被动触发执行的，同时执行上链操作是需要支付一定的成本。众筹建池的业务中，当众筹期结束后，需要一笔交易触发，以改变众筹池合约状态，并且创建公开池，这需要发起交易，第一时间将业务流程往后推进。因此我们引入了预存结算费用，以覆盖这笔交易的成本。

1. 项目方在创建众筹池的时候，向智能合约预存供 众筹期结束后的结算费用（当前为 0.2ETH）
2. 众筹期结束时，任何人（包括项目方）均可发起交易，即结束众筹，创建公开池。执行交易的人将会获得预存的结算费用

5.3 流动性保护

除了交易者之间的「起跑公平」，交易者和项目方之间，也要维持一种平衡制约的关系。越平衡，越有助于市场的健康发展。因此我们设计了 流动性保护 这一机制：

1. 现货市场的买盘由用户充值的资金构成，卖盘由众筹期后剩余的代币构成
2. 这些初始流动性都属于众筹建池的发起人，但流动性保护期内，发起人不能撤出流动性
3. 任何人都可以像在 AMM 中那样继续添加流动性，只不过 PMM 的资金利用率更高
4. 该现货市场遵循既定的价格曲线：买入代币，价格就会变高；卖出代币，价格就会变低

5.4 手续费设计

我们针对众筹池留有手续费的配置功能，任何众筹池均可针对不同的用户，设置对应的手续费。配合手续费机制，简单列举可实现的玩法：

1. 众筹池针对特权用户设置手续费 0%，其他用户 100%。则实现白名单的定向众筹效果
2. 众筹池针对用户的 vSYN 余额，设置不同的阶梯费率，则实现平台 vSYN 持有者 的打新折扣
3. 收取的手续费，可用于在二级市场回购 SYN，赋能代币价值

5.5 众筹建池优势

1. 投资者买币的钱并没有被滥用，而是建立了一个流动性市场。
2. 项目方有动力认真工作，维护二级市场表现。不然最终能够获得的资金就会变少。
3. 对于新资产：发币既上所，一步到位。不论筹集到的买盘有多少，都可以为代币提供充足的卖盘流动性，方便后续大量资金进场。
4. 对于已经上市但流动性不充足的资产：可以通过众筹一次性释放大额卖盘流动性，提高流动性溢价。
5. 相比于联合曲线发行：公平起跑，避免科学家抢跑
6. 相比于 AMM 二池挖矿：不需要通胀代币来支付流动性租金，代币分发到投资人手里而非“挖卖提”的人手里。
7. 相比于拍卖：众筹建池兼容拍卖功能，却不只是简单的募资。在众筹结束后，立即为你建立拥有充沛流动性的市场。得益于 PMM 算法的灵活性，即使没有募集到很多钱，仍然可以建立一个卖盘流动性非常充足的市场，这是 AMM 所做不到的。

5.6 升价与固定价格众筹

众筹当前支持升价与固定价格这两种模式，其中两者有相同点，也有不同点。

相同点：

- 参与众筹的人，结束时购买代币的成本相同
- 结束众筹后，均会第一时间建立流动性池，开启交易，且交易初始价格为众筹的成本价
- 两种模式均可设置硬顶
- 超募的资金，在众筹结束后，可被提取

不同点：

- 众筹成本价的变化：

    - 对于升价众筹，众筹成本价将会沿着价格曲线，呈上升趋势变化。该价格曲线采用 pmm 算法，在创建众筹池的时候，设置 K，以及 I，该曲线会随着买入 quote 数量变多，而推高众筹的成本价
    - 对于固定价格众筹，众筹成本价是初始设定后，不再变化，技术实现上，固定价格众筹是一种特殊的升价众筹，即价格曲线中 K 设置为 0，这样曲线则会变为横线，达到固定价格众筹的效果
- 硬顶的设置方式：
    - 对于升价众筹，硬顶设置是传入固定的值，当众筹资金超过该值，则价格曲线不再上升，即众筹成本价不再变化，超过硬顶的部分可在众筹结束由参与者提取。同时也支持无硬顶的模式
    - 对于固定价格众筹，硬顶设置是按照比例的方式，因为众筹成本价固定，项目方提供的 Base 数量固定，因此可众筹的资金上限是固定的，我们系统默认是 50%的比例，即一半 Base 用来众筹，一半的 Base 用来结束后提供流动性
- 冷静期的概念：
    - 升价众筹的模式，会随着参与者存入的 quote 数量变多，而抬高所有参与者的众筹成本，这样对于先进场的参与者，存在很大变数，会导致最终众筹成本价超过自身的心理预期上限，因此我们设计了冷静期，在众筹结束后，会有一段的冷静期，这段期间内，参与众筹的人可以选择退出
    -

6、授权及权力

6.1 授权

每个 *Synallage pair* 智能合约中都有两个特殊角色：*admin* 和 *supervisor*。
在这里，我想介绍一下*管理员*和*主管*的权限范围以及背后的设计原理。

主管的权力是 *admin 的一部分*，*主管*和 *admin* 均具有 A 级权限。A 级权限包括：

- 禁止交易
- 禁用存款
- 设定 GAS 价格限制

admin 是唯一具有 B 级权限的*管理员*，其中包括：

- 变更管理员
- 变更主管
- 变更维护者
- 更改 oracle
- 设置流动性提供者费率
- 设定维护者费率
- 设置 K
- 促进贸易
- 启用存款
- 最终结算

级别 A 权限可以概括为“冻结状态”，即系统的某些功能可以紧急停止，但是状态不能更改。为了限制的功率*管理*，往往采取的行动*管理员*必须要经过一个复杂的管理过程。为了抵御风险，我们需要一个更灵活的*主管*而不是*管理员*来执行一些不太敏感但可以显着降低系统风险的操作。

B 级权限基本上涵盖了*合约*的所有方面。之所以设计如此多的可变参数，是为了更好地适应瞬息万变的市场环境。它还为将来的治理留出了空间。

值得指出的是，没有人可以禁止用户提取代币。非监护权是 Defi 最重要的原则。

6.2 去中心化自治

我们认为，Synallage 交易所将完全由社区管理，并由三个 DAO 控制

- *Admin DAO*

担任管理员，是所有问题的最终调解人。

- *Risk Control DAO*

担任主管并紧急处理所有风险事件。

- *Earn DAO*

分配维护者的收入。
当启动时，所有主管部门均由该团队管理。随着社区对 Synallage 的更多了解，我们将逐步将所有权利归还给社区。尽管此过程尚无时间表，但我们确实打算遵循该过程。

步骤：

1. 将管理员设置为具有每日限额的多签名钱包
2. 部署 *SynallageWild*：允许任何人创建自己的 Synallage
3. 发行治理令牌
4. 设置维护者以赚取 DAO
5. Set Admin to Admin DAO
6. 设置主管为风险控制 DAO

每个步骤的目的是什么？

1. 所有管理员操作均带有公共公告期，以避免单点故障
2. 任何人都可以创建一个新的 *Synallage 对*，并使用它来为其令牌提供流动性。这标志着代码已返回社区
3. 发行治理令牌并制定令牌分配计划，这将启动退出流程
4. 移交利润分配责任以赚取 DAO
5. 在将管理权限移交给 DAO 之后，团队没有实际的控制权，仅保留控制风险的权利
6. 团队彻底卸任，标志着朝着完全权力下放的最后一步

7、NFT 市场

7.1 简介

对于一个 NFT 或者一组 NFT（例如一个创作者的系列作品），甚至几组 NFT（例如包含不同类别的若干个 NFT），也可以用类似的方式定价：将 NFT 打散成碎片，并为其建立二级市场。
任何有影响力的个体或组织，可以通过发行 NFT 及碎片化代币，低门槛地捕获市场价值。投资者可以通过买卖和手续费分成获得收益及风险；买断所有碎片代币的藏家可以享受到和 NFT 所有者同等的收益；以至于发展出基于 NFT 碎片的金融衍生品。

相比于其他流动性机制，要么定价与资金量绑定，要么只支持单一价格曲线。在 Synallage NFT，你可以不花 1 分钱（除了 gas 费），无需质押任何资金，就可以主动为碎片代币设置始发价格。你还可以灵活调整价格曲线，调整盘口和深度

7.2 NFT 的碎片化

质押 NFT（或多个 NFT）到 NFT Vault 中， NET Vault 将自动生成一个 ERC20 代币合约。NFT Vault 的拥有者可以设置进入二级市场的代币比例，和预留向一级市场/创作团队/社区激励的代币分发。NFT Vault 的拥有者在后续可以抵押更多 NFT 进入 NFT Vault。
举例，我发了一枚 NFT。我抵押这个 NFT 到 NFT Vault，自动得到一个 ERC20 代币，我可以设置代币名称为 FRAG，总供应量为 10,000，不可增发。我设置 15%的代币，以 1 年线性解锁释放到我指定的版权所有公司的钱包地址，85% 以 1 美金=1 FRAG 的价格，直接进入流动性池中进行流通。FRAG 的价格随着交易发生涨跌。
当然我也可以为动漫的每个角色都发行一枚 NFT，将这一组 NFT 都质押到 NFT Vault 中。

7.3 低成本流动性池

NFT Vault 会自动建立 Trading Pool，并将进入市场的 FRAG 代币全部抵押进去。初始价格由 NFT Vault 的拥有者定义，即可开始销售 FRAG。随着交易者买入，FRAG 价格会自动提高。FRAG 的市值即为 NFT 的估值。

由于 NFT Vault 的碎片已经在市场上流通，普通用户可以只购买 FRAG，便可享受 NFT 价格上涨的福利。如果藏家要想将 NFT Vault 买断，他需要立即支付当前 NFT 的估值。这笔钱将进入 NFT Vault 合约，同时 NFT Vault 中包含的所有 NFT 将转移给藏家。
与此同时， Trading Pool 的参数调整，恒定以藏家成交时的 FRAG 价格买卖 FRAG。从此时开始，FRAG 价格不会变动，FRAG 持有人随时可以退出。
值得注意的是， NFT Vault 的 买断并不是一个强制的流程，NFT Vault 的创建者可以设置保护期以免除买断的选择，甚至可以选择无法买断 NFT Vault。

8、回测

8.1 背景

PMM 代表主动做市商，它实际上是流动性提供者（LP）使用的定量交易策略。为了帮助 LP 了解 PMM 的 ROI，我们进行了回测，以演示 PMM 在不同市场环境中的性能。

8.2 方法

对 PMM 的评估集中在这两个方面：利润和损失。有限合伙人的利润是周转率乘以手续费率。尽管必须从两种角度解释损失，但交易对手风险和套利交易。在这种情况下，可以忽略交易对手的风险，因为 PMM 已建立了一种限制这种风险的机制。此外，风险来自正常用户的交易，这些交易几乎是随机的，并且在统计上是相对平衡的。套利交易是不可避免的，并且造成了大部分损失，因为链上的甲骨文价格总是被推迟出市。因此，在下面的回测中，我们关注这两个关键值：

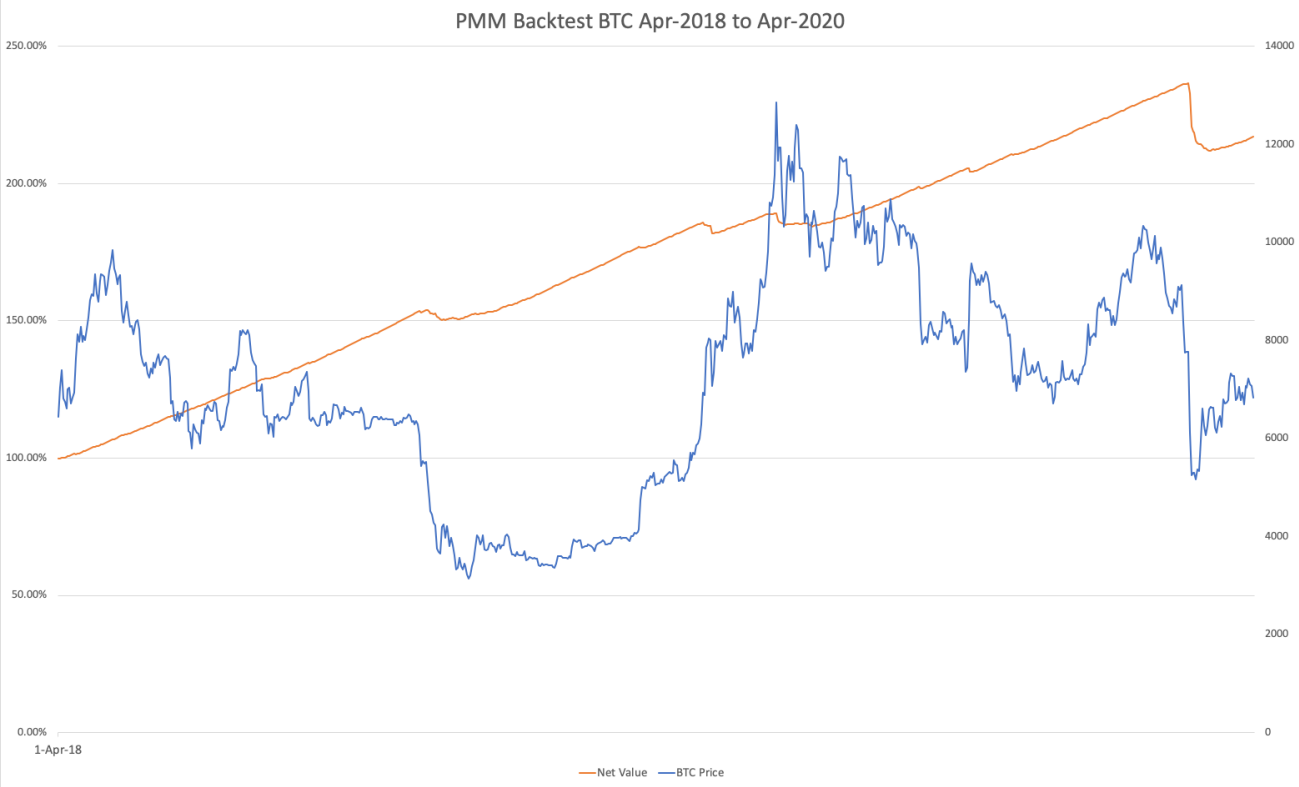
- 周转率（明智的选择）
- 套利损失（明智的损失）

8.3 利润评估

假设：

- 我们的池大小是 uniswap 池大小的 1/10
- 基本令牌和报价令牌具有相同的值
- PMM 参数 k = 0.1
- 费用率 0.3%

这些假设不是任意设定的。在这种情况下，PMM 可以提供与 Uniswap 相同的流动性，因此可以合理地假设 PMM 具有与 Uniswap 相同的交易量。但是，由于存在聚合器，因此假设 PMM 占 Uniswap 交易量的一半更为现实。根据历史数据[5]，PMM 的每日周转率约为 100%，ROI 为 0.3%。



8.4 损失评估

评估套利损失更为复杂，因为之前尚未部署过类似 PMM 的算法。最好的选择是使用最严格的标准进行回测。以下是假设：

- Onchain 预言机的价格总是被延迟从市场价格
- 只要价格偏离市场价格超过 0.5%（链接阈值），Oracle 的价格更新
- 套利者总是有足够的资金，绝不会错过任何交易
- 套利者的外部成本为 0.2%（包括 CEX 费用和天然气成本）

我们使用 BTC 价格从 2018 年 4 月至 2020 年 4 月回测了 1 分钟的间隔。

回测涵盖了大多数市场环境，包括牛市和熊市，甚至包括 3 月 12 日的黑天鹅事件。我们得出的结论是：

- 在大多数市场环境中，手续费收入足以弥补套利损失，并提供很高的回报率（年利率约为 80%）

- 当市场波动剧烈时，尽管涨跌，LP 都会损失大量资金

简而言之，PMM 在市场不景气时获利，而在市场波动时则亏损。

8.5 优势与不足

大多数量化策略仅在市场价格上涨或下跌时才产生利润，而在市场持平时则无事可做。相反，当价格几乎持平时，PMM 可以带来可观的利润。此外，与 AMM 不同，PMM 从来不需要 LP 以一定比例存放基础资产和报价资产。相反，LP 可以根据需要存放任何数量的任何资产。因此，当市场不稳固时，PMM 可以作为原始策略的补充。

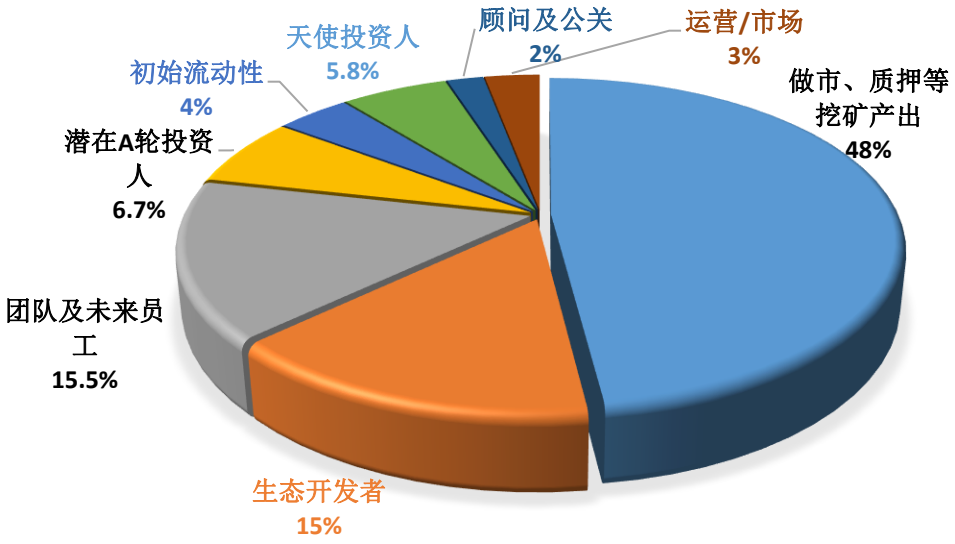
尽管如此，我们必须指出它的缺点。俗话说，没有免费的午餐。当市场动荡时，LP 遭受重大损失。有限合伙人应在风险与收益之间取得平衡。因此，我们建议交易者在预测市场动荡时撤回其资产。作为一个分散的项目，我们所能做的非常有限。但是，我们将尽力调整系统参数以帮助 LP，尤其是在发生黑天鹅事件时。

此外，回测的固有缺点之一是它无法模拟 100%的真实交易。但是，为了减轻这种风险，我们以最保守的假设进行了回测。LP 仍应确定他们在多大程度上信任回测结果。

9、SYN 代币经济

9.1 简介

SYN 代币总量 10 亿，分配如下



- 除了治理权，SYN 代币有 2 个新功能：
  - 持有者将享有 IDO 和众筹建池的打新额度。
  - SYN 平台的交易手续费折扣。
- 引入 vSYN 作为会员证明（proof of membership），质押 100 个 SYN，可以铸成一个 vSYN，vSYN 不支持转账。
- vSYN 持有者享有与持有 SYN 一样的权益，此外享有交易手续费分红和会员奖励。
- 将 vSYN 赎回为 SYN 代币，需缴纳「退会费」给未退出的会员。

- 将会展开交易挖矿和联合多挖，以激励平台的用户增长。

9.2 SYN 价值捕获

SYN 是一个治理代币，同时也被赋予一定的功能。持有 SYN，你将享有以下权益：

- 提案和投票权
- SYN 平台上的 IDO 和众筹的认购份额
- 交易手续费折扣

vSYN 是一种会员凭证，会员系统为忠诚的持币用户设立。持有 vSYN，你将享有以下权益：

- 交易手续费分红
- vSYN 会员奖励
- 提案和投票权
- Synallage 平台上的 IDO 和众筹的认购份额
- 交易手续费折扣

9.3 铸造与赎回

1、铸造 vSYN 得到会员奖励

质押 100 个 SYN 可以铸造成 1 个 vSYN。vSYN 不可转账。vSYN 可获得会员奖励：

- 每个区块释放 6 个 SYN 代币，奖励给 vSYN 持有者。
- vSYN 持有者按比例分得 SYN 会员奖励。
- 邀请其他人铸造 vSYN，额外获得被邀请人奖励的 10% 。

2、赎回 vSYN 缴纳退会费

把 vSYN 赎回成 SYN，需要按比例缴纳退会费。这笔退会费，会以 vSYN 的形式，即时分配给未退出的所有 vSYN 持有者。

定义“vSYN 数量*100”除以“SYN 流通数量”为「SYN 忠诚指数」，忠诚指数越高，退会费越低：

- 当忠诚指数大于 0.5 时，有超过 50%的流通 SYN 被抵押，退会费达到下限，5%。
- 随着忠诚指数下降，退会费逐渐提高。
- 当忠诚指数小于 0.1 时，只有少于 10%的流通 SYN 被抵押，退会费达到上限，15%。

下面我们给出更具体的公式：（定义忠诚指数为 x，罚金率为 y）

- 当 x>0.5 时，y = 0.05
- 当 x<0.1 时，y = 0.15
- 当 x>0.1 && x<0.5 时，y = 0.175 - 0.25 * x

9.4 总结

代币承载了「激励增长」与「捕获价值」的双重功能。团队始终将这两个功能视作代币经济设计的核心。

我们会以高性价比的激励活动分发代币，帮助平台和社区增长。同时，代币将用于捕捉平台的全部价值，并分配给忠诚持有者。

在代币总供应中，预留了高达 48% 用于社区激励。这部分数额如此巨大，以至于我们无法在一开始就确定它们的使用方法。同时，Synallage 的业务场景越来越丰富，用户数量越来越多，如何捕捉价值也成为团队的重要课题。

58,000,000 个 SYN 代币，用于天使投资者。这部分代币将在代币发行后即解锁流通。
潜在 A 轮投资者的 67,000,000 SYN 代币。这部分代币将在代币发行后的一年锁定期，然后在每个以太坊区块的未来 1 年内线性归属。
155,000,000 个 SYN 代币给核心团队/未来雇用，这部分代币将在代币发行后的一年锁定期，然后在每个以太坊区块的未来 1 年内线性归属。
40,000,000 SYN 代币保留用于初始 SYN 产品（IDO），这部分令牌将在 IDO 之后立即流通。
30,000,000 SYN 代币，用于运营，市场营销活动，合作伙伴关系，交易所上市或将来使用。
480,000,000 SYN 代币保留用于社区奖励。令牌的这一部分将分发给参与协议的支持者。
150,000,000 SYN 代币，用于生态开发者奖励。
20,000,000 SYN 代币，用于顾问及公关。

在 SYN 建立审慎，真正去中心化的治理模型的愿景中，个体交易者和流动性提供者（LP）在确保生态系统作为其参与者的完整性方面扮演着至关重要的角色。团队认识到他们在促进平台增长方面的重要性，并坚信随着平台的规模扩大，早期采用者应因其对平台的信念而获得相应的回报。这就是为什么团队打算以公平和透明的方式将代币分发给 LP 的原因。
各种 DeFi 项目已通过经验证明，进行流动性挖掘是一种非常有效且有吸引力的激励参与者的方式，团队可以考虑在需要时采用此方案。而且代币的挖掘和分配策略可以在将来由 DAO Governance 进行修改。

参考

[1]https://zh.wikipedia.org/wiki/Bid%E2%80%93ask_spread
[2]https://dodoex.io
[3]https://github.com/sushiswap/sushiswap-settlement
[4]https://docs.umaproject.org/developers/dvm-integration
[5]https://info.uniswap.org/pair/0xb4e16d0168e52d35cacd2c6185b44281ec28c9dc