Mai3：一种基于 AMM 的无需许可的永续合约协议

1. 简介

Mai Protocol v3 是 MCDEX 推出的一种基于自动做市商（AMM）的去中心化永续合约协议。

永续合约是一种价格锚定底层资产的价格指数、没有到期日且支持保证金交易的金融合约。

本协议的目标是使得任何人都可以在区块链上无需许可的创建、交易 DeFi 永续合约。首先，任何人只需要提供底层资产的价格指数（index price）就可以通过本协议在链上创建永续合约。永续合约可以使用任何 ERC20 代币作为抵押物。再者，本协议为永续合约专门设计了一种高资金效率的 AMM。我们希望通过 AMM 解决永续合约的流动性问题。任何人都可以给通过向 AMM 存入抵押物的方式给 AMM 添加流动性并获得可观的做市收益。最后，任何人都可以无需许可的交易永续合约。交易员的保证金以非托管的方式质押在智能合约内。交易过程也完全在链上智能合约里完成。

协议的智能合约经过了严格的第三方审计，协议也没有管理员密钥（Admin key），从而最大化的保证了协议的安全性与去中心化特性。

我们认为无需许可是本协议成功的最大关键。由于这一特性本协议可以赋能整个社区共同建设 MCDEX 生态。任何人都可以方便的、低成本的创建并运维各种链上、链下资产的衍生品。我们相信，在 MCDEX 社区的共同建设下，MCDEX 上的永续合约资产会极大丰富，交易量也会不断上升。

2. 永续合约

2.1 基于 AMM 的市场结构

本协议完全使用 AMM 进行交易。关于 AMM 的详细技术设计，请参考《MAI v3 AMM 设计文档》。

本协议的市场结构可以简单理解为于永续合约版的 Uniswap。市场中有如下角色：

a) AMM: 每个永续合约都有一个独立的自动做市商。自动做市商充当中心化对手方的角色，为永续合约提供持续的流动性。像一个正常的交易员，AMM 也有独立的保证金账户，AMM 的也可能会有持仓头寸。
b) Operator: Operator 是永续合约的创建者和运营者。

如何成为一个 Operator:

i. 创建永续合约，设置永续合约的初始参数（例如保证金率、AMM 风险参数等等）。永续合约的 AMM 有一组风险参数。通过调整这些参数，可以改变 AMM 的做市风险、交易深度、滑点、盘口价差等等。
ii. 为合约购买（或直接提供）Oracle 服务。本协议定义了一种 Oracle 接口，现有的各种 Oracle 服务可以很容易的对接到本协议。另一方面，Operator 也可以自己为永续合约提供 Oracle 数据。
iii. 协议允许 Operator 在创建永续合约时为每个风险参数设置一个有效范围。Operator 可以根据市场情况在在这个范围内动态调整风险参数的设置。
iv. 当 Operator 希望调整参数范围时，可以发起治理提案。（见 2.9 AMM 参数与治理）
v. Operator 可以转移自己身份给其他地址，也可以销毁 Operator 角色。没有 Operator 的永续合约将完全由 LP 治理。

Operator 收益：

i. Operator 可以设置一定比例的运营手续费，从而从每笔交易中获利。
ii. MCDEX 也会向一些 AMM 的 Operator 提供 MCB 流动激励。(见 3 MCB tokenomics)
iii. 参与 AMM 的治理

Operator 的风险：无

c) **Liquidity Provider:** AMM 的**流动性提供者**

如何成为 LP：

i. LP 向 AMM 的资金池存入资金

ii. LP 会收到 AMM 资金池的相应份额

LP 的收益：

i. 固定比例的交易手续费

ii. 买卖价差(spread)及滑点(slippage)带来的收益(profile)

iii. 交易员支付的资金费用

iv. 强制平仓罚金

v. MCDEX 会向一些 AMM 的 LP 提供 MCB 流动激励（见 3 MCB 经济模型）。

vi. LP 可以参与 AMM 的治理（见 2.10 AMM 参数与治理）

LP 的风险：当 AMM 具有头寸时，AMM 具有风险暴露，如果此时指数价格变化，可能造成持仓亏损。这部分亏损会被所有 LP 分担。

d) **Trader：**交易员是市场中最主要的参与方。交易员通过与 AMM 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 AMM 相互成交，所有的交易必须通过 AMM 达成。交易员在交易过程中，需要向 AMM 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。

e) **Keeper：**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。（见 2.4 强制平仓）

f) **Delegator：**代理是一类特殊的角色。每个保证金账户都可以设置自己的代理人。代理人可以操作账户进行交易（包括直接与 AMM 交易及通过 Broker 交易）。但代理人无法从账户中取出资金。通过代理人功能，可以实现冷热钱包分离及交易策略托管等功能。

2.2 资金费用

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 AMM 设计中，由于交易都必须经过 AMM 达成，所以如果 AMM 没有头寸时，可以认为市场的多空需求是平衡的。此时 AMM 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 AMM 持有某个方向的头寸时，AMM 给出的报价也会向相应方向偏移。当 AMM 持多头时，AMM 报价会向低于 index 的方向偏移，反之 AMM 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 AMM 持仓相反的头寸征收资金费用支付给与 AMM 持仓相同的头寸(包括 AMM)。资金费率与 AMM 持仓量正相关。即 AMM 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 AMM 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 AMM 相同的头寸，赚取资金费用。根据 AMM 的设计，向 AMM 添加流动性或与 AMM 交易减少 AMM 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。

2.3 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，$\Delta N > 0$意味着该交易员做多，而$\Delta N < 0$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：

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

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（当使用以 Uniswap 为例的去中心化预言机时)。 M_{im}是永续合约的初始保证金费率。

头寸盈亏的计算如下：

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

用户可以在任何时间提取 MCDEX 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：

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

交易员务必确保保证金账户余额不小于维持保证金M_{mm}：

$$P_{mark}\Delta N M_{mm}$$

M_{mm}是永续合约的维持保证金费率。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。

2.4 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：

i. 通过 AMM 强制平仓：被强制平仓的头寸将通过 AMM 平仓。这也意味着头寸被转移给了 AMM。强制平仓罚金将进入 AMM 的资金池。Keeper 可以获得 "Keeper Gas Reward" 数量的资金作为清算奖励。

ii. 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。

2.5 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 AMM 的流动性不足或者清算不及时出现清算损失（Liquidation Loss）时，AMM 中的保险基金会首先用于支付清算损失。如果 AMM 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。

2.6 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 AMM 参数确定）的资金归属保险基金，剩余罚金归属清算人（AMM 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 AMM 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。

2.7 限价与止损单

直接与 AMM 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，我们提供了相对中心化的限价单和止损单功能。交易员可以签名一个限价单或止损单，并把订单发送到其信任的 “Broker “服务器。Broker 服务器不断观察链上 AMM 的报价，并在 AMM 报价符合交易员订单需求的情况下，向链上智能合约提交订单。链上智能合约收到 Broker 提交的订单后，会首先验证订单的有效，并随后按照订单内容执行订单。

值得注意的是，Broker 不会对收到的订单进行撮合，所有的订单按先入先出的顺序与 AMM 成交。由于 Broker 代替交易员支付了上线的 Gas 费，Broker 可以向交易员收取一部分费用。

2.8 安全性

我们深知安全性是这类协议最重要的关键。在本协议发布时，所有的智能合约及后续升级都必须经过严格的安全审计才能上线。AMM 的金融结构设计也经过了同行评审。

为了最大化本协议的去中心化特性，协议代码中没有任何管理员密钥（Admin Key）。

另一方面，任何人都可以无需许可的创建永续合约。虽然 Operator 只被授予了有限的权限，在一定程度上提高了永续合约的安全性，但交易员需要仔细甄别选择交易的永续合约，并承担相应的风险。我们鼓励 Operator 选择去中心化的 Oracle 服务，并将风险参数的范围设置在尽量小的区间内（甚至让参数不可改），从而最小化交易员的信任成本。

2.9 推荐（referral）

本协议支持给于推荐人一定的推荐佣金。交易时（直接与 AMM 交易或者通过 Broker 下订单）可以指定一个推荐人。推荐人可以从这笔交易的 Operator 手续费与 LP 手续费中获得一定比例的佣金。返佣比例由 AMM 的治理确定。通过这种方式，有用户资源的机构可以运营自己的前端 UI，并通过向 AMM 导入交易员的方式获取收益。

2.10 AMM 的参数及治理

AMM 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。AMM 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 AMM 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。

AMM 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 Mai3 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 MCDEX 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
AMM 做市风险参数	一组控制 AMM 做市商风险的参数	通过治理修改参数有效范围 Operator 可在范围内整

值得注意的是，每个 AMM 都有一组做市商风险参数，这些参数决定了 AMM 的以下做市特征：盘口价差（Spread）、滑点（Slippage）、AMM 最大持仓规模、AMM 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 AMM 的去中心化程度。

除了修改 AMM 的参数的提案外，还有 3 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%：

i. 升级 AMM 的智能合约代码，这使得 AMM 具有了升级的能力；
ii. 使永续合约进入交割状态；
iii. 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；

2.11 多链部署

我们认为不同的公链都有各自的用户和生态。本协议在公链的选择上是中立的。为了最大化本协议的使用场景，本协议的智能合约可以被部署到各种公链上。MCDEX DAO 将作为主体支持本协议在各个公链上的发展，推动 MCDEX 生态不断扩张壮大。

3. MCDEX DAO

3.1. 治理

MCDEX 社区已经发型了 MCDEX 治理代币 MCB，并开展了一系列的治理工作。在 Mai3 协议发布的同时，我们将围绕 MCB 建设 MCDEX DAO。MCDEX DAO 将是整个 MCDEX 社区的核心。MCDEX DAO 的使命是：推动 MCDEX 生态的持续发展。

MCDEX DAO 拥有一个金库（Vault）。金库内的资产来源于以下方面：

i. 从 MCDEX 生态捕获的手续费分成；
ii. 按 MCB 经济模型增发的 MCB；
iii. 其他向 MCDEX DAO 支付的费用；

金库的资金服务于 MCDEX DAO 使命，其具体用途包括不限于以下方面：

iv. 流动性激励：向 AMM 的 LP 支付奖励；
v. 治理激励：向参与社区治理的 MCB 持有人支付奖励；
vi. 开发及运营激励：向社区开发者、社区管理员支付奖励；
i. 支付代码审计等必要的费用；
ii. 为 MCDEX 生态内的产品添加流动性；
iii. 从二级市场回购 MCB，购得的 MCB 作为金库的资产；
iv. 为 MCB 提供流动性（向 Uniswap 的 MCB 资金池提供流动性）；

MCB 的持有人拥有 MCDEX DAO 的治理权。MCDEX DAO 实行链下讨论，链上治理的方式。

由于是链上治理，所以每个提案其实都是一个可执行的智能合约。为了方便提案，MCDEX DAO 需提供常用提案的智能合约工厂（Factory）。

MCDEX DAO 的治理内容包括以下方面：

i. 管理金库资产的具体使用；
ii. 以 MCDEX DAO 作为 Operator 运营数个永续合约；
iii. 必要时选举出多签人，由多签人代表 DAO 行使日常 Operator 操作；
iv. 升级 MCDEX DAO 的智能合约；

MCDEX 治理提案需由 MCB 持有人发起，提案发起人持有的 MCB 投票权不得低于已发行总量的 1%。提案的投票率不得低于已发行总量的 10%。提案发起人默认投赞成票。

MCB 持有人可以将投票权委托给另一个 MCB 持有人。

提案的投票时间为 72 小时，议提通过后的时间锁为 48 小时。参与投票需要质押 MCB。如果提案通过，投赞成票的 MCB 将在提案执行后 72 小时解锁，投反对票的 MCB 在投票结束后立刻解锁；如果提案没有通过，则参与投票的所有 MCB 将在投票结束后立刻解锁。

3.2. MCB 经济模型

原有的 MCB 的代币经济模型有其不合理之处，过快的通胀对已有 MCB 持有人造成了很大的压力。为此，我们将在 Mai 3 正式发布前与社区一起探讨新的 MCB 经济模型，即 MCB 的发行规模、发行对象和发行速度。

新代币经济模型的几点原则如下：

i. 已经流通中的 MCB 继续保持流通；
ii. MCB 必须从 MCDEX 生态中捕获价值；
iii. 由于流动性是所有衍生品最重要的特性，我们依旧需要增发 MCB 进行流动性激励；
iv. 新的经济模型必须充分考虑已有 MCB 持有人的利益；