MCDEX: DeFi 永续合约交易平台

刘杰

1.概述

人们在不断探索区块链技术的应用场景。这其中基于智能合约技术开展的去中心化金融业务（DeFi）无疑是区块链应用的重要方向。在稳定币、借贷、交易等场景下，已经有一些 DeFi 项目做了很好的探索。从用户规模、抵押的资金量等方面看，这些项目也取得了初步的成功。然而，目前的 DeFi 产品依旧有以下两个问题：

1. 交易类 DeFi 产品主要面向交易员，然而具有交易能力的用户在 DeFi 用户中只占极少比例，普通用户无从使用交易类 DeFi 产品；
2. 抵押借贷类产品相对风险很低，但存款理财的收益率也较低，在低风险借贷类产品和高风险交易类产品之间缺乏结构性的产品满足不同风险倾向用户的投资需求；

MCDEX 的使命是让投资更简单。我们希望基于区块链技术，打造安全、易用的去中心化金融平台，让更多的用户以更容易的方式投资 DeFi 产品并获得收益。

当前 MCDEX 平台上的主力产品是去中心化永续合约。永续合约是 MCDEX 金融服务中最重要的底层资产。MCDEX 永续合约的金融结构完全参考了 CeFi 中成熟的设计，其价格锚定现货指数又提供了最大 10 倍杠杆的功能。另一方面，MCDEX 的永续合约又是完全去中心化的，其工作机制可以完全脱离链下设施，从而为在永续合约基础上构建去中心化结构性金融产品提供了可能。

MCDEX 的永续合约由 AMM 提供链上流动性入口及产生资金费率（Funding rate），这一设定保证了 MCDEX 永续合约完全去中心化的内核（kernel），也是永续合约可以被其他结构化产品组合的关键。由于 AMM 的滑点相较传统 CeFi 交易所更高，为了降低交易滑点提供更好的流动性，在 AMM 之外，我们为用户提供了链下高速订单簿作为交易永续合约的入口。由于做市商的引入，链下订单簿提供了非常好的流动性。最后，由于套利者的存在，链下订单簿的流动性和交易需求也会间接传导到链上 AMM，并由 AMM 提供了整个市场的资金费率。

我们推荐对流动性敏感的用户直接使用订单簿交易。我们将 AMM 作为链上其他智能合约交易永续合约的入口。

永续合约是一种非常灵活的底层资产。我们将利用结构化产品扩大永续合约的使用场景、提高永续合约的流动性。我们发现，大量普通用户缺乏交易永续合约的能力。为了让更多用户可以投资 DeFi 产品并从中获利，MCDEX 将在永续合约基础上推出去中心化的结构化产品。我们正在开发自动交易机器人智能合约和社交交易智能合约。用户只需向这类智能合约中存入资金就可以用合约的策略交易永续合约进而获取利润。用户的投入这类结构化产品的资金会被锁在智能合约内，从而最大化资金的安全性。这两类合约的区别是，交易机器人智能合

约的交易策略是完全公开在链上，而社交交易智能合约的策略是由社交交易员或量化基金提供的。我们将和社区一起基于永续合约开发更多结构化产品，满足不同风险偏好用户的需求。

不断提高安全性是 MCDEX 最首要的任务。我们邀请了最专业的团队审计智能合约代码。并从 Oracle、风控、全局清算等方面不断加强整个系统的安全性。我们希望通过持续的努力，不断完善 MCDEX 的安全机制、最大化产品的安全性。

我们希望将 MCDEX 打造成一个完全去中心化的 DeFi 平台。我们将发行 MCDEX 的平台币 MCB，并将治理权转移到 MCB 的持有人。另一方面，MCB 持有人也将捕获整个 MCDEX 平台的价值。随着 MCB 流动性的增大，我们将不断扩展 MCB 的功能和使用场景。MCB 也将被用于激励生态参与者为 MCDEX 的良性发展做出贡献。在基金产品发布后，我们会启动流动性挖矿，将 MCB 分配给基金持有人，进而激励整个平台的流动性。

2.永续合约

永续合约是 MCDEX 金融服务中最重要的底层资产。该合约的金融结构完全参考了 CeFi 中成熟的设计。永续合约利用资金费用机制使得价格锚定指数。同时，MCDEX 永续合约又是基于保证金交易的，从而提供了最大 10 倍的杠杆交易功能。与传统永续合约不同的是，MCDEX 永续合约是完全去中心化的，其功能完全由以太坊上的智能合约实现。其工作机制可以完全脱离链下设施，从而为在永续合约基础上构建去中心化的结构性金融产品提供了可能。

2.1 资金费用机制（Funding payment）

永续合约是一种没有到期日的金融合约。永续合约通过资金费用机制使得合约交易价格锚定底层资产价格指数。永续合约基于保证金交易，从而可以实现杠杆。

资金费用机制模拟了在现货保证金交易（spot margin trade）市场中的机制。现货的保证金交易中，由配资方借出资金，交易者借入资金交易实现杠杆。交易永续合约无需配资方，合约多头和空头相互借入对方资产并相互收取利息。例如，对于 BTC-USD 永续合约而言，合约多头相当于向合约空头借入美金用于买入比特币，合约空头相当于向合约多头借入比特币用于买入美金。当市场多头需求旺盛时，借入美金的需求随之上升，借入美金的利率也就上升，从而增加了多头持仓成本，抑制市场的做多需求；反之，当市场空头需求旺盛时，借入比特币的需求随之上升，借入比特币的利率也就随之上升，从而增加了空头持仓成本，抑制市场的做空需求。永续合约巧妙的模拟上述过程，当市场多头需求强于空头需求造成交易价格超过指数时，设置多头利率高于空头利率，从而多头向空头支付的净利率为正数，即多头向空头付钱，进而压制多头鼓励空头使得价格回归指数；反之，当市场空头需求强于多头需求造成交易价格低于指数时，设置多头利率低于空头利率，从而多头向空头支付的净利率为负数，即空头向多头付钱，进而压制空头鼓励多头使得价格回归指数。

实际环境下，我们往往不单独设置多头利率和空头利率，而是直接使用多头利率与空头利率的差值作为资金费率（funding rate）。当市场价格高于指数时，设置资金费率为正数，使得

多头向空头付费，压制多头，降低市场价格；反之，当市场价格低于指数时，设置资金费率为负数，使得空头向多头付费，压制空头，提升市场价格。

从上述描可以看到，永续合约的关键机制就是按市场多空需求情况合理设置资金费率，从而调节市场需求，进而使得市场价格稳定在围绕指数的合理范围内。

MCDEX 永续合约的资金费率计算参考了 Deribit 永续合约的资金费率方法。首先，通过订单簿上的订单情况计算出一个市场公允价（Fair Price）。公允价定义为某一给定深度（例如 1BTC）下多头订单的平均价格与空头订单的平均价格的中间价。有了市场公允价之后，可以计算出标记价格（Mark Price）。标记价格是用于计算仓位的初始保证金和维持保证金的价格。

$$\text{Mark Price} = \text{Index Price} + \text{EMA}(\text{Fair Price} - \text{Index Price})$$

上式中，EMA 是指数滑移动平均函数，这个函数计算了一段时间内公允价与指数价格的价差的移动平均值。实际使用中，标记价格会被限制在指数价格的某个范围内（例如+-0.5%）

进而我们可以定义溢价率(Premium Rate)：

$$\text{Premium Rate} = (\text{Mark Price} - \text{Index Price}) / \text{Index Price}$$

溢价率反映了市场多空的需求情况，当溢价率为正数时，说明多头需求强于空头，反之说明空头需求强于多头。

永续合约的资金费率即设置为一个与溢价率正相关的值。公允价与指数价格之间往往存在天然的价差，为了消除这种价差的影响。我们在溢价率上增加一个阻尼函数(Dampener)得到资金费率。（阻尼值 Dampener 是一个系统常数）：

$$\text{Funding Rate} = \text{Max}(\text{Dampener}, \text{Premium Rate}) + \text{Min}(-\text{Dampener}, \text{Premium Rate})$$

实际使用中，我们将上式计算的 Funding Rate 通过一个门限函数，限制资金费率在某个范围内(例如+-0.45%)。得到资金费率后，将资金费率作为利率即可计算某段时间（Time）内多头寸需要向空头支付的利息(Interest)：

$$\text{Interest} = \text{Position Value} * \text{Funding Rate} * \text{Time}$$

当资金费率是负数时，表示空头需要向多头支付的利息。

值得注意的是，即使没有订单成交，只要订单簿上有多空双方的订单，就可以从订单簿获得公允价进而计算资金费率，这是从订单簿计算资金费率的一个优点。

当设计去中心化永续合约时，最关键的问题也是如何计算资金费率。一种朴素的做法是，直接将订单簿搬到链上，从链上订单簿按传统 CeFi 方式计算资金费率。这种做法的缺点是，链上订单簿的效率很低，下单撤单的成本都很高，不利于做市商做市，从而流动性较差。另一种朴素的做法是，将订单簿放在链下，订单匹配后在链上执行,同样从订单簿计算资金费

率。这种做法的缺点是中心化程度较高，永续合约的核心参数资金费率依赖链下设施，当订单簿故障时，链上资金费率无法更新。这一方法的另一个缺点是，必须通过链下订单簿成交，其他智能合约无法与链下订单簿交互，也就无法在永续合约之上构建其他结构化产品。

为此，MCDEX 的永续合约通过引入自动化做市商 AMM 解决上述问题。AMM 可以看做是一种按预设做市商策略提供做市服务的智能合约。多头和空头用户都可以通过与 AMM 交易获得合约头寸。AMM 的定价公式提供了多空两个方向的连续的做市深度，并会根据市场需求自动调节盘口价格。所以，AMM 给出的盘口价格是一个天然的“市场公允价”，我们将 AMM 的公允价代入上述资金费率的计算公式就可以计算出合理的标记价格和资金费率。这一设计使得 MCDEX 永续合约的资金费率计算完全在链上完成。另一方面，通过 AMM 其他智能合约也可以进入合约头寸，从而为构建上层结构化产品提供可能。

我们将 AMM 作为 MCDEX 永续合约的重要内核。另一方面，由于当前公链速度的限制，线下订单簿的流动性在绝大多数时候依旧优于 AMM。为此，我们也引入了链下订单簿为用户提供更优的流动性。但链下订单簿与 AMM 没有直接的联系，我们也不从链下订单簿计算资金费用。由于套利者的存在，链下订单簿的交易需求会被传递到 AMM，从而改变 AMM 的公允价格，进而间接影响全局的资金费率。

关于 MCDEX 永续合约资金费率计算的更多的技术细节可以参见[1][7]。

2.2 合约规则

MCDEX 永续合约具有与 CeFi 永续合约的类似的规则：

交易员与对手方以某个进入价格（Entry Price）进入合约多头或空头。进入头寸时交易员的保证金余额必须大约初始保证金（IM=10%）。当保证金余额低于维持保证金（MM=7.5%）时，系统会清算部分头寸使得保证金余额满足维持保证金需求。

合约的 PNL 和保证金计算方法如下：
多头 PNL=(Mark Price – Entry Price）* Size
空头 PNL=(Entry Price – Mark Price) * Size
初始保证金 = Mark Price * Size * IM
维持保证金 = Mark Price * Size * MM
其中标记价格(Mark Price)是由 Index 加上 AMM 溢价率(Premium)计算出的一个标记值。交易员可以随时通过向保证金账户存入或取出保证金来改变保证金账户的有效杠杆。另一方面，MCDEX 永续合约的 PNL 可以随时取出，也就是 PNL 总是“已实现的 PNL”。

另一方面，交易员可以在市场上以某个退出价格（Exit Price）关闭仓位。则此时交易员平仓后的 PNL 为：
多头平仓 PNL=(Exit Price – Entry Price）* Size
空头平仓 PNL=(Entry Price – Exit Price) * Size

值得注意的是，上述公式中的价格均是以抵押物为计价单位的价格。例如，对于用 USDC 作为抵押物的 ETH 永续合约，那么价格就是以 USDC 为单位的 ETH 价格（既以 ETH 的美元价格计价）。然而，MCDEX 的永续合约可以使用各种代币作为抵押物，当抵押物与计价单位不一致时需要做对应价格转换后再代入上述公式。例如，MCDEX 目前的主力合约是 ETH-PERP。这是一个以 ETH 做抵押物，以 ETH 的美元价格作为计价单位的美元合约（这种合约也被称为“反向合约“）。我们需要将美元计价的 ETH 价格取倒数得到以 ETH 计价的美元价格，再代入上述 PNL 公式：

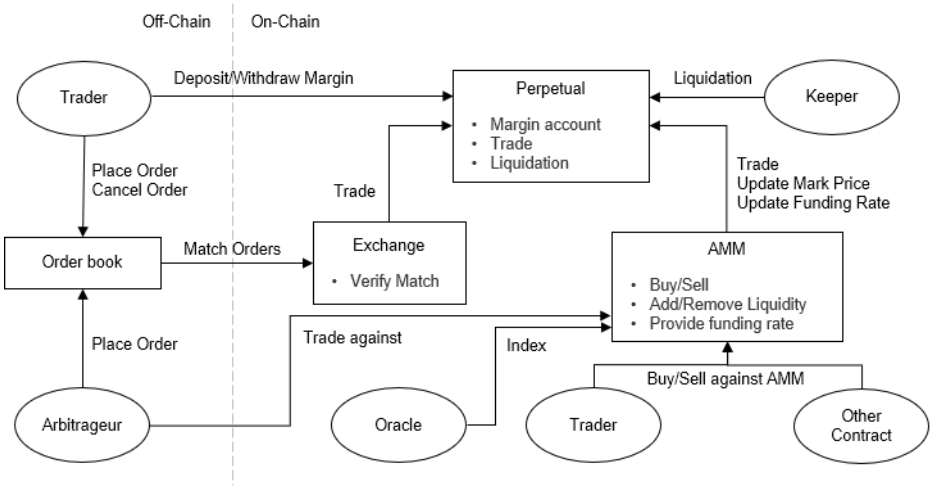
ETH 多头 PNL=(1/Entry Price – 1/Mark Price) * Size

ETH 空头 PNL=(1/Mark Price – 1/Entry Price) * Size

最后，MCDEX 永续合约会对持有仓位的保证金账户以资金费率收取/给予利息，这一过程是连续进行的，每秒的资金费用都会结算到保证金的账户的余额中。

2.3 智能合约

如下图所示，MCDEX 的永续合约由以太坊上的三个智能合约组成：Perpetual、AMM 和 Exchange。这里介绍这三个智能合约的关系和功能。



2.3.1 Perpetual

Perpetual 智能合约管理永续合约保证金账户，存储保证金余额、头寸等数据，实现交易、清算、资金费用机制、社会化损失等基础功能。交易员将保证金存入合约建立保证金账户后方可以通过 AMM 或 Order Book 进行交易。如果交易员没有合约头寸，交易员可以随时取出全部保证金。另一方面，如果交易员有头寸，交易员可以将超过初始保证金（10%）的余额从合约中取出。当保证金账户里有合约头寸后，保证金账户会连续不断的按资金费率支付/接收利息。当保证金账户的保证金余额低于维持保证金（7.5%）时，守门员（Keeper）会以标记价格清算保证金账户。被清算的账户需要支付罚金（2.5%）。如果保证金账户在破产前不能被及时清算，那么产生的穿仓损失首先会由保险基金承担，保险基金无法承担的部分会由全体对手方持仓数量分担损失（社会化损失 Socialize the loss）。任何人都可以调用清算接口成为守门员，更多的守门员会提高系统的清算能力。

2.3.2 AMM

如“机制”节介绍的，AMM 是 MCDEX 永续合约的重要内核。AMM 提供了链上交易入口及资金费率。AMM 在 Perpetual 合约中有一个独立的保证金账号，也就说对于 Perpetual 合约来说，AMM 正如一个普通的交易员一样具有独立的保证金账户。AMM 合约接收来自预言机提供的价格指数，并按指数与“公允价“的价差计算“溢价率”，进而计算“资金费率”和”标记价格”。和其他 AMM 产品类似，流动性提供者（LP：Liquidity Provider）向 AMM 添加流动性并分享手续费收益，任何人都可以成为 LP 以提高 AMM 的流动性。普通交易员或其他的智能合约总是可以以 AMM 定价公式给出的价格与 AMM 交易（做多或做空）。

当前 AMM 使用了经典的恒定乘积(xy=k)定价公式[2]。这个公式在 Uniswap 等项目中得到了充分验证。我们认为使用这一公式作为 AMM 的起步是一个很好的选择。在套用这个定价公式时，我们首先令 AMM 的保证金账户只有多头头寸且总是足额抵押的。这保证了 AMM 的账户永远不会被清算，即 AMM 的保证金账户总是安全的。再者，我们将 AMM 的可用保证金余额代入公式中的 x ，AMM 账户的多头头寸数量代入公式中的 y。当交易员通过 AMM 做多时，交易员的多头头寸增加，AMM 的多头头寸数 y 减小、可用保证金余额 x 增大；反之，当交易员通过 AMM 做空时，交易员的空头头寸增加，AMM 的多头数 y 增大，可用保证金余额 x 减小。从而该定价公式可以给出与 AMM 交易的价格。而 x/y 也作为 AMM 的“公允价格”。更多关于恒定乘积定价公式用于 MCDEX 永续合约的技术细节可以参考[7]。

然而，恒定乘积定价公式的缺点也非常明显：资金效率较低、交易滑点较高。MCDEX 社区也在积极探索使用更好适合永续合约的 AMM 公式。社区已经提出了一种基于 Oracle 和风险暴露的永续合约 AMM 定价公式。新公式利用在永续合约中已经存在的 Oracle 快速发现市场价格以减少套利空间。同时，新公式基于 AMM 的风险暴露调整价格，鼓励 AMM 回归风险中性，进而进行有限深度的做市以提高 AMM 资金效率。新公式的具体细节和讨论可见[3]。当我们充分验证了新公式的可行性后，我们会升级 AMM 切换为新的公式。

最后，非常值得注意的是 AMM 和订单簿（见 2.3.4）的关系。链下订单簿与 AMM 没有直接的联系，我们也不从链下订单簿计算资金费用。由于套利者的存在，链下订单簿的交易需求会被传递到 AMM，从而改变 AMM 的公允价格，进而间接影响全局的资金费率。也就是说，AMM 的资金费率可以调节包括链上 AMM 与链下订单簿的整体的市场供需，从而使交易价格锚定指数价格。

2.3.4 Exchange

Exchange 合约是为链下订单簿提供的交易接口。链下订单簿是当前 MCDEX 永续合约最重要的流动性入口。交易员向订单簿提交订单，并由订单簿撮合。订单簿服务器调用 Exchange 合约的接口向链上提交撮合结果。Exchange 合约校验撮合结果中的订单签名及撮合结果，一旦校验成功，Exchange 合约调用 Perpetual 合约完成最终交易。

AMM 和订单簿具有不同的使用场景。由于当前链下订单簿具有比 AMM 更好的流动性，我们推荐对去中心化要求不高的交易员直接使用订单簿交易。另一方面，我们目前将 AMM 作为一个链上流动性入口，这个流动性入口更多是为其他智能合约应用服务的。例如，在我们即将推出的链上自动交易机器人合约中，交易机器人给出交易策略，并调用 AMM 的交易接口完成交易，整个过程完全在链上完成。

最后，Exchange 合约提供了代理（Proxy）功能，每个永续合约账号都可以指定另一个账户作为自己的代理人。代理人可以用委托人的账户在订单簿上下单，但代理人不能提取委托人账户中的资金。这个功能增强了账户安全性。用户可以用冷钱包创建保证金账户，并将另一个热钱包设置为账户的代理人，之后使用热钱包下单交易。另一方面，代理功能也扩展了 MCDEX 永续合约的使用场景，我们基于该功能开发了“社交基金产品”（见第 3 章）

2.3.5 Oracle

Oracle 合约提供永续合约的底层资产的价格指数。Oracle 是整个永续合约系统非常关键的环节。当前 MCDEX 的永续合约使用 ChainLink 的 Oracle 数据。MCDEX 使用的 ChainLink 的 Oracle 的数据精度为 0.5%。根据我们的回测，这一精度基本可以满足当前永续合约对于价格指数的需求。随行业的整体发展，我们也会不断使用新的 Oracle 技术以提高永续合约的产品质量和安全性。

关于 MCDEX 永续合约的更多的技术细节可以参见[7]。

2.4 安全性

我们始终将安全性作为 MCDEX 的首要考量。由于去中心化永续合约的业务相对复杂，对安全性的挑战就相对更高。我们对于 MCDEX 永续合约在代码安全性、全局清算机制、Oracle 安全、风控等方面都做了着重的安全加强。

2.4.1 代码安全性

作为一个基于智能合约的 DeFi 产品。智能合约代码的安全性是整个产品安全性的关键。我们在开发智能合约时总是将安全性作为最重要的考虑，我们总是优先使用成熟稳健的技术开发我们的产品。我们对 MCDEX 永续合约的代码做了充分的测试，对于所有可能被运行的代码分支做到了 100%的测试覆盖率。

另一方面，MCDEX 与业界最优秀的安全团队合作，委托他们对 MCDEX 的智能合约进行全面的安全审计：

1. 基于 Market Protocol 的 MCDEX Mai Protocol V1 智能合约由 Chain Security 审计（Chain Security 也是 Market Protocol 的审计方）。审计报告见[5]；
2. 实现永续合约的 MCDEX Mai Protocol V2 由 OpenZeppelin 和 Consensys 分别审计。审计报告见[6]；

MCDEX 的未来的升级和新产品都会持续委托行业内最优秀的安全团队进行代码审计。

2.4.2 管理员权限

我们在打造 MCDEX 的 DeFi 产品时，力求做到没有管理员密钥（admin key）。然而，由于永续合约业务的复杂性，MCDEX 永续合约还是有管理员密钥的。在 MCDEX 的平台币 MCB 发行后，我们会将管理员权限转移到链上投票合约，即将管理员权限移交给全体 MCB 的持有人（见第 4 章）。除了管理员权限，永续合约中还有两个管理权限：

1. 暂停/恢复取款权限
2. 暂停/恢复合约功能权限

上述两种管理员权限都需要由管理员密钥持有人授权。这两种权限主要用于风控 (见 2.4.5)

永续合约管理员权限的详细清单见[7]。

2.4.3 全局清算机制

在极端情况下，可以触发永续合约的全局清算。全局清算是最后的安全防御机制，用于应对市场极端波动造成的大量穿仓及安全攻击造成的异常。全局清算是一个两阶段的过程。在第一阶段，如果系统数据遭到了恶意破坏（例如错误的指数价格），则错误数据可以被强制修正，保证金不足的账户也可以在这个阶段被清算。当进入到第二阶段后，交易员可以以全局清算价格取回剩余的保证金。

全局清算需要 Admin 权限发起并执行。Admin 权限目前由开发团队持有。该 Admin 权限将会尽快转移给平台币 MCB（见下文）的持有人。平台币持有以投票的形式行使 Admin 权限并发起全局清算。

2.4.4 Oracle 安全

永续合约的整体机制依赖 Oracle 的正确性，错误的指数信息将会严重破坏永续合约的正确性，损坏交易员的利益。为此，MCDEX 正在引入多重检查机制，避免单一 Oracle 对系统的影响。当前，我们正在引入 Coinbase Oracle 和 MarkerDao Oracle 作为候补 Oracle，当 Chainlink 的价格指数与候补 Oracle 的误差超阈值时（5%），Chainlink 的数据会被拒绝更新到 MCDEX 永续合约中，交易功能也会自动暂停。同时，也会触发链下风控机制，如果事态严重，我们会启动全局清算机制将合约强制交割，最大化保护交易员的资产安全。加强 Oracle 的安全性也不是一蹴而就的事情，随着行业中 Oracle 技术的不断成熟，我们也会通过去中心化治理的方式不断升级 Oracle 以最大化合约安全性。

2.4.5 风控

MCDEX 永续合约的业务逻辑相对复杂，面对的风险挑战也相对较高。为了最大化的用户的资金安全，我们用链上和链下两种方式开展风控工作。

链上风控是一种通过链上智能合约实施的完全去中心化的自动风控机制。链上风控程序由管理员部署，并由管理员授予风控程序“暂停合约功能”的权限。当链上风控策略被触发时，链上风控程序可以暂停整个合约的功能。这之后，管理员可以根据具体情况采取进一步措施，例如发起全局清算或者恢复合约功能。然而，受限于智能合约的能力，目前链上风控的能力还很有限，只有简单的风控策略可以在链上实施。目前 MCDEX 永续合约有一条链上风控策略：当社会化损失的规模达到某一个阈值时，停止合约功能。

链下风控是由链下监控程序自动执行的风控机制。链下风控的优势是可以实现各种复杂的风控策略，缺点是这种风控方式的中心化程度相对较高。我们最小化链下风控的处置权限，仅授权链下风控程序“暂停取款的权限”。当链下风控被触发时，风控程序会发出报警并暂停合约的提款功能，此时包括存款、交易等其他功能完全不受影响。管理员可以随后介入进一步的调查处置。如果事态严重，管理员可以触发全局清算流程。在全局清算流程中，管理员可以修复合约中错误的数据，从而最大化保证用户的资产安全。

链下监控程序监控的主要数据有：

1. 合约内资金情况
2. Oracle 数据正确性
3. 保证金质押率及清算情况
4. 链上合约交易情况

和链上风控一样，我们会开源所有的链下风控策略。随着 MCDEX 的社区的不断建设，我们将不断丰富风控策略，并将尝试授权更多有经验和能力的团队共同开展链下风控工作。

3. 结构化产品

永续合约是 MCDEX 最重要的底层资产，也是 MCDEX 平台捕获市场价值的关键。MCDEX 所有工作的核心即是围绕这一底层资产开展。这一去中心化的金融资产是完全开放的。由于 AMM 提供了链上流动性接口，人们可以方便的在 MCDEX 永续合约之上构建更多丰富的结构化产品。这些产品可以扩大 MCDEX 永续合约的使用场景，提高永续合约的流动性。

我们将从两方面推动基于 MCDEX 永续合约的结构化产品建设。一方面，永续合约的金融结构非常适合对冲和投机，具有广泛的应用场景。我们将努力向 DeFi 世界推广 MCDEX 永续合约，推动在其他 DeFi 产品中使用 MCDEX 永续合约，使得 MCDEX 成为这些产品的投资组合中的资产之一。另一方面，为了大大降低用户的投资门槛，使得大量缺乏交易能力的用户可以参与 DeFi 产品投资并获得收益，我们也在基于永续合约打造一款结构化的基金产品。这种基金产品具有两种形式：机器人基金和社交基金。

3.1 机器人基金

机器人基金是一种自动交易 MCDEX 永续合约的智能合约。机器人基金是完全开源且免费的，用户投资机器人基金无需支付额外费用，在获得盈利后也无需给机器人分成。

机器人基金有独立的 MCDEX 永续合约保证金账户。对于 MCDEX 永续合约来说，机器人就是一个普通的交易员。机器人的交易策略实现在智能合约里。机器人根据市场数据（例如指数价格）自动执行交易策略，给出目标仓位。机器人给出相对于标记价格的最大滑点，并允许任何人调用接口驱动机器人与 AMM 进行交易，从而实现目标仓位。套利者为了获利，将驱动机器人与 AMM 进行交易，从使得交易机器人的仓位总是符合策略给出的目标仓位。

另一方面，任何普通用户都可以将资金存入机器人基金智能合约并获得基金份额。用户的资金将被加入机器人的 MCDEX 永续合约保证金账户。机器人将使用用户资金进行交易。用户在一个最低持仓时间之后可以选择退出基金份额。在用户退出基金时，一部分归属用户的仓位会被平仓。平仓完成后，用户可以按持有的基金份额取回基金净值，实现投资盈亏。

3.2 杠杆代币

杠杆代币是一种很受普通用户欢迎的投资品。永续合约的有效杠杆会随着头寸盈亏不断变化，当头寸获得盈利时有效杠杆下降，当头寸获得亏损时有效杠杆上升。如果用户需要获得固定的杠杆需要通过不断增减仓位进行调仓（rebalance）。而杠杆代币是一种杠杆恒定的投资品，例如 3x 做多 ETH 和 3x 做空 ETH。杠杆代币通常通过永续合约实现。在 CeFi 中，基金管理员不断调整基金的永续合约仓位，从而将基金的有效杠杆锁定在固定值。基于这类基

金发行的份额代币即为杠杆代币。

基于自动交易机器人，可以很容易的实现杠杆代币。只需要部署一个交易策略为固定杠杆倍数的交易机器人基金，那么该基金合约的份额代币就是对应的杠杆代币。由于这种去中心化的杠杆代币完全不依赖人类基金管理员（或者说基金管理员是链上的机器人），相比中心化的方案具有较大的安全性优势，是 DeFi 用户进行杠杆投资的有利工具。

3.3 社交基金

社交基金是一种类似传统 GP/LP 结构的投资基金。社交交易员作为 GP，负责基金交易策略的制定和执行。投资者可以投资基金成为基金的 LP。当基金获得盈利后，GP 从盈利中提取一定比例的分红。

和机器人基金类似，每个社交基金都有独立的永续合约账户。用户可以投资基金从而获得基金份额也可以在合适的阶段退出基金实现盈亏。

与机器人基金不同的是，社交基金的交易策略由社交交易员进行管理。社交交易员被设置为基金账户的代理人（见 2.3.4）。社交交易员通过订单簿为基金账户下单执行自己的交易策略。除了盈利后分红，社交交易员无法从基金账户中提取资金。除了通过 MCDEX 的用户界面（UI）下单，社交交易员还可以通过订单簿的 API 进行交易。很多在中心化交易所交易的量化团队非常熟悉这种 API 的交易方式。他们可以方便的对接到我们的平台上，成为社交交易员。社交基金智能合约使得社交交易员只需专注于交易本身，而无需处理原本繁琐的 LP 入金、出金、分红等工作。对于普通投资者而言，只需关注基金的投资回报，而无需担心资金被挪用的问题。由此，社交基金产品构建了一个方便安全的连接交易员和投资者的平台。

3.4 流动性挖矿

为了鼓励更多用户投资基金，进而增加整个 MCDEX 的流动性。我们将分配一定比例的 MCB（见第四章）用于对基金用户的激励。用户只需向基金合约中存入资金，成为基金的持有人，就能按持有的基金净值规模分得 MCB，这也被称为“流动性挖矿”。每天挖矿产生的 MCB 的总量是固定，挖矿产出按基金净值在各个基金之间进行分配。也就是说，基金净值规模越大，获得的挖矿收入也越多。在相同的初始资金下，基金的业绩越好则净值增长越快，从而获得的挖矿收益也更多，这会激励用户选择业绩更好的基金。最后，对于社交基金，一定比例的挖矿收益会归属于社交交易员。

3.5 更多应用场景

我们将和社区一起打造更多基于永续合约的结构化产品，满足不同风险偏好的用户的需求。例如可以设计一种分层的结构化产品：底层是具有安全垫的优先层，用户投资该层即相当于投资低风险的固收产品；上层是高风险的劣前层，具有更高风险承受能力的用户可以投资该层产品获得更大的回报。我们希望通过结构化产品，为用户提供一种简单的 DeFi 投资品，以满足不同类型用户的需求。

4.治理与 MCB

在我们开发 MCDEX 平台上的各种产品时，非常希望这些产品一旦部署后就无需治理或修改调整，例如用于交易 Market Protocol 合约的 MCDEX Mai Protocol V1 就是一个几乎无需治理的交易层智能合约。然而，类似 MCDEX 永续合约这样相对复杂的产品，依旧有不少治理工作。MCDEX 永续合约的治理工作主要包括以下几个方面：

1. 修改合约参数：手续费率、初始/维持保证金率、清算罚金率等；
2. 批准合约升级；
3. 授权链上、链下风控；
4. 执行全局清算；

我们希望将 MCDEX 打造成一个完全去中心化的 DeFi 平台。这不仅仅要求我们的产品是基于智能合约技术的去中心化产品，也要求我们的治理过程是由社区主导的民主的去中心化治理过程。为了能更好的执行去中心化治理的目标，本着"谁使用、谁获益、谁治理"的原则，我们将发行 MCDEX 的平台币 MCB。MCB 代币将作为 MCDEX 的去中心化治理的投票币。从而，MCDEX 的治理权利将由 MCB 的持有人共同持有。

MCB 将具有以下功能：

1） 治理币。MCB 是 MCDEX 平台的治理代币。MCDEX 平台的治理权由 MCB 的持有人所有。MCB 的持有人通过投票履行治理权。
2） 价值捕获。MCDEX 平台订单簿的 100%交易手续费，AMM 的 20%的手续费（剩余 80%归于 AMM 的 LP）将用于买入 MCB 并销毁。
3） 提供 AMM 流动性。我们将在后续逐步升级 AMM，使用 MCB 作为 AMM 逻辑上的抵押物，从而使得 MCB 可以为 AMM 提供流动性。
4） 承担清算风险并获得清算收益。我们将在之后的升级中，使得 MCB 的持有人共同作为清算人，承担所有的清算风险。同时我们也会将所有的清算罚金用于购入 MCB 并销毁，从而使得 MCB 可以捕获所有的清算收益。

功能 2-4 非常依赖 MCB 的流动性。尤其是最后两个功能，其成功运转的前提是 MCB 具有很好的价值基础和流动性。这也是为什么我们选择逐步添加 MCB 功能的原因。我们希望随着 MCDEX 业务的逐渐开展，在市场对 MCB 价值的认知逐步加深、MCB 流动性逐渐增强的过程中逐步添加 MCB 的功能。

MCB 的总量为 100,000,000 个，MCB 的分配方式如下：

1. 25%归属创始团队和早期投资人，2.25%在 2 年内线性解锁，22.75%在 4 年内线性解锁；
2. 25%归属 MCDEX 基金会用于代币出售，获得的资金用于支付开发、审计、做市商、市场推广等支出；
3. 50%用于用户激励。每年至多有 5%的 MCB 会用于用户激励。

由于 MCDEX 的业务和产品将不断发展，新的产品会不断被加入 MCDEX 平台，在不同阶段我们需要激励的对象和激励方式也往往不同，所以，我们不会在一开始就将用户激励的规则固定下来。我们将分批次开展不同的用户激励活动。每轮激励活动由 MCDEX 社区发起，给出激励的提案：包括不限于用于激励的 MCB 数量、激励对象和激励方式。激励提案由 MCB

持有人投票审议通过后执行。我们将根据具体情况激励 MCDEX 平台的各种参与方，包括不限于：吃单者（Taker）、流动性提供者（LP）、开源交易策略贡献者、社交交易员、结构化产品的持有人、扩大永续合约使用场景的 DeFi 开发者等等。

5.路线图

2020 年 Q2

发布永续合约产品

2020 年 Q3

发布自动交易及社交交易产品

首次 MCB 代币融资

流动性挖矿

2020 年 Q4

上线新的 AMM 公式

发布去中心化杠杆代币

MCB 用于 AMM 流动性激励

MCB 用于链上治理

MCB 捕获平台手续费

IDO（Initial DEX offering）

2021 年

增强 MCB 的功能：

- 使用 MCB 为 AMM 提供流动性
- 使用 MCB 承担社会化损失
- 使用 MCB 捕获清算罚金

引入 optimistic rollup 机制提高交易性能

为 MCDEX 平台引入更多类型的金融资产

参考

[1] Perpetual Reference. https://mcdex.io/references/#/en/perpetual

[2] Y. Zhang, X. Chen, and D. Park, “Formal specification of constant product (xy=k) market maker model and implementation,” 2018.

[3] M. Lei and T. Zhu, [mip2] Proposal: A New Perpetual AMM Pricing Formula With High Capital Efficiency. https://github.com/mcdexio/mips/issues/2

[4] Perpetual Technical Guide. https://mcdex.io/references/#/en/perpetual-tech

[5] CHAINSECURITY, Mai 协议审计报告. https://github.com/mcdexio/mai-protocol/blob/master/audit/ChainSecurity_MaiProtocol.pdf

[6] OPENZEPPELIN SECURITY, MCDEX Mai 协议审计报告. https://blog.openzeppelin.com/mcdex-mai-protocol-audit

[7] MCDEX documents. https://github.com/mcdexio/documents