MiniSwap

The MiniSwap Research Lab

Lab@MiniSwap.org

Abstract. MiniSwap 是一个分布式的自动化交易平台，支持用户交易不同区块链生态系统提供的各种各样的金融产品。MiniSwap 将使用其代币（MINI ）来启动初始化 MiniSwap 生态系统并回报社区。MiniSwap 生态系统代币总数为 10 亿枚 MINI 。代币有两种不同方式产生。第一种是在初始化阶段，1.57 亿枚 MINI 将以 30 轮私募形式发行。在私募结束后代币将用于社区奖励计划。私募共分 30 轮，每轮代币价格上涨约 7.53%。随着轮次的增加，MINI 的价格也不断增加。
私募之后，任何参与者均可获得 MINI 代币作为奖励。对于 MiniSwap 中的每笔确认交易，价值约为其交易费 2 倍的代币将被挖出。其中约 1/2 的代币用来返还给交易者，1/2 的代币分发到流动性提供者。而这笔交易费会用来在交易池中购换 MINI 代币。所购换代币的 1/2 用来分发给所有 MINI 持有者，余下的代币将被销毁。
本白皮书介绍了 MiniSwap 的总体设计及其其四个阶段的启动计划，包括生态建设，分布式交易平台，分布式金融产品，以及分布式的自动跨链互操作系统来来支持用户对不同区块链系统的金融产品进行无缝交易。

1 简介

自比特币诞生以来 [4]，已有超过 5,000 种加密货币相继问世。目前加密货币总市值已超过 2640 亿美元 [1]，且其日交易量已经高达 1140 亿美元 [1]。为了给加密货币交易者提供更便捷的服务，各区块链加密货币交易平台也相继成立。然而，绝大部分交易平台是中心化的，并且代为管理用户的私钥。这就使得用户的私钥及其对应资产完全受控于中心化的交易平台。这非但极其不安全，且违背了区块链技术去中心化金融思想的初衷。

去中心化交易平台 (DEX) 的出现解决了这个问题。任意用户均可在去中心化的交易平台上面购买和出售加密资产而无需信任任何一个中心化的实体。在 2019 年，共有超过 250 个去中心化交易平台问世。他们的年交易量达到了约 24 亿美元 [2]。目前中心化的交易平台日交易量可以高达五百亿美元 [5]，所以相对而言去中心化交易平台还只停留在起步阶段，未来还有非常大的发展空间。

目前大多数去中心化交易所都是采用基于哈希时间锁定合约（HTLC）的原子互换协议（Atomic Swap Protocol）。这种协议支持交易双方在无需可信第三方的基础上完成加密货币的交易。不过最近一些科研显示现有的原子交换协议存在一些弊端，包括确认时间长、交易不公平等缺点 [3]。为此，我们推出 MiniSwap — 一个开源且支持互操作性的平台，其可用于支持分布式应用，加密经济原语，并且可以通过跨链组建一个区块链分布式金融生态网络。

MiniSwap **将分四个阶段启动**。在第一个阶段，我们通过生态系统启动计划和初始化奖励来初始化我们的平台，任何人都可以加入我们，成为 MiniSwap 生态系统的重要组成部分并获得这个平台的代币（MINI ）。并且支持者越早加入，可获得的奖励就越多。

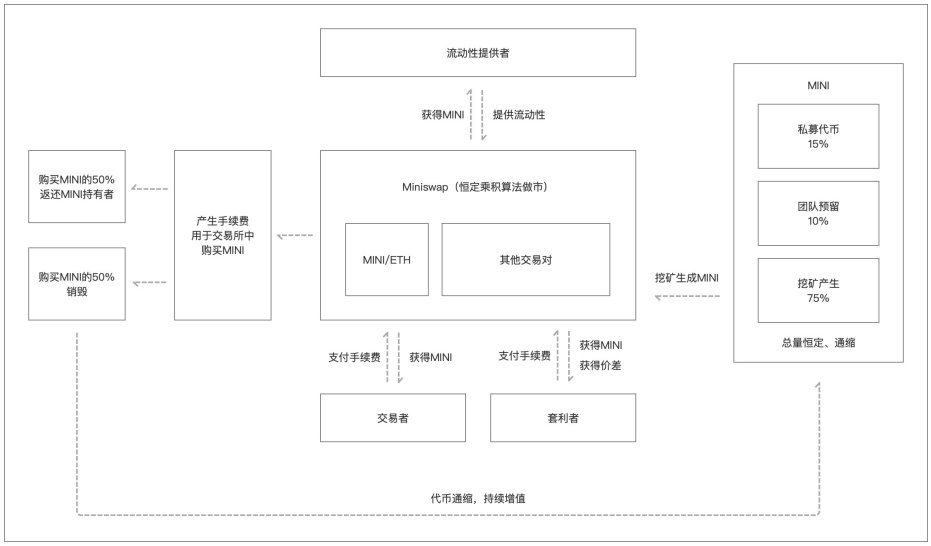

Fig. 1. 架构总览

在第二阶段，我们将在以太坊上建立一个去中心化和自动化的交易平台 MiniSwap Genesis 。通过流动池机制，MiniSwap Genesis 可支持以太坊链上的全部币种对的交换。MiniSwap Genesis 采用“交易即挖矿” 模式 (trans-fee miningmodel) 来保证 MINI 的发行。所有参与者，包括交易者，流动性提供者和 MINI 代币有者，将分别获得一定量的 MINI 作为交易奖励，流动性提供奖励和分红奖励。

在第三阶段，我们将推出 MiniSwap DeFi – 基于 MiniSwap Genesis 平台并扩展推出多类去中心化金融产品，例如期权和期货。这将使 MiniSwap 成为一个完善的加密金融生态系统，而并非只是一个用于交换服务的流动池。在最后一个阶段，我们将启动 MiniSwap Global 平台。该平台将以分布式的自动跨链互操作来支持用户对不同区块链系统的金融产品进行无缝交易。

2 概述

用户类型。 我们考虑四种类型的用户，即初始支持者，交易者，流动性提供者和 MINI 持有者。初始支持者指在第一阶段加入并帮助 MiniSwap 建立生态的早期用户。只要将自己的币转入 MiniSwap 智能合约账户，就可成为早期支持者。交易者指通过 MiniSwap 协议完成任意交易的用户。例如，用 USDT 交换 ETH 的用户就是交易者。流动性提供者是指根据合约政策将任意代币对存入流动池的用户。某位用户存入 X 单位的 ETH 和 Y 单位的 USDT，然后根据 MiniSwap 合约中定义的函数 $f(\cdot)$ 判定 $X = f(Y)$。持有 MiniSwap 生态代币的用户都称为 MINI 持有者。

设计架构。 图 1 为 MiniSwap 的设计架构。MiniSwap 的代币（MINI ）可以通过两种方式挖得。首先，每个早期支持者都可以通过参加 MINI 的购买来

支持建立 MiniSwap 生态，MINI 的价格随时间 (轮次) 增加。换句话说，如果支持者是最早加入 MiniSwap 的，其购买 MINI 的价格也就是最低的。其次，MiniSwap 采用 “交易即挖矿” 模式，每笔有效交易都会挖出 MINI ，具体将在第 4.3节中详细说明。根据算法 1中所定义，每笔交易都会使 MiniSwap 销毁部分 MINI 代币。MiniSwap 还向所有参与者提供各种去中心化金融产品，例如期权和期货。此外，MiniSwap 还将支持跨链交易，以连接由不同公链支持的生态系统网络。

社区奖励计划。 社区奖励计划提供三种奖励，包括早期支持者奖励，交易奖励和流动性提供奖励。虽然早期支持者奖励 (请参阅第 3节) 仅可用于第一个阶段来初始化生态，但其他奖励 (请参阅第 4节) 都可用于 MiniSwap 的任意阶段。

3 生态启动计划和奖励

我们通过生态初始化代币来启动 MiniSwap 并回报我们的社区。MiniSwap 生态系统代币总数为 10 亿枚 MINI 。其中，1.57 亿枚 MINI 将以私募形式发行。私募后用户可以通过社区奖励计划来获得代币。早期支持者奖励是为 MINI 生态的早期投资人所设。共有 30 轮兑换机会，用户可用 ETH 来兑换 MINI 代币。随着轮次的增加，MINI 的价格也不断增加。所以，支持者越早加入生态启动计划，可获得的奖励受益就越高。

设 P_k 为 MINI 在第 k 轮的美元价格，N_{ETH}^k 为第 k 轮接受的 ETH 的总量。对于所有的轮数 $k \in [1, 30]$，该轮 MINI 的价格为

$$P_k = 0.93^{30-k} \cdot P_{30},$$

其中 $P_{30} = 0.02$ 是最后一轮（第 30 轮）私募的预设价格。对于任意一轮，该轮接受的 ETH 总量可以由以下公式求得：

$$N_{ETH}^k = 10(k+1)$$

任意一轮发型的代币总数 N_{MINI}^k 可以由下列公式求得：

$$N_{MINI}^k = \frac{246 \cdot N_{ETH}^k}{P_k}$$

所以，在第 k 轮时，如果该轮接受的 ETH 总数还未达到时，一个早期投资人可以用 α ETH 换取的代币数量为 $\frac{\alpha}{P_k}$，价格为 P_k。图 2 把所有计算结果更直观的表示出来.

4 MiniSwap 作为去中心化交易所

MiniSwap Genesis 是基于以太坊的去中心化和自动交易平台。它利用了两个关键概念。第一个关键概念是流动性池，流动性提供者将代币添加到池中，交易者可以交换以太坊链上任何的一对代币。第二个关键概念是交易即挖矿模式，交易者的每笔交易都会获得 MiniSwap 提供的奖励。并且，对于每一笔交易所有的流动性提供者和 MINI 持有者还将获得额外社区奖励。

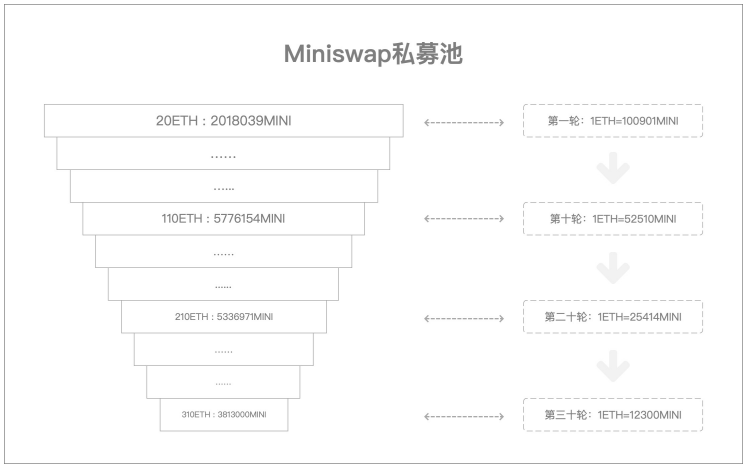

Fig. 2. 私募池计划

4.1 价格预言机

MiniSwap 将动态调整任何给定代币对的价格。我们使用从 t_i 到 $t_{i+\Delta t}$ 的长度为 Δt 时间段内的累积平均价格得出预期价格。这样可以减少参与者和矿工恶意操纵潜在价格的损害。设 N_i^A 为在时间 ti 内流动池中可用代币 $A \in \mathcal{T}$ 数量，其中 $\mathcal{T}$ 是以太坊所支持的所有代币的集合。

设 p_i 为时间 t_i 时的价格。精确来说，从时间点 t_i 开始经过后 Δt 时间后，使用代币 $A \in \mathcal{T}$ 来兑换 B 代币的购买价格 $p_{i,\Delta t}$ 为:

$$p_{i,\Delta t} = \frac{\sum N_j^A}{\Delta t \sum N_j^B}, \text{ where } j \in [i+1, i+\Delta t] \tag{1}$$

任何参与者都可以访问该预言机来估算价格，即某个时间段的平均价格。

我们现在来分析用瞬时价格可能出现的问题。设 $\bar{p}_i^{A,B}$ 为在时间点 t_i 用代币 A 购买一个单位代币 B 的瞬时价格（就是未使用累积权价格）。计算方法如下

$$\bar{p}_i^{A,B} = \frac{N_A}{N_B} \tag{2}$$

我们同样知道

$$\bar{p}_i^{B,A} = \frac{N_B}{N_A} \tag{3}$$

现在，让我们假设一个攻击者想要通过操纵价格来从 MiniSwap Global 的美式期权获利（如第 6章所示）。设 n_A 为攻击者拥有代币 A 的数量。如果在时间点 t_{i+1} 攻击者将所有 n_A 个代币 A 抛出购买 B，那么该时间点交易后的顺势价格则变为

$$\bar{p}_{i+1}^{A,B} = \frac{N_A + n_A}{N_B - n_B} \tag{4}$$

$$= \frac{N_A + n_A}{\frac{N_A \cdot N_B}{N_A + n_A}} \tag{5}$$

这个价格变化值 $\Delta\bar{p}^{A,B}$ 为

$$\Delta\bar{p}^{A,B} = \frac{N_A}{N_B} - \frac{N_A + n_A}{\frac{N_A \cdot N_B}{N_A + n_A}} \tag{6}$$

$$= \frac{N_A^2 - (N_A + n_A)^2}{N_A \cdot N_B} \tag{7}$$

可以看到 n_a 的大小对于瞬时价格 $\bar{p}^{A,B}$ 的影响非常大。同样，这个对反向瞬时价格 $\bar{p}^{B,A}$ 的影响也是非常大的。对这样攻击者就可以成功从美式期权对 A 和 B 两种代币同时进行套利。这其实是我们累积权平均价格只考虑一个离散时间点的特殊情况。通过使用累积权平均价格，我们可以减小 n_a 对价格的波动，使其难以预测从而降低风险。

4.2 流动性池

MiniSwap 通过流动池为任意资产对提供流动性。对于任意一堆数字资产 $(A, B \in \mathcal{T})$，MiniSwap 去中心化交易所的的储备金存储都遵照以下的线性关系

$$N_t^A \cdot N_t^B = K, \tag{8}$$

其中 K 是预定义的常数。

流动性提供者根据线性关系，将自己的代币投入到流动池中，即对于每个要存入的代币 A，流动性提供者还需要根据定义的关系将一些代币 B 放入池中。交易者可以交换 MiniSwap 中可用的任何资产对。资产交换可以通过智能交易合约无缝完成并且没有确认延迟。设 n^A 为交易者想要用于购买代币 B 的代币 A 的数量，f 为交易所产生的交易手续费，交易者将获得 n^B 个代币 B，如下列公式所述。

$$n^B = N_t^B \cdot \frac{K}{N_t^A + n^A - f} \tag{9}$$

4.3 交易即挖矿及奖励计划

交易及挖矿。对于 MiniSwap 中的每笔确认交易，如果其交易费为 f ETH，那么就会有价值为 $(\lambda_1 + \lambda_2) \cdot f$ ETH 的代币被挖出。其中 λ_i 为奖励参数 $(i \in [1, 2])$。交易费为交易金额的 0.3%。我们将在后文详细说明这个参数的设置和意义，以及如何分布奖励给参与者。

每日可以开采的 MiniSwap 代币数量有一个上限。令包含第一个 MINI 交易的区块的高度为 S，设 Y 为当前块的高度，X 为采矿奖励最大值的区块数量

调整间隔（大约为一个月，按照区块数量来计算）。那么每天（根据区块数量来计算）最多挖出的 MINI 数量计算如下：

$$Max(0.7^{\lfloor \frac{Y-S}{X} \rfloor} \cdot C_1, C_2),$$

其中 $C_1 = 500{,}000$，$C_2 = 18{,}000$.

奖励计划。对于 MiniSwap 中的每笔记录交易，所有 MINI 持有者，流动性提供者，交易者都将获得一份奖励。设 p 为 MINI 在 ETH 中的累积平均价格，R_1 为对交易者的奖励; R_2 为对流动性提供者的奖励; R_3 为对 MINI 持有者的奖励。设 $\lambda_i \in [0, 2]$ 为奖励参数，其中 $i \in [1, 2]$ 并且 $\lambda_1 + \lambda_2 = 2$。算法 1定义了对不同参与者的奖励。

Algorithm 1 奖励分发算法

Input:
奖励参数：λ_i for $i \in [1, 2]$;
f: 交易费;
p: MINI 的累积平均价格（单位为 ETH）;
X: 流动池中 MINI 的总数;
Y: 流动池中 ETH 的总数.
Output:
R_1: 给交易者的奖励;
R_2: 给流动性提供者的奖励;
R_3: 给 MINI 持有者的奖励。

1: $i = 1$
2: **while** i<4 **do**
3: **if** $i! = 3$ **then**
4: $R_i = \frac{f \cdot \lambda_i}{p}$
5: **else**
6: $R_i = \frac{f}{2p}$
7: **end if**
8: $i+ = 1$
9: **end while**
10: Destroy R_3 MINI ▷ 销毁 R_3 MINI
11: $X = X - 2 \cdot R_3$
12: $Y = Y + f$

对于 R_2 和 R_3，每一个都按比例分享奖励。直观地来说，当处理包含手续费 f 的交易时，共有价值为 $(\lambda_1 + \lambda_2) \cdot f$ 的 MINI 代币被挖出，其中

- 价值 $2f$ ETH 的 MINI 代币将被挖出;
- 其中比例为 λ_1 的手续费（f）将会以 MINI 代币的形式返还给交易者作为交易奖励。λ_1 的默认值为 “1”，即交易者将获得 100% 的交易费返还作为奖励。
- 其中比例为 λ_2 的手续费（f）将会以 MINI 代币的形式返还给流动性提供者作为提供奖励。λ_2 的默认值为 “1”。流动性提供者将获得一定比例的手续费作为奖励，这个比例是流动性提供者在流动池中拥有的资金占比。

– 这笔手续费（f）用来注入交易池中并换取 MINI 代币。换取的代币一半进行销毁，一半按比例发放给所有的 MINI 持有者。所以对于每笔交易，价值 50% 交易费的 MINI 代币会被销毁，价值 50% 的 MINI 代币会发放给 MINI 持有者。

5 分布式金融系统

在 MiniSwap 的第三阶段，我们将引入 MiniSwap DeFi 以支持各种去中心化金融产品。这将创建一个具有丰富功能的 MiniSwap 生态系统。MiniSwap DeFi 的第一个金融产品为美式期权。

美式期权 [6]，简单来说就是用户在我们平台购买一定数量的期权权益（可理解为开仓），系统根据用户购买的方向和未来一段时间行情的走向，判定用户的盈利或亏损，并反馈给用户。期权种类（又称期权周期）就是期权的时间期限，我们平台开通的期权种类分为 1 分钟，3 分钟，5 分钟，15 分钟，30 分钟，1 小时，12 小时，24 小时。在期权到期之前，用户可以选择提前行权（平仓），也可以等待期权到期后，系统自动行权（平仓）。行权后的收益或亏损，以行权时的行情价和开仓价格来判断。

权利金 (premium) 就是当前购买 N 个期权，用户需要支付的 USDT 数额，即可以理解为开仓保证金数额；用户如果亏损，亏损的数额不会超过权利金的数量。权利金是根据期权价格和购买数量计算出来的。计算公式为：权利金 = 购买期权数量 * 期权价格（加价）。

保本价格（break-even price）顾名思义就是用户保全权利金的行情价。当行情价，沿着用户的购买方向（做多或做空）波动到保本价格时，用户才能保本，否则用户就会亏损。所以期权可以理解为，用户刚开仓时就是亏损的，必须行情价波动到保本价才能回本，行情继续沿着购买方向波动就会盈利。

美式期权作为金融合约，能够使买家在不迟于约定的时间以预先确定的价格购买或出售资产。预先确定的价格称为执行价格 (strike price, SP)，约定的时间称为期权周期。每个期权都有一个期权价格 (intrinsic value, IV)。期权价格是期权的执行价格和基础市场的现行价格 (current price, CP) 之间的差异。对于看涨期权，内在价值是通过从基础价格 (underlying price) 中减去执行价格计算得出的。相反，看跌期权的内在价值是通过从执行价格中减去基础价格计算得出。

Algorithm 2 盈亏计算

1: premium = $N \times$ intrinsic value
2: break-even price = intrinsic value + underlying price
3: R = current price − break-even price
4: **if** $R > 0$ **then**
5: 　用户收益为 $N \cdot R$
6: **else**
7: 　用户亏损 $Min(-R \cdot N, premium)$
8: **end if**

当用户在任何时候 (不迟于约定的时间) 行使合约时，在我们的看涨期权中，算法 2计算该用户的利润和损失。

假设：用户开仓购买了 2 个 btc 的 5 分钟做多期权，当前 btc/usdt 行情价为 7000，

期权价格为 8.16 usdt，保本价格（break-even price）为 7000 USDT + 8.16 USDT = 7008.16 USDT,用户的开仓权利金为 2×8.16 USDT = 16.32 USDT。如果用户选择执行期权，将会发生以下情形:

- 当比特币价格行情波动到 $P \leq 7000$ USDT，且用户行权平仓，那么用户亏损数额为 16.32 USDT;
- 当比特币价格行情波动到 7000 USDT $< P <$ 7008.16 USDT, 且用户行权，则用户亏损数额为 $2 \times (7008.16 - P)$ USDT;
- 当比特币价格行情波动到 $P = 7008.16$ USDT, 且用户行权，那么用户不亏不赚，用户收回 16.32 个 USDT 的成本投入;
- 当比特币价格行情波动到 $P > 7008.16$ USDT 并行权，用户盈利，且盈利数额为 $2 \times (P - 7008.16$ USDT).

美式期权保险简介。用户在开仓购买期权时，可以选择购买期权保险。期权保险可以在用户亏损时，给予用户赔付一定数量的资金。期权保险赔付，有特定的行情价格区间，并不是只要用户亏损就会赔付，并且保险赔付的数额为保证金的一部分，并不是全额赔付。

比如说，用户开仓购买了 1 个 BTC 的 10 分钟做空期权，当前 BTC/USDT 行情价为 5000，期权价格为 12 USDT，保本价格为 4988，权利金为 1 BTC * 12 USDT =12USDT。用户开仓时，用户花 1 USDT 购买了最高赔付数额为 5 usdt 的赔付保险，赔付区间为 4990-4995。

按上述条件计算，会有以下几种情况：

- 当行情波动到 5000.9999，且用户行权平仓，那么用户亏损数额为 12 USDT。
- 当行情波动到 4988-5000 之间并行权，用户亏损数额为 12 USDT ＞亏损＞ 0 USDT。
- 当行情波动到 4990-4995 之间并行权，用户亏损但是用户会获得保险赔付，赔付数额为：5 USDT ＜赔付额＜ 0。
- 当行情波动为 4998 并行权，用户不亏不赚，用户收回 12 个 USDT 的成本投入。
- 当行情波动小于 4998 并行权，用户盈利，且盈利数额大于 0 个 USDT。

以上举例为做空，做多的逻辑和做空相同，只不过方向和做空是反的，此处不赘述。

6 分布式金融系统生态网络

我们将在第四阶段启动 MiniSwap Global ，使得 MiniSwap DeFi 可以在不同区块链生态系统之间进行通信，这将使得 MiniSwap 成为去中心化，可共享和自动化的平台，用于交易不同区块链生态系统提供的各种各样的金融产品。MiniSwap Global 还将建成生态系统网络，允许不同区块链平台无缝交易。我们初步计划采用类似 Cosmos 框架的设计和原子交换 [3] 协议。前者可以让交易者更快速的完成交易，后者可以使交易者完全不经过任何第三方来做完全的点到点的交易。更多详细信息请参照即将发布的白皮书。

References

1. coinmarketcap.com: Global Charts: Total Market Capitalization (2020), https://coinmarketcap.com/charts/
2. Frost, L.: Ethereum DEX trading volumes are rising rapidly in 2020 (2020), https://decrypt.co/27556/ethereum-dex-trading-volumes-are-rising-rapidly-in-2020
3. Han, R., Lin, H., Yu, J.: On the optionality and fairness of atomic swaps. In: Proceedings of the 1st ACM Conference on Advances in Financial Technologies, AFT 2019, Zurich, Switzerland, October 21-23, 2019. pp. 62–75. ACM (2019)
4. Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)
5. Top Cryptocurrency Exchanges List (2020), https://nomics.com/exchanges
6. Option style — Wikipedia, the free encyclopedia (2020), https://en.wikipedia.org/w/index.php?title=Option_style&oldid=966400380