CoFiX 兑换协议产品文档

1、简介

本文档是对“CoFiX：一种可计算的金融交易模型” 白皮书所描述的金融交易模型的实现设计。主要包括价格计算、交易、做市商、异常处理等机制和前端页面交互定义。

2、系统角色

角色	定义
交易者	参与 CoFiX 交易的对象，可以是某个以太坊钱包或者合约地址
做市商	参与 CoFiX 做市的对象，是交易者的对手盘，为交易提供流动性，可以是某个以太坊钱包地址或者合约地址
治理者	参与 CoFiX 系统治理的对象，是 CoFiX 的治理代币持有者，通过发起投票修改和升级 CoFiX 系统。（前期由管理员多签账户代理）

3、价格计算机制

3.1、价格来源

CoFiX 协议的价格来源于 NEST 预言机，每个交易池对应一个 NEST 预言机价格源，例如：

ETH: USDT 交易池，价格从 NEST 的 ETH/USDT 预言机调用。

ETH：HBTC 交易池，价格从 NEST 的 ETH/HBTC 预言机调用。

在 NEST 系统里，一个报价对对应一个预言机，详见 NEST 预言机文档

3.2、价格补偿系数 K

由于 NEST 价格和均衡价格存在一定的偏差和延时(可以理解成去中心化的成本)，因 此 CoFiX 在应用该价格时需要对风险给出一些补偿，确保做市商有动力持续做市。补偿系数记为 K，该系数与波动率 σ 和延时变量 T 有关，当交易者进行交易时，并不

是直接使用 NEST 价格 P，而是使用：

买入时：$P'_b = P * (1 + K)$

或者：

卖出时：$P'_s = P * (1 - K)$

这里的买入和卖出都是相对价格 P 所对应的本位资产来说的，例如价格 P 是以 ETH 为本位的， 即一单位 ETH 等于多少 USDT、HBTC 等资产，则买入和卖出指的是买入和卖出 ETH（卖出时其实就是买入本位资产所对应的另一方资产）。

同样做市商在进入和退出做市时，计算净值用 的价格变量也是 P' 而不是 P，这一价格称之为交易价格。 详细计算方式见附件“CoFiX 价格偏差系数（K）计算说明“

3.3、预估价格和执行价格

由于以太坊一笔交易由发起到执行需要一定的等待时间，并且 NEST 预言机价格一直处于更新状态，因此交易发起和实际交易打包成功时的价格会存在一定的差异。这里我们先定义一下预估价格和执行价格。

预估价格：P_{es}	用户或者做市商在发起交易时看到的参照价格，取自 NEST 预言机最新历史价格。 这个价格主要是前端用来进行交易价格展示以及兑换金额、认购份额、赎回资产数量的预估计算。
执行价格：P_{ex}	交易执行时，实际调用的 NEST 预言机最新价格。

由预估价格和执行价格可以计算实际成交价差 P_d：

$$P_d = | P_{ex} - P_{es} | / P_{es}$$

当前设定当 P_d>1%时发出的交易会被 revert

3.4、预言机价格调用费

当向 CoFiX 发起交易、赎回、认购操作时，会向 NEST Protocol 调用预言机价格、因此用户需要向预言机支付对应的调用费，收费标准取决于 NEST Protocol，目前调价格的收费是 0.01 ETH。

4、做市商机制

做市商是 CoFiX 交易流动性提供者，可以通过转入资产为某个交易池提供流动性来获得收益。CoFiX 支持单边资产做市，通过对应交易池的基金净值以及份额来进行资产管理。

4.1、做市商份额

份额代表着 CoFiX 某个资产池所拥有的做市资产比例凭证。当做市商向交易池转入资产进行做市时，获得 X-Token。当做市商想退出时，通过转出并销毁 X-Token，赎回对应价值的资产。

每个做市资金池拥有独立的 XToken，按照交易对创建时间顺序对 XToken 进行命名为 X_{T1}、X_{T2}、X_{T3} …

4.2、交易池创建和初始化

任何人都可以选择一个 NEST 预言机来创建对应的 CoFiX 交易池，该交易池使用对应预言机的价格，并且在创建时进行净值和份额的初始化。以 ETH:USDT 资产池为例，当市商池在创建时：

净值初始化为 1

初始发行份额数量 S_0 为：

$S_0 = A_u/P'_b + A_e$

其中：$P'_b = P * (1 + K)$，P 为 ETH/USDT 的当前价格，K 为当前补偿系数

A_e 为做市资产 ETH 初始数量

A_u 为做市资产 USDT 初始数量

4.3、做市商净值

净值代表着某个资产池中，每个份额（XToken）的 ETH 本位价值。每当有交易、认购、赎回操作时，对净值进行更新。以 ETH:USDT 资产池为例，净值计算公式为：

认购时：$N_P = (A_u/P'_s + A_e)/S$

赎回时：$N'_P = (A_u/P'_b + A_e)/S$

其中：

S 为 ETH:USDT 资产池总发行份额

ETH 做市资产总量 = A_e

USDT 做市资产总量 = A_u

$P'_b = P * (1 + K)$

$P'_s = P * (1 - K)$

P 为 ETH/USDT 的当前价格， K 为当前补偿系数

4.4、份额认购

认购代表着参与某个交易池做市，在转入资产同时获得份额对应 XToken。以 ETH: USDT 资产池为例：

Alice 转入 a 个 ETH 参与认购做市，那么获得的 XToken 数量 s_1 为：

$s_1 = a/N_P$

其中：N_P为当前认购时候的净值

同理 Alice 若转入 b 个 USDT 参与做市，那么此时 alice 获得的 XToken 数量 s_2 为：

$s_2 = b/P'_b/N_P$

其中：N_P为当前认购时候的净值， $P'_b = P * (1 + K)$

4.5、份额赎回

赎回代表着退出某个交易池做市，通过转入对应 XToken 按照当前净值兑换任意一边资产，转入的 XToken 会进行销毁。以 ETH: USDT 资产池为例：

Alice 转入 c 个 XToken，那么可以兑换出来的 ETH 数量 e 为：

$e = c * N'_P * (1-\theta)$

其中：N'_P为赎回时的净值，θ为交易手续费系数

可以兑换出来的 USDT 数量 u 为：

$u = c * N'_P * P'_s * (1-\theta)$

其中：N'_P为赎回时的净值，θ为交易手续费系数，

$P'_s = P * (1 - K)$，P 为 ETH/USDT 的当前价格， K 为当前补偿系数

5、交易机制

5.1、ETH 对 ERC-20 交易

以 Alice 使用 ETH 兑换 USDT 以及 使用 USDT 兑换 ETH 为例：

交易者 Alice 使用 a 个 USDT 兑换出 x 个 ETH，计算过程为：

$x = (a/P'_b)*(1-\theta)$

其中：$P'_b = P * (1 + K)$，P 为 ETH/USDT 的当前价格 ； K 为当前补偿系数；θ为交易手续费系数。

交易者 Alice 使用 b 个 ETH 兑换出 y 个 USDT，计算过程为：

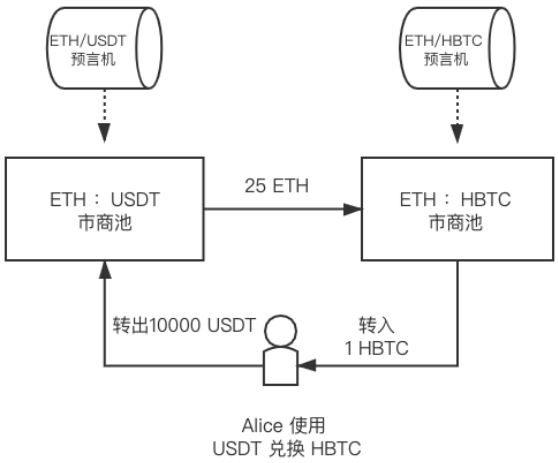
$y = b*P'_s*(1-\theta)$

其中：$P'_s = P * (1 - K)$，P 为 ETH/USDT 的当前价格 ； K 为当前补偿系数；θ为交易手续费系数。

5.2、ERC-20 对 ERC-20 交易

当有多个不同市商池时，可以通过调用 2 个 ETH:ERC-20 市商池，通过一笔交易完成 ERC-20:ERC-20 兑换。

原理示例：



计算过程以 Alice 使用 USDT 兑换 HBTC 过程为例：

那么, 当 Alice 使用 *a* 个 USDT 兑换出 y 个 HBTC, 计算过程为：

1）使用 USDT 兑换出 x 个 ETH

$x = (a/P'_{1,b})*(1-\theta)$

2）使用 x 个 ETH 兑换出 y 个 HBTC

$y= x*P'_{2,s}*(1-\theta)$

3) 1 和 2 步骤合并可以得出，使用 a 个 USDT 可以兑换出的 HBTC 数量为

$y= (a/P'_{1,b}) *P'_{2,s}*(1-\theta)^2$

其中:

P_1 为 ETH/USDT 预言机价格，k_1 为 ETH:USDT 交易池价格补偿系数; P_2 为 ETH/HBTC 预言机价格 ,k_2 为 ETH:HBTC 交易池价格补偿系数; θ为交易手续费系数。

6、风险控制

6.1、交易延时控制

考虑到以太坊存在交易拥堵，长时间无法打包的情况。因此，当一笔交易发出去后，实际成交的即时价格与交易发起时的预估价格可能会存在较大的偏差，因此引入一个变量，交易有效时间 t

1）交易发起时，时间为 t_0

2）交易打包成功时，时间为 t_1

3）那么，当 $t_1-t_0> t$ 时，此笔交易将视为交易不成功，返回用户交易资产。

4）当前设定 t=600s

6.2、 停机机制

当波动率上升到一个极端情况，或者 NEST 系统被攻击时，需要 CoFiX 启动应急方案，主要是为了保护交易双方，特别是做市商。此时系统可以设置停机机制，即触发 一类条件时暂停交易。目前设置的停机条件有 5 类，当达到停机条件时，发出的交易会被 revert:

1） K_0 值超过一个范围，目前设定为 $K_0>5\%$ 。

2）波动率 σ 上升到一个范围，目前设定为 σ>0.1%/秒 。

3）预言机价格间隔：T>900 秒。

4）交易打包延迟：t>600 秒。

5）实际成交价差：P_d>1%。

具体停机参数的计算见”CoFiX 价格偏差系数（K）计算说明”

是执行价格和预言机价格差的比例

7、流动性挖矿激励系统

7.1、矿池总量:

系统有三个矿池，即交易矿池 A，做市商矿池 B，节点矿池 C，其数量如下：

矿池 A：总量不固定，单位佣金出矿量也随做市商单位区块出矿量、池子总份额和净值的改变而变化，

矿池 B：当前每个区块固定出矿 4 个，240 万个区块后变成 3，

矿池 C：当前每个区块固定出矿 4/9 个，240 万个区块后变成 3/9，

7.2、交易者挖矿模型：

交易者每笔挖矿都会产出一定的 CoFi，其中 80%归该交易者，10%归节点矿池，10%归做市商矿池。每笔产出的 CoFi 主要取决于该笔交易支付的佣金：

1.假设该笔交易的规模为 x_t(ETH)，佣金为 $y_t=x_t*\theta$(ETH)，

2.单位佣金（1ETH）挖出的 CoFi 标准量为 a_t , a_t的计算公式如下：

$$a_t = (b_t/q) * 2400000/(X_t * N_p*0.3)$$

其中：

b_t为做市商矿池在当前时刻的单位区块出矿量

X_t为当前交易对池子的总份额

N_p为当前交易对池子的净值

q为做市商矿池的交易池个数

3.考虑到连续若干笔交易规模过大，会导致出矿不受控制，因此我们设计了密度衰减指标，其核心参数如下：

1）单笔交易触发密度衰减的阈值为$L*\theta*a_t$，其中 L=100（ETH）

2）假设连续两笔交易之间的区块间隔为 s，则密度参数:

$$f_t=\begin{cases}f_{t-1}*(300-s)/300+y_t*a_t & s\le 300\\ y_t*a_t & s>300\end{cases}$$

3）为了确保交易池两端资产的平衡，在挖矿中加入一个平衡系数 λ， λ计算如下：

假设交易者用资产 V_x兑换资产 V_y， 交易池内资产 V_x总量为 U_X，资产 V_y总量为 U_Y（按交易时的价格换算成 ETH），λ的值的大小取决于U_X/U_Y的值的大小，具体公式如下：

$$\lambda=\begin{cases}0.50, & U_X/U_Y\ge 10\\ 0.75, & 10>U_X/U_Y\ge 3\\ 1.00, & 3>U_X/U_Y\ge 0.33\\ 1.25, & 0.33>U_X/U_Y\ge 0.1\\ 1.50, & U_X/U_Y<0.1\end{cases}$$

4）出矿量公式：

y_t对应的出矿量 $A(y_t)$计算如下：

$$A(y_t)=\begin{cases}0.8*y_t*a_t*\lambda & f_t\le L*\theta*a_t\\ 0.8*y_t*a_t*L*\theta*a_t*(2f_t-L*\theta*a_t)/{f_t}^2*\lambda, & f_t>L*\theta*a_t\end{cases}$$

注：1）$0.125A(y_t)$流向节点矿池，记为$R(y_t)$，即出矿的 10%；

2）另外 $0.125A(y_t)$流向该笔交易对应的做市商矿池，记为$I_j(y_t)$，j 是第 j 个交易池，参见做市商挖矿模型。

7.3、做市商挖矿模型：

假设有 q 个交易池可以参与挖矿，对应的 Xtoken 依次记为 X_{T1}、X_{T2}…X_{Tn}，则做市商矿池等比例分成 q 个子矿池，即 B_1、B_2...B_q。某个池子 B_j, 以及做市商 m 在时刻 $h_{m,t}$-

$_1$($h_{m,t-1}$表示做市商 m 的第 t-1 次操作对应的时刻)存入 B_j 矿池合约的 X_j 的数量余额 $x_{m,t-1}$，则做市商在其后一个时刻 $h_{m,t}$，无论执行存入、取出、领取三种操作的任何一种，都可以挖出 CoFi，且其出矿量为：

$$B_{m,t}(x_{m,t-1}) = (G_{m,t} - G_{m,t-1}) * x_{m,t-1}$$

公式注释：

1.$x_{m,t-1}$本次操作前存入合约余额

2.$G_{m,t}$为做市商 m 本次操作的出矿系数，$G_{m,t-1}$为该做市商地址的上一次操作的出矿系数，G_t是一个公共变量，任何做市商在执行存入、取出、领取操作都可以改变这个参数，G_t计算方式如下：

$$G_t = G_{t-1} + (b_t * (h_t - h_{t-1}) + \sum I_j(Y_i))/X_t$$

其中：G_0=0，$\sum I_j(Y_i)$的求和区间为 h_t 到 h_{t-1},

公式注释：

1）b_t为矿池 B 在 h_t 时刻的单位区块出矿量,初始b_0=4，过 240 万个区块衰减到上期值的 0.8，并取整数，衰减到 1 后保持不变，则 b_1=3、b_2=2、b_3=1 、b_4=1…

*2）$I_j(Y_i)$*为 h_{t-1} 到 h_t 期间 j 交易池交易挖矿分给做市商的部分

3）X_t为 t 时刻 j 矿池存入的 X_{Tj} 的总余额

7.4、节点挖矿模型：

节点总量为 100 个，与做市商类似，节点持有者将节点存在节点矿池合约，并在每次存入、取出、领取操作时根据给定的算法获得对应的 CoFi。和做市商类似，节点矿池也存在一个出矿系数，每次操作基于 该挖矿系数出矿。

假设某节点持有人 m 在时刻 $h_{m,t-1}$，($h_{m,t-1}$表示 m 的第 t-1 次操作对应的时刻)，存入矿池合约的节点的数量余额$n_{m,t-1}$，则 m 在其后一个时刻 $h_{m,t}$，无论执行存入、取出、领取三种操作的任何一种，都可以挖出 CoFi，且其出矿量为：

$$C_{m,t}(n_{m,t-1}) = (D_{m,t} - D_{m,t-1}) * n_{m,t-1}$$

公式注释：

1. $n_{m,t-1}$本次操作前存入合约余额

2. $D_{m,t}$为 m 本次操作的出矿系数，$D_{m,t-1}$为 m 上一次操作的出矿系数，D_t是一个公共变量，任何节点持有人在执行存入、取出、领取操作都可以改变这个参数，D_t计算方式如下：

$$D_t = D_{t-1} + (c_t * (h_t - h_{t-1}) + \sum R(y_t))/N_t$$

其中： $D_0=0$

公式注释：

1）c_t为矿池 C 在 h_t时刻的单位区块出矿量,初始$c_0 = b_0/9$，$c_t = b_t/9$

2）$\sum R(y_t)$为 h_{t-1}到 h_t期间交易池交易挖矿分给节点的部分

3）N_t为 t 时刻存入节点矿池的节点 token 总余额

7.5、CoFi 分红及回购模型：

参与挖矿的交易池，其所有交易佣金 ETH 进入系统分红池，其中 α 比例用于分红，1-α 用于回购，回购机制在 CoFi 上线 CoFiX 后由 DAO 另行设计。

假设 CoFi 持有人 m 在时刻 $h_{m,t-1}$，($h_{m,t-1}$表示 m 的第 t-1 次操作对应的时刻)，存入分红合约的 CoFi 数量余额$n_{m,t-1}$，则 m 在其后一个时刻 $h_{m,t}$，无论执行存入、取出、领取三种操作的任何一种，都可以分得 ETH，且分红数量为：

$$E_{m,t}(n_{m,t-1}) = (F_{m,t} - F_{m,t-1}) * n_{m,t-1}$$

公式注释：

1.$n_{m,t-1}$本次操作前存入合约余额

2.$F_{m,t}$为 m 本次操作的分红系数，$F_{m,t-1}$为 m 上一次操作的分红系数，F_t是一个公共变量，任何节点持有人在执行存入、取出、领取操作都可以改变这个参数，F_t计算方式如下：

$$F_t = F_{t-1} + \alpha * \sum y / N_t$$

其中：$F_0 = 0$

公式注释：

1）$\sum y$为 h_{t-1}到 h_t期间挖矿交易池中交易者支付的所有手续费

2）N_t为 t 时刻存入分红合约的 CoFi 总余额

8、治理 （待定）CoFiX DAo

8.1 、治理阶段

CoFiX 协议社区治理分为 2 个阶段。

第一阶段，由 10 个多签超级管理员地址来主导，负责对 CoFiX 早期阶段进行合约升级、参数调整。管理员地址主要由社区 KOL、早期投资人、合作项目方等多方组成。

第二阶段，超级管理员退出，进入社区治理阶段，合约升级、参数调整等决议需经过社区投票通过后方可执行。

8.2、 社区治理流程

1.决议发布

- 设置好修改参数或者部署好升级相关的决议合约，并且开源。

- 质押一定数量的 CoFi Token，通过投票工厂合约对决议发起投票。

- 在 CoFiX 社区治理前端页面对投票进行发布。

2.投票期

- 投票周期为 7 天

- 投票周期内 CoFi Token 持有者可以直接使用存入在收益合约的 CoFi 进行投票。

- 投票率一旦超过 51%，该合约进入公示期。

3.公示期

- 投票公示期为 3 天

- 期间投票者可以对投票进行撤销

- 撤销后，如果票选低于 51%，则退回到投票期。之后再次达到 51% 投票进入公示期 3 天重新倒计时。

4.投票结束

- 投票持续 7 天没有达到 51% 投票率，则该决议被视为不通过。

- 决议通过 3 天公示期后，进入可激活状态，任何人可以激活使得改合约部署并生效。

8.3、 社区治理类型

投票类型	详细介绍
激活挖矿	激活某一个交易对挖矿功能
关闭挖矿	关闭某一个交易对挖矿功能
挖矿权重分配	重新分配各个交易对做市商挖矿比例
交易对手续费费率	调整处于挖矿模式下交易池的手续费
合约升级	对合约进行替换

附件

CoFiX 价格偏差系数(K)计算说明_.doc