N 次方互换平台

链上华尔街
给人民 N 次方

N 次方基金会

简介

本文介绍了一个 自动做市商（AMM）平台，含有币/币互换、可清算牛熊证合约，聪期权，以及挂钩币。通证/通证交换，名为 Powerswap （N 次方互换），有两种类型的参与者，投资者和流动性提供者。投资者使用 Powerswap 交换数字通证，并与流动性提供者进行交易。Powerwap 使用幂函数和不变与虚拟记账法。与恒定积 AMM 不同，幂函数和 AMM 有高市场深度。虚拟记账进一步减少了矿工在一区块内的原子套利。可清算的牛熊证合约（CBBC）允许投资者使用其拥有的任何通证来高杠杆投机比特币、以太坊和黄金的价格。CBBC 合约有三种类型，投资者、流动性提供者和清算方。投资者与流动性提供者交易，使用任何类型的通证来推测标的资产的价格变动。清算者确保投资者的权益不会跌破零，并在用户账上余额低于预先指定水平时清算投资者账户。 CBBC 与传统期货合约相比的优势在于，它允许投资者使用自己的通证进行投机。聪永久期权（SPO） 合约具有指数衰减，允许以更高杠杆投资，并进一步简化定价。它与固定到期期权的不同，因为期权永远不会过期，但回报会衰减。即使合同过半期，这份合同仍将给投资者以希望。与 CBBC 一样，SPO 允许投机 BTC，ETH 和黄金结算在任何替代硬币。我们还讨论了智能合约

的平台币问题，并计划使用 Powerswap 合约和由智能合约控制的灵活供应提供 XIAN 现金流支撑的挂钩通证。挂钩通证可以用来做借贷市场的工具。

目录

1、 介绍

区块链技术已经存在了 10 多年，但实际应用却很少。最近的一个发展是使用去中心化交易所进行交易。去中心化交易所（DXes）的交易量最近激增。特别是， 恒定积自动做市商 （AMM） 处于领先地位.我们使用 AMM 设计讨论一些协议。我们考虑币/币交换，可清算的牛熊证合约，聪永久期权合跃，最后基于现金流的稳定通证设计。

2、 N 次方互换

我们提出了一个新的协议，具有相同的功能，与 Uniswap 类似，但是有较小的滑点，同时通过虚拟余额，避免区块内套利，并降低区块间套利。

我们从固定价格案例开始

$$x + P_{\frac{y}{x}} y = k$$

以 USDT 和 UCNY 对应 x,y.UCNY 价格大约是 1/6.5 USDT。

当价格波动时，我们不能有一个恒定的价格等式。考虑以下幂函数变化

$$x^r + \left(P_{\frac{y}{x}} y\right)^r = k$$

请注意，当$r = 1$ 时，此方程减小为线性函数

$$x + P_{\frac{y}{x}} y = k$$

当$r = 0$时，此方程趋近到

$$\ln(x) + \ln(y) = constant$$

等效于 ，即 Uniswap 协议。因此$xy = constant$， 幂函数和不变曲线位于恒定积和恒定和曲线之间。 所以当 r>0 时，N 次方互换的滑点要低于 uniswap.我们暂时把 r 定在 0 和 1 之间。

2.2、 流动性提供者

智能合约根据以下公式生成流动性通证。让$DX，DY$为添加到流动性池的通证数量。 $TX，TY$成为当前流动性池中的通证数。

$$\frac{DX}{DY}=\frac{TX}{TY}$$

然后，生成的流动性通证的数量由以下公式给出

$$DLT=TLT\left(\left(1+\frac{DX+DY}{TX+TY}\right)^{F}-1\right)$$

请注意，当$DX+DY$很小时，这会近似为线性关系。 一个近似值是

$$\frac{DLT}{TLT+DLT}=\frac{1-\sqrt{1-\frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}}{2(1-F)}$$

$$\frac{DLT}{TLT}=\frac{1-\sqrt{1-\frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}}{1-2F+\sqrt{1-\frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}}$$

让

$$\theta=\sqrt{1-\frac{4F(1-F)(DX+DY)}{DX+DY+TX+TY}}$$

我们有

$$\frac{DLT}{TLT}=\frac{2F*(DX+DY)}{TX+(1-2F)(DX+DY)+(TX+TY+DX+DY)\theta}$$

进 一步的泰勒扩展， 我们得到以下近似

$$DLT=\frac{TLT\times F\times(DX+DY)}{TX+TY+(1-F)^{2}(DX+DY)}$$

因此，随着流动性通证的铸造，流动性通证的价格更高。

另一方面，当流动性通证被烧毁时，用户分别接收 $Dx，Dy$ 数量的 X,Y 通证

$$Dx = Tx\left(1 - \left(1 - \frac{DLT}{TLT}\right)^{\frac{1}{F}}\right),$$

$$Dy = Ty\left(1 - \left(1 - \frac{DLT}{TLT}\right)^{\frac{1}{F}}\right).$$

泰勒扩展到，我们有

$$Dx = Tx\left(\frac{1}{F}\frac{DLT}{TLT} - \left(\frac{1}{F} - 1\right)\left(\frac{DLT}{TLT}\right)^2\right),$$

$$Dy = Ty\left(\frac{1}{F}\frac{DLT}{TLT} - \left(\frac{1}{F} - 1\right)\left(\frac{DLT}{TLT}\right)^2\right).$$

2.3， 反套利

币币交换时，用上一个区块的价格定价。这样矿工无法在区块内套利，这将显著增加 LP 供应商的利润。此外，我们用虚拟余额来更新价格，也就是说，币量的变化不是立刻导致币价改变，而是以一种指数衰减的方式来影响币价，这一点类似于 1inch，从而减少跨区块套利的期望利润。

2.3， 交易费

将来，16%的交易费可以作为平台收入，打进平台币的地址上去，转给平台通证"牛熊币"（TBBC）的所有者，稍后将仔细介绍

3、可清算牛熊证合约

3.1， CBBC

可清算的**的牛熊证合约**，为投资者提供了杠杆.它于 2001 年在欧洲和澳大利亚首次推出，现已在英国、德国、瑞士、意大利和香港流行。CBBC 在欧洲和香港的投资者之间有大量交易，因为它迎合了个人投资者的行为偏见（比如对偏度的偏好）。

CBBC 有两种类型的合约，牛证和熊证。通过牛证，投资者可以捕捉到其潜在的价格上涨。熊证让投资者、在下跌的市场上获利。

在我们的智能合约中实施的 CBBC 永远不会过期，但是，任何人都可以在价格低（高）于清算价格时清算牛（熊）证头寸。合同持有人也可以随时清算其头寸。此外，为了避免流动性提供者的风险太大，最大收益上限为与杠杆成正比的上限。投资者可以收到的最大价格变化是初始价格倍数百分比，目前设置为 10%。

CBBC 的一个属性是，它迎合了那些喜欢偏度的人，因为最近的行为金融研究表明，偏度也很重要。投资者对偏度有不同的偏好和看法的时候，他们愿意使用 CBBC 来交易。

3.2， 乘积 CBBC

通常，CBBC 使用其中一个交易对作为结算通证进行交易。例如，让 ETH/USDT 成为 CBBC 交易的价格，然后回报将以 USDT 的单位为单位，即 ETH 的价格变化（以 USDT 为单位）。

乘积 CBBC 与 外汇市场里的 quantos 类似，因为价格以一个通证报价，但结算在另一个通证中。例如，ETH 的价格在 USDT 中报价，但结算以 UCNY 表示，另一个通证，多头合约的损益为 （P2-P1）*UCNY，熊合约的损益为 （P1-P2）UCNY。

乘积 CBBC 允许 UCNY 持有者推测 ETH / USDT 价格变化，而无需首先转换为 USDT ，当 UCNY / USDT 流动性较低且 UCNY 价格可能被操纵。

3.3， CBBC 智能合约

CBBC 智能合约有三种类型的参与者、投资者、流动性提供者和调用方。

1:投资者：这类玩家随时可以开仓和关闭头寸。

投资者需要填好他想要投入的初始资本，杠杆水平，牛或熊。智能合约将决定清算价格、行权价格和上限（多头）或下限（熊）。行权价格将使投资者的权益定为零。清算价格是行权价格和当前标的通证价格的平均值。 :

2:流动性提供者：流动性 提供者与投资者交易。 他们收取交易费。此外，由于投资者使用高利润，流动性提供者在多数时间赚钱，因此他们的回报有负的偏度

3: 清算工： 清算工可以是任何试图清算头寸的人。当清算工清算多头仓位时，如果价格低于清算价格，则清算成功。否则，清算失败，仓位保持不变。同样，当呼

叫者清算熊证头寸时，如果价格高于清算价格，则清算成功，投资者头寸被清算。否则，调用失败，仓位保持打开状态。

3.4、 CBBC 平台通证 （牛市和熊市合约的通证，TBBC）

Token of Bull and Bear Contract (TBBC)是 CBBC 平台通证，也是整个平台的通证。对于使用 X 通证作为结算通证的 CBBC 合约，交易费用的 1/3 将发送到 X/TBBC N 次方互换合约，相应的 TBBC 将转移到 TBBC 持有者拥有的池中。.这样， TBBC。 的价格就会对 X 升值。此外，TBBC 池的所有者将有更多的 TBBC。随着更多投资者使用这些合约，TBBC 将升值更多

4， 聪期权合约 （SPO）

4.1，SATOSHI PERPETUAL OPTION (SPO)

在比特币的设计中，采矿奖每四年减半一次。这一特征类似于放射性指数衰减。在下面的期权合约中，我们采用类似的设计，我们将这些期权合约称为聪期权合约。

$$C(t) = 2^{-t/\tau}\frac{1}{n}\left(\left(\frac{S(t)}{K}\right)^{n} - 1\right)^{+} KX(t)$$

$$P(t) = 2^{-t/\tau}\frac{1}{n}\left(1 - \left(\frac{S(t)}{K}\right)^{n}\right)^{+} K\,X(t)$$

我们考虑 n=0、1、2，它对应于对数、线性和二次项。 此外 ， 我们考虑以下二元聪期权合约。

$$C(t) = 2^{-t/\tau}1_{S(t)>K}KX(t)$$

$$P(t) = 2^{-t/\tau}1_{S(t)<K}KX(t)$$

价格将采用双跳连续时间模型确定，按照 Duffie, Pan & Singleton（2001）。

聪期权合约的一个优点是，使用智能合约实现这些合约是最简单的。智能合约的一个特性是，很难去寻找过去的价格，因此，我们不能用比较低的费用读过去的价格。对于合约的开仓和平仓，它必须以去中心化的方式操作，用户发出聪期权开仓平仓的价格仅仅依赖上一个区块的价格，这样的智能合约，矿工费用就比较低。

3.3， SPO 智能合约

SPO 智能合约设有投资者、流动性提供者两种玩家。

投资者：这类玩家随时可以开仓和关闭头寸。

投资者需要填写他想投入的初始资本、半衰期和合约的行权价格。合约的价格及其头寸将由 SPO 智能合约决定。投资者的回报是正偏度。

流动性提供者：流动性提供者与投资者交易。流动性提供者收取交易费。此外，由于投资者使用高利润，流动性提供者多数时间赚钱，因此他们的回报有负的偏度。

任何人可以选择成为投资者或者流动性提供者。所以聪期权提供了一个給偏度爱好不同的人的一个场所。

5， 平台币池

交易费用得到的所有通证将通过 N 次方互换转为 TBBC，TBBC 将发送到 TBBC 池。这样，TBBC 的价格就会上涨，TBBC 池子的所有者将获得更多的 TBBC。

在启动阶段，2500 万 TBBC 被发送到智能合约里。5000 流动性币被创建并发送到发起人。之后，使用幂函数公式确定流动性币的铸造和销毁。

让总平台流动性通证为 TPL，平台总锁仓 Totbbc = Totaltbbc，存款是 Dotbbc =depoittbbc。 存款后得到的流动性币数量是 DPL， DPL 由以下公式算出

$$DPL = TPL\left(\left(1+\frac{DOTBBC}{TOTBBC}\right)^{F}-1\right)$$

F 起始设置为 0.5，随着流动性池子增加趋近于 1

利用一些近似， 我们得到

$$\frac{DPL}{TPL}=\frac{1-\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}{1-2F+\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}$$

$$\frac{DPL}{TPL}=\frac{1-\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}{1-2F+\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}}$$

L 和

$$\theta_{TBBC}=\sqrt{1-\frac{4F(1-F)DOTBBC}{DOTBBC+TOBBC}}$$

$$\frac{DPL}{TPL} = \frac{2F * DOTBBC}{TOBBC + (1-2F)DOTBBC + (DOTBBC + TOBBC)\theta_{TBBC}}$$

泰勒扩展， 我们有

$$DPL = \frac{TPL * F * DOTBBC}{TOTBBC + (1-F)^2 DOTBBC}$$

使用以下公式获取接收 TBBC 的流动性通证销毁换得

$$DOTBBC = TOTBBC\left(1 - \left(1 - \frac{DPL}{TPL1}\right)^{1/F}\right)$$

Taylor 扩展得到

$$DOTBBC = TOTBBC\left(\frac{1}{F}\frac{DPL}{TPL} + \left(1 - \frac{1}{F}\right)\left(\frac{DPL}{TPL}\right)^2\right)$$

平台通证将收到 Powerswap 合约的 1/6 交易费用，CBBC 和 SPO 合约的 1/3 交易费用将最终全部发送到平台池。请注意，随着替代通证的交易费用转换为 TBBC 并添加到 TBBC 平台池中，TBBC 的价格将会增加。因此，平台池的流动性持有者将以更高的价格获得更多的 TBBC。

6， 挂钩通证

稳定币是加密货币市场的重要组成部分。有三种稳定币：稳定币用法定货币作为抵押品，如 USDT，USDC;使用数字资产作为抵押品的稳定硬币，如 DAI ；和稳定币使用纯算法，如 Ampleforth 和 Basis。第一类将承担大量的法律成本，而不是真正去中心化。第二类稳定币的设计中，当数字资产崩溃过快时，使用数字抵押品的稳定硬币可能会崩溃。最后，基于算法的稳定硬币没有任何价值支持，持有这些稳定硬币的人可能会遇到重大损失，而不能保底。

这里我们提供一个新的概念叫做挂钩稳定币。我们将使用交易所的现金流来支持挂钩。我们暂时计划创建四枚挂钩硬币，PBTC，PETH，PUSD 和 PGLD，分别与 BTC，ETH，USDT 和 PAXG 挂钩。 PBTC 将固定在 BTC 的万分之一， PETH 与 Eth 的千分之一挂钩， PUSD 1：1 与 USDT 挂钩， PGLD 与 PAXG 的千分之一挂钩。

挂钩稳定币的工作原理是这样的。 以 Usdt 和 Pusd 为例 。我们将创建两个智能合约。第一对是 PUSD/TBBC，第二对是 PUSD/USDT。随着 TBBC 的价值因平台智能合约的现金流而增加。这在 PUSD/TBBC、PUSD/USDT 和 TBBC/USDT 之间创造了套利机会。套利者将把 PUSD 移出 PUSD/USD，并移动到 PUSD/TBBC。因此，PUSD 将升值超过 USDT。我们开始用大量的 PUSD 和 QUSD 等量挂钩。开始时 QUSD 和 USDT 是 1:1， 当 QUSD/USDT 的价格变化超过 1.05 倍的时候，我们就重新改变供给，PUSD 的数量改变的倍数为 QUSD/USDT 的价格变化。这样 PUSD/USDT 的价格就恒定到 1 左

右。每次改变的时候，价格和时间都会记录下来。。注意当价格增加时，所有 PUSD 的数量相应增加。在价格降低时，原始账户之外的其他账户里的 PUSD 数量都会按比例减小，因此，PUSD/USDT 的价格将限制为 1/1.05 和 1。05 之间的间隔。其他稳定币的原理也一样。

我们设计类似于 Ampleforth。但是，有两个关键区别。首先是重新基础供应的不对称性。当挂钩币的价值增加时，所有 PUSD 的数量将在我们的设计中增加，这一点在 Ampleforth 设计中也是如此。然而，当挂钩币的价值减少时，原始账户之外的币的数量会相应减少。这种设计将降低恶意打压稳定币币价的动力。其次，其他稳定币没有现金流的支持。相反，我们设计中的挂钩币有智能合约的交易费支持。

有了挂钩通证，我们可以开发用数字通证为抵押的可借贷智能合约，这样我们就可以做空挂钩币所对应的通证。通过抵押借到稳定币，可以用来购买比特币或以太，用来增加杠杆，扩大收益。通过抵押借到比特币，以太或黄金的挂钩币，可以用来做空标的资产。

7， 融资

Powerswap 平台具有币/币交换、可清算牛熊证、聪期权，以及基于现金流的新挂钩稳定币的设计。稳定币可用于贷款，因为用户更喜欢其借贷价格稳定的通证。Powerswap 将是投资者各种金融需求的一站式服务。

对于衍生工具，用户将能够从比特币，以太坊和 Paxos 金币的价格变化。这将是用户第一次能够使用他们手中的任何硬币进行交易。使用 CBBC 和 SPO，他们将能够选择自己选择的杠杆。

挂钩稳定币的设计将允许用户能够借用稳定的硬币使用他们的数字资产作为抵押品，稳定币可用于贷款，因为用户更喜欢其借贷价格稳定的通证。

TBBC 的总供应量会恒定在 5000 万 TBBC，永不增加。N 次方互换平台计划筹集 150 万美元，1000 万 TBBC。其余 4000 万将用于社区奖励。融到的这笔资金将用于增加 N 次方互换智能合约的流动性，雇佣更多的程序员来改善客户体验，并吸引更多的通证在 N 次方互换平台上市。N 次方互换平台去中心化，任何人可以选择自己的角色。TBBC 还将用作投票工具，以确定该平台的未来发展。

8， 投资和回报

投资者如何参与 N 次方互换平台？投资者可以通过多种方式从 N 次方互换平台中获利。

1： 流动性挖矿，所有的 TBBC 都将打入一池子里，池子的一半通证将奖励給参与交易的投资者，两年内线性奖励完毕。所有参与交易的都可以得到奖励。两年之后剩余池子里的通证的一半又会线性释放，循环往复。

2： 购买 TBBC，并存入所有权池。投资者将收到所有衍生品交易费用的 1/3，以及 N 次方互换交易费用的 1/6。

3.增加流动性，把通证注入 N 次方互换流动性池，包括交易对和衍生品流动性池。投资者将获得交易对交易的 5/6 和衍生品交易的 2/3 费用。

4.参与者奖励：只需使用 N 次方互换对交易，并在衍生品中持仓。一年后，任何一个参与者都会收一定数量的 TBBC。

5.流动性挖矿：流动性提供商可以放弃交易费用，而是选择接收 TBBC。通过参与业主池，他将分享未来交易费用的整个平台。