NEST Protocol：一种分布式价格预言机网络

更新时间：2020.06.05　　版本号 V3.0

大部分 DeFi 协议都需要价格数据，特别像稳定币、期货等合约资产，需要价格进行清算。价格是 DeFi 的核心风险，因此本文提供的价格预言机方案，对 DeFi 的重要性毋庸置疑。

1. 价格 oracle 的挑战

目前 DeFi 常用的价格预言机，一般由“可信”节点采纳中心化交易所的价格，以数据的形式上传到链上，供 DeFi 调用。此方案存在一个根本性的问题，即价格没有进行有效验证。有些 DeFi 采用去中心化交易所的价格，但由于交易深度低，很容易被攻击。是否存在一种对价格进行直接验证的预言机，能保证价格准确、及时，且攻击成本极高？同时，该方案是分布式的，即不存在中心化的风险。总结起来为以下 5 点：

1）价格具备准确性：能真实反应市场价格

2）价格具备灵敏性：对市场价格的反应足够快

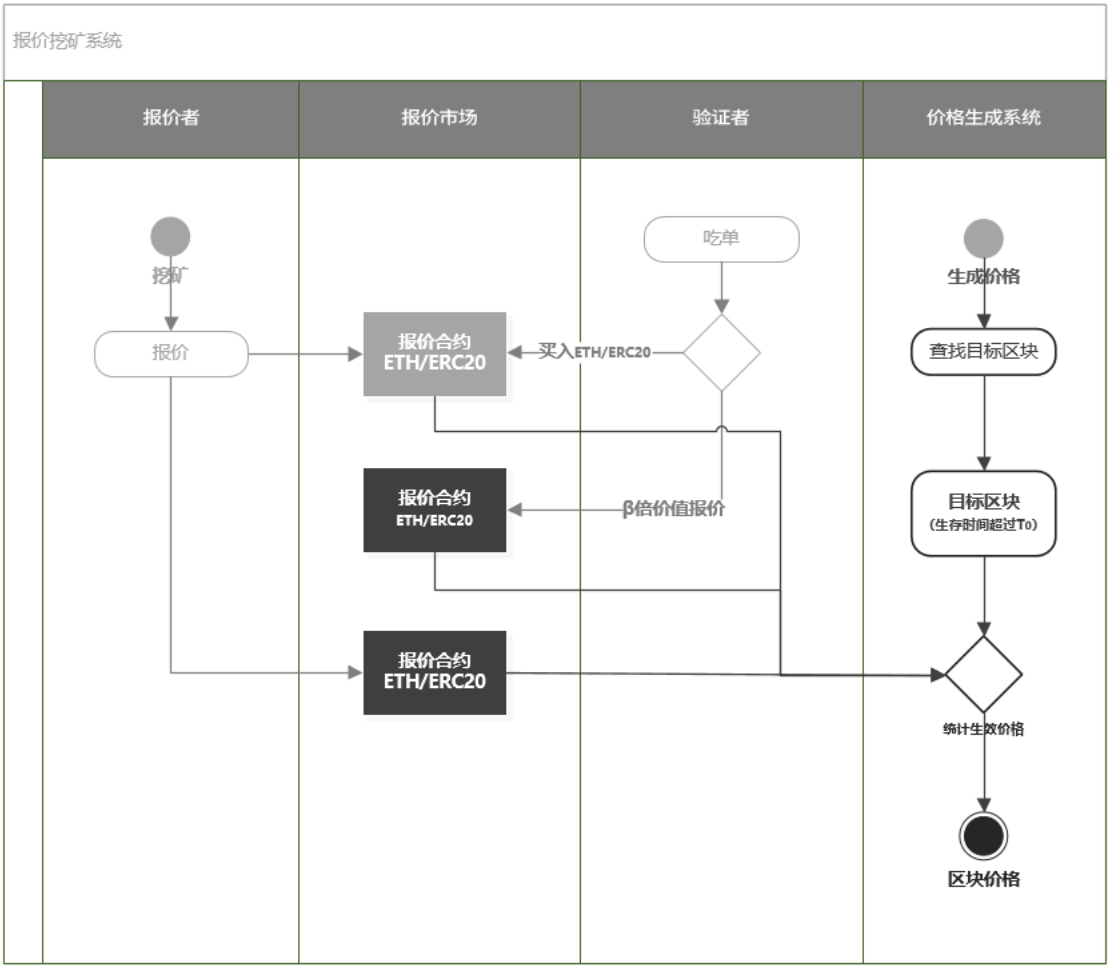
3）价格具备抗攻击性：扭曲或者影响真实价格的成本极高

4）对价格进行直接验证：且验证者是任意第三方，同时不需要审查或门槛

5）报价系统是分布式的：不需要审查或门槛，可以自由进入或退出

2. NEST 的解决方案

NEST 提供一种创造性方案，包含抵押资产报价、套利验证、价格链以及 BETA 系数等模块，组成一个完整的 NEST-Protocol。以以太坊网络为例， NEST-Protocol 的示意图如下：



1）角色定义

NEST-Protocol 中的参与者定义如下：

报价者：协议中提供报价的参与者，包含报价挖矿的矿工以及成交并报价的验证者。

A 矿工：提供报价并支付佣金获得 NEST（ERC-20Token），矿工的集合记为 O，任何人都可以成为矿工。

B 验证者：如果某个报价偏离市场价格，验证者可以以该价格与报价资产成交，从而获得收益。验证者在成交的同时，需要强制报价，该报价不用支付佣金也不参与挖矿。验证者集合记为 A，任何人都可以成为验证者。

价格调用者：调用 NEST 提供的报价并付费的合约或账户称之为价格调用者，价格调用者的集合记为 C，任何合约和账户都可以成为价格调用者，一般为 DeFi 协议。

2）报价挖矿及价格验证

以 ETH/USDT 为例，某个矿工 o 打算报价 1ETH=100USDT，他需要将报价资产 ETH 和 USDT 转入报价合约，规模为 xETH 和 100xUSDT，支付的佣金为 λxETH，按照支付的佣金规模参与挖矿，获得 NEST。整个过程完全开放，任何人都可以成为矿工，且价格和规模由其自主设定。

矿工 o 将资产和价格提交到报价合约后，任意验证者 a 认为该价格有套利空间，便可以按照 o 的报价

1ETH=100USDT，成交掉 ETH 或者 USDT。这一机制，保证了报价要么是市场上的公允价格，要么是报价者认可的等效价格（即在 o 看来，1ETH 和 100USDT 是等价的，所以无论验证者成交哪种资产都是无差异的），这一过程即价格的验证期。从本质上讲，报价矿工在验证期内提供了一个看涨看跌的双向期权，执行价格即为其报价，验证者如果发现存在套利机会就执行该期权。因此，矿工要最小化自己的成本，就需要报出在验证期内最不可能被成交的价格，这意味着矿工报价对未来价格有一定预测和发现功能。对于验证者而言，是否套利（执行期权）取决于报价与市场均衡价格的偏差大小，我们将验证者采取行动的最小偏差称之为最小套利空间，这一数值取决于验证周期的长短和交易成本。报价挖矿的过程用公式表达如下：报价者 o 报价 p，即 1ETH=pUSDT，资产规模为 xETH，则对应 USDT 数量=x*p，参与挖矿的佣金规模为 w=λ*x，验证者 a 可以以价格 p 成交 xETH 或者 x*p 的 USDT。

3）价格验证期

从报价时间算起，任何一次报价的验证期都是有限的，记为 T_0，它决定报价者承担风险的周期和价格的灵敏度。验证期过后，**没有成交的报价称之为生效报价，包含价格和报价规模（p，x）两个变量，**生效报价形成 5）所说的区块价格；而被验证者成交的报价则不被采纳，如果某个报价有一部分成交，则剩余部分也是生效报价，即（p，x′）。价格验证期过后，报价者的剩余资产以及被成交的资产可以随时取回。

验证周期影响矿工的报价成本和价格准确性，时间越长，期权成本越高，对未来价格的预测越困难，按照当前 DeFi 对价格的需求以及主流资产的波动率，将 T0 设计成 10 分钟或者 5 分钟都是合理的（可以根据以太坊网络性能和验证者的规模优化调整，最佳的当然是 1 分钟以内了）。注意，一个价格度过了验证周期，说明该价格与当前市场均衡价格之间不存在套利空间（由 T0 和交易成本决定最小套利空间的大小），从而近似代表当前价格，因此 T0 的存在并不意味着价格的延迟。

4）价格链

根据上面的约定，验证者在对某个报价者价格成交后，需要强制报一个新的价格（可以理解为，验证者销毁了一个报价，就需要留下一个新的报价）。如 a_1 与某报价者 o 的价格 p_0 成交（o 的报价规模为 x），他需要同时报一个价格 p_1 到合约内，其规模为 x_1，即需要将 x_1 个 ETH 及 x_1*p_1 个 USDT 打到合约中，但此时不必再支付佣金，也不参与挖矿。如果有套利者 a_2，与 a_1 的报价成交，他就需要报价 p_2，其规模为 x_2，如此类推，就形成了一个以 TO 为最大报价时间间隔的连续价格链：p_0—p_1—p_2...，报价资产链为 x—x_1—x_2...

5）区块价格

NEST 预言机的价格是按照区块记录的，每个区块形成一个价格，由该区块内生效的报价按照一定的算法生成，该价格称之为区块价格或者 NEST-Price。假设某一区块的生效报价为（p_1，x_1），（p_2，x_2）（p_3，x_3）…则该区块价格 $P=\sum pi*xi/\sum xi$，如果该区块没有生效报价，则沿用上一个区块价格。

6）价格序列与波动率

以太坊网络的每个区块对应一个 NEST 价格，从而形成价格序列。价格序列拥有重要意义，包含：

A. 提供均价供 DeFi 调用，包括连续 N 个区块的算术平均价格，Ps=∑P/N；或者连续 N 个区块加权平均价格 Pm=∑P*Y/∑X，其中 X=∑Xi，为上述生效报价。

B. 提供波动率指标供大部分衍生品 DeFi 调用，如连续 50 笔报价的滚动波动率，或者 DeFi 自定义的各种波动率。

C. 其他统计量。

7）抗攻击算法

如果调用 NEST 价格的 DeFi 资产规模较大，可能存在攻击者。攻击者篡改某个正常报价 p_0，将其改为 p_1，或者攻击者恶意成交，以期望价格一直不更新（因为价格一旦被成交了就无法采纳并更新）。攻击者愿意牺牲掉 P_1 与 P_0 的价差，以换来更大的收益，这样价格机制就会失效。那么，NEST 如何防范此种攻击？

我们通过提高攻击者的成本来防范攻击：

首先，价格链本身就是一种抗攻击机制，即攻击者攻击完价格后必须留下一个价格以及该价格对应的资产。这意味着攻击者攻击后，要么留下正确的价格，要么留下一个套利空间，市场上必然会有验证者来套利并修正报价。

其次，为了放大攻击者的成本，对所有验证者的报价规模进行如下安排：验证者成交的规模为 x_1，则其同时报价的规模 $x_2=\beta x1$，其中 $\beta>1$，即验证者必须以一倍以上的规模来报价。我们以 $\beta=2$ 为例，初始报价为 x=10 个 ETH，则全部成交的情况下，$x_1=20$，$x_2=40$，$x_3=80$...以此类推。攻击者要么暴露给市场极大的套利机会（规模以级数上升，这种攻击几乎是无效的），要么依据市场价格不断动用极高规模的资产进行自成交，以延缓价格被采纳的机会。

目前在 ETH 上每个区块最多可以报价 20 笔，报价也是分布式随机进入，如果假设每个区块有 1 笔报价，报价规模为 10 个 ETH，$T_0=5$ 分钟，那么通过攻击，使得 NEST 在一个小时内无价格更新，需要动用的资产规模将接近 2^12*25*10=100 万个 ETH。如果 $\beta=3$，则该数据趋近于 ETH 的数量极限，这种抗攻击性是任何中心化交易所都做不到的。

8）激励及经济

矿工通过支付 ETH 佣金，以及承担一定的价格波动风险来获得 NEST；而验证者则基于价格的偏差计算直接的获利，并承担成交报价的风险。因此对验证者而言，其成本收益相对较为清晰。对矿工而言，其报价挖矿的模型需要相应的经济学基础。

我们将矿工贡献的所有 ETH，记为 X，定期（一般按周）全部返还给 NEST 持有人。该过程构建了一

个自动分配的模型，从而使得每个 NEST 具备了内在价值，该价值在链上可证。但仅仅依靠报价挖矿者的 ETH 是不足以完成逻辑的闭环的，这就回到我们构建价格预言机的初衷：链上的价格事实对所有的 DeFi 产品都是根本需求，是 DeFi 最重要的基础设施。因此任何 DeFi 开发者或用户在调用 NEST-Price 的时候，都应该支付相应的费用，此部分收益记为 Z。因此 NEST 对应的价值记为 X+Z。而从总体上来说，获得 NEST 支付的成本为 X，即 NEST 从总体上是创造了价值的。

可以理解成 NEST 的整体价值大于整体成本，但对于每个矿工而言，它的成本是不确定的，这里就存在交易的可能，不同成本的 NEST 所有者在整体价值大于整体成本的背景下，进行买卖交易，从而达到均衡，这种均衡类似于股票市场的均衡。

NEST 系统的所有 Token 全部由挖矿产生，不预留或者预挖，产生 NEST 的所有成本全部返回给 NEST 持有人，NEST 只是用于激励。NEST 模型实现了完全的去中心化，不对任何人设置门槛，其特点与比特币类似。NEST 协议升级采用 DAO 的方式，即提案者发起，社区投票，按照一定比例通过并运行，该比例一般为 51%。

3. NEST-Price 的应用

当我们拥有了链上价格时，依赖于均衡价格的 DeFi 产品便可以设计了，在这里我们简单列举几类：

1）**均衡币**：一种通过超额抵押，以及市场套利机制形成的代表了经济均衡的数字资产，该资产代表了价格之间的均衡兑换关系。均衡币可以视为链上的计价单位，由 Token 生成合约，套利机制及反馈修正机制组成，除了其风险收益结构比较稳定外，其重要意义在于：首先是完全内生的经济单位，跟随整个公链如以太坊经济体变化而增加或减少；其次是在链上可证，且风险收益结构不同于 ETH。

2）**去中心化交易**：传统的去中心化交易以点对点报价撮合为主，此方向不正确，因为现代交易所的核心是双边拍卖，对报价双方的价格强制排序和强制成交，这涉及的计算与区块链当前共识计算的机制不匹配。有意义的去中心化交易应该是自由做市商制度的，即对于报价的双向强制接纳，且做市商可以是任意参与者，这一点在我们的报价机制里可以完美的实现。

3）**自动结算型抵押借贷**：由于拥有了链上价格，涉及到平仓或者自动结算的借贷合约，即可引用该价格完成某些约束条件的触发。

4）**期货**：一种分布式期货的模型，类似于均衡币，引入任意第三方的清算，能够放大对远期交易的交易规模，或者直接捕捉交易价格波动的收益。这在之前是不可能被设计出来的，一般意义的期货都需要中心化机构进行强制平仓等，但分布式期货不承担中心化风险。

5）**波动率产品**：基于对均衡价格的波动率设计的衍生品，用来对冲或者平滑衍生品风险，由于有链上均衡价格序列，这一产品也成为可能。

以上仅以金融领域最基础的产品为例，通过 NEST-Price 的导入，实现了完全去中心化的金融产品设计，且不同于最简单的点对点的交易。由于有全局变量的引入，整个 DeFi 便进入快车道。至于为何 DeFi 需要全局变量，这是因为金融本质是一般均衡的，而非局部均衡，不是简单的局部供给需求关系决定，需要基于全市场的套利机制完成有效定价，不是商品经济的规律。因此简单的点对点交易并不能解决根本的金融问题，而既不承担中心化风险，又具备一般均衡特征，就需要类似价格序列等全局变量了，这一变量不能中心化的引入，因此我们的预言机方案是整个去中心化金融领域的根本性基础设施。

4. NEST-Price 的引用风险

和一切金融产品或者金融服务一样，NEST-Price 不可能没有风险，这里对 NEST-Price 的引用风险做出简单的描述，当然可能存在其它未被描述到或者认知到的风险：

1）由于最小套利空间的存在，对于价差精度要求极高的金融服务，在使用 NEST-Price 时，可能会出现一些风险，在设计上需要做出一定的补偿。

2）市场套利机制的深度不够，即套利者不充分，明明存在巨大的机会，却没有人理会。这是需要市场接受度和认知度的，是行业发展深化的问题。

3）虽然无法攻击价格，但可以通过攻击 NEST 来间接攻击价格机制，比如占有 51% 以上的 NEST，然后对重要参数进行修改，使得报价机制失效。这一问题可以通过对关键参数限定来防范，同时提升 NEST 市场规模，使得 51% 攻击难以实现。

4）代码漏洞或外部重大变化的风险，如果以太坊底层代码、NEST 系统代码出现漏洞，或者外部环境发生较大变化，会对价格调用者造成影响，这可以通过链上治理及合约分叉来修正。