nest

NEST 协议: 去中心化（上）鞅网络

nestprotocol.org

2023 年 1 月 21 日

摘要

本文主要介绍并讨论了 NEST 协议中创造性的思想和主要机制。为了彻底通过去中心化的方式去解决链上交易的各种问题，我们基于区块链技术定义了一种全新的交易范式：鞅交易。并由此设计了一种革命性的交易网络：鞅交易网络。鞅交易为价值不确定的资产和收益提供了高效且低成本的交易范式，可以说鞅交易和鞅网络开创了崭新的和市场经济平行的经济理论。

目录

1 背景介绍 **3**

2 帕累托交易与市场网络 **3**

3 鞅交易与鞅网络 **4**

4 NEST 与 NEST 代币、P 资产 **6**

5 鞅信息流 **9**

6 NEST 预言机 **11**

7 鞅函数与 NESTcraft **11**

8 应用空间 **13**

9 均衡与价格 **15**

10 风险管理与时间价值 **16**

11 优势与改进空间 **17**

12 总结 **18**

A NEST Oracles **18**

B The Accuracy of the NEST Price **32**

1 背景介绍

比特币 (BTC) 创造了去中心化货币范式，形成一个全新的去中心化的货币网络，现在使用的国家和人越来越多。而以太坊 (Eth) 则创造出了去中心化资产范式：通过 Erc20 带来 DeFi 等链上应用的发展；通过 Erc721 带来了 NFT 等数字藏品的资产化与全球化，从而形成一个全新的去中心化资产网络。

但在交易领域，链上或者链下世界基本一致，都在延续匹配撮合的帕累托交易范式，也就是目前大家常说的市场机制。这一机制要求明确的买卖双方，并由法律保护交易的执行。在链上，智能合约取代了了法律这个保护者的角色，降低了交易的信任风险，链上交易成为很多人期待的新事物。但匹配撮合在链上存在更多其它的问题，比如撤单成本高，流动性差，区块打包延时等。

为了解决这些问题，Uniswap 提出了 AMM 机制，通过限制卖方行为而为提供了一定的流动性，但由于价格反馈不够及时容易被套利，以及大量 TVL 带来资源浪费。我们认为这并不是最好的链上交易解决方案。本文将在当前区块链技术下提出一种全新的交易范式——鞅交易，及其形成的去中心化交易网络-鞅网络。这一新交易范式很好的利用了区块链先确认资产存在，再确认法律关系的技术特点，通过风险共担方式为交易者提供近乎无限的流动性。这一全新的交易范式真正完全适用于链上世界，且具有革命性的意义。

2 帕累托交易与市场网络

在传统经济里，市场是由其参与者们基于各自的禀赋，进行讨价还价并完成资源财富交换和分配的一种机制。千千万万的理性参与者在同一个博弈网络里进行讨价还价，当双方效用都无法在不降低对方效用的前提下进一步改善时，便达成了帕累托均衡。我们可以把这种基于讨价还价的交易机制称之为“帕累托交易”。理论上的均衡往往很难实现或者验

证，由于真实世界需要考虑交易成本，信息对称，资产流动性等复杂的因素。均衡只是理想情况下，理论化的概念。在这样的背景下，各种中介机构就成了降低交易成本，特别是降低搜索和匹配成本的重要市场参与者。见图 1 和图 2。

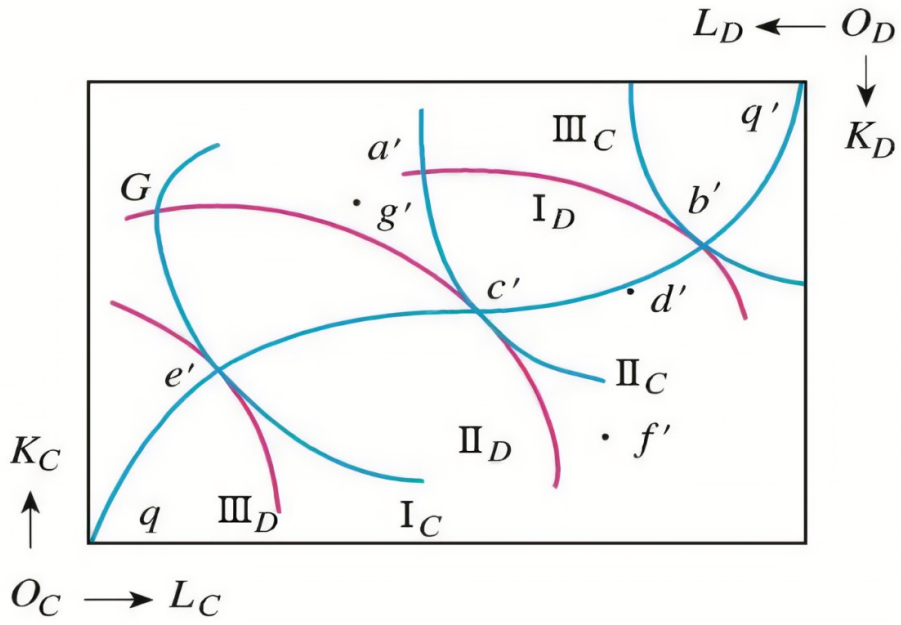


图 1: 艾奇沃斯方框

而当涉及价值不确定的商品，资产或处理不确定的收益时，这种交易范式就变得不再有效。比如，我们无法为风险资产设计一套基于效用无差异曲线切线的理论。在这种背景下，我们需要寻找新的交易模型。

3 鞅交易与鞅网络

在考虑经济活动中存在大量不确定的回报时，我们可以在帕累托交易之外定义一种新的交易范式. 这个交易范式来自于一个随机过程的概念，鞅——如果对于任何一个时间 t 和未来的时间 $t+s(s \geq 0)$，随机过程 X_t 满足 $X_t = \mathbb{E}(X_{t+s}|Xt)$，这个随机过程就被称为鞅。如果基于一个鞅，交易者在 t 时刻支付 X_t，并在 $t+s$ 时刻得到 X_{t+s}, 我们便称这一交易为鞅交易 (这里 s，≥ 0 是交易现金流流出和流入时间差，流出河流入

二者可以是无限接近的时间点，甚至是同一个现实时间点，比如智能合约一笔交易内)。如果所有参与者对随机的风险收益寻找到各种鞅并进行鞅交易，那么这些鞅和鞅交易就构成了一个鞅网络。以上定义虽然简单，但是它揭示了一个很重要的思想：面对不确定收益时，我们需要在一个是鞅的信息流下交易，才会得到公平的结果。

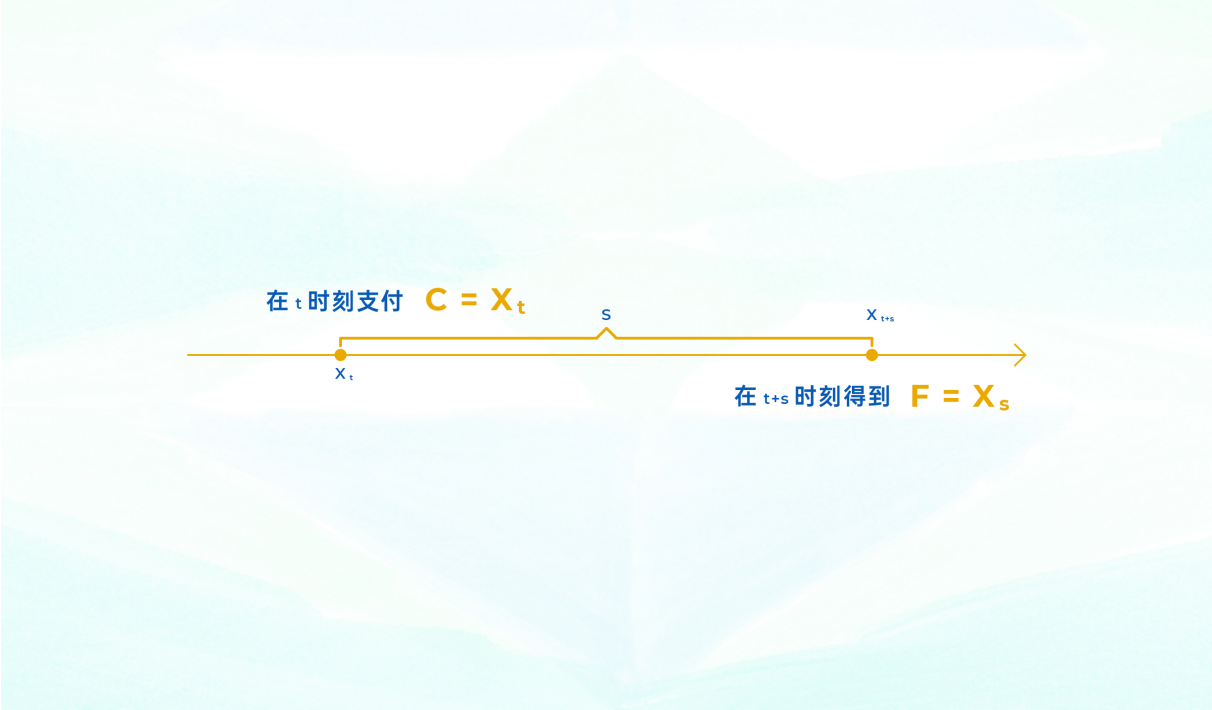


图 2: 货币单位变换鞅交易

交易的价值单位是什么其实并不重要。是苹果，橘子，美金还是 BTC，本质都一样。但本文的目的并不是想建立一套基于鞅交易的理论，而是试图建立一个基于数字货币的去中心化鞅交易网络，因此我们将交易的标的，定位为链上的数字资产。

最一般的鞅交易，可以是任何两个交易者之间的点对点交换。这种需要匹配撮合的交换在传统市场网络里更多是依靠各种中介来完成的。我们不打算引入任何中介，而是通过提供给所有交易者一个无限供给的卖方来实现。这样做的好处是为交易者将原来撮合匹配的成本完全省去了。我们这样建立的去中心化网络具备以下特征：

1. 每一笔交易都是鞅交易：$C = Xt = \mathbb{E}(X_{t+s}|Xt) = F$，其中 C 为鞅

交易的成本，F 为收益。

2. 交易的标的是链上数字资产，在本文中是指基于 ERC20 开发的 NESTtoken。比如在 t 时刻支付 X_t 个 NEST，在 $t+s$ 时刻得到 X_{t+s} 个 NEST。

3. 所有交易者都直接和一个无限供给的卖方 (ILM，Infinite Liquidity Maker) 交易，这个卖方就是 NEST 合约本身。

4. 买入的数字资产进入合约（销毁），结算的数字资产通过合约即时增发出来。

5. 我们为了让整个网络进入收敛状态，允许将鞅放宽为上鞅：$X_t \geq= \mathbb{E}(X_{t+s}|X_t)$。简单说来就是，当前支付的成本要大于未来收益的期望值。

从整体上看，该网络与市场网络具备了如下差异：

1. 无限供给：只要手上有 NEST，就不必担心因为缺少市场流动性而难以交易，交易者需要的任何基于鞅信息流的交易都可以得到满足，因此其供应是不会因为交易对手而受规模限制的。

2. 风险共担：所有持有 NEST 的人一起来承担 NEST 供给减少和增加的风险和收益，这也正好是区块链及分布式网络的特征。而在传统市场网络里，风险管理主要依靠做市商对冲，把风险转嫁给市场，这样的对冲的成本往往非常高。

这些和传统市场的差异会带来一些全新的概念和现象，作为一种社会性尝试，我们期待其价值将和 BTC/ETH 一样具有创造性和冲击力。

4 NEST 与 NEST 代币、P 资产

按照上述讨论，在去中心化鞅价值网络 NEST 里，以 NEST 作为价值单位，NEST 合约作为万能交易方，只要存在一个鞅信息流 X_t，$t \geq 0$，

任何人都可以在 t 时刻支付 X_t 个 NEST，然后在 $t+s$ 时刻得到 X_{t+1} 个 NEST。我们在类似以太坊这样的公链上开发 NEST 系统，整个 NEST 都是基于智能合约的完全去中心化协议。其实现过程如下图：

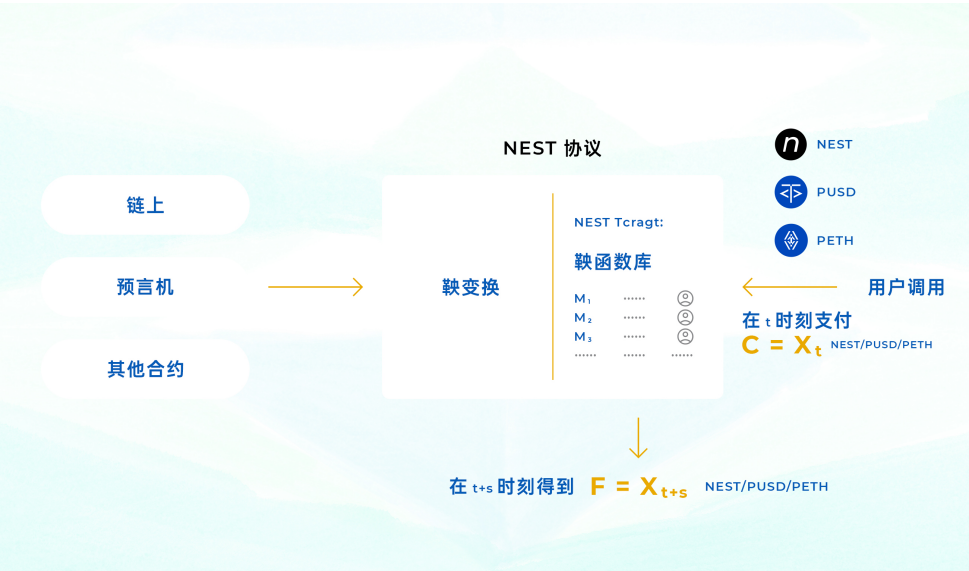


图 3: NEST 流程图

在上面的示意图中，任何给定的鞅化的信息流都可以被用于鞅交易。每个参与者独立的完成自己的交易，不必担心整个系统的安全和稳定性。而 NEST 代币最开始全部通过预言机挖矿产生，当其流通到市场后，其分布将逐渐变得分散和去中心化。

在有了大量鞅信息流情况下，一个比较自然的想法就是将不同的鞅信息流，也就是鞅交易，进行线性组合，这样就可以衍生出更多的应用。这种类似于以太坊虚拟机的设计，会极大提升 NEST 的应用范围，将 NEST 变成了一个链上的基础设施，让任何人都可以基于 NEST 设计出更多的应用，我们把它称之为鞅函数库。

其示意图如下：

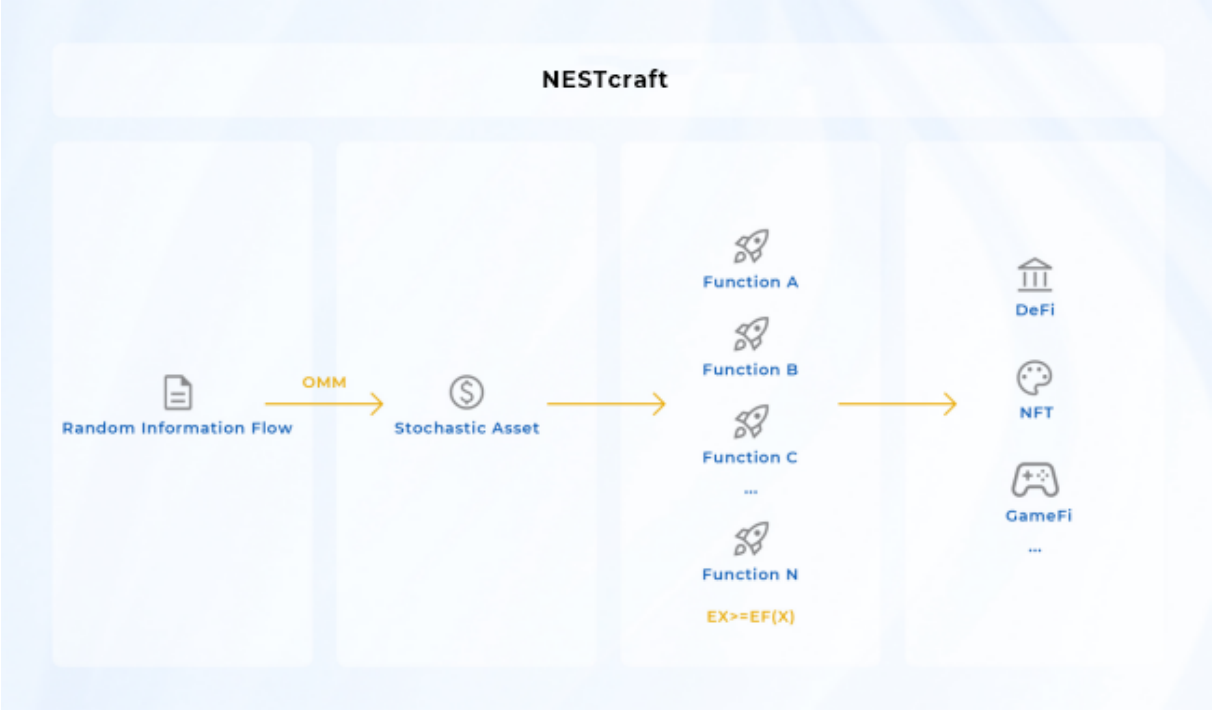


图 4: NES 函数库

在 NEST 流动性更大的时候，我们可以引入 NEST/USD 预言机，从而将交易对标的资产从 X 个 nest 变成 X 个 USD 的 nest，这样能满足许多试图基于法币本位建立对冲头寸的需求。

还有一个更具冲击力的想法则是，除了 NEST 作为鞅网络的原生价值单位外，我们还可以引入 PUSD，PETH，PBTC 等 USD/ETH/BTC 的等价资产作为鞅交换的价值单位，这样整个网络的应用将更为广阔。不过需要考虑的是以上等价资产的价值稳定性，需要提前做一些流动性头寸安排。整体上来说，NEST 将提供更为去中心化和更有防御力的稳定币或平行资产（与某些链外资产等价）。

示意图如下:

图 5: 鞅交易

5 鞅信息流

链上鞅信息流主要来自于公链本身的随机数据源及去中心化预言机提供的价格信息流或其他随机信息流，当然，任何确定的信息流本身就是鞅，只不过是 X_t 和 X_{t+s} 二者相等。

给定一个确定分布的随机信息流，我们可以进行一些函数变换得到想要的鞅信息流，我们可以称这一过程为鞅变换。理论上，我们有大量可行的鞅变换，在给定计算复杂性下都可以在智能合约里实现。然而获得有稳定分布的随机变量比较困难，这也是我们在前面的论述里提到，所以我们尽可能设计成系统收敛 (通货收敛，数量随时间下降) 的上鞅模型，这样对于一些分布虽然不稳定但仍然容易估计其上下界的随机信息源，我们可以得到一系列的上鞅信息流，用于交易的设计，只要买方能接受即可。

在以太坊 POW 时代，类似 HASH 这样的随机信息源或者随机变量源的安全性取决于矿工的分布和对应的激励设计。但到了 ETH2.0 时代，我们不再能简单使用这一类随机信息源来进行鞅变换了。而来自于信标链的一些随机源可以在受控制的条件下采用（比如规模和范围），但使用

前需要将其转化成鞅。

还有一类鞅信息流，主要是一些标的资产的有效价格，这一类信息流需要通过预言机获得。我们可以在价格是几何布朗运动 (GBM) 的假设下将价格信息流设计成一类鞅，处理他们非常方便。但现实的价格信息不可能完全符合 GBM 假设，因此需要考虑适度放宽参数的取值，将价格信息流调整成上鞅。这比较容易实现，也不完全依赖于严格的假设。

基于预言机确实能提供一个大类的鞅信息流，但预言机的去中心化设计较为困难，目前市场上绝大部分预言机是中心化的，存在节点或者组织的中心化风险。我们为此设计了基于博弈论的去中心化预言机 NEST 预言机。

我们还可以从链上其他信息源如智能合约协议等处获得一些随机信息流，并将其变换成鞅。这意味着我们的鞅信息流的来源将极其具备拓展性和开放性。

示意图如下：

图 6: 鞅变换

6 NEST 预言机

NEST 预言机是目前市场上唯一真正去中心化的预言机：给定链外一个价格流，如何设计一个去中心化博弈，使得该博弈均衡能输出一个价格流，并保证该价格流与链外价格流偏差尽可能小。NEST 预言机通过报价挖矿、双向期权、验证周期、价格链及 β 系数等模块解决了这一问题，这是一个极其完美的设计。NEST 提供的价格序列，并不改变资产价格的分布，而是接近一种离散的取样模型，这是由去中心化博弈的结构决定的，报价偏差和报价密度取决于套利市场的深度和 NEST token 的价格。总体来说，NEST 提供了一个有效的去中心化预言机，保持了价格的基本性状。

NEST 预言机是完全开放的博弈网络，理论上可以提供一切价格信息流，但从整个网络的安全性来说，用于鞅函数的价格信息流依然会被约束在少量市场较为有效的去中心化资产上，比如 BTC/ETH 等。NEST 预言机的具体实现机制及其性能特征详细请看附件。

7 鞅函数与 NESTcraft

给定的随机信息流可以进行各种函数变换，从而得到一系列的鞅，这些鞅都可以用于 NEST 的鞅交易。我们将这些用于鞅化随机信息流的函数成为鞅函数。如果我们放宽鞅的标准，选择接受更多上鞅，则会使得交易的适用范围变得更大，但是除非这些鞅对于交易者是不敏感的，否则容易减少需求，降低参与的积极性。当然，这样只是为交易者增加了多种选择，这样的设计只要有人接受，就是在原来基础上提供了更多的供给。

考虑到智能合约对资源的约束，我们会有选择性的确定一些基础变换函数簇。一般来说，多项式函数以及指数、对数函数、最值函数等在现实中使用较多，我们会基于这些较为常见的函数设计基础函数簇。每一个基础函数对应一个鞅成本，调用函数即需支付该成本。

公式如下：

- $m_1 = ax + c$：

  成本为：$C = aS_0 + c$，结算值为：$F = aS_t \exp(-\mu t) + c$。

- $m_2 = ax^2 + c$：

  成本为：$C = a{S_0}^2 + c$。结算值为：$F = a{S_t}^2 \exp(-2\mu t - \sigma^2 t) + c$。

- $m_3 = ax^{-1} + c$:

  成本为：$C = a{S_0}^{-1} + c$。结算值为：$F = a{S_t}^{-1} \exp(\mu t - \sigma^2 t) + c$。

- $m_4 = ax^{\frac{1}{2}} + c$:

  成本为：$C = a{S_0}^{\frac{1}{2}} + c$。结算值为：$F = a{S_t}^{\frac{1}{2}} \exp(-\frac{1}{2}\mu t + \frac{1}{8}\sigma^2 t) + c$。

- $m_5 = alnx + c$:

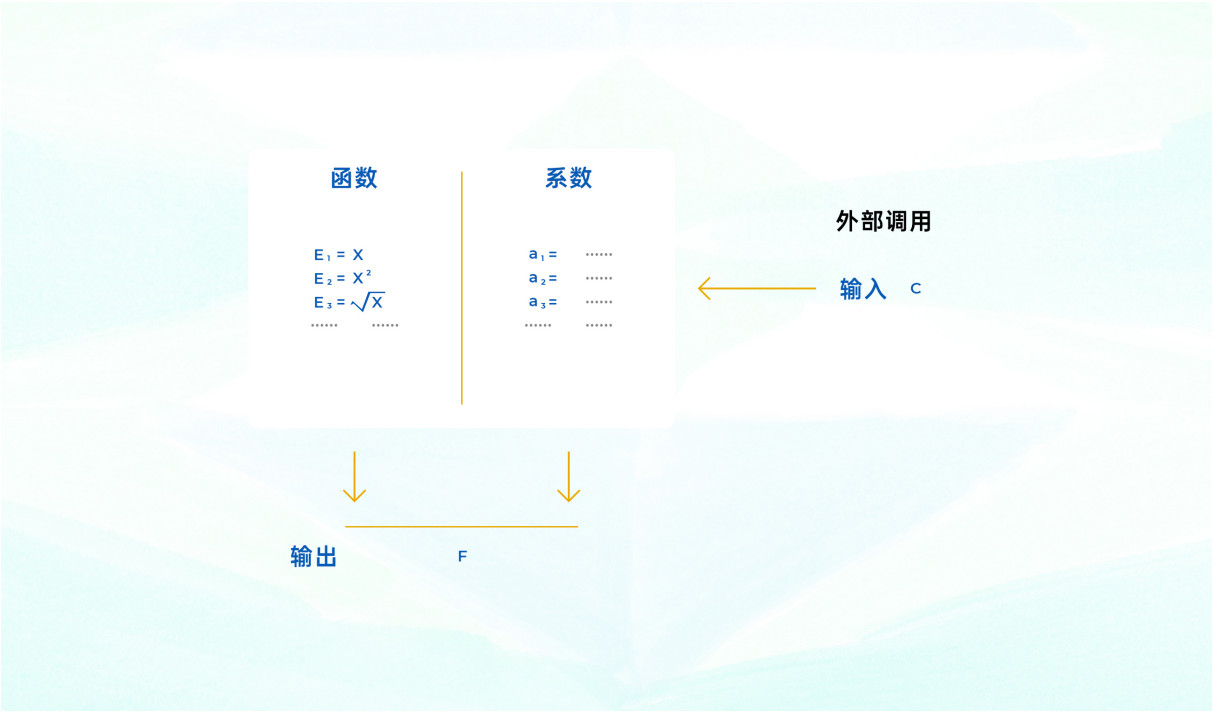
  成本为：$C = alnS_0 + c$。结算值为：$F = a(lnS_t - \mu t + \frac{1}{2}\sigma^2 t) + c$。

  当然，我们也可以将这些鞅进行线性组合，输出更为复杂的鞅：

$$F = M\Lambda^T + \lambda_0 = \lambda_0 + \lambda_1 m_1 + \lambda_2 m_2 + \lambda_3 m_3 + \lambda_4 m_4 + \lambda_5 m_5$$

其中，$\Lambda = \{\lambda_1, \lambda_2, \lambda_3, \lambda_4, \lambda_5\}^T$。

我们将这一系统称之为鞅函数库，或者 NESTcraft。如果社区愿意，可以为 NESTcraft 提供一个前端页面，链接 EVM，这样只需要写出必要的函数组合，一个简单的交互即能生成该合约，其后即可源源不断实现该表达式的鞅交易。NESTcraft 示意图如下：



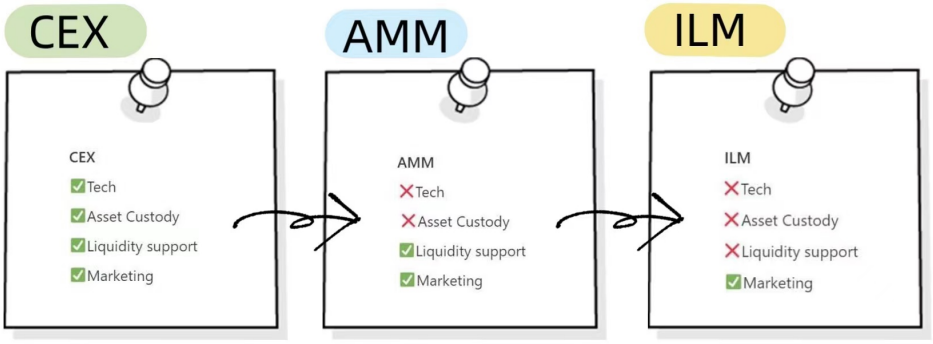
NESTcraft 可以根据链上需求持续拓展基础函数库，从而提升 NEST 的应用范围，这是 NEST 具备较大拓展性的基本特征。

8 应用空间

这一网络提供了大量的应用可能，我们可以简单列举一些：

1. 去中心化合约交易所。大家知道衍生品交易所需要解决技术支持、资产托管（风险管理）、流动性支持和市场营销，如果使用 NEST 协议，则开发一个去中心化合约交易所只需要做一个前端页面即可，因此省去了前面三样成本，只需要专注于市场营销。

   示意图：



2. 金融衍生品超市。基于 NESTcraft，可以设计大量全新的金融衍生品，如障碍期权，亚式期权、双向期权等等，一类有意思的收益诸如开方收益、平方收益、指数收益也可以很轻松的设计出来。

3. 链上、链下风险对冲。由于很多时候，链下的对冲没有供应方，因此 NEST 可以为很多链下交易提供大量的对冲交易，不受做市商的影响。而链上的交易，也可以基于 NEST 实现一键对冲，最典型的就是 Uniswap 的 LP 一键对冲，其对冲函数为——-，只需要在 NESTcraft 里写下这个公式，支付对应的成本即可一键对冲。

   设 Uniswap 的 LP 提供 (x_0, y_o) 数量的代币 (U，E)，那么价格为 $S_0 = \frac{x_0}{y_0}$，AMM 参数为 $k = x_0 y_0$。假设 (U, E) 的价格参数为 (μ, σ^2)，T 为对冲时间 (以年为单位)。

   在 t_0 时刻用户支付：$x_0(e^{\mu T} - 2e^{\frac{\mu T}{2} - \frac{\sigma^2 T}{8}} + 1)$ 单位的 NEST。则在 t，$t \in [0, T]$ 时刻结算可以得到：$\sqrt{k}(S_t/\sqrt{S-0} + \sqrt{S_0} - 2\sqrt{S_t})$ 单位的 NEST。超过 T 时刻执行得到：$\sqrt{k}(S_T/\sqrt{S-0} + \sqrt{S_0} - 2\sqrt{S_T})$ 单位的 NEST。

4. 元宇宙、GAMEFI 的经济骨架。由于 NEST 提供了一系列的鞅函数，这样围绕确定性数学关系、概率关系、随机过程的公平游戏，都可以

调用 NEST 函数来开发，从而实现不同游戏的统一价值度量，即使某个游戏开发者跑路，其核心价值依然在 NEST 里得到保留，并且可以跨越到其他基于 NEST 开发的游戏里进行整合和兑换。

5. 抽签、道具合成、彩票等。一些基于随机性的基础设计，只需要一些分布函数即可实现，这一类应用最为简单。

6. 一些其他的独特应用。一个开放网络总会带来更多可能，很多有价值的应用在基础函数存在的情况会被更有创意的提出来，我们预计会有很多超出本文描述的新应用，新事物产生。

NEST 的应用空间是在 ETH 之上做了延伸：ETH 可以处理一般的确定函数，而 NEST 的机制则处理了随机函数。因为 ETH 的代币发行是采用的确定性算法，独立于链上应用，因此其对应用端信息的反馈是不足的，而 NEST 的代币发行（增发）是跟随场景的，更接近于随时保证市场出清的货币目标。

9 均衡与价格

我们这里主要以 NESTtoken 来论述系统的均衡。一开始 NESTtoken 全部通过预言机挖矿产生，后面 NEST 流通到市场后，逐渐走向分散和去中心化。当越来越多的人参与到 NEST 网络时，交易数量增多，数额增大，结果使得交易结果逐渐符合大数定律。NEST 的期望供给值在上鞅的作用下会变得越来小，而其需求则不断扩大，这样形成一种价格持续上涨的内在机制。我们可以从下图看到，NEST 供给将围绕一根向下收敛的曲线上下波动，我们把这种波动称之为二阶矩特征，在下面风险管理里会提到，我们可以通过一些二阶矩管理降低波动的幅度。

示意图如下：

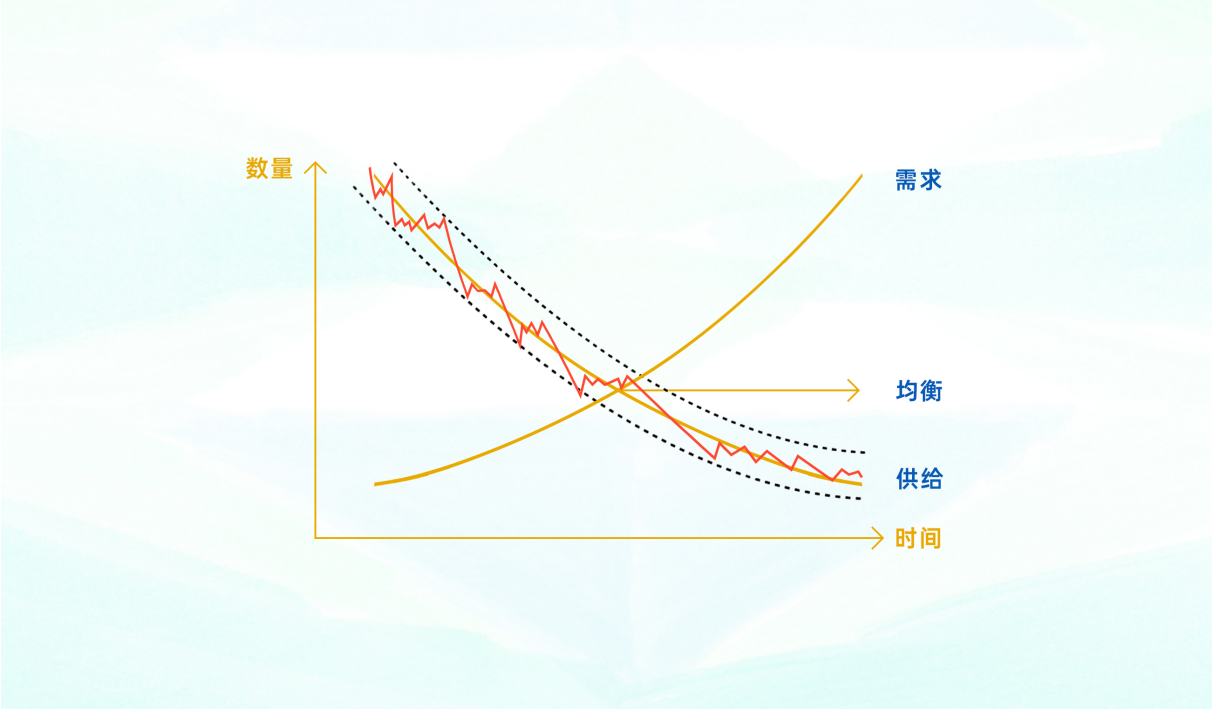


图 7: 供需均衡

10 风险管理与时间价值

对于 NEST 网络而言，虽然可以通过一些上鞅的设计使得其总供给持续减少，但总会出现一个短期的波动，诸如小概率事件，市场失灵等等，会带来短期供给围绕期望值波动。为了降低波动的幅度，特别是应对极端变化，我们可以进行二阶矩管理，一般的思路有：

1. 动态的鞅参数
2. 截口管理
3. 规模抑制
4. 某些应用设计自动“涨价”算法

在 NEST 网络里，我们也可以设计一种时间价值，从而控制网络的整体发展，并创造一类链上收益源。这种设计不困难，比如让系统为用户每年提供一定的抵押 NEST 的回报，就可以产生一种竞争性的 NEST 利

率，来度量持有 NEST 的意愿。这一设计极为开放，可以从规模、收益率、时间周期等变量上自由设置，可以在 NEST 持有足够分散后，衍生出更多金融应用。

11 优势与改进空间

通过上述描述，NEST 作为一种去中心化的（上）鞅网络，它提供了实现不同于市场网络的全新范式，这种范式具备如下优势：

1. 作为一种去中心化的价值网络，它提供了不同于市场网络的交易和风险管理范式，能更简洁和低成成本的应对风险资产或者不确定收益的交易，包括能够提供近乎无限的流动性、无需撮合匹配、没有信息搜寻成本。

2. 作为新一代的 DEFI 基础设施，不需要提供 TVL，不会造成资源浪费，也没有对应的交易滑点，跨链成本更低（不用复制 TVL）。

3. 作为一种开放的可编程的网络，能够为更多的应用场景提供服务，具备极大的拓展性。

4. 其供给因为上鞅的缘故长期走向通缩，因此具备内在的价格上涨动力。

5. 当网络参与者持币足够分散时，越来越多的交易实现均衡，会形成一种近乎保证市场时刻出清的完美货币形态。

当然，NEST 网络也有很多可以持续改进的地方，比如摄入更多的信息流，提升博弈网络的安全性更灵活的二阶矩管理以及更低成本的鞅函数簇等等。在性能上，NEST 的链上效率有一定的提高空间。

12 总结

基于鞅交易和鞅网络的概念我们设计并发布了 NEST 协议。NEST 协议包括三个主要模块：NEST 预言机，NEST 资产，以及 NESTcratft。NEST 预言机为链上世界提供了通过完全去中心化博弈获得的价格。NEST 资产通过信息资产化产生，为报价者们提供了奖励，并为 NEST 上的鞅交易提供了货币单位。其内在的成本机制保证系统供给量收敛，有着内在的价格上涨逻辑, 而其价值的收益和风险由所以持有者共同承担。NESTcraft 则将各种链上随机源转换为丰富的鞅函数库，通过 ILM(Infinite Liquidity Maker) 机制为投资者解决了流动性不足的问题，并提供了多种多样可自定义的鞅交易选择，为鞅交易网络的建立提供了基础条件。NEST 协议可以用于：去中心化合约交易所，金融衍生品超市，链上、链下风险对冲，元宇宙，GAMEFI 的经济骨架，抽签，道具合成，彩票以及一些其他的独特应用。通过鞅交易的设计，NEST 协议解决了传统的帕累托交易难以解决的随机资产和收益的交易难题，并基于区块链技术的特点，大幅提高了链上交易的效率，降低了成本。

附录 A NEST Oracles

1 Introduction: The Challenge of Price Oracles

Price oracles commonly used in the DeFi industry generally reflect the asset price of centralized exchanges by "trusted" nodes, where the price is "uploaded" to the chain for usage by DeFi protocols. There is a basic problem with verifying such price data. Some DeFi projects utilize price data gathered from decentralized exchanges, however, because transaction volume is minimal, the pricing data is readily manipulated and vulnerable to attack. This creates a clear market need for an Oracle solution that directly checks the pricing to ensure the information is correct and timely but is also prohibitively expensive to attack. This system should also be decentralized to reduce the risks of centralization.

Oracle price data must meet the following key requirements:

- Accuracy: The price data on the oracle should truly reflect the market price.
- Price sensitivity: The price data on the oracle should react fast enough to market movements.
- Attack resistance: The cost of distorting or affecting the real price is extremely high for any attackers.
- Direct verification: The verifier can be any third party, and no centralized review or threshold is required.
- Distributed quotation system: no centralized review or threshold is required, and anyone can freely join or leave at any place and at any time.

2 NEST Solution

NEST provides a creative solution, including collateral asset quotation, arbitrage verification, price chain, beta coefficients, and other modules to form a complete NEST protocol. Taking the Ethereum network as an example, the schematic dia-

gram of the NEST protocol is described in Figure 1 below and we will discuss the details in the following subsections.

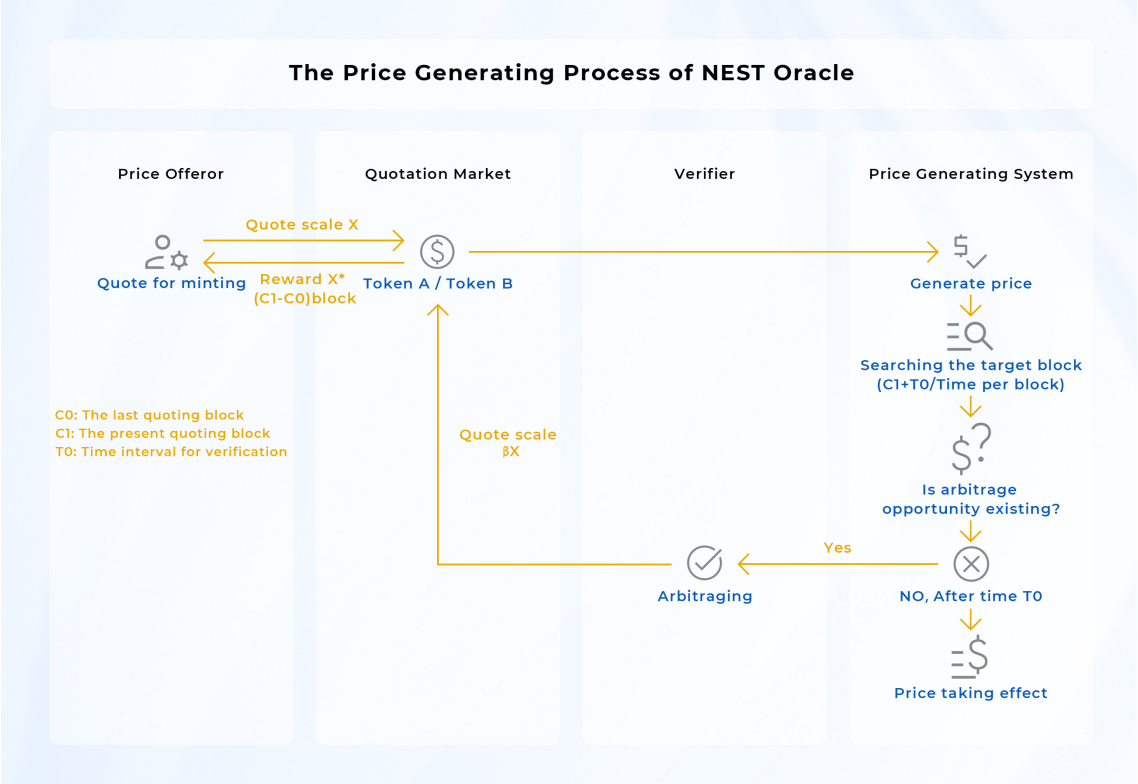


Figure 1: Diagram of NEST Protocol

2.1 Price Model of NEST Oracle

NEST oracle is the only truly decentralized oracle on the market today: given an off-chain price stream, how to design a decentralized game such that the game equilibrium can output a price stream with the smallest possible deviation from the off-chain price stream. NEST oracle solves this problem with quotation mining, two-way options, validation cycles, price chains and β factors. NEST provides a price sequence that does not change the distribution of asset prices but approaches a discrete sampling model, which is determined by the structure of the decentralized game, where the quote deviation and quotation density depend on the depth of the

arbitrage market and the price of the NEST token. Overall, NEST provides an efficient decentralized oracle that maintains the fundamental traits of asset prices. In practice, we tend to use highly efficient market prices, and hence choose the most liquid underlying assets such as BTC and ETH, etc.

The basic price model follows the Geometric Brownian Motion (GBM) model. Considering the characteristics of prices deviation and discrete time, we correct the prices using the k-factor as follows,

$$k = \max(\frac{|p_2 - p_1|}{p_1}, 0.002) + \sqrt{t} \cdot \max(\sigma, \sigma_0) \tag{1}$$

where p_2 and p_1 represent the current and previous prices respectively, t, measured by second, represents the difference between the time transaction happens and the time p_2 becomes effective. Furthermore, σ the instantaneous volatility follows

$$\sigma = \frac{|p_2 - p_1|}{p_1\sqrt{T}}$$

where T represents the time-lapse between p_1 and p_2 becoming effective. σ_0 denotes the regular volatility, set by the protocol (generally different values for different financial products).

The correct procedure follows

- when it comes to a call option, the long price is $(1 + k)p$ while the short price is $\frac{p}{1+k}$
- when it comes to a put option, the long price is $\frac{p}{1+k}$ while the short price is $(1 + k)p$

where p represents the base price.

Since price is verified on-chain, NEST has provided an open and transparent ecosystem for everyone. One of the most important points is openness: anyone can start a price information flow and motivate price providers to mint any kind of token. For example, a project can set up the price pair of its own token to USDT, and motivate others to provide price information by rewarding them with this token. This would help any project to expand the number of minters in its ecosystem.

2.2 Roles of NEST Protocol Actors

Participants in the NEST protocol are as below:

- Price Makers: The participants who submit price quotations to the protocol. This includes miners who quote prices for mining and verifiers who complete the transaction and quotation.
  - Miners: Providing quotations to receive NEST (ERC-20 Token). Miners are denoted as O, and anyone can become a miner.
  - Verifiers: If the quotation price deviates from the market price, the verifier can trade a quoted asset at the quoted price to earn revenue. The verifier needs to "force" a quotation at the time of the transaction and does not need to pay a commission nor participate in mining. Verifiers are denoted as A, and anyone can become a verifier.
- Price Callers: The contract or account that "calls" the NEST protocol quotations and pays the fee is called a price caller. Price callers are denoted as C. Any contract or account can become a price caller, but this will generally be reserved for other DeFi protocols and institutions.

2.3 Quotation Mining and Price Verification

One can easily start a quotation channel via NEST protocol where he/she needs to set the quotation pairs (one channel allows multiple pairs), quotation scale, commission fee, the token and scale of the collateral, etc.

Taking ETH/USDT as an example, miner O intends to quote a price of 1 ETH = 100 USDT. At this time, miner O needs to input the collateral NEST and the quoted assets, ETH and USDT, into the quoted contract. The scale is x ETH and $100x$ USDT, and the paid commission is λx ETH. Miners participate in mining based on a commission scale to earn NEST. The whole process is completely open and transparent, that is, anyone can assume the role of O, and the price and scale are set independently.

After miner O submits the collateral, assets and price to the quoted contract, verifier A believes that the price presents an arbitrage opportunity, and can trade either ETH or USDT at the quote from miner O, which is 1 ETH = 100 USDT. This mechanism ensures that the maker's price is either the fair price in the market or the equivalent price of the two assets recognized by himself/herself. In the view of miner O, 1 ETH and 100 USDT are equivalent, so it does not matter which asset the verifier trades. This process is the price verification period.

Essentially, miners, through quoting, also provide either bullish or bearish two-way options during the verification period, with the strike price as its quoted price. Verifiers, then, execute this option if they find that there is an arbitrage opportunity. Therefore, if miners want to minimize their costs, they need to report the price that is least likely to be traded during the verification period. This allows the miner's quotation has a certain ability to forecast future prices. For the verifier, whether they choose to arbitrage (execute) depends on the difference between the quote and market price. We call the minimum difference the verifier will take action on the "minimum arbitrage space"; this value also depends on the length of the verification period and the transaction cost.

The formula for quote mining is expressed by the following formula: Maker O quotes p, that is, 1 ETH = p USDT, the asset scale is x ETH, so the corresponding USDT quantity = $x \cdot p$. The commission scale for participating in mining is $w = \lambda \cdot p$, and verifier A can use the price p to trade $x \cdot p$ USDT for x ETH.

2.4 Price Verification Period

Opened quotes have an allotted period of time attached, denoted as T_0. This time determines the period of risk the maker takes and the price sensitivity. After the verification period, quotations that have not been traded are called "effective quotations" which includes two variables - price and quotation scale (p, x). Effective quotations form the block price mentioned in section 2.6. However, the price quoted that is already traded by the verifier will not be adopted. If a certain quoted price

is partially traded, the remaining part is also an effective quote, i.e. (p, x'). After the price verification period is complete, the maker's remaining assets will be made available to withdraw at any time.

The verification cycle affects miners, quotation costs, and price accuracy. The longer the time, the higher the option cost, and the more difficult it is to predict the future price. Judging by current DeFi market demands for price data and the volatility of mainstream assets, a reasonably set T_0 is between 5 to 10 minutes (pending adjustments and optimization based on the ETH network capacity and verifiers, scale, with the optimal time being within 1 minute). Note that if a price has passed the verification cycle, it indicates that there is no arbitrage space between this price and the current market equilibrium price (the minimum arbitrage space is determined by T_0 and transaction costs), thus representing the approximate current price; the existence of T_0 does not mean a delay in prices.

2.5 Price Chain

According to the above agreement, the verifier needs to force a new price after accepting the transaction of a maker. To put it simply, the verifier needs to offer a new price to close the opening left by the rejected price. For example, verifier A_1 and maker O accept the transaction with the price of p_0 (the maker O's quotation scale is x_0 with the collateral scale of y_0), so A_1 needs to quote a price p_1 to the contract immediately with the asset scale of x_1, and transfer x_1 ETH and $x_1 \cdot p_1$ USDT together with the collateral y_1 to the contract. Commission and mining participation rewards are not paid at this time. If verifier A_2 accepts the transaction with A_1, A_2 needs to quote the price p_2 with the asset scale of x_2 and the collateral scale of y_2. A continuous price chain with T_0 as the maximum quotation interval is formed:

$$p_0 \to p_1 \to p_2 \cdots$$

the quoted asset chain is

$$x_0 \to x_1 \to x_2 \cdots$$

and the collateral asset chain is

$$y_0 \to y_1 \to y_2 \cdots .$$

2.6 Block Price

The NEST Oracle determined price is recorded on the blockchain, with each block recording a price. The effective price in the block is generated by a certain algorithm. The price is called the block price or NEST-Price. Assuming the effective quotation of a block is (p_1, x_1), (p_2, x_2), $(p_3, x_3) \cdots$ the block price is

$$P = \frac{\sum_{i=1}^{M} p_i \cdot x_i}{\sum_{i=1}^{M} x_i}$$

where M represents the number of effective quotations in this block. If there are no effective quotations in a current block, the price of the most recent block will be used.

2.7 Price Sequence and Volatility

Each block of the Ethereum network corresponds to a price on NEST, thereby forming a price sequence. The price sequence has important functions, including:

- Provide an average price for DeFi operations, including the arithmetic average price of N consecutive blocks $j = 1, \cdots, N$

  $$P_s = \frac{\sum_{j=1}^{N} P_j}{N} ,$$

  or the weighted average price of N consecutive blocks:

  $$P_m = \frac{\sum_{j=1}^{N} P_j \cdot Y_j}{\sum_{j=1}^{N} Y_j}$$

  where $Y_j = \sum_{i=1}^{M_j} x_{ij}$ represents the total asset scale of all effective quotations in block j and M_j the number of effective quotations in block j.

- Provide volatility indicators for most DeFi derivatives, such as rolling volatility of 50 consecutive quotes, or various other volatility indicators customized for DeFi purposes.

- Other statistics.

2.8 Attack-Resistant Algorithm

If the scale of DeFi assets calling the NEST-Price is very large, there is a huge opportunity for attacks. An attacker may tamper with a normal quote, p_0, and changed it to p_1, or the attacker may trade maliciously, hoping that the price will not be updated (as prices cannot be adopted and updated once the price has been traded). With attackers willing to sacrifice the price difference between P_1 and P_0 in exchange for greater profits, the price-setting mechanism becomes invalid. So how does NEST prevent these kinds of attacks?

By increasing the cost for attackers. First, the price chain itself is an attack-resistant mechanism: attackers must offer an alternative price and the corresponding assets at this price after attacking the price. After the attack, attackers must either offer the same "correct" price or leave an arbitrage opportunity. There must be a verifier in the market to recognize the arbitrage opportunity and revise the quote.

Secondly, in order to amplify the cost to the attacker, we arrange every verifier's quotation asset scale as follows: the scale of the verifier's transaction is x_1, and the scale of the simultaneous quotation is $x_2 = \beta x_1$ with $\beta > 1$. Therefore, the verifier must quote at a price more than double the scale of the quotation. Notice that we only allow this amplification for quotation asset up to 4-round verification. On the other hand, we also enlarge the collateral asset in the same way but without 4-round limitation. As an example of $\beta = 2$, the quoted asset chain and the collateral asset chain in section 2.5 follow as

$$x_0 \to \beta x_0 \to \beta^2 x_0 \to \beta^3 x_0 \to \beta^4 x_0 \to \beta^4 x_0 \to \cdots \to \beta^4 x_0 \to \cdots$$

and

$$y_0 \to \beta y_0 \to \beta^2 y_0 \to \beta^3 y_0 \to \beta^4 y_0 \to \beta^5 y_0 \to \cdots \to \beta^n y_0 \to \cdots$$

respectively.

Attackers either offer huge arbitrage opportunities to the market (the scale increases by levels, making this kind of attack almost ineffective) or must continue to use an extremely high volume of assets to self-deal based on the market price to delay the opportunity for price adoption. For example, assuming that the verification period is set as $T_0 = 5$ minutes, if miner O makes one quotation at present, to prohibit this quotation become the effective price in coming 1 hour, the attacker needs at least $6144y_0$ collateral asset and $32x_0$ each quoted asset. Furthermore, the attacker needs at least $12284y_0$ collateral asset and $300x_0$ each quoted asset to paralyze NEST quotation for 1 hour if the miners make the quotation every 5 minutes in the coming 1 hour. Notice that the quotation channel zero set $y_0 = 100,000$ NEST. Only focusing on the collateral asset, 1,228,400,000 NEST makes this attack plan almost impossible to fulfill considering that the total circulation of NEST is not over 3 billion. This kind of attack-resistant ability cannot be achieved by centralized exchanges.

2.9 Incentives and Economics

Miners obtain NEST Tokens through paying ETH commissions and taking certain price fluctuation risks. Verifiers earn profits directly based on the calculation of price deviation while also bearing the risk of the quoted transaction, so for the verifiers, the cost/benefit is relatively clear. For the miners, the model of quotation mining requires a corresponding economic foundation. ETH contributed by miners is denoted as X, and will be returned back to NEST holders regularly, usually on a weekly basis. This process builds an automatic distribution model, so that each NEST Token has intrinsic value, which is verifiable on-chain. Only relying on the quotation miner's ETH is not enough to complete the logical closed-loop system, which returns to the original intention of constructing the price oracle. The fact that the on-chain price is a core demand for all DeFi products means it is often regarded as the most integral part of DeFi infrastructure. DeFi developers and users should pay the corresponding fees when using NEST-Price denoted as Z. Therefore, the

value of NEST is denoted as X+Z. In general, the cost of obtaining NEST is X and NEST creates value for NEST holders throughout the whole ecosystem. The value of NEST is typically greater than the overall cost. For each miner, the cost is uncertain, so there exists a trading possibility. Under the assumption that the overall value is greater than the overall cost, NEST holders with different costs can compete with each other to achieve organic equilibrium, which is similar to the equilibrium found in the stock market. All tokens in the entire NEST ecosystem are generated by mining, and there is no reservation or pre-mining. All costs of generating NEST will be returned to NEST holders, and NEST is only used for incentives. The NEST model achieves complete decentralization, as anyone can join the system, and its characteristics are similar to that of Bitcoin. The NEST protocol upgrades the DAO method, where adjustments need to be first proposed and then approved by a 51% majority via community voting before being implemented.

2.10 The New Characteristics of Latest NEST

The most recent version of NEST is NEST 4.4. The new characteristics of NEST 4.4 compare to the early versions are:

- Improved techniques: allow price offering for multiple assets, in one smart contract, one can start the price information flow for more than ten different assets. In this way, gas fee can be saved handsomely. The efficiency of uploading information is much better.

- Improved economic models: cancel the quotation commission fee. Calling quotation price from NEST is also free now. In the meantime, the mint production is reduced to 1/6 compared to before. The circulation increases slower, slower than 3% per year. In the long run, these changes will guarantee the increasing value of NEST. The total number of NEST will not exceeding 3,000,000,000 (3 billion). The threshold of price information offering is lower, only 0.01 ETH and assets of the same value is needed to be deposited.

3 The Application of NEST-Price

Although NEST focuses on on-chain price data, it can also design price-equilibrium products including the following:

(1). Equilibrium Token: A digital asset that represents economic equilibrium formed by excess collateralization and market arbitrage mechanisms. This can also represent the equilibrium exchange relationship between prices. Equilibrium tokens can be regarded as on-chain valuation units composed of token generation contracts, arbitrage mechanisms, and feedback correction mechanisms. The important significance of equilibrium tokens is in their unique foundation, which increases or decreases following the changes of the entire public chain, such as the Ethereum blockchain. Secondly, they can be proven on chain with a risk-reward structure different from ETH.

(2). Decentralized Transactions: Traditional decentralized transactions are mainly based on peer-to-peer quotation matching. This is fundamentally flawed, as the core of modern exchanges is bilateral auctions, which have the characteristics of forced ordering and forced transactions at prices for both parties. This type of feature involves calculation characteristics, which do not match the current serial queuing mechanisms of the blockchain. A meaningful decentralized transaction would be a market-making system, that is, a two-way forced acceptance of quotations, which can be achieved perfectly with the NEST quotation mechanism.

(3). Automatic Settlement Mortgage Loan: Due to on-chain data, a loan contract that involves liquidation or automatic settlements can quote prices and automatically trigger restrictions, so that loan behavior is not limited to the options of contract structures.

(4). Futures: A distributed futures model is similar to an equilibrium token currency, but it also introduces arbitrage from any third party. This can am-

plify the transaction scale of forward transactions or directly earn revenue from transaction price fluctuations. This was impossible to design before now. All general futures require a centralized institution to perform forced liquidations, but distributed futures do not bear the risk of centralization.

(5). Volatility Products: Derivatives based on the volatility of equilibrium prices are used to hedge or smooth derivatives risks due to the on-chain equilibrium price sequence.

The above only takes the most basic products in finance as an example. Through using NEST-Price, a complete spectrum of decentralized financial products that differ from previous basic peer-to-peer transactions can be designed. Due to the introduction of global variables, the entire DeFi ecosystem is set to enter a new era. As for why DeFi needs global variables, this is because of the nature of finance and general equilibriums, rather than partial equilibriums. A simple local supply and demand relationship is insufficient; there needs to be an effective and complete pricing system based on the whole market arbitrage mechanism. This is not possible for the commodity economy, as simple peer-to-peer transactions cannot solve fundamental financial problems. However, in order not to bear the risk of centralization but also to have generally equal characteristics, global variables like "price" are needed. This variable cannot be introduced centrally, so our oracle scheme is a fundamental part of the infrastructure underpinning the entire field of decentralized finance.

4 Quotation Risk of NEST-Price

As with all financial products and services, NEST-Price is not without risk. Whilst many risks are unable to be described or recognized due to their inherently personal nature, here is a brief description of the quotation risk of NEST-Price:

(1). Due to the existence of the minimum arbitrage, there may be some risks when using NEST-Price for financial services that require extremely high price accuracy. This should be taken into account when designing.

(2). The market arbitrage mechanism is not aggressive enough, which is reflected in inadequate efforts by arbitrageurs. When there is a huge opportunity for arbitrage, no one notices it. This requires higher market acceptance and recognition as the industry develops further.

(3). Although the price cannot be attacked directly, the price mechanism can be attacked indirectly through attacks on NEST. For example, attackers can take more than 51% of the NEST tokens and then modify important parameters to invalidate the quotation mechanism. This problem can be prevented by limiting key parameters while increasing the NEST market's size, making 51% of attacks more difficult to achieve.

(4). The risk of code vulnerabilities or significant external changes. If there are vulnerabilities in the underlying Ethereum code, the NEST system code, or a significant change in the external environment, the price caller will be affected. This can be corrected through on-chain governance and contract forks.

附录 B　The Accuracy of the NEST Price

The Accuracy of the NEST Price

NEST Research Academy

September 2020

ABSTRACT

This short article develops a model to estimate the difference between the NEST price and a source price, e.g. price from an exchange. Under plausible assumptions, we show that the difference can be as small as 0.003 when volatility is small. It can even be lower if the transaction cost in the blockchain gets lower.

1. Model Setup

A *price-provider* is an individual who inputs a price into the NEST system and waits for a certain number of blocks passing to be verified by other individuals. The operation is equivalent to write an American type call and put option that anyone else can exercise it by using the input price as the exercise price. Thus, the price-provider shall minimize the value of this option by carefully choosing an input price. Precisely, the price-provider's objective problem is

$$P^* = \arg\min_P \left(\max_\tau E^Q[e^{-r\tau}|S_\tau - P|] \right), \tag{1}$$

where $\tau \leq T_0$ is a stopping time and T_0 is a fixed time horizon[1] , P is the input price decided by the price-provider. In other words, the price-provider has to minimize the value of one American type option by choosing an appropriate exercise price P. Here asset price $S_t, t \geq 0$ shall be referred to the price in an exchange at time t. Thus, the market is complete and we price the derivative in a risk-neutral framework by taking the expectation under the risk-neutral probability Q.

Denote the solution to the above problem by $P^* = P(S_0; \sigma)$, where σ is the volatility of the source price sequence S_t. Noting that the price-provider inputs a price optimally based on all of his information from a centralized market and/or from the decentralized world.

1.1 Arbitrageur

The price-provider writes an American option when he inputs a price K. It seems that anybody can exercise the option without any cost. However, the NEST requires that the one (arbitrageur) who exercises the derivative must input another price and lock in as much as β times the original asset requirement. In other words, to exercise one option, the arbitrageur

[1]For the NEST system, the time horizon T_0 actually is random because the time interval between two successive Ethereum blocks is. The framework in this note can be extended to study this case.

has to write β units of the same type of American options, where $\beta > 1$ is a specific multiplier.

One arbitrageur who wishes to make profit from the derivative can construct (sell) a portfolio in the outside market that replicates the derivative. Then the arbitrageur can make a risk-free profit the same as the value of the derivative. However, there is risk that the arbitrageur can not obtain the opportunity to exercise the derivative because it is competitive to take the arbitrage. Therefore, instead of making the risk-free profit, a realistic strategy is to make a *quick* profit in the sense of statistic arbitrage as follows.

The arbitrageur does nothing but waits until the difference between the outside asset price and the input price P is sufficiently large. Then he exercises the option and buys or sells in the exchange simultaneously to make money without any risk. Such an opportunity may not be available for all time, but in long time there are many chances. So statistically the arbitrageur can make money.

We calculate the following objective function for the arbitrageur:

$$\max_{\tau} E[(|S_\tau - P| - A)1_{|S_\tau - P| > A, \tau < T_0}], \tag{2}$$

where A represents all costs of the transaction, including Ethereum transaction fee and the value of the derivative multiplied by β. The stopping time τ in the above indicates that the arbitrageur will wait for the best time to take the arbitrage. However, considering the competitive environment, most likely, the profit is taken when the first time a target is reached. So the objective function turns to be

$$E[(|S_\eta - P| - A)1_{\eta \leq T_0}], \tag{3}$$

where $\eta = \inf\{t : |S_t - P| - A > \epsilon\}$ and ϵ is the minimum target profit of the arbitrageur. Along with the arbitrage-taking method (3), the corresponding loss (or the cost of inputing a price) of the price-provider is

$$E(|S_\eta - P|1_{\eta \leq T}).$$

The price-provider shall minimize the cost by choosing an appropriate K. That is, the objective function of the price-provider is

$$\min_P E[|S_\eta - P|1_{\eta \leq T_0}].$$

In fact, we should price it in a risk-neutral sense:

$$V^*(0) = \min_P E^Q[e^{-r\eta}|S_\eta - P|1_{\eta \leq T_0}],$$

where r is the risk-free interest rate. It yields that the price-provider can construct a portfolio in the outside market to hedge this derivative, so that his loss is a deterministic value same as V^*.

2. A Solution of the Model

Given the design of the NEST, we let

$$A = \beta V^*(\eta),$$

where $V^*(\eta)$ denotes value of the same derivative at time η. We let ϵ be the transaction fee in the blockchain (the gas fee).

Aware of the way the option is exercised, the price-provider actually considers the objective problem as follows.

$$V^*(0) = \min_P E^Q[e^{-r\eta}|S_\eta - P|1_{\eta \leq T_0}] = \min_P E^Q[e^{-r\eta}(A+\epsilon)1_{\eta \leq T_0}] = \min_P E^Q[e^{-r\eta}(\beta V^*(\eta)+\epsilon)1_{\eta \leq T_0}]. \tag{4}$$

We assume that the asset price follows a Brownian motion with drift:

$$S_t = S_0 + \mu t + \sigma Z_t,$$

where Z_t is a standard Brownian motion. Then $V^*(\cdot)$ is identical at any time. The recursive formula (4) is simplified (for a stationary solution under constant state variables μ and σ)

$$V^* = \min_P E^Q[e^{-r\eta} 1_{\eta \leq T}](\beta V^* + \epsilon). \tag{5}$$

Exploiting the density function of η, the first hitting time of Brownian motion, we can evaluate the expecation in (5) and solve for V^* and P^* numerically.

Set $\mu = r = 0$, $\epsilon = 0.003$ (the gas fee of one transaction in the Ethereum divided by 10 (ETHs)), $S_0 = 1$, we obtain the following results.

For $\sigma = 0.0001,\ 0.001,\ 0.003$ per second:

$\beta = 1.5$: $V^* = 0.0030, 0.0104, 0.0327$; probability of arbitrage: 0.0726, 0.3353, 0.3765

$\beta = 2$: $V^* = 0.0003$, 0.0092, 0.0291; probability of arbitrage= 0.0792, 0.4301, 0.4755,

$\beta = 3$: $V^* = 0.0002$, 0.0074, 0.0233; probability of arbitrage= 0.0894, 0.6064, 0.6696,

where the probability of arbitrage is defined by $E^Q[1_{\eta \leq T}]$. For all of these cases, the optimal input-price $P^* = S_0 = 1$. Since S_t is assumed to be a Brownian motion without a drift, this answer is obvious.

The sensitivity analysis regarding verification during time T, probability of arbitrage, β, volatility σ are shown in Figure 1 and 2.

2.1 Difference between NEST Price and Price of Exchange

By the preceding analysis, the difference between the NEST price and the price from an exchange is bounded by $a := \beta V^* + \epsilon$. Figure 3 indicates the upper bound can be as small as 0.003. The upper bound can be decreased if the transaction (arbitrage) cost in the blockchain becomes small. Alternatively, We may increase the asset requirement of inputing

a price to decrease the relative weight of ϵ. For example, if we increase the asset requirement to 50 ETHs, the difference bound turns to be 0.002 only.

Figures

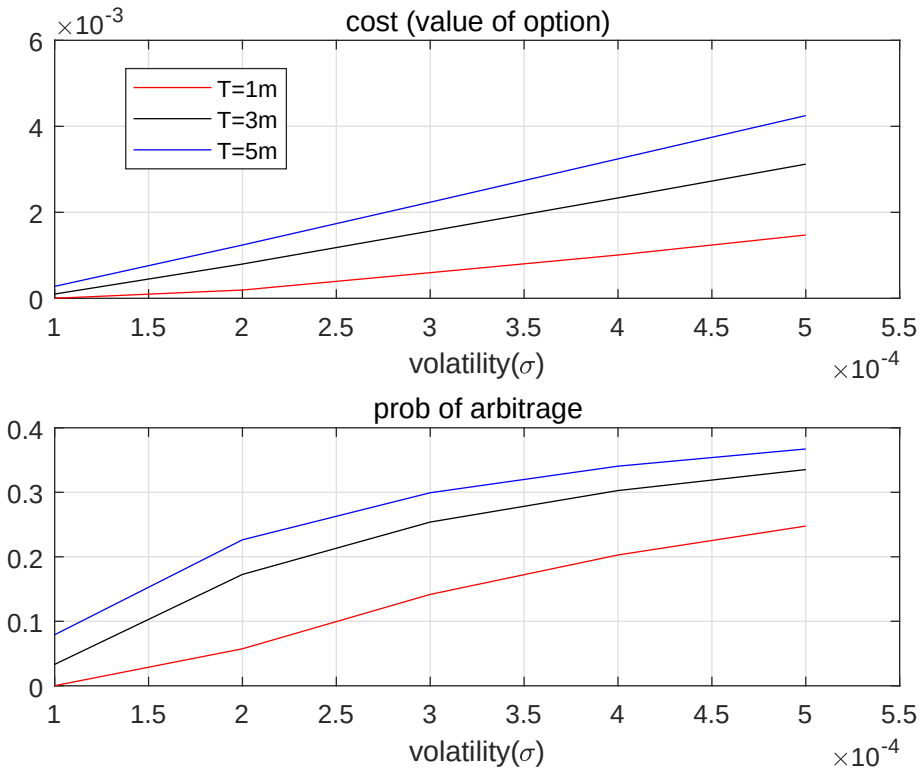


Figure 1. This figure depicts effects of volatility σ on cost of price-inputing and probability of arbitrage.

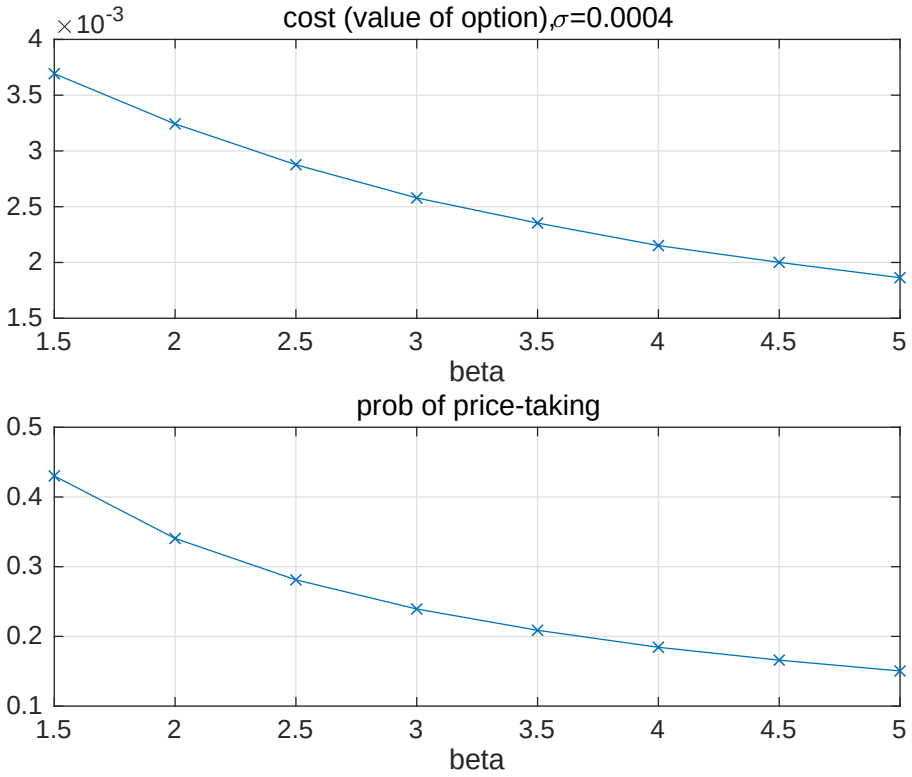


Figure 2. This figure depicts the effect of β on cost of price-inputing and probability of arbitrage.

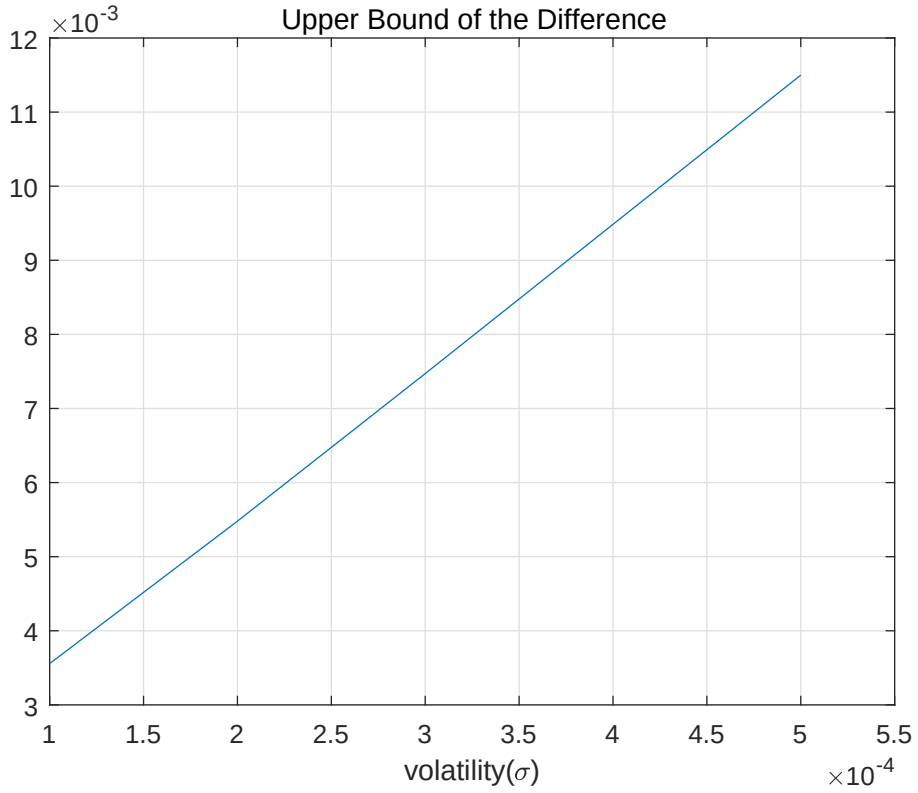


Figure 3. This figure shows the upper bound of difference between the NEST price and the price of an exchange at the same time.