nest

Protocol Whitepaper

NEST Protocol: A Game Theoretic Price Oracle Network

V 4.4

nestprotocol.org

June 2, 2022

Abstract

Most Decentralized Finance (DeFi) protocols require price data of various assets to settle on-chain contracts, and this is especially true for assets involving stablecoins and futures, which require the underlying assets' spot price information. The price information is one of the primary sources of risk in the DeFi industry in most cases. As a result, the stability and security of pricing oracles are critical to the future of decentralized finance.

Contents

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.

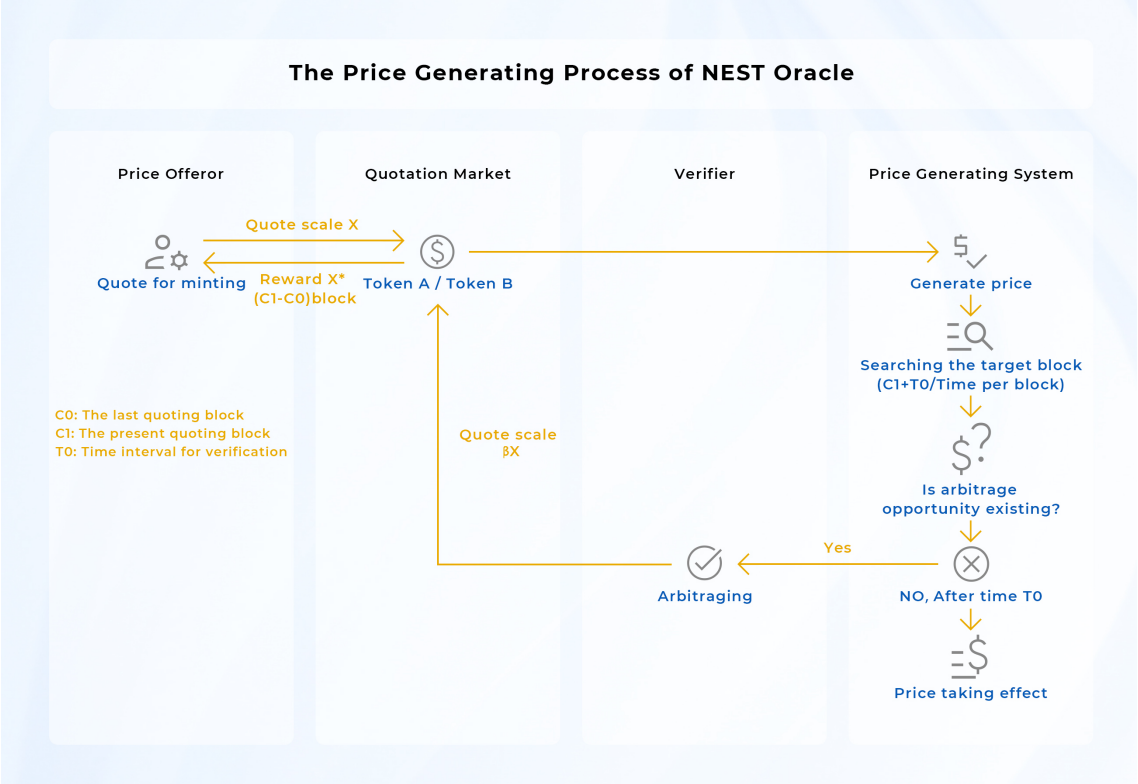

Figure 1: Diagram of NEST Protocol

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 increase the collateral asset in the same way but without 4-round limitation. As an example, for $\beta = 2$, the quoted asset chain and the collateral asset chain in section 2.5 are as follows:

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

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.