NEST Protocol: A Distributed Price Oracle Network

Most Decentralized Finance (DeFi) protocols depend on price data, and this is especially the case for contract assets such as stablecoins and futures which require a liquidation price. Price is, therefore, a core risk in the field of DeFi, meaning price prediction oracles provided herein are very important to the future of blockchain finance.

1. The Challenge of Price Oracles

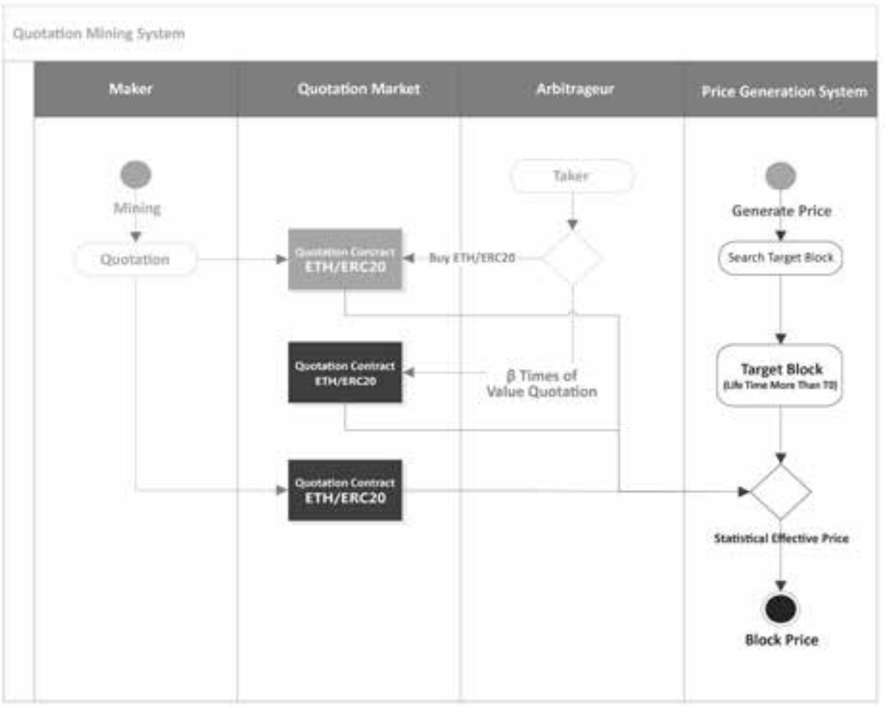
Price oracles commonly used in the DeFi industry generally reflect the asset price of centralized exchanges by “trusted” nodes, where the price is “uploaded” to the chain to be used by DeFi protocols. There exists a fundamental problem with the verification of such price data. Some DeFi projects use price data extracted from decentralized exchanges, but due to low transaction volume, the pricing data can be easily manipulated and susceptible to attack. This raises a very clear market requirement for an oracle solution that directly verifies the price to ensure the information is accurate and timely, but also prohibitively costly to attack. This system should also be distributed to avoid the risks of centralization.

Oracle price data must satisfy the following 5 key points:

1) Accuracy: truly reflects the market price
2) Price sensitivity: reacts fast enough to market movements
3) Attack resistant: the cost of distorting or affecting the real price is extremely high
4) Direct verification: the verifier is any third party, and no centralized review or threshold is required
5) Distributed quotation system: no centralized review or threshold is required, and anyone can freely join or leave

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 diagram of the NEST-Protocol is as follows:



1) Roles of NEST Protocol Actors

Participants in the NEST-Protocol are as below:

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.

A. Miners: Provide quotations and pay commission to receive NEST (ERC-20 Token). Miners are denoted as *O,* and anyone can become a miner.

B. 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 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) Quotation Mining and Price Verification

Taking ETH/USDT as an example, miner O intends to quote a price of 1ETH = 100USDT. At this time, miner O needs to input the quoted assets, ETH and USDT, into the quoted contract. The scale is xETH and 100xUSDT, and the paid commission is λxETH. 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 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 O, which is 1ETH = 100USDT. 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. In the view of O, 1ETH and 100USDT 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 an either bullish or bearish two-way option during the verification period, with the strike price as its quoted price. Verifiers, then, execute on 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 that 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 as 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, 1ETH = pUSDT, the asset scale is xETH, so the corresponding USDT quantity = $x*p$. The commission scale for participating in mining is $w=\lambda*x$, and verifier *A* can use the price p to trade USDT for xETH, or $x*p$.

3) Price Verification Period

Opened quotes have an allotted period of time attached, denoted as *T0*. 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 point 5. However, the price quoted that is then 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, 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 T0 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 T0 and transaction costs), thus representing the approximate current price; the existence of T0 does not mean a delay in prices.

4) 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, *A1* and maker *O* accept the transaction with the price of *p0* (the maker *O*'s quotation scale is x), so *A1* needs to quote a price $p1$ to the contract immediately with the scale of $x1$, and transfer $x1$ETH and $x1*p1$USDT to the contract. Commission and mining participation rewards are not paid at this time. If verifier *A2* accepts the transaction with *A1*, *A2* needs to quote the price *p2* with the scale of *x2*. A continuous price chain with *TO* as the maximum quotation interval is formed: *p0—p1—p2* ..., and the quoted asset chain is *x—x1—x2* ...

5) 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 ($p1, x1$), ($p2, x2$), ($p3, x3$)… the block price is $P=\sum pi*xi/\sum xi$. If there are no effective quotations in a current block, then the price of the most recent block will be used.

6) 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:

A. Provide an average price for DeFi operations, including the arithmetic average price of N consecutive blocks, $Ps = \sum P / N$, or the weighted average price of N consecutive blocks: $Pm = \sum P * Y / \sum X$, and $X = \sum Xi$, which is the aforementioned effective quotation.

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

C. Other statistics.

7) 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, $p0$, and changed it to $p1$, 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 $P1$ and $P0$ 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 scale as follows: The scale of the verifier's transaction is $x1$, and the scale of the simultaneous quotation is $x2 = \beta x1$ with $\beta > 1$. Therefore, the verifier must quote at a price more than double the scale of quotation. As an example of $\beta=2$, if the initial quotation is x=10ETH and in the case of all transactions, then $x1$=20, $x2$=40, $x3$=80 ... and so on. 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.

At present, each block on the ETH blockchain can only be quoted with a maximum of 20 trades with quotations also being distributed randomly. If there is 1 quote in every block and the quotation scale is 10 ETH, and $T0$ = 5 minutes, then the assets required for NEST to have no price update for an hour through attacks will be close to 2 ^ 12 * 50 * 10 ETH, which is nearly 2 million ETH. If β = 3, the data is approaching the total number of ETH in the entire market. This kind of attack-resistant ability cannot be achieved by centralized exchanges.

8) 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 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 in 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 usually 51% majority via community voting before being implemented.

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 equilibrium token currency, but it also introduces arbitrage from any third party. This can amplify the transaction scale of forward transactions or directly earn the 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 differs 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 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, 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 modifying 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% 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.