

피스 네트워크(Pyth Network)

해당 번역본은 이용자가 디지털자산 관련 정보를 편리하게 확인할 수 있도록
단순 참고용으로 번역된 것이며, 투자 권유를 목적으로 하지 않습니다.
그 내용이 정확하지 않을 수 있으므로 정확한 정보 습득을 위해서는
원문을 참고하시거나 원문 작성 주체 측에 문의하시기 바랍니다.
두나무는 해당 번역본 내용의 진실성 및 정확성을 보장하지 않고,
제공된 정보에 의한 투자 결과에 대하여 어떠한 책임도 지지 않으며,
투자 손실은 투자자에게 귀속됩니다.

PYTH 네트워크: 퍼스트파티 금융 오라클

PYTH 데이터 협회

버전 2.0

2023년 9월 28일

금융 시장 데이터는 종종 제한된 기관 및 사용자 집단에게만 접근이 허용됩니다. 전통적인 시장은 일반적으로 실시간 및 과거 가격 피드에 대한 엄격한 통제를 유지합니다. 암호화폐 시장은 현재 이러한 장벽이 상대적으로 낮지만, 이러한 상황이 계속 유지된다는 보장은 없습니다. 그 결과, 가장 시기적절하고 정확하며 가치 있는 정보에 접근할 수 있는 것은 선택된 일부 사용자에게 한정됩니다.

피스 네트워크는 이러한 가치 있는 금융 시장 데이터를 디파이(DeFi) 애플리케이션과 일반 대중에게 제공하는 것을 목표로 합니다. 네트워크는 거래 회사, 마켓메이커, 거래소 등 시장 참여자들이 자신들의 기존 운영 과정에서 수집한 가격 데이터를 공유하도록 인센티브를 제공합니다. 네트워크는 이러한 퍼스트파티 가격 데이터를 집계하고, 이를 온체인에 게시하여 온체인 또는 오프체인 애플리케이션에서 사용할 수 있도록 합니다.

초기 백서에서는 솔라나(Solana) 블록체인에 초점을 맞춘 프로토콜 초기 설계를 제안했습니다. 이번 두 번째 버전은 피스 생태계의 현재 상태를 반영하도록 설계를 업데이트했습니다. 특히, 본 버전에서는 타겟 체인으로의 가격 전달을 위한 새로운 크로스체인 모델을 설명합니다.

피스 데이터 협회(이하 “협회”)는 피스 네트워크 참여자 커뮤니티와 협력하여, 본 백서를 통해 피스 네트워크의 현재 상태를 설명합니다.

1 개요

피스 프로토콜은 참여자들이 다양한 상품(예: BTC/USD)에 대한 가격 업데이트를 지속적으로 게시하도록 인센티브를 제공하도록 설계되었습니다. 각 상품은 현재 가격과 가격의 불확실성을 나타내는 신뢰 구간(confidence interval)을 포함하는 가격 피드를 가집니다. 예를 들어, 현재 BTC/USD 피드는 가격이 $65,000 \pm 50$ 이라고 표시할 수 있습니다.

각 상품의 피드는 온체인에 게시되며, 이를 읽는 **소비자(consumers)**는 블록체인 기반 프로그램(다양한 블록체인 상) 또는 오프체인 애플리케이션일 수 있습니다. 온체인 프로그램은 개별 **게시자(publishers)**들의 가격 피드를 집계하여 각 상품의 가격 피드를 생성합니다.

프로토콜은 고품질의 시의성 있는 가격 정보를 제공할 수 있는 퍼스트파티 데이터 제공자들을 게시자로 유치하도록 설계되어 있습니다.

따라서, 프로토콜에는 다음과 같은 두 가지 참여자 그룹이 존재합니다:

- **게시자(Publishers)**는 가격 피드를 게시하고 그 대가로 수수료를 받습니다. 게시자는 일반적으로 정확하고 시의성 있는 가격 정보에 접근할 수 있는 시장 참여자입니다.
- **소비자(Consumers)**는 가격 피드를 읽고 해당 데이터를 스마트 계약이나 dApp에 통합합니다. 이 과정에서 소비자는 데이터 접근을 위해 프로토콜에 수수료를 지불합니다.

수수료는 타겟 체인에서 피스 가격 업데이트당 고정 비율로 부과됩니다(예: 업데이트당 0.0001 ETH). 소비자는 시장 데이터를 위해 피스를 통합한 온체인 프로토콜의 사용자이며, 이러한 프로토콜은 다양한 블록체인에서 실행될 수 있습니다.

피스 가격을 다양한 소비자에게 제공하기 위해, 프로토콜은 다중 블록체인 환경에서 작동해야 합니다. 피스 프로토콜은 **피스넷(Pythnet)**이라 불리는 앱체인을 사용하여 각 가격 피드의 상태를 저장하고 업데이트합니다. 피스는 각 게시자가 검증인(validator)으로 참여하는 권한증명(Proof-of-Authority) 블록체인입니다. 피스 가격은 웜홀(Wormhole) 네트워크와 같은 탈중앙화 크로스체인 메시징 프로토콜을 이용한 크로스체인 아키텍처를 통해 이 앱체인에서 다른 타겟 체인(target chains)으로 방송됩니다. 피스으로부터 데이터를 방송함으로써, 프로토콜은 다수의 타겟 체인을 손쉽게 지원할 수 있으며, 이를 통해 소비자는 자신이 사용하는 블록체인에 관계없이 피스 데이터를 활용할 수 있습니다.

이러한 아키텍처 내에서, 앞서 언급한 참여자들은 두 가지 메커니즘을 통해 상호작용합니다. 이 두 메커니즘은 위에서 언급한 여러 체인 중 하나에서 구현됩니다:

- **가격 집계(Price aggregation)**는 개별 게시자들의 가격 피드를 결합하여 상품의 단일 가격 피드를 생성합니다. 이 메커니즘은 소수의 게시자 그룹이 가격에 과도한 영향을 미치지 못하도록 설계되어 견고한(가격 조작에 강한) 가격 피드를 생산하도록 합니다. 이 메커니즘은 피스 상의 온체인 프로그램으로 실행됩니다.
- **피스 거버넌스(Governance)**는 다른 메커니즘의 상위 수준 매개변수를 결정합니다.

핵심적인 과제는 이러한 메커니즘을 다양한 형태의 가격 조작에 견고하도록 설계하는 것입니다. 고려해야 할 두 가지 주요 공격 유형은 다음과 같습니다:

1. 참여자가 게시자로 등록한 뒤 오라클 가격을 조작하려는 시도를 할 수 있습니다. 가격 집계 메커니즘은 게시자가 집계 가격에 미치는 영향을 제한함으로써 이러한 공격을 방지하도록 설계되었습니다. 또한, 커뮤니티는 게시자들이 프로토콜을 사용하는 방식을 결정하며, 평판이 높고 신뢰할 수 있는 참여자들로 게시자 집합을 제한할 수 있습니다.
2. 악의적인 행위자가 거래소에서 가격을 인위적으로 움직여 피스의 집계 가격에 영향을 미치려 할 수 있습니다. 다양한 거래소로부터 데이터를 공급받는 여러 게시자들의 존재와 견고한 가격 집계 메커니즘은 이러한 가격 조작 시도의 위험을 줄여줍니다.

2 크로스체인 아키텍처

피스는 게시자들이 피스에서 가격 데이터를 제공하며, 그곳에서 (다음 섹션에서 설명할) 집계 메커니즘이 집계 가격을 생성합니다. 집계된 가격은 이후 다른 블록체인으로 방송 및 전송되어 소비자가 이를 사용할 수 있습니다. 피스는 가격 게시, 집계, 그리고 다른 블록체인으로의 전송 시작과 관련된 프로그램과 활동만 존재하는 애플리케이션 특화 블록체인입니다. 피스의 합의 모델과 런타임은 솔라나를 기반으로 합니다.

성공적인 크로스체인 아키텍처는 다음과 같은 여러 중요한 특성을 충족해야 합니다:

1. **거래 비용 최소화.** 여러 블록체인에서 가격 피드를 유지하려면 각 체인마다 거래 수수료(즉, 가스비)를 지불해야 합니다. 이러한 비용이 누적되면 참여자에게 과도한 부담이 될 수 있습니다.
2. **고빈도 및 저지연 가격 업데이트 지원.** 이 두 가지 특성은 시의성 있는 가격 정보를 필요로 하는 애플리케이션에 필수적입니다.
3. **다수의 블록체인으로 확장 가능.** 다양한 런타임, 합의 모델, 가스비 구조를 가진 여러 블록체인에서 가격 데이터 사용 사례가 존재합니다. 가격 데이터의 크로스체인 전송 비용이 지나치게 높다면 이러한 모든 체인을 지원하기 어렵습니다.
4. **다수의 가격 피드로 확장 가능.** 피스 프로토콜은 암호자산 및 비암호자산 전반에 걸쳐 광범위한 가격 피드를 지원할 수 있어야 합니다. 여러 블록체인으로 확장하는 경우와 마찬가지로, 크로스체인 전송 비용이 과도하게 높으면 이러한 확장은 불가능합니다.

이 크로스체인 아키텍처는 세 부분으로 구성된 워크플로우를 통해 이러한 과제를 해결하는 “풀(pull)”형 오라클 구조입니다.

1. 가격 업데이트 게시

워크플로우의 첫 번째 단계는 효율적이고 저비용으로 온체인에 가격을 게시하는 것입니다. 높은 가스비가 발생할 수 있는 범용 블록체인과 달리, 피스에서는 권한을 부여받은 게시자(permissioned publishers)가 무료로 업데이트를 게시할 수 있습니다. 이러한 게시자는 유효한 가격과 신뢰 구간(confidence)을 포함한 가격 업데이트를 온체인 오라클 프로그램에 제출하며, 해당 프로그램은 이를 관련 온체인 가격 계정의 필드에 저장합니다. 오라클 프로그램이 호출되면, 가격 계정 내의 가격을 대상으로 집계가 수행됩니다.

2. 가격 전파 작업

두 번째 단계는 피스 합의 과정의 일부로서 피스 검증인들이 수행하는 가격 전파 작업입니다. 오라클 프로그램이 게시자들의 가격을 각 피드별로 집계한 뒤, 해당 슬롯에서 업데이트된 가격 피드의 집계 가격을 메시지 버퍼 프로그램에 전달합니다.

메시지 버퍼 프로그램은 다른 체인으로 전송될 메시지를 생성할 수 있도록 하며, 권한이 부여된 프로그램만 호출할 수 있습니다. 이 과정에서 메시지 버퍼는 업데이트된 가격 피드의 집계 가격을 저장합니다. 이후 검증인은 메시지 버퍼의 계정을 읽고, 앞서 언급한 가격들을 트리의 리프(leaf)로 하는 **머클 트리(Merkle tree)**를 구성합니다. 그런 다음 웜홀(Wormhole) 네트워크와 같은 크로스체인 메시징 프로토콜을 통해 트리의 루트를 다른 체인으로 전파합니다.

웜홀 네트워크는 한 블록체인의 데이터를 다른 블록체인에서 읽을 수 있도록 하는 탈중앙화 크로스체인 메시징 시스템입니다. 전파 작업은 높은 빈도로, 즉 피스 블록 시간의 주기로 호출되도록 설계되었습니다. 전파의 출력은 검증된 머클 트리 루트의 스트림이며, 이는 크로스체인 메시징 인프라를 통해 접근 가능하고, 트리의 데이터는 일정 기간 동안의 과거 슬롯에 대해 피스 상에서 공개적으로 확인할 수 있습니다.

3. 타겟 체인에서의 릴레이

세 번째 단계는 릴레이(relaying)로, 피스 가격이 제공되는 타겟 체인에서 이루어집니다. 각 타겟 체인은 모든 피스 가격 피드에 대한 가격을 저장하는 피스 수신자(receiver) 계약을 가집니다. 이러한 계약은 저장된 가격을 업데이트하기 위한 퍼미션리스(permissionless) 작업을 구현합니다.

이 작업의 입력은 검증된 머클 트리 루트, 해당 머클 트리의 리프를 나타내는 특정 심볼의 가격 업데이트, 그리고 그 리프에서 루트로 이어지는 경로입니다. 후자의 두 항목은 피스에서 공개적으로 접근 가능합니다. 이 작업은 메시지에 대한 다양한 검증(예: 서명 검증, 루트-리프-경로 조합 검증 등)을 수행하며, 업데이트가 유효한 경우 새로운 가격이 피스 수신자 계약에 저장됩니다.

피스 가격의 소비자는 퍼미션리스 가격 업데이트를 직접 호출해야 합니다. 즉, 가격을 사용하기 전에 체인에 가격 업데이트를 “풀(pull)” 해야 합니다. 피스 수신자 계약에 저장된 가격은 업데이트되지 않으면 시간이 지나며 오래된 값이 됩니다. 피스 가격 피드를 통합한 프로토콜은 가격의 최대 허용 경과 시간(staleness)에 대한 제한을 둘 수 있습니다. 이러한 프로토콜과 상호작용하는 사용자는, 현재 온체인 가격이 오래되었을 경우 상호작용 전에 반드시 퍼미션리스 업데이트를 호출해야 합니다.

이 설계에서 소비자는 가격이 실제로 필요할 때만 피스 가격 피드를 업데이트하는 데 따른 거래 비용을 부담합니다. 이 특성이 바로 크로스체인 아키텍처가 앞서 제시한 목표를 달성하는 방식입니다. 방송 컴포넌트는 다수의 가격 피드에 대해 고빈도의 가격 업데이트를 스트리밍하면서도 거래 비용을 발생시키지 않습니다. 이러한 가격 업데이트 중 상당수는 타겟 체인에 기록되지 않으며, 따라서 비용이 발생하지 않습니다.

타겟 체인에서의 거래 비용 또한 최소화됩니다. 소비자는 특정 연산에 필요한 시점에만 가격 업데이트를 호출하기 때문입니다.

2.1 업데이트 수수료

소비자는 피스 수신자 계약에서 가격 업데이트 작업을 호출하기 위해 프로토콜에 업데이트 수수료(update fee)를 지불해야 합니다. 수수료는 타겟 체인의 네이티브 토큰으로 부과됩니다.

2.2 비교: 풀(Pull) vs 푸시(Push)

대부분의 오라클은 전통적으로 **푸시(push) 아키텍처**를 사용해 왔습니다. 이 구조에서 오라클은 범용 블록 체인에 가격을 게시하고, 경우에 따라 해당 체인에서 집계 작업까지 수행합니다. 오라클은 가격을 최신 상태로 유지해야 하므로 정기적으로 트랜잭션을 전송해 온체인 가격을 업데이트해야 합니다. 이러한 트랜잭션은 업데이트 빈도, 지원하는 가격 피드 및 블록체인 수, 심지어 게시자 수에 비례하여 가스비가 증가합니다. 또한, 푸시형 오라클은 가격 업데이트 트랜잭션이 다른 네트워크 활동과 경쟁하므로 신뢰성이 떨어질 수 있습니다. 네트워크 혼잡이 발생하면 오라클 업데이트가 온체인에 반영되지 못할 수 있습니다.

반면 피스의 풀(Pull) 모델은 저비용 체인에서 가격 게시와 집계를 수행합니다. 피스는 Solana의 포크로, 저지연 및 고빈도 가격 업데이트를 지원합니다. 피스 트랜잭션은 게시자에게 무료로 제공되므로 오라클의 운영 비용이 크게 절감됩니다. 다른 블록체인으로의 가격 방송은 여전히 가스비가 발생하지만, 푸시 모델과 달리 수요와 무관하게 업데이트를 전송하지 않습니다. 피스는 소비자가 가격 업데이트를 요청할 때만 가스비를 지불합니다.

그 결과, 가스 사용은 더 목표 지향적이고 효율적입니다. 따라서 피스는 더 빈번한 가격 업데이트를 수행할 수 있고, 푸시형 오라클보다 더 많은 가격 피드 및 블록체인으로 확장할 수 있습니다. 또한 풀 모델은 신뢰성 문제에도 영향을 받지 않습니다. 타겟 체인의 네트워크 혼잡은 게시자들이 피스에 가격을 게시하는 능력에 영향을 미치지 않으며, 충분한 거래 수수료를 지불할 의사가 있는 사용자는 언제든지 타겟 체인에서 피스의 가격을 가져올 수 있습니다.

피스 아키텍처의 또 다른 장점은 지수 가중 이동 평균(EMA)과 같은 상태 기반 계산(stateful computation)을 처리할 수 있다는 점입니다. 이러한 계산은 과거에 게시된 데이터의 시간 가중 결합입니다. 푸시형 오라클은 업데이트 빈도가 낮기 때문에 이러한 계산을 온체인에서 수행하기 어렵습니다. 예를 들어, 업데이트 주기가 10분인 경우 5분 EMA를 구성하기 어렵습니다. 반면 피스는 피스에서 400ms마다 가격 업데이트에 접근할 수 있으므로, EMA 및 기타 시간 기반 조합을 손쉽게 구성할 수 있습니다.

3 가격 집계

가격 집계 메커니즘은 각 게시자의 가격 및 신뢰 구간 피드를 결합하여 단일 집계 가격 및 신뢰 구간 피드를 생성합니다. 예를 들어, 한 게시자가 BTC/USD 가격을 52,000 USD $\pm$ 10으로, 다른 게시자가 \$53,000 $\pm$ 20으로 보고한 경우, 가격 집계 결과는 52,500 USD $\pm$ 500이 될 수 있습니다.

이 메커니즘은 온체인 프로그램의 일부이며, 게시자가 가격 업데이트를 제출할 때 트리거됩니다. 특정 슬롯에서 첫 번째 가격 업데이트가 이루어지면, 자동으로 이전 슬롯의 가격들이 집계됩니다.

가격 집계 알고리즘은 세 가지 특성을 갖도록 설계되었습니다:

1. **조작 저항성** — 게시자의 의도적 혹은 비의도적 조작에 강해야 합니다. 예를 들어, 대부분의 게시자가 가격을 100 USD로 제출하고, 한 게시자가 80 USD를 제출하더라도 집계 가격은 여전히 \$100 근처에 머뭅니다. 이 특성은 소수의 게시자가 시장과 동떨어진 가격을 제출하더라도 집계 가격의 정확성을 유지할 가능성을 높입니다. 그림 1(a)는 이 시나리오를 보여줍니다.

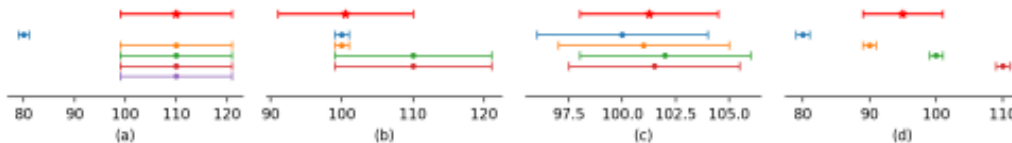


그림 1: 집계 절차의 시나리오. 가는 막대는 각 게시자의 가격과 신뢰 구간을, 굵은 빨간 막대는 결과로 얻어진 집계 가격과 신뢰 구간을 나타냅니다.

2. **정확도 수준이 다른 데이터 소스의 적절한 가중치 부여.** 피스 프로토콜은 게시자들이 서로 다른 수준의 정확도를 갖고 있음을 반영하기 위해 신뢰 구간을 제출할 수 있도록 합니다. 예를 들어, 일부 게시자는 거래소일 수 있습니다. 거래소마다 유동성이 다르며, 유동성이 낮은 거래소일수록 유동성이 높은 거래소보다 매수/매도 스프레드가 더 넓은 경향이 있습니다. 이로 인해 한 거래소가 101 USD $\pm$ 1로 보고하고, 다른 거래소가 110 USD $\pm$ 10으로 보고하는 상황이 발생할 수 있습니다. 이 경우 집계 가격은 110 USD보다는 101 USD에 더 가깝게 형성됩니다. 그림 1(b)는 이러한 상황을 보여줍니다.
3. **게시자 간 가격 변동을 반영하는 집계 신뢰 구간.** 실제 시장에서는 특정 상품의 단일 가격이 존재하지 않습니다. 상품은 여러 거래소에서 동시에 약간 다른 가격으로 거래됩니다. 또한 상품의 스프레드는 가격 정밀도의 근본적 한계로 작용합니다. 집계 신뢰 구간은 거래소 간의 변동성과 이러한 한계를 모두 반영합니다. 그림 1(c)와 (d)는 거래소 간 가격 변동이 존재하는 두 가지 사례를 보여줍니다.

가격 집계 알고리즘은 가중 중앙값(weighted median)의 변형을 사용합니다. 알고리즘의 입력에는 각 게시자의 스테이크 가중치(stake-weight)가 포함됩니다. 초기에는 이 가중치가 균등하게 설정되지만, 향후 커뮤니티 결정에 따라(예: 원 백서에 언급된 데이터 스테이킹 메커니즘을 활용해) 추가적인 방식으로 설정될 수 있습니다.

알고리즘의 첫 번째 단계에서는 각 게시자에게 세 개의 투표권을 부여합니다 — 하나는 그들의 가격에서, 다른 두 개는 가격 ± 신뢰 구간에서의 투표입니다. 그런 다음, 이 세 투표에 대해 스테이크 가중 중앙값을 계산하여 집계 가격을 도출합니다. 두 번째 단계에서는 집계 가격으로부터 스테이크 가중 25번째 및 75번째 백분위수까지의 거리를 계산하고, 이 중 더 큰 값을 집계 신뢰 구간으로 선택합니다.

이 간단한 알고리즘은 일반 중앙값(median)의 일반화 형태입니다. 대부분의 사람들은 중앙값을 데이터 집합의 중간값, 즉 50번째 백분위수로 이해합니다. 그러나 중앙값은 또한 다음의 목적 함수를 최소화하는 값 R 으로 정의됩니다:

$$\sum_i |R - p_i|$$

여기서 p_i 는 i 번째 게시자의 가격입니다. 이 함수는 R 이 게시자의 가격 p_i 와 얼마나 떨어져 있는지에 따라 패널티를 부여합니다.

제안된 알고리즘은 다음의 식을 최소화하는 집계 가격 R 을 계산합니다:

$$(1/3)\sum_i s_i |R - p_i| + (2/3)\sum_i s_i \max(|R - p_i| - c_i, 0),$$

여기서 s_i 는 게시자의 스테이크 가중치이며, c_i 는 게시자의 신뢰 구간입니다.

이 목적 함수는 두 가지 역할을 합니다. 첫째, 게시자의 스테이크에 따라 가중치를 부여하여 스테이크가 낮은 게시자는 가격에 거의 영향을 미치지 못하게 합니다. 둘째, 일반 중앙값 목적 함수에 두 번째 항을 결합하여, R 이 게시자의 신뢰 구간 밖에 있을 때만 패널티를 부여합니다.

4 거버넌스

온체인 거버넌스는 다음과 같은 역할을 수행할 것으로 예상됩니다:

- 업데이트 수수료의 크기 결정
- 게시자에 대한 보상 분배 메커니즘 결정
- 블록체인 전반의 온체인 프로그램에 대한 소프트웨어 업데이트 승인
- 피스에 상장되는 상품과 그 기준 데이터(예: 가격의 소수점 자릿수, 참조 거래소 등) 결정
- 게시자가 가격 피드 데이터를 제공하기 위한 권한 부여 방식 결정

5 토큰 분배

카테고리	언락 (Unlocked)	락 (Locked)	총계 (Total)
게시자 보상(Publisher Rewards)	0.5	21.5	22
생태계 성장(Ecosystem Growth)	7	45	52
프로토콜 개발(Protocol Development)	1.5	8.5	10
커뮤니티 및 런칭(Community and Launch)	6	0	6
프라이빗 세일(Private Sales)	0	10	10
총계(Total)	15	85	100

표 1. 락 및 언락된 PYTH 토큰의 할당. 락된 토큰은 토큰 발행 후 6, 18, 30, 42개월 시점에 순차적으로 언락됩니다.

총 10,000,000,000개의 PYTH 토큰이 존재하며, 총 공급량은 증가하지 않습니다. 또한 85%의 토큰은 초기에는 계약상 락(Locked) 상태로 유지됩니다. 락된 토큰은 토큰 발행 후 6개월, 18개월, 30개월, 42개월**에 순차적으로 언락됩니다. 이 일정은 시간이 지남에 따라 점진적으로 언락된 토큰 공급량이 증가하도록 설계되었습니다. 나머지 15%의 PYTH 토큰은 초기부터 언락된 상태입니다. 락 및 언락된 토큰의 공급량은 표 1에 제시된 카테고리별로 배분됩니다.

6 결론

본 백서는 정확하고 고해상도의 금융 시장 데이터를 온체인에서 손쉽게 접근할 수 있도록 하는 오라클 프로토콜을 제안합니다. 이 프로토콜은 데이터 게시자와 소비자를 조정하는 자급적 탈중앙화 네트워크(self-sustaining decentralized network)로 설계되었습니다.

프로토콜은 고품질의 가격 데이터를 제공할 수 있는 게시자를 유치하고, 소비자들의 데이터 사용으로부터 수집된 수수료를 통해 게시자에게 인센티브를 제공합니다.

이러한 메커니즘은 악의적 공격자가 프로토콜을 조작하여 이익을 취하는 것을 방지하는 데 도움을 줍니다.