

Title: [ARFC] Pyth to support AAVE on Optimism as a secondary oracle

Author: [@KemarTiti](#) - Contributor, [Pyth Data Association](#)

Date: 2023-05-30

Summary

Following discussions with the BGD Labs team and the AAVE community, we are excited to propose Pyth as a backup oracle for AAVE on Optimism. We recognize the importance of diversity among DeFi infrastructure providers, particularly for systemically important protocols like AAVE, and believe endorsing Pyth as a backup oracle constitutes an advancement in realizing that objective.

We are confident that incorporating Pyth as a secondary oracle will yield clear and material benefit for AAVE, its participants, and the wider community. These benefits are rooted in three core principles: resilience, competition, and decentralization.

- Resilience

: The core function of any secondary oracle is to serve as a backup data source. If the primary oracle experiences downtime or becomes compromised, secondary oracles can step in and provide the necessary data to ensure the continued operation of critical collateralization monitoring. This redundancy creates a more resilient AAVE and reduces the risks associated with any potential single point of failure.

- Competition

: Pyth's presence as a secondary oracles on AAVE introduces competition among other providers as well — which drives innovation and continued improvements in data quality, costs, latency, and security, ultimately benefiting the AAVE in the process.

- Decentralization

: Incorporating secondary oracles providers add an added dimension of decentralization. By relying on multiple data sources, AAVE become less susceptible to the centralizing influence of any single oracle provider, thereby reinforcing the core principles of decentralization and censorship resistance.

About Pyth

The Pyth Network serves as an oracle provider, delivering financial market data to an array of blockchains. Pyth's market data is sourced from 80 primary data providers, encompassing some of the world's most prominent exchanges and market-making enterprises. Presently, the oracle hosts over 200 price feeds spanning diverse asset classes, including US equities, commodities, foreign exchange, and cryptocurrencies.

Pyth's price feeds have been meticulously engineered for speed, precision, and dependability. It's price feeds update multiple times per second—[live price updates](#) can be viewed on here. Each price update is an aggregate of reputable data providers' reported prices. This aggregate price is determined by robust [aggregation](#) procedures to ensure that colluding (or mistaken) providers cannot materially influence the aggregate price.

Pyth has already proven to be a robust and reliable oracle provider on Optimism. Functioning as the principal oracle for the Synthetix protocol, Pyth has efficiently served 40 perpetual markets with \$10B Traded Volume for over 5 months. More broadly, to date (launched in mid December 2022), the Pyth has already delivered close to 1.5 million price updates on-chain—with an ATH of 25K on-chain price updates in a single day.

Robustness through Data Providers

Pyth counts its highly reputable data providers as its flagship strength. The Pyth Network boasts 80 leading data providers spanning the largest crypto exchanges and leading market making firms. To better illustrate, we highlight a subset of the providers behind Pyth's ETH and BTC symbols.

- Binance —

Pyth data provider since Nov 2022, Binance is the largest crypto exchange by volume and market share, facilitating nearly \$10 billion in trading volume in the past 24 hours alone.

- Optiver

— Pyth data provider since October 2022, Optiver is a global market maker with offices in Amsterdam, London, Chicago, Austin, Sydney, Shanghai, Hong Kong, Singapore and Taipei. By providing liquidity on multiple exchanges across the world in various financial instruments the firm participate in the safeguarding of healthy and efficient markets.

- Jane Street

— Pyth data provider since August 2021, Jane Street is a quantitative trading firm and liquidity provider widely regarded for its proprietary trading models and quantitative computing power that places them at the forefront of market structure in equities, bonds, options, and ETFs globally. In 2020, Jane Street traded more than \$17 trillions worth of securities.

- OKX —

Pyth data provider since October 2022, OKX is the second biggest global crypto exchange by trading volume. Trusted by more than 20 million global customers, OKX is known for being one of the fastest and most reliable crypto trading platforms for investors and trades everywhere.

- Wintermute

— Pyth data provider since March 2022, Wintermute is a leading global algorithmic trading firm in digital assets. They provide liquidity algorithmically across over 60 centralized and decentralized exchanges and facilitate the OTC trading of 250+ tokens, with average daily volume of over \$5 billion.

- Virtu Trading

— Pyth data provider since June 2021, Virtu Financial is one of the worldwide leaders in trading and execution services providing liquidity for over 25,000 securities, spread over 235 venues and 50+ countries. Virtu handles nearly ~30% of market orders placed by retail investors in the US and accounted for nearly 10% of the total US stock trading volume in December 2020.

Pyth's data publishers are well-known and established leaders in their respective industries and markets — and thus confront significant reputational and financial consequences should they attempt to partake in malicious activities as data providers.

More information on Pyth's +80 data providers can be found [here](#).

Resilience through Price Aggregation

Pyth robustly aggregates the quotes of these data providers to provide another level of protection against accidents or manipulation. This prevents any single data provider from materially influencing the Pyth price for their own economic gain. For example, even if publishers are submitting a price of \$100 and one publisher submits a price of \$80, the aggregate price should remain near \$100 and not be overly influenced by the single outlying price.

Scenarios for the aggregation procedure. The lower thin bars represent the prices and confidence intervals of each publisher, and the bold red bar represents where we would like the aggregate price and confidence to be.

Pyth can attribute this robustness to its simple yet comprehensive two-step aggregation algorithm. In the first step, data publishers provide three votes on the price of the asset — one vote at their price and one vote at each of end (+/-) of their confidence interval — following which Pyth simply calculates the median of all the votes. The second step computes distance from the aggregate price to the 25th and 75th percentiles of the votes, then selects the larger of the two as the aggregate confidence interval.

This process acts like a hybrid between a mean and a median, giving confident publishers more influence, while still capping the maximum influence of any single publisher. The algorithm has an interpretation as computing the minimum of an objective function that penalizes the aggregate price from deviating too far from the publishers' prices. In addition to producing high fidelity price, Pyth also provides confidence that is representative of the estimated uncertainty of the price, allowing protocols to actively adjust their risk parameters.

Pyth has proven to be consistent and reliable. For example, defining downtime as a period in which the most recent Pyth update was at least 5 slots (~2 secs) old, Pyth had 99.97% uptime for ETH/USD over the one-week period of March 28, 2023 through April 4, 2023. When that definition is altered to allow a max staleness of 10 slots (~4 secs), Pyth had 100% uptime for that feed over that period.

Pyth's Architecture

Pyth runs aggregation for its Pythnet Price Feeds on its own application-specific blockchain called Pythnet. Prices are delivered from Pythnet to other blockchains via the [Wormhole interoperability protocol](#) and a permissionless price update model.

[Pythnet](#) is a proof-of-authority chain where the data providers run the validators for the network. This blockchain serves as the computation substrate to securely and reliably combine the data providers' prices into a single aggregate price for each Pyth price feed. Pythnet forms the core of Pyth's cross-chain price feeds that serve all blockchains.

Pyth bridges prices from Pythnet to other blockchains using Wormhole. Wormhole is a generic cross-chain message-passing protocol that allows anyone to send secure messages between blockchains. Pyth sends a continuous stream of price messages from Pythnet through Wormhole. These messages are signed such that anyone can validate their authenticity. Anyone can post one of these messages on a target chain that Pyth supports to permissionlessly update the

on-chain price.

Pyth's permissionless update model allows for several different integration strategies. For example, protocols can be designed to update the Pyth price and consume it in the same transaction. Alternatively, an off-chain service can regularly push price updates on-chain, and protocols can directly read the on-chain price.

Integration with Aave

Based on discussions with BGD Labs, we have determined that a push-based integration is the most straightforward. The AAVE protocol already has a notion of a backup oracle provider that Pyth can fit into with minimal development work. In this integration, Pyth will adapt to the contracts' interface of the AaveOracle smart contract — reading on-chain prices for any of the supported assets, in a similar way to any other integrated oracle.

In order to support this integration, the Pyth Data Association will operate a price pusher. This pusher will regularly update Pyth's on-chain price on Optimism for all assets supported by Aave (DAI, USDC, USDT, AAVE, LINK, OP, BTC, ETH, stETH). This design allows Aave to natively read the Pyth prices on Optimism at no extra cost. The Price Pusher will update all the following assets prices on Optimism: DAI, USDC, USDT, AAVE, LINK, OP, BTC, ETtH, stETH, at a frequency of every 30 minutes or 0.25% price deviation (whichever is faster).

The Pyth Data Association will sponsor a grant to update the Pyth prices on Optimism for no less than 3 months. Based on the selected parameters and analysis of historical pricing data, price updates for volatile assets (BTC, ETH, OP, AAVE, LINK, stETH) are expected to be triggered about 100 times per day while stablecoins would normally be updated every 30 minutes (or 50 times per day). Altogether, we estimate a total of 500 transactions per day (as Pyth can batch multiple updates into one transaction).

Simulating a push-based Pyth over April 2023 with updates every 1200s or during any 15bps deviation—Chainlink's current parameters—Pyth performs well with strong price-robustness and accuracy.

Ending Thoughts

Selecting an oracle, even for backup support, requires careful consideration of several factors, such as accuracy and robustness. Pyth's proven track record, robust design, and reputable data providers make it a strong candidate to support AAVE's oracle needs. We are happy to answer any questions.