

# How To Tell If Your Oracle Relationship Has Trust Issues

By: engn33r

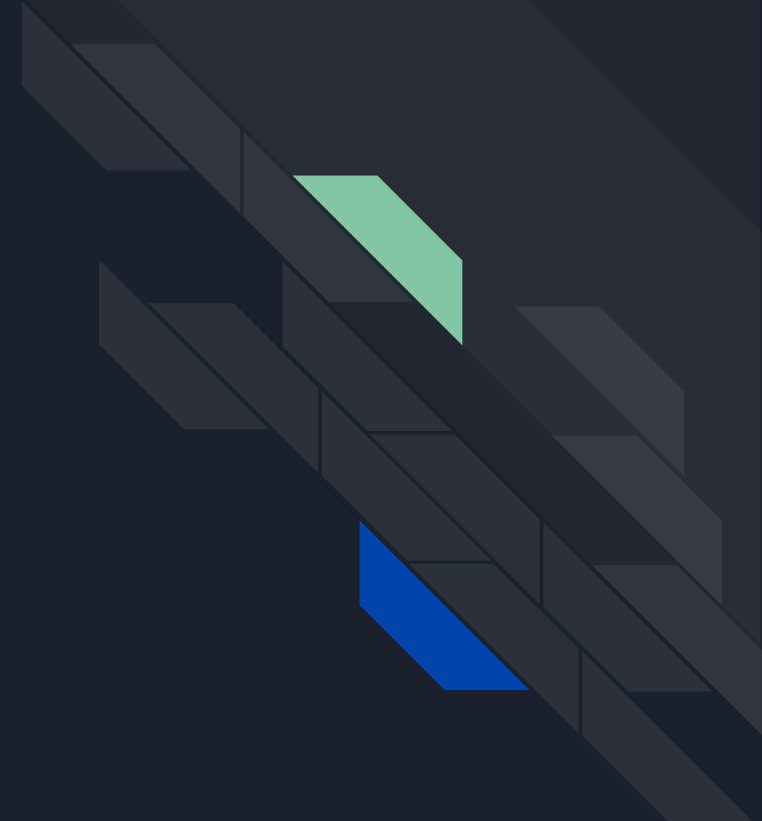
Devconnect 2025

# Summary

How DeFi prices work

Oracle Risks

Recent incidents



# World's Fastest Intro

I'm eng33r, I read/write code



yAudit



yAcademy



twyne



## Slides QR Code



<https://engn33r.com/devconnect2025.pdf>

# DeFi in 2025



# TradFi Prices

**Coinbase Global Inc.**

AFTER HOURS

**\$207.01**

▼ -0.59 -0.28%

After Hours Volume: **157.76K**

Last Updated: May 17, 2024 7:59 p.m. EDT  
- Delayed quote

CLOSE	CHG	CHG %
<b>\$207.60</b>	<b>8.43</b>	<b>4.23%</b>

VOLUME: **8.69M**

65 DAY AVG: 12.29M

71% VS AVG

**OVERVIEW** PROFILE CHARTS FINANCIALS

**KEY DATA**

OPEN	DAY RANGE
<b>\$205.66</b>	<b>199.83 - 210.67</b>

**Coinbase Global, Inc. (COIN)** ☆ Follow

**207.60 +8.43 (+4.23%) 207.07 -0.53 (-0.26%)**

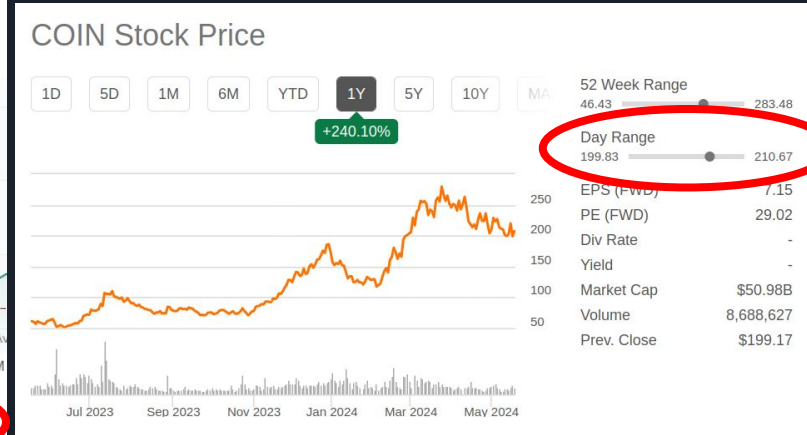
At close: May 17 at 4:00 PM EDT After hours: May 17 at 7:59 PM EDT

1D 5D 3M 6M YTD 1Y 5Y All

6:15 PM 6:30 PM 6:45 PM 7:00 PM

Volume Not Av

Previous Close	<b>199.17</b>	Day's Range	<b>199.83 - 210.67</b>
Open	<b>205.31</b>	52 Week Range	<b>46.43 - 283.48</b>
Bid	<b>207.53 x 100</b>	Volume	<b>8,688,627</b>
Ask	<b>207.76 x 200</b>	Avg. Volume	<b>11,777,426</b>



# "DeFi" Prices

Binance

OKX

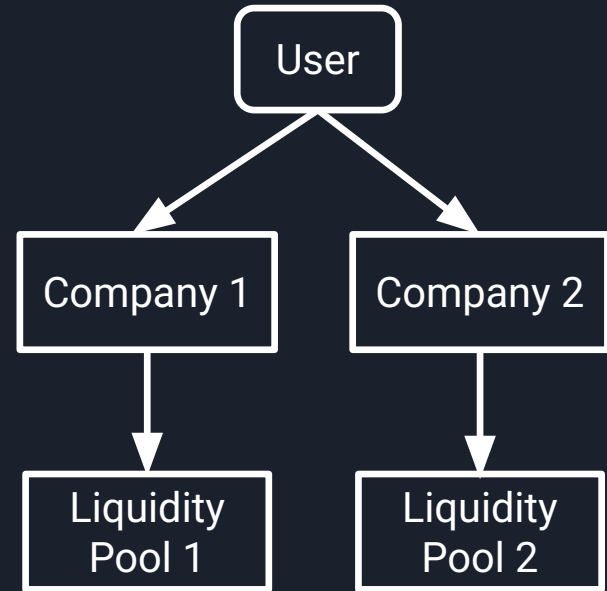
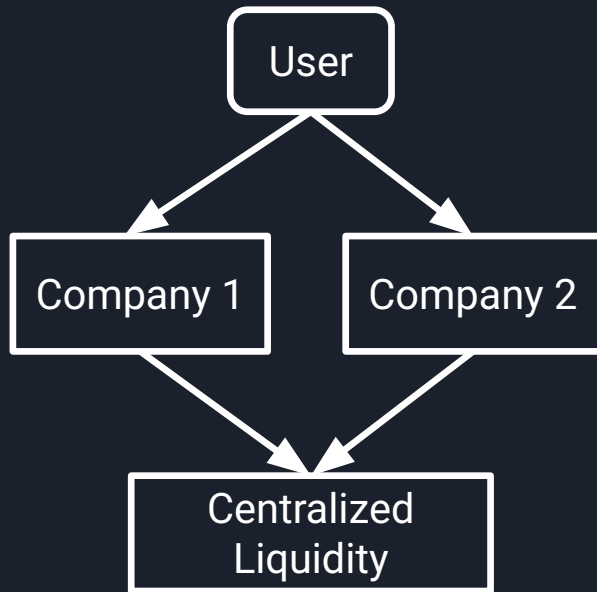
## 24hr Lows

- Kucoin: \$3001.70
- Binance: \$3007.07
- OKX: \$3018
- Kraken: \$3023.62

Kucoin

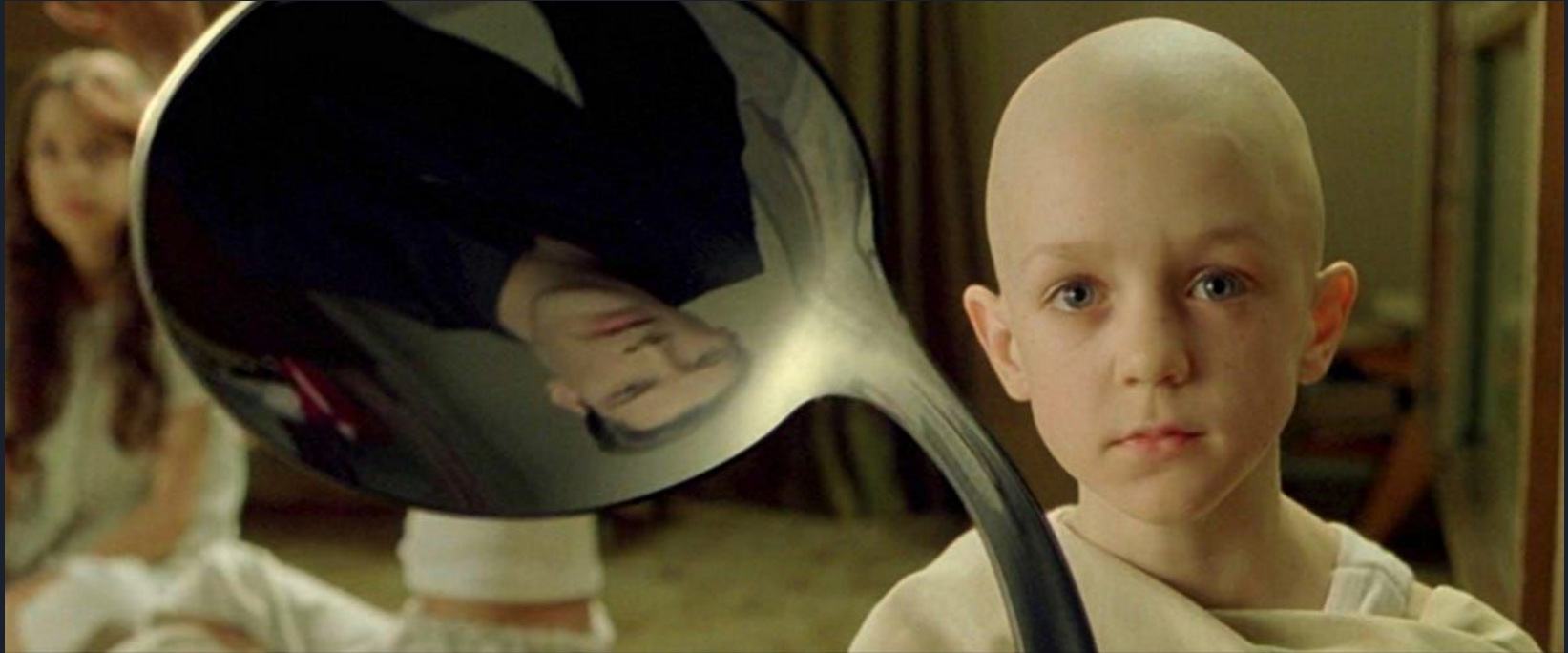
Kraken

# TradFi vs. DeFi





DeFi: There is no “price”





## To Recap

- 01 Price data is needed almost everywhere
- 02 There is no single price used everywhere
- 03 But we need to generate a single price

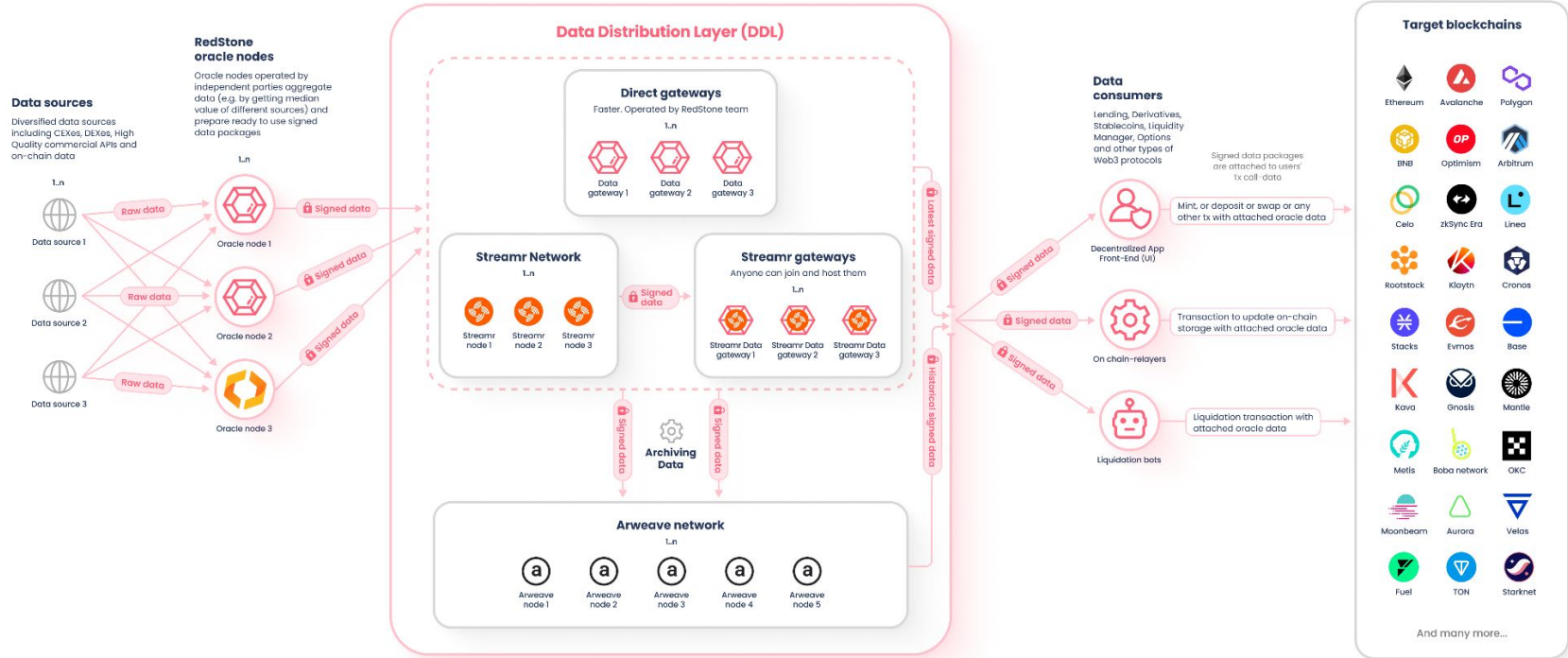


# The Solution

# The Solution



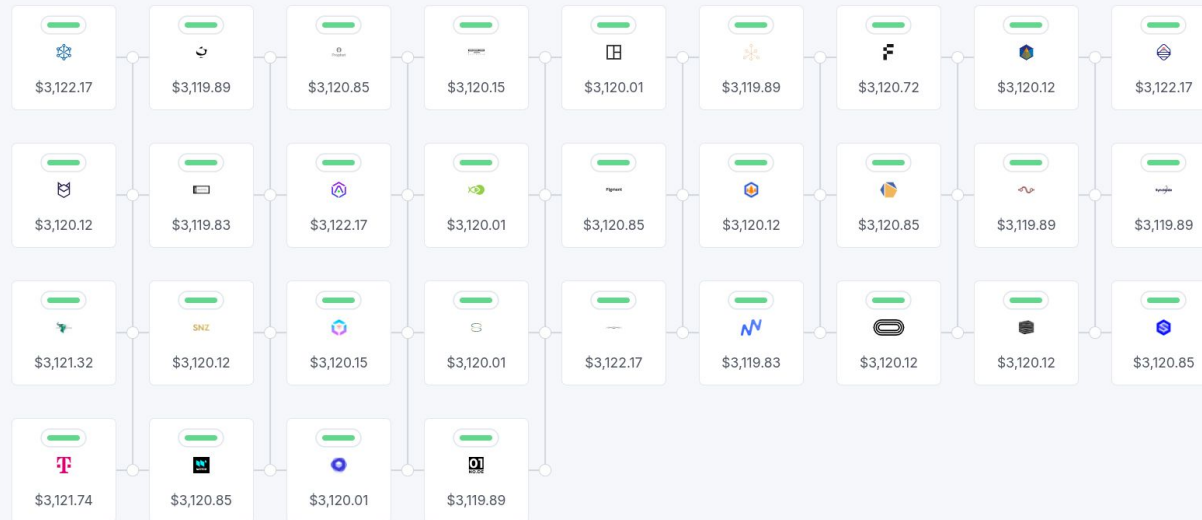
# The Solution



# The Solution

## Oracles data

### Oracles



#### Legend

Responded

Awaiting response

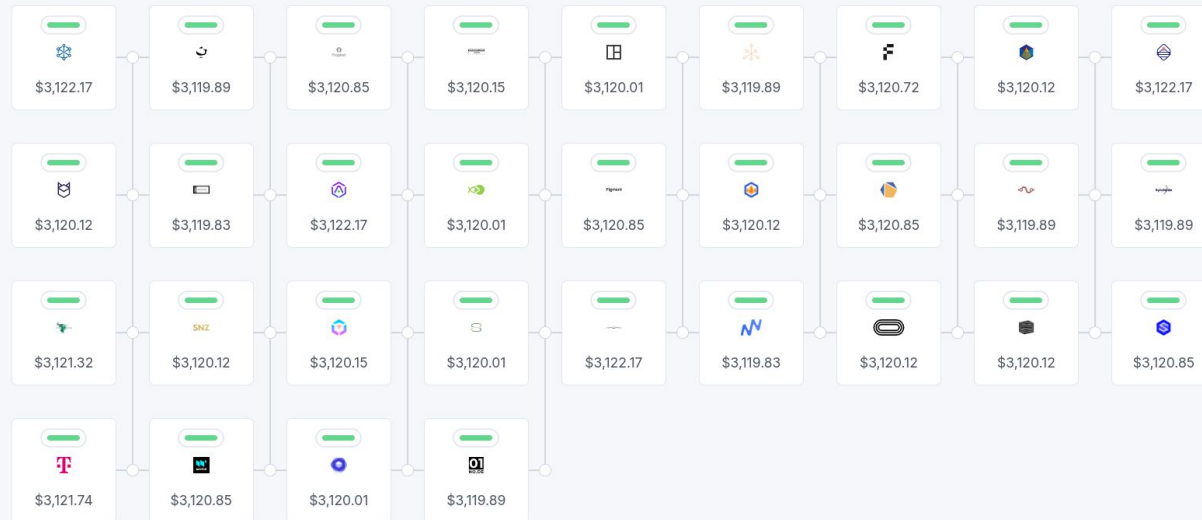
## The Solution



# Can I trust everyone here?

## Oracles data

### Oracles



#### Legend


Responded



Awaiting response




# Can I trust everyone here?

Data / Data Feeds /


 **AGEUR / USD** Angle Protocol

 Crypto  Stablecoin

Answer ⓘ

 \$1.0905

Network

 Polygon Mainnet


Tier ⓘ


High Market Risk

Trigger parameters ⓘ


Deviation threshold 0.1% Heartbeat 23:46:19

Data / Data Feeds /


 **AAVE / ETH** Aave


 Crypto

Answer ⓘ

 ₿0.026900

Network

 Ethereum Mainnet

Also on other networks 


Tier ⓘ



Medium Market Risk

Trigger parameters ⓘ


Deviation threshold 2% Heartbeat 22:20:34

Data / Data Feeds /


 **VELO / USD** Velo

 Crypto  Crypto

Answer ⓘ

 \$0.13816703

Network

 Optimism Mainnet

Tier ⓘ

New Token

Trigger parameters ⓘ

Deviation threshold 0.5% Heartbeat 23:54:12

# Can I trust everyone here?

## Data Feed Categories

### ● Medium Market Risk Feeds

These feeds also follow a standardized data feeds workflow to report market prices for an asset pair. The pair in question may have features that make it more challenging to reliably price, or potentially subject it to volatility which may pose a risk in some use cases. While the architecture of these feeds is resilient and distributed, these feeds carry additional market risk.

Types of market risk that may lead to a feed being categorized as Medium Market Risk include:

- Lower or inconsistent asset volume may result in periods of low liquidity in the market for such assets. This, in turn, can lead to volatile price movements
- A spread between the price for this asset on different trading venues or liquidity pools.
- Market Concentration Risk: If the volume for a given asset is excessively concentrated on a single exchange, that trading venue could become a single point of failure for the feed.
- Cross-Rate Risk: The base asset trades in large volumes against assets that are not pegged to the quote asset. As a result, the price of this specific asset pair may fluctuate even if the underlying asset is not being traded.
- The asset is going through a significant market event such as a token or liquidity migration.
- The asset has a high spread between data providers, the root cause of which is often one of the above factors.



# Can I trust everyone here?

Deprecation dodgeball for devs

<https://docs.chain.link/data-feeds/deprecating-feeds>

getAnswer



THIS FUNCTION IS DEPRECATED. DO NOT USE THIS FUNCTION.

latestAnswer



THIS FUNCTION IS DEPRECATED. DO NOT USE THIS FUNCTION.

latestRound



THIS FUNCTION IS DEPRECATED. DO NOT USE THIS FUNCTION.

latestTimestamp



THIS FUNCTION IS DEPRECATED. DO NOT USE THIS FUNCTION.

Data / Data Feeds /



## Pudgy Penguins Floor Price

Crypto

NFT

Answer ⓘ



10.3305

10.3305

Network



Ethereum Mainnet

Tier ⓘ

Deprecating

Data / Data Feeds /



## Bored Ape Yacht Club Floor Price / ETH

Crypto

NFT

Answer ⓘ



Ξ11.7654

Ξ11.7654

Network



Arbitrum Mainnet

Tier ⓘ

Deprecating

Can I trust everyone here?



Can I trust everyone here?





# Can I trust everyone here?

## Selecting Quality Data Feeds

---

When you design your applications, consider the quality of the data that you use in your smart contracts. Ultimately you are responsible for identifying and assessing the accuracy, availability, and quality of data that you choose to consume via the Chainlink Network. Note that all feeds contain some inherent risk. Read the [Risk Mitigation](#) and [Evaluating Data Sources](#) sections when making design decisions. Chainlink lists decentralized data feeds in the documentation to help developers build new applications integrated with data.



# Can I trust everyone here?



[Home](#) [Price Feeds](#) [Express Relay](#) [Entropy](#) [Get In Touch ↗](#)

[Search documents](#)

[Schedule Price](#)

[Updates](#)

[Create TradingView Charts](#)

[Derive Cross Rate](#)

[Migrate an App to Pyth](#)

[Use Pyth for Morpho](#)

## Adversarial selection

Pull updates give users of Pyth Network some ability to select which price to use in a transaction. This ability is highly circumscribed by various constraints: on-chain prices must move forward in time and cannot be from too far in the past. However, users can still choose any price update that satisfies these constraints. This ability is functionally equivalent to latency: it allows users to see the price in the future before using a price from the past.

How do you feel about your relationship?





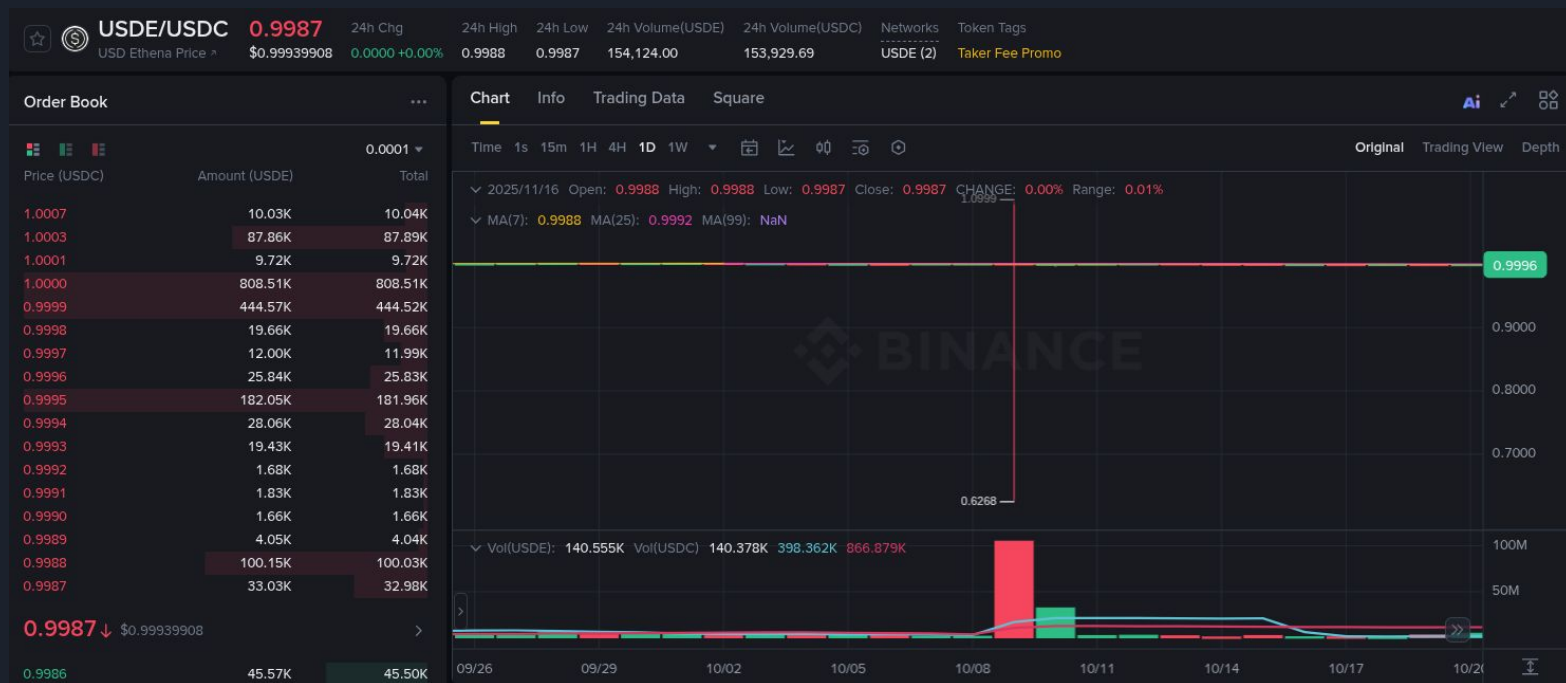
And now for some recent events

## **THE \$19 BILLION ORACLE DUMP**



# 10/10/25 USDe Binance depeg

USDE Low: 0.6268 (38% below peg)



# 10/10/25 USDe Binance depeg

**WBETH Low: 0.2012 (80% below peg)**



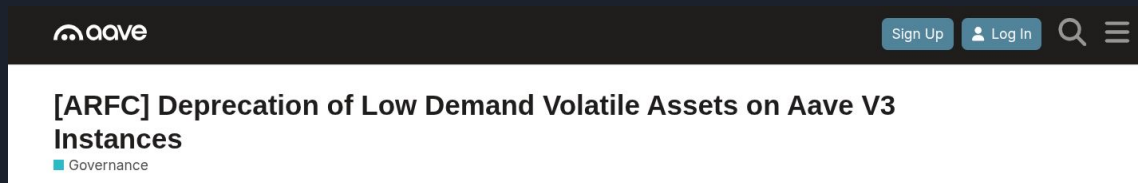
# 10/10/25 USDe Binance depeg

**BNSOL Low: 0.1286 (87% below peg)**



# USDe Binance depeg results

Depreciation of low volume assets after \$500k bad debt on Aave





# USDe Binance depeg results

## Lesson:

1. Don't rely only on internal orderbook oracles for pricing
2. Make sure the oracle price data is using a deep liquidity source
3. Depegging of correlated assets is **BAD** for everyone



# USDe Binance depeg results

- 01 \$19B destroyed by bad Binance oracles
- 02 Depogs ONLY impacted Binance pricing, DeFi didn't depeg
- 03 Everyone in the ecosystem loses

## Another recent event



**Moonwell** 🟡  
@MoonwellDeFi



We are currently investigating a misreported price for wrsETH.

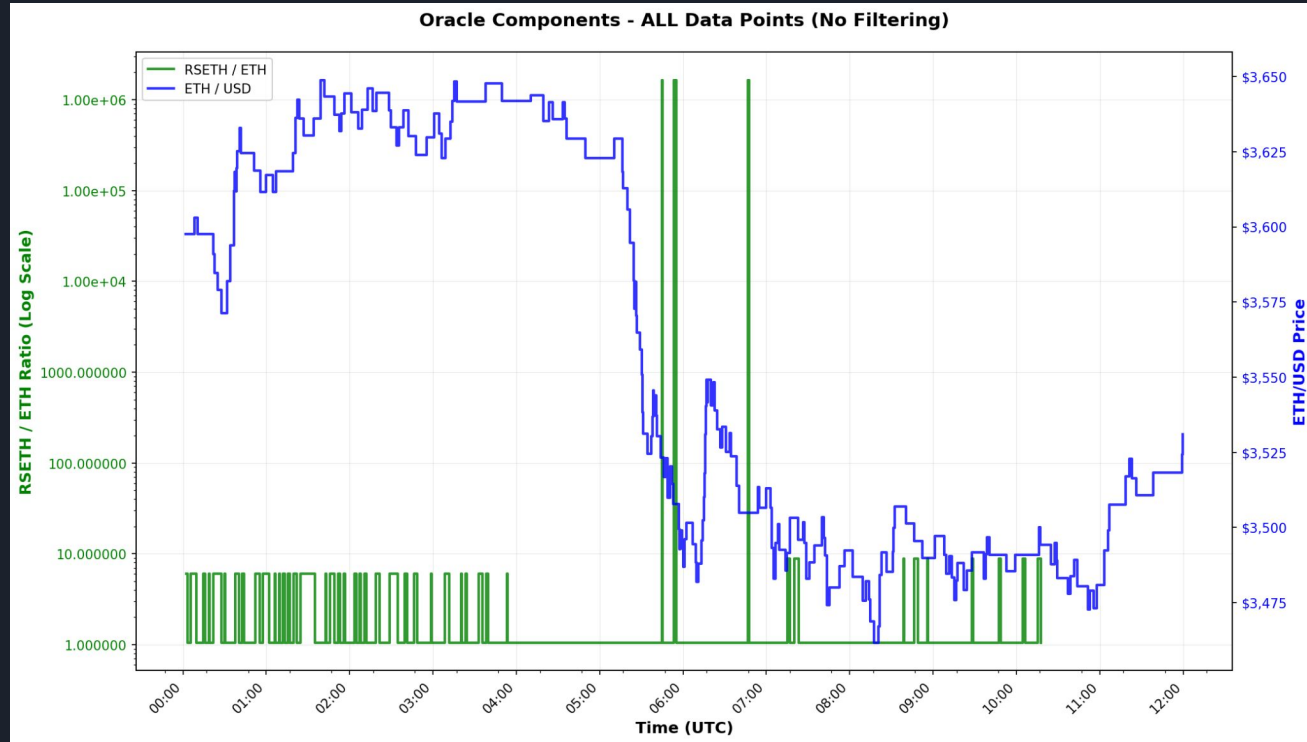
The risk manager for the wrsETH Core Market on Base and OP Mainnet has significantly reduced the supply and borrow caps in these markets.

We will share more information as it becomes available.

12:03 PM · Nov 4, 2025 · **53.1K** Views

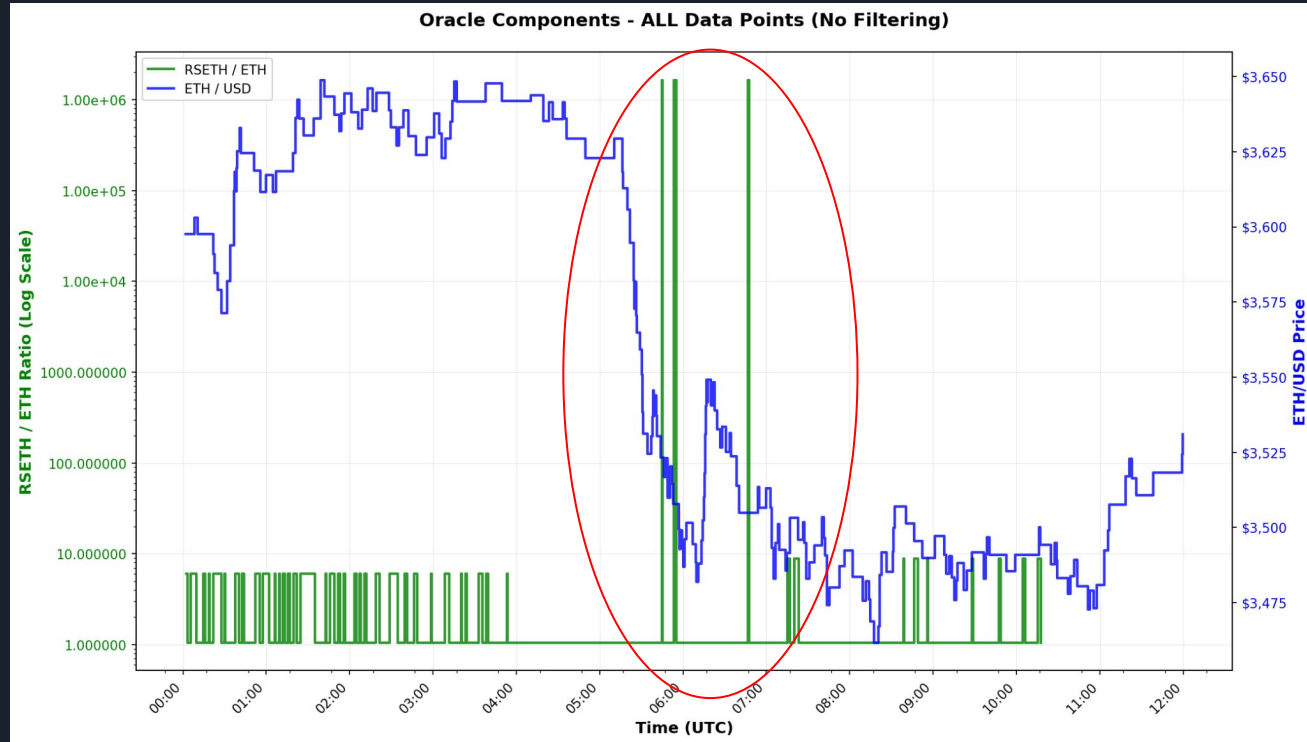


# Can you spot the problem?



Impacted oracle: <https://basescan.org/address/0x4a61db12d0cb4293d799ecdd82e5994b5746f850>

# Can you spot the problem?



Impacted oracle: <https://basescan.org/address/0x4a61db12d0cb4293d799ecdd82e5994b5746f850>



Can you spot the problem?

**Chainlink oracle glitch costs Moonwell  
\$1M as DeFi suffers another exploit**

# Can you spot the problem?

Data

answer : 1649934607354199816332700

transmitter : 0xc04a3C4aBF8995Da051140f552Cb4eB086185836

observations : 1054227129414975900

1054316022961676400

1054316022961676400

1055981600197286400

1056070493743986900

1649934607354199816332700

1649934607354199816332700

1649934609108670598643200

1649934609197564145343700

1649934609197564145343700

observers : 01020406070508030009

rawReportContext : 00000000000000000000FF27F6D70FBE846768EBA2B013701A88000352B403

Dec

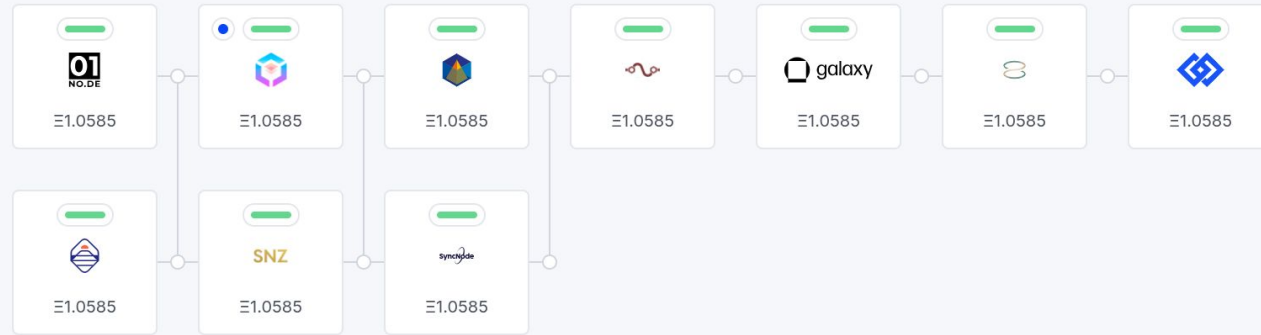
Hex

5 vs 5

# Can you spot the problem?

## Oracles data

### Oracles



### Legend



Responded



Awaiting response



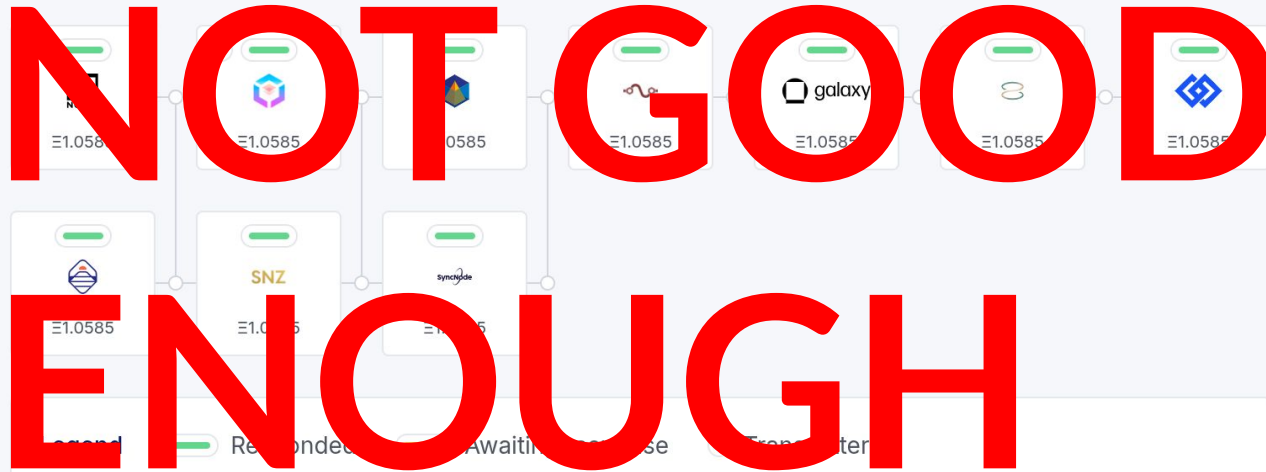
Transmitter

Can you spot the problem?

## Oracles data

Oracles

**NOT GOOD ENOUGH**





# Moonwell oracle incident results

## Lesson:

1. Oracles should not rely on markets which can be manipulated
2. There must be guardrails on oracle pricing data, ESPECIALLY for correlated assets. There is no realistic scenario where the price should be allowed to jump by over 1,000,000x in a single block (or any reasonable time period)



# Summary

- 01 DeFi price oracles are a foundational piece of this ecosystem
- 02 DeFi price oracles are a difficult (and potentially unsolved) problem
- 03 Managing all possible oracle risks is HARD even in 2025



The End

Questions?

