GYROSCOPE

Designing Resilient Oracles

The Consolidated Price Feed

Ariah Klages-Mundt, Steffen Schuldenzucker

Superluminal Labs

Blockchain Oracle Summit, 21 July 2023

Motivation: Gyroscope

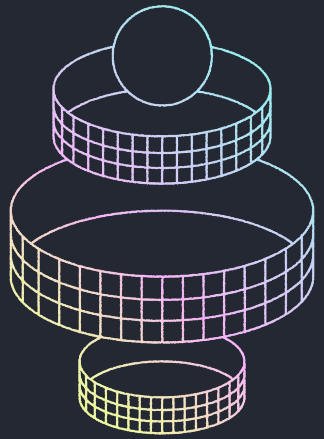
Gyroscope is a set of new infrastructure advancements that unlocks a new, third path between algorithmic and centralized stablecoins.

→ A new more resilient stablecoin: **GYD**

Gearing up for mainnet launch: August/Q3 2023

Proto system (live on Polygon): app.gyro.finance/

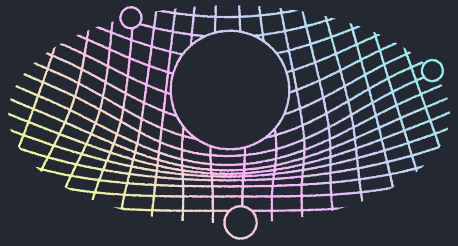
GYROSCOPE



Resilient defence

Reserve assets and yield sources diversified by design.

Dynamic Stability Mechanism automatically adapts to maintain stability and liquidity.



Liquidity network

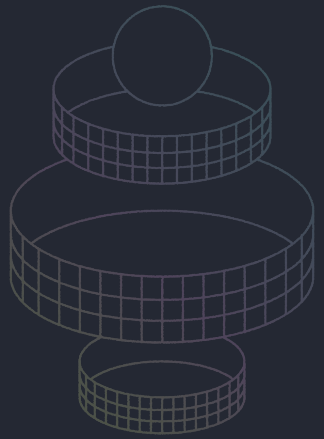
More efficient Concentrated Liquidity Pools.

Redundant and independent liquidity channels.

Redundancy

Consolidated Price Feed and Circuit Breaker systems protect protocol when prices are uncertain.

Gyroscope



Resilient defence

Reserve assets and yield sources diversified by design.

Dynamic Stability Mechanism automatically adapts to maintain stability and liquidity.

Liquidity network

More efficient Concentrated Liquidity Pools.

Redundant and independent liquidity channels.

Redundancy

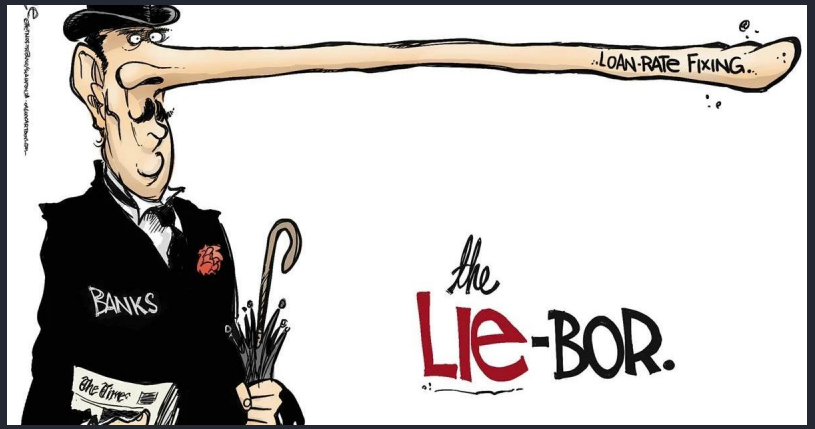
Consolidated Price Feed and Circuit Breaker systems protect protocol when prices are uncertain.

The oracle problem

- Financial contracts require secure data feeds
- How do we build these in resilient ways?
- Not unique to blockchain

Example: LIBOR manipulation (2003-2012)

- Manipulate interest rate data used in many contracts
- Deutsche Bank, Barclays, Citi, JP Morgan +
- Banks submitted incorrect data to force LIBOR to their advantage (make positions profitable)



Takeaways

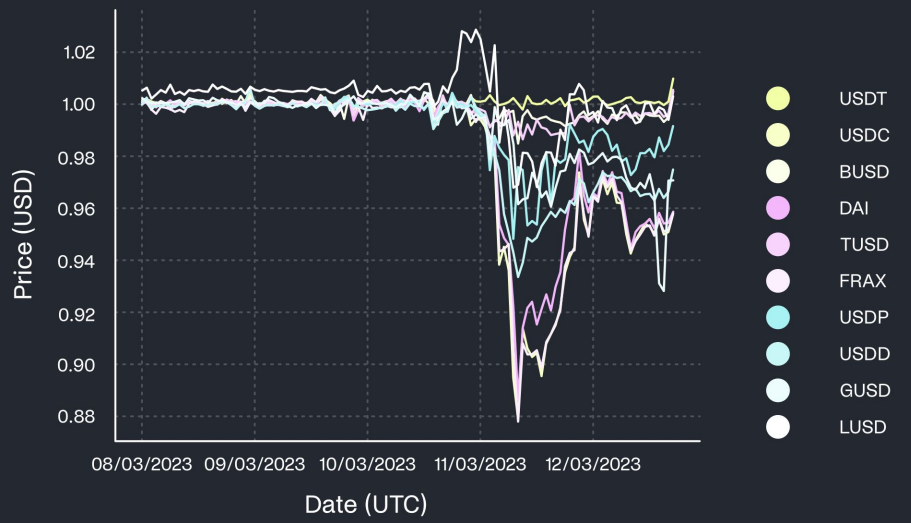
- Known issue even with high reputation entities
- Can blockchain help us build more resilient feeds?

In blockchain applications: need price data

- Some price processes take place off-chain (on CEXs)
- And these processes involve off-chain assets (USD) and *can't* happen on-chain
- Important: dangerous to use stablecoins as quote asset in place of USD (example: Mar 2023)

Need oracles to import these prices on-chain

- Oracle price correctness can't be fully verified
- Can only authenticate that provider is who they say they are



All of DeFi relies on oracles

Stablecoins
Price their reserve assets

Insurance
Trigger condition and how much to pay out

Lending
Compute collateralization, trigger liquidation

Derivatives
Compute payments, trigger position closure

...

Current oracle approaches come with challenges

Centralized Oracles
Requires trust in a central data provider.

Medianizing (Chainlink)
Off-chain aggregation + on-chain verification. →
Essentially a trusted multisig, potential collusion.

DEX TWAPS
- Manipulable when liquidity is low (e.g. INV, Apr 2022), more so after the merge, but quantifiable costs
- slow
- only for on-chain assets (no USD)

Betting Markets / Data Derivatives
Potential collusion / Keynesian beauty contest

Topics

I. New oracle approach: validating *likelihood* of oracle integrity

II. First instance: Gyroscope's Consolidated Price Feed (CPF)

III. Research into new data sources for CPFs

IV. Future directions

New approach: validating *likelihood* of oracle integrity given other observable variables

Input data
- On- and off-chain sources
- Price and possibly non-price data

Mechanism that we need to design: system of no-arbitrage conditions on input data

Output data
- Price estimates
- Signal about likelihood of oracle integrity

Motivation / use case of this design

Treat oracle data as *candidate* prices and consolidate with on-chain data.
Goal: *fast* but with added safety guarantees!

Protocols can use oracle integrity signal (new info) to improve security:

- Trade off liveness ↔ economic security
  - ⚠ Current Default: Security ?, Liveness ↑↑
  - Gyroscope: Security ↑, Liveness ↓
  - Lending Protocols: Pause borrowing.
- Decide which oracle they want to use

What this mechanism should aim to do:

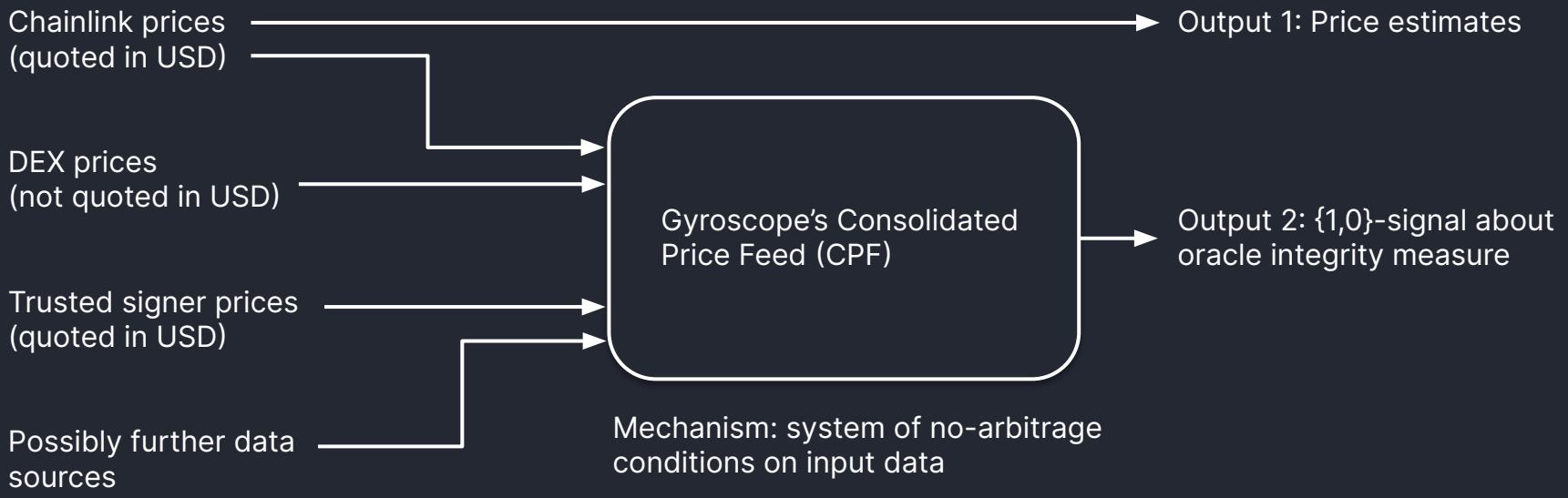
- Speed
- Liveness (most settings)
- Detect stale prices
- Costly to manipulate price estimates
- Costly to manipulate signal of oracle integrity
    - A DoS: potentially affect liveness of protocols using the price feed

Why this is hard:

- Formulating system of no-arbitrage conditions to get these properties isn't straightforward
- Balance security models, manipulation costs, failure points of different data sources
- Cover corner cases of stablecoin pricing

II. Gyroscope’s Consolidated Price Feed (CPF)

First version of this new approach: Gyroscope's Consolidated Price Feed (CPF)



Vector of Oracle Prices = a solution to a system of equations

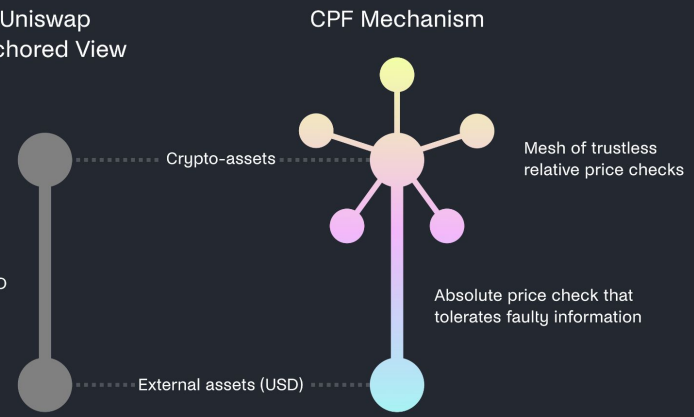
Oracle USD prices p_i solve

$p_{i/j}$, some on-chain source $\approx \frac{p_i}{p_j}$ relative

$\tilde{p}_i$, some on-chain source $\approx p_i$ absolute

For at least a spanning tree of (i,j) pairs.
Pull $p_{i/j}$ from a resilient, but not perfect, data source.
No arbitrage bounds.
Can use multiple checks.

For at least one i.
Pull $\tilde{p}_i$, some source from a resilient, but not perfect, data source.
Can use multiple checks.

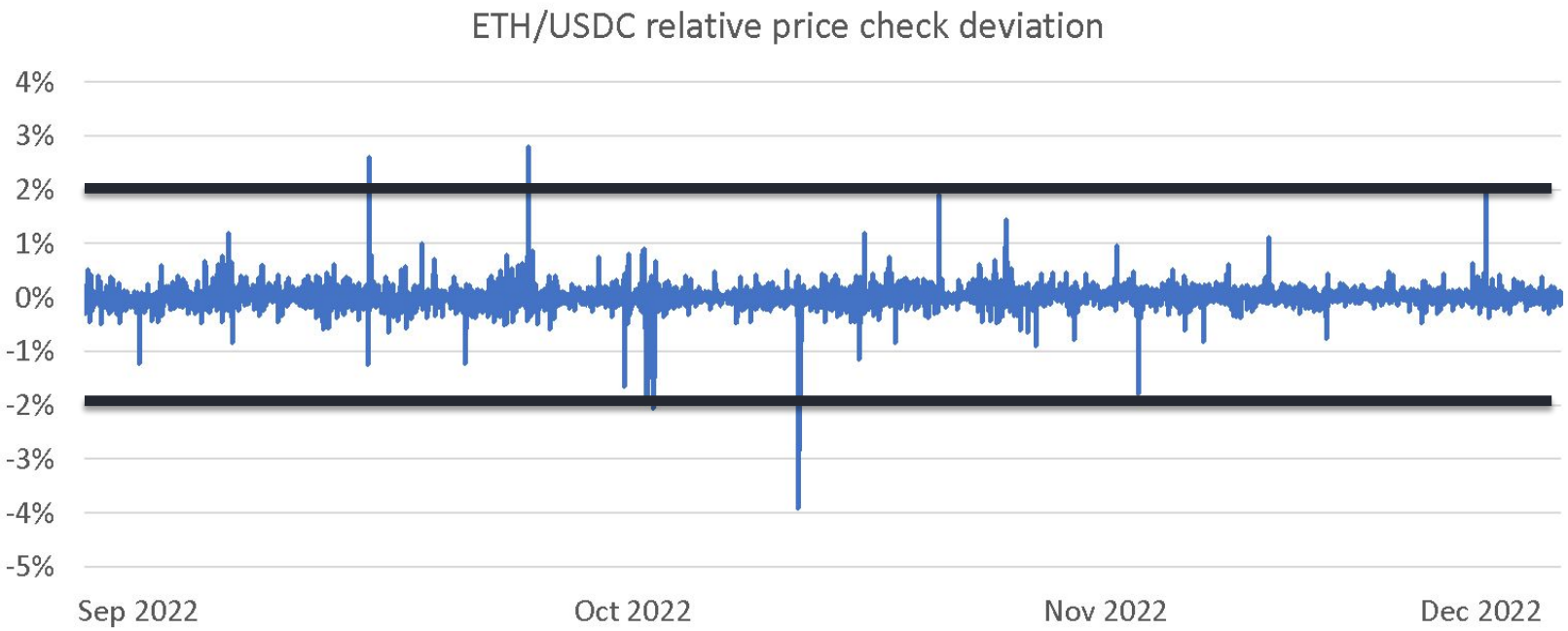


Relative Price Checks via DEX TWAPs

- Manipulation cost ↔ pair liquidity
- Manipulation → Check *fails*!

$$\frac{|p_{i/j,DEX\ TWAP} - \frac{p_j}{p_j}|}{p_{i/j,DEX\ TWAP}} \leq \varepsilon_{i,j}$$

Historical discrepancy in relative prices: WETH/USDC



Absolute Price Checks

- Choose reference asset i.
  - ⚠ Absolute price sources are significantly error/manipulation-prone!
  - ➔ Use multiple!
- DEX TWAPS: i/b pairs where b is a stablecoin.
- Signed (centralized) prices $p^k_{i,signed}$

$$m := \begin{cases} \min\left\{p_{i/b,\ \text{DEX TWAP}} \mid b \in B\right\} & \text{if } |B| \leq 2 \\ \text{secondMin}\left\{p_{i/b,\ \text{DEX TWAP}} \mid b \in B\right\} & \text{if } |B| > 2 \end{cases}$$

$$\tilde{p}_i := \text{median}\left(\left\{p^k_{i,\ \text{signed}} \mid k \in E\right\} \cup \{m\}\right)$$

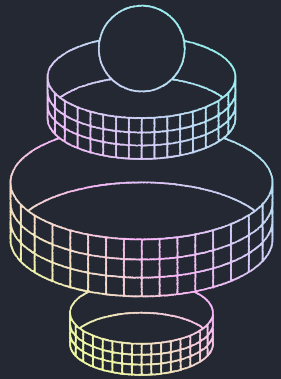
require:

$$\frac{|p_i - \tilde{p}_i|}{\tilde{p}_i} \leq \varepsilon_i$$

Complementary Safety Measures in Gyroscope

Excessive flow circuit breaker; oracle guardians

Pause a reserve vault in case of extreme in/outflow, or manually



Manipulation-resistant LP share pricing

Compute equilibrium, not momentary LP share values.

Flash Crash Circuit Breaker (inactive)

Invalidate prices during extreme short-term movement.

III. Research into new data sources for CPFs

[Submitted on 28 Mar 2023]

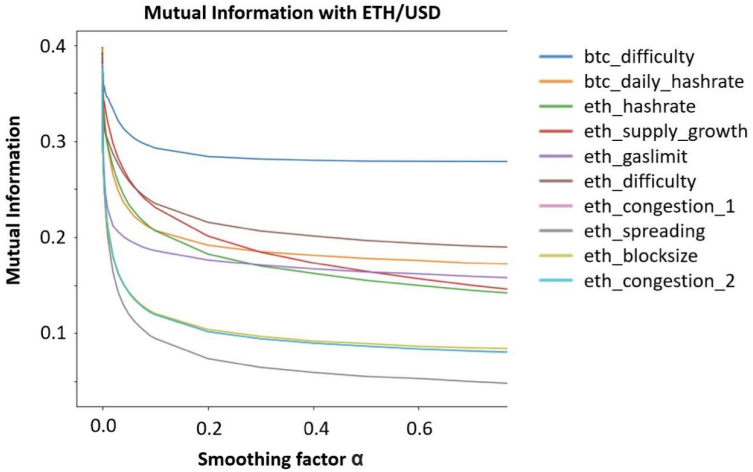
Oracle Counterpoint: Relationships between On-chain and Off-chain Market Data

Zhimeng Yang, Ariah Klages-Mundt, Lewis Gudgeon

https://arxiv.org/abs/2303.16331

Can non-price chain data help sense-check prices?

- Aim: recover off-chain price signal from non-price chain data
- Context: agents incorporate off-chain prices (e.g., ETH/USD) into on-chain decisions
  - *Some* causal relationship here likely (both in economic models and empirical)
- Want: alternative trustless input for absolute price checks
- This data can be manipulated, but costly to do so (part of on-chain markets)



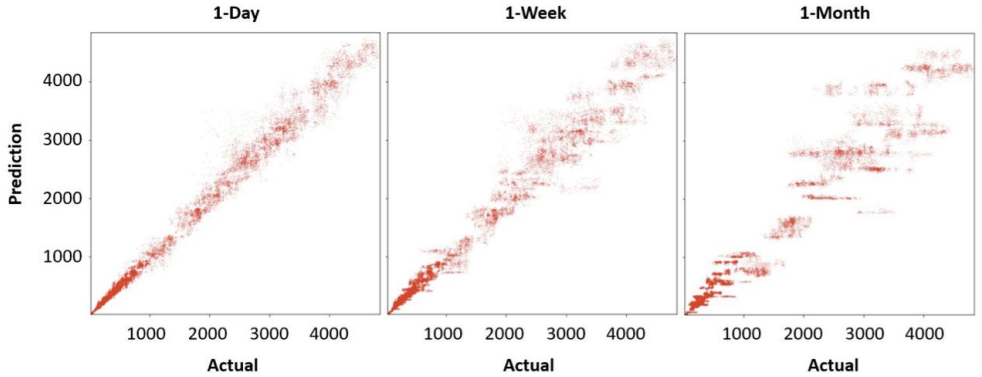


Fig. 5: Recovered price vs actual for random forest with given retraining periods.

Future directions

Research topics

- **Optimally calibrating a CPF:** balancing security models and gas costs
  - Can formulate as optimization problem given existing work on e.g., TWAP manipulability
  - Aim: improve the properties achieved by the mechanism

- **Incorporating further data sources into a CPF:**
  - Difficulties: modeling approach, accessing some chain data within EVM, factoring manipulability into model

- **Expanded mechanism:** switch btw price feeds or provide uncertainty bounds

- **Model the economics of oracles:** how are incentives affected by this architecture?
  - Can model as capital structure models. Interchange oracle provider with governors in existing models: https://arxiv.org/abs/2006.12388 https://arxiv.org/abs/2109.08939
  - *Idea:* CPF adds constraints to these models that tend to increase incentive compatibility of oracle provider

Economically securing oracle networks

- Current stake-slashing criteria for oracle networks
  - Suffers beauty pageant problem (same as oracle problem)
  - Rely on consensus of other node operators, but the consensus is not provably correct

- Designing alternative criteria: an ‘optimistic’ version of CPF
  - Oracle node operators report both prices and {0,1} whether CPF conditions would be violated (without executing)
  - Anyone could prove if the latter was reported incorrectly ⇒ slash node operator

Conclusion

- DeFi depends on oracle prices but they’re often taken at face value.
- Our Solution: Consolidated Price Feed (CPF)
    - Validate implied relative prices, absolute price level against on-chain data sources.
    - Additional safety measures: Circuit breakers, equilibrium LP share pricing.
    - Speed of Chainlink / Chronicle, but with more safety guarantees on top.
    - Live on Polygon (soon Ethereum)

Paper & Docs:

gyro.finance / @gyrostable