Recently there have been concerns raised about the long-term security of Time-Weighted Average Price (TWAP) oracles as implemented by Uniswap, especially related to the Proof of Stake transition and more sophisticated MEV capabilities.

I've been working on a new price oracle implementation that computes the median price during a specified window of time. Median is believed to be more secure against attackers who can manipulate an AMM price over several blocks in a row, since the outlier values will be thrown out unless the attacker can persist them for half the window size.

Since this is a ground-up redesign of the oracle mechanism, I've also tried to improve on it in some other areas as well:

- Computes both the median and

the geometric TWAP concurrently and returns both, so that the oracle consumer can decide which to use.

- If the window cannot be satisfied because the record needed has already been overwritten in the ring buffer, it returns the longest available window instead of throwing an error. Instead, the consumer can decide what to do.
- Typical gas required to read the oracle is much smaller than Uniswap3, and is competitive with centralised oracles like Chainlink for most assets.
- Gas used is independent of the ring-buffer size

Of course there's no such thing as a free lunch and there are some trade-offs as well:

- Worst-case gas usage is higher than Uniswap3 (although in my opinion this is manageable – see the documentation)
- In theory, adversarial input data could cause the gas to balloon, although I have a proposed fix for this (comments appreciated!)
- In theory, adversarial input data could cause the gas to balloon, although I have a proposed fix for this (comments appreciated!)
- Price resolution is 0.3% (compare Uniswap3 at 0.01%, and Chainlink at 1%)
- The maximum time window that can be requested is 65535 seconds (about 18 hours 12 minutes)
- The time window must always be aligned to the present – you cannot query historical windows
- Only price can be queried, not pool liquidity

I've also created a simulation that replays Swap

logs from mainnet into my proof of concept as well as a stripped down version of Uniswap3. This lets us compare the resulting prices and gas usage. As a teaser, here's one of the images output from the simulation:

[

simulation

1915×967 159 KB

](https://ethresear.ch/uploads/default/original/2X/3/3821bbeabd1340f5bc577e65a49cb5e9bef20f3d.png)

Check out the docs for a more detailed explanation of how it works. And more pictureshttps://github.com/euler-xyz/median-oracle

Thanks in advance for any feedback!