TWAP Oracles after The Merge

•••

Mark Toda

Who is this guy

Solidity / blockchain engineer since 2017

Currently hacking @ Uniswap Labs

Previously designed protocols @ Buttonwood (crypto bonds), Arcade.xyz (NFT lending), BitGo

TWAP Oracles Now

Safe & Decentralized On-chain Price Feed

❌ AMM *spot* prices can be manipulated

✅ Use time-weighted average price instead

- Still possible to manipulate
- TWAP increases the cost of an attack *significantly*
- And requires multiple blocks, so attacker takes risk

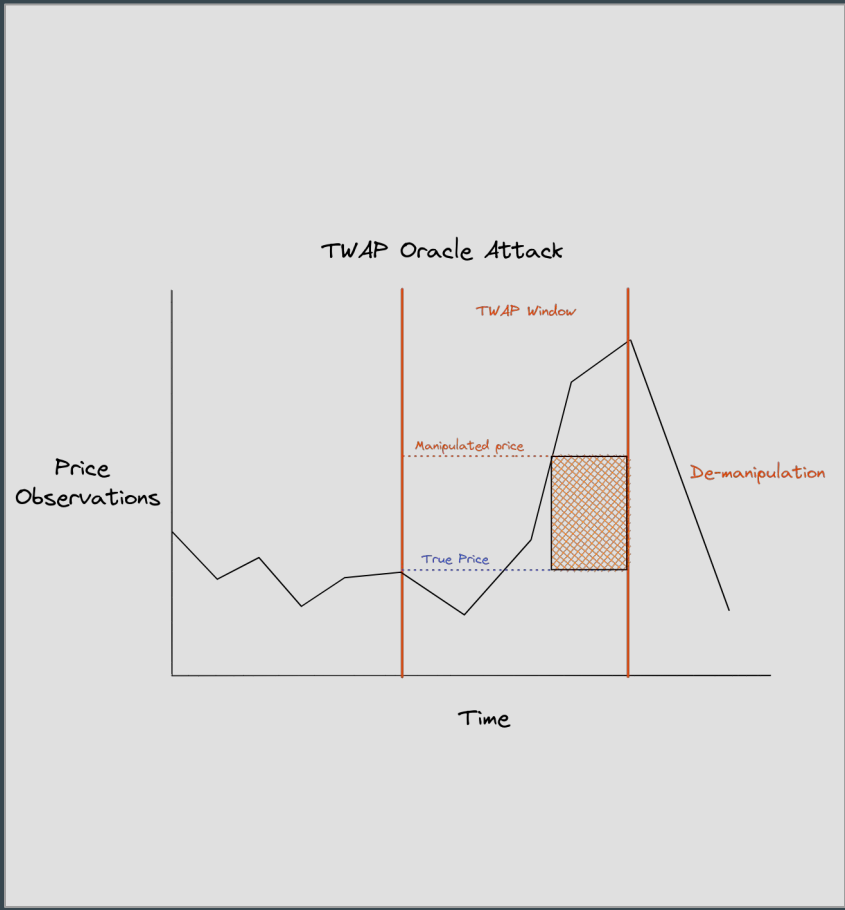
Anatomy of TWAP manipulation

3 Stages:

- Manipulate the price
- Use the manipulated price for something
- De-manipulate the price to recoup costs

Example uses:

- Take under-collateralized loan
- Liquidate healthy vaults



It’s super hard

Cost of TWAP manipulation

$23.7 trillion – capital required to move ETH/USDC UniswapV3 TWAP 30%

- Assuming 144 block TWAP window at current liquidity (~30 mins)

The attacker then waits until the next block where it must:

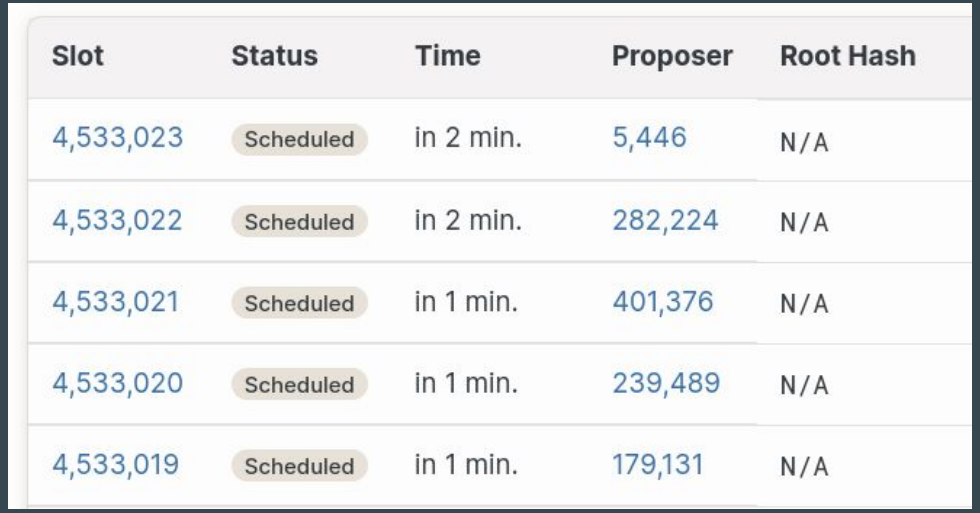
- *Compete* to profit from the manipulation
- *Compete* to recoup its upfront cost

Data from https://oracle.euler.finance/

What changes with the Merge?

Predictability!

Block producers know their assignments several minutes in advance



Slot	Status	Time	Proposer	Root Hash
4,533,023	Scheduled	in 2 min.	5,446	N/A
4,533,022	Scheduled	in 2 min.	282,224	N/A
4,533,021	Scheduled	in 1 min.	401,376	N/A
4,533,020	Scheduled	in 1 min.	239,489	N/A
4,533,019	Scheduled	in 1 min.	179,131	N/A

beaconcha.in

So?

Allows for easier multi-block manipulation:

- Get assigned multiple blocks in a row
- Buy the block before yours (e.g. with Flashbots)
- Multi-block bundles?

Potential for risk-free manipulation attacks

It’s still hard

Cost of TWAP manipulation under PoS

Same situation as before: 30% TWAP move on ETH/USDC UniswapV3 with 144 block window (~30 minutes)

2 blocks in a row:

- $23.7 trillion — same capital requirements as before
- Risk-free de-manipulation

3 blocks in a row: $9.5 billion capital required

5 blocks in a row: $103 million capital required

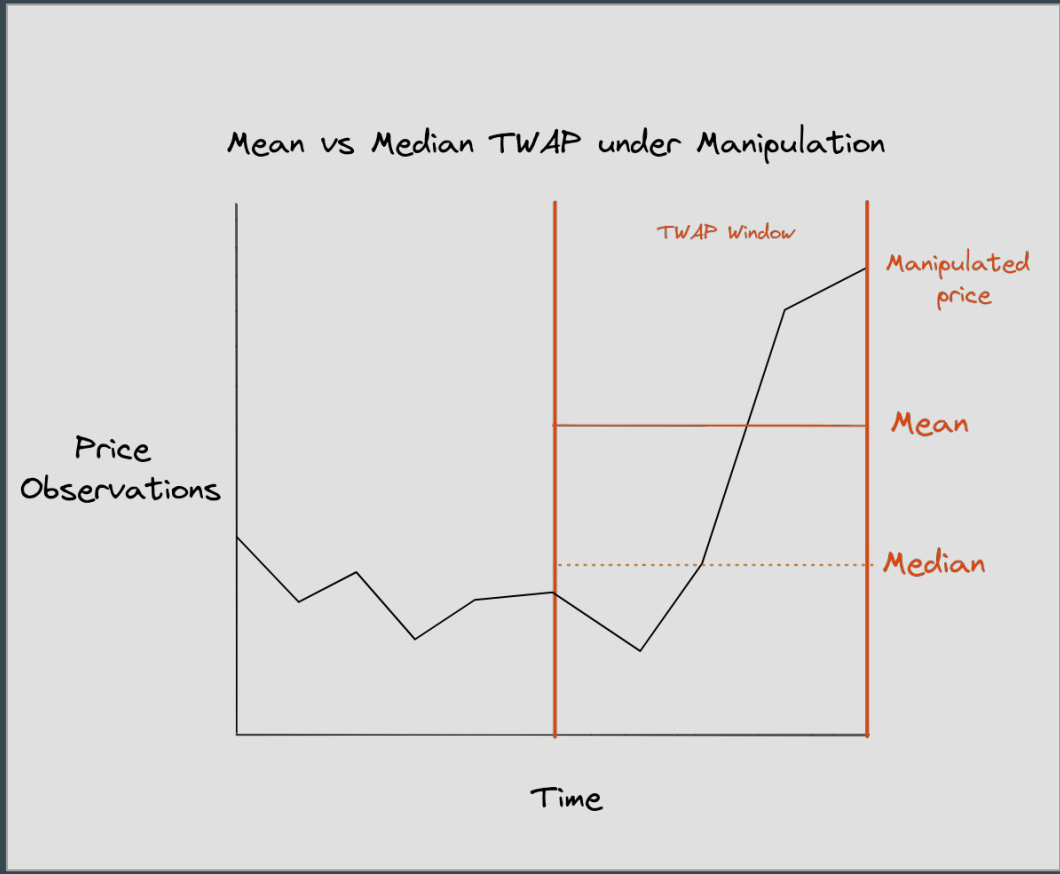
Data from https://oracle.euler.finance/

How to improve?

Medians!

Filters outliers

Need to manipulate (n / 2 + 1) blocks in the window to affect the median *at all*



Median TWAP manipulation under PoS

73

Number of blocks *in the window*
needed to manipulate the TWAP price

... good luck with that


Thanks :)

 @marktoda

References

- Lots of conversations w/ Uniswap & Euler teams
- Doug Hoyte - ETHResearch post
- Doug Hoyte - Median TWAP PoC
- ETH Zurich - TWAP manipulation research

Appendix

But UniswapV3 uses Geometric Mean

True, but mostly because it means the oracle only needs to track a single accumulator

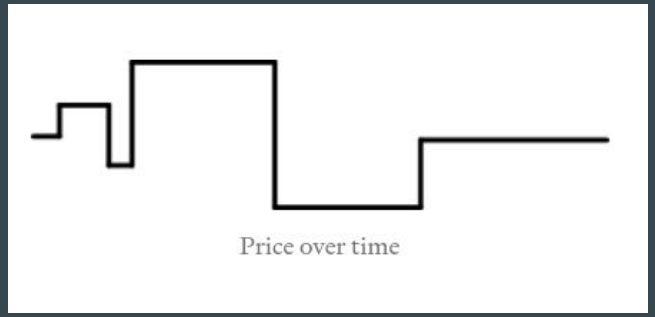
- Because the inverse of the geometric mean == the mean of the inverses
- Eg. 1 / TWAP for A/B == TWAP for B/A

It doesn't really help with oracle manipulation

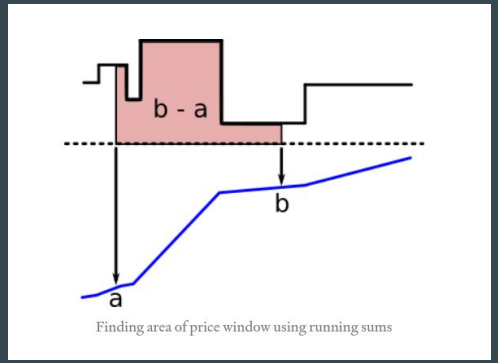
Other options?

- Use a larger window
  - Trade off price sensitivity for manipulation cost
  - Even small increases in window size increase cost of manipulation by a lot
- Be selective with pools
  - This is also true in PoW
  - More, widely spread liquidity helps

OK I oversimplified TWAPs



⇒



b - a = price-seconds in window
(b - a) / seconds = average price

https://blog.euler.finance/moving-average-filters-ac8913263d64