I’m interested if someone considered using an offchain oracle. I’m going to implement it and would like to check if perhaps someone else tried it before.

A traditional oracle works by frequently putting data feed into a smart contract. If we want to have a fairly recent data we need to spend a lot of gas and send a lot of transactions. This may not be problematic for feeds which are heavily used but doesn’t seem right if the feed is used scarcely.

The solution I’m considering is to have the oracle provide the feed value through HTTP API rather than put it on blockchain. The record would include the current blockNumber and the signature. A transaction using this value would need to provide: { value, blockNumber, signature }

and the smart contract of the oracle would validate that the signer is among the trusted providers and that blockNumber

isn’t stale (with some defined tolerance).

Comparing with a traditional oracle the history of the feed looked up on blockchain would only include the blocks in which the value was used, not every Xth block like in a traditional one. The gas costs of maintaining the feed is shifted from the data providers to feed users which is desirable in our usecase.

The whole idea is somewhat similar to how 0x protocol works. In a sense, 0x fill()

method relies on offchain oracle (taker) to provide the data of order to fill, while the feed input is signed by the maker.

Has something like this been done before? Anyone sees week points of this design ?