One challenge of present-day decentralized oracle schemes is that they become unsafe if the amount of funds whose destination is affected by the oracle exceeds the market cap of the oracle token; if this happens, then token holders have the incentive to collude to give false answers to seize the funds. In such a case, the oracle would of course be forked and the oracle token would become worthless, but it would nevertheless be net-profitable for oracle participants.

The following is one possible alternative oracle design to fix this. We set up a contract where there are 13 “providers”; the answer to a query is the median of the answer returned by these providers. Every week, there is a vote, where the oracle token holders can replace one of the providers. This vote could be a simple vote, or it could be some more complicated mechanism such as quadratic vote or even futarchy.

The security model is simple: if you trust the voting mechanism, you can trust the oracle output, unless 7 providers get corrupted at the same time. If you trust the current set of oracle providers, you can trust the output for at least the next six weeks, even if you completely do not trust the voting mechanism. Hence, if the voting mechanism gets corrupted, there will be able time for participants in any applications that depend on the oracle to make an orderly exit (this would not be enough for long-term oracle needs such as Augur, but would suffice for eg. financial synthetics).