Hi Ethresearch,

Would love your thoughts on my idea, a proof-of-work oracle. Basicatlly it works as an oracle schema that implements a mineable proof of work (POW) competition to eliminate reliance on trusted third parties for access to off chain data. Users engage in a POW competition to find a nonce which satisfies the requirement of the challenge. The users who find a nonce which correctly solves the POW puzzle input data for the POW Oracle contract and receive native tokens in exchange for their work. The oracle data submissions are stored in the smart contract for use by other on-chain operations

To give an even simpler explanation, think mineable token, but with each solution submission, you get to put in some data (say BTC/USD price). The first n solutions are accepted and then the median is rewarded (neighboring answers get “uncle” rewards) in the form of a newly minted POW oracle (POWO) tokens. The median value is then timestamped and placed into a time series array which can be accessed through a getter function which charges parties a small amount of POWO tokens.

Here’s a picture:[

pow_oracle

1083×758 56.3 KB

](https://ethresear.ch/uploads/default/original/2X/1/14584ff6ec5dc984189a8b531c9fc836abe47085.png)

My team and I built a POC at a hackathon last weekend here : https://github.com/DecentralizedDerivatives/MineableOracle

(shockingly we lost the hackathon to an ERC20 token)

But I’d love to hear if you guys like the idea, have any questions or we’re just completely missing something