Note: Very similar to the topic being discussed atIncentives for running full Ethereum nodes, but I wanted to have a focused discussion on this particular mechanic.

Problem

As running a full node becomes more and more expensive due to the cost of storing and maintaining full state, we need a way to incentivize multiple parties to actually

store the full state.

Solution

- Periodically, the system asks everyone to commit (encrypted) what is at a particular address in state.
- Anyone can commit that they know what is at that address along with staking some amount of coins.
- Some time later (short duration) everyone reveals what they believe is at that address.
- Anyone who is right, gets a share of minted coins proportionate to their stake.
- Anyone who is wrong or doesn't reveal loses their stake.

Implementation Detail Problems

- How to choose what data to ask for? Want random selection, but also want the answer to not be 0

99% of the time.

Issues

- The target data becomes unavailable between the start of the round and the reveal phase as a selfish miner does not want to share the data during this time. IMO, this is acceptable but it does pressure the rounds to be short (maybe just a few blocks).
- An attacker can subvert the system by running a full node and sharing data during the rounds. This attack would be to make it so the system doesn't realize that full nodes are disappearing because they are not being rewarded. It is an odd attack, but I don't have a great solution for it.
- Proof pools. Someone can run a full node and then sell answers to the question to users in exchange for a small fee. Due to merkle tree magic, it is possible for this information sharing to be trustless, and with ZK proofs you can even (in theory) prove that you have the information prior to sharing it. This could result in a single actor running a full node and selling the information to others during the round. The saving grace here is that anyone can "break" this system by buying the data from the pool (at as low cost as possible) and then making it public for free. This devolves into something similar to the attack mentioned above.

Given the above issues, it feels like the worst case scenario is "no worse off than now" with no incentive to run a full node and some minted coins (inflation) being distributed to anyone who participates in the degenerate system and the best case scenario (no attackers) we are rewarding people who run full state nodes via some minted coins.

I'm curious if people have any other thoughts on what is wrong with such a system or ideas on how to resolve any of the above problems?