Summary

This proposes to allow users to stake rETH to become an aztec sequencer. It won't necessarily require using EigenLayer's smart contracts (it's optional, there can also be custom contracts deployed for this) more so the concept made popular by EigenLayer: Leveraging already existing ETH instead of a new token to run additional decentralized services.

It is very hard to introduce a new token and create a significantly big set of people holding that token without too much centralization in ownership. ETH had to exist many years to reach the levels of decentralization in holders it currently has. Using ETH as collateral for nodes that fulfill other duties not part of the core protocol allows these nodes to instantly benefit from the decentralized base of ETH holders.

There are at least 2 ways to leverage a protocol such as EigenLayer: a) Allow stakers to set their withdrawal address to an EigenLayer smart contract so it can add additional slashing conditions b) Allowing to re-stake using a liquid staking derivate such as rETH. This proposal proposes using b) the LSD token rETH. The advantages are as follows:

- even small holders with <32 ETH can join and fulfill aztec sequencing duties
- we separate the role of the ETH validator and aztec sequencer. These two things are not required to be fulfilled by the same entity. Thereby we lower the bar to become an aztec sequencer and make that position more inclusive (similar effect as the first point)

The result could be a PoS protocol similar to that used by Ethereum L1 where rewards are soley comprised of fees generated on the aztec rollup. rETH penalties could be distributed to all aztec sequencers proportional to their rETH staked.

Details

The idea is to basically copy the Ethereum L1 consensus protocol with a few changes. Where L1 PoS continuously selects the next block proposer we would select the next sequencer.

Ethereum mints new ETH to guarantee liveness of the L1 layer. While it is an open question if the protocol requires this or would be able to run solely on transaction fees rollups are in a good position to test this hypothesis. The trust guarantees rollups inherit from L1 put them in a great position to adopt a PoS mechanism similar to that of Ethereum L1 but only use transaction fees as revenue for its node runners (sequencers) while also slashing staked collateral.

Using rETH in contrast to ETH has the advantage of not creating an opportunity cost of missed L1 staking revenue for people wanting to participate in running the aztec protocol.

For slashing there are at least two possibilities of what to do with the staked rETH:

1. Send the slashed rETH to a burn address (such as 0x000000…)
2. Send the slashed rETH to all the aztec sequencers proportional to their staked rETH

I'm proposing 2 as I don't see a reason to not keep that economic value within the aztec ecosystem as an additional incentive for the network. The offending slashed sequencer would still suffer an economic penalty even when receiving a small fraction of it back.

Comparisons

In contrast to other solutions I've seen that introduce their own token aztec sequencers would benefit instantly from a superior decentralization of their core token. Another advantage is that possible claims of a potential new token being a security to be used against certain key actors of the protocol that would probably hold a disproportionately big amount of that token would be weakened if not completely invalidated.

Also if a new token is used for such duties the protocol risks a vampire attack where all the open source code is simply re-deployed without that new token.

Feasibility

I think it would be very feasible to implement this within the next 6-12 months since there's no need to completely re-invent the wheel here. A big chunk of the code could be forked and adapted from existing Ethereum PoS implementations swapping out the used ETH for rETH.