There’s a ‘Nullifier set state growth’ problem with zcash-like protocols like ours. The amount of nullifier data to store grows with every transaction, and can never be deleted by full nodes.

- If Aztec 3 has 1 tps, and if each tx created only 2 new nullifiers, that’d be nullifier state growth of 1tx * 2nullifiers * 32bytes * 31,536,000sec/yr = 2GB per year.
- If Aztec 3 has 10tps, and each kernel circuit allows for 16 new nullifiers, that’d be 10tx * 16nullifiers *… = 161 GB/yr

And if we get more ambitious with scaling, the state growth increases.

Case study: the ZCash blockchain has apparently been growing at 0.78GB/day in the latter half of 2022, apparently due to an attacker spamming the chain with cheap txs which create nullifiers. (It quadrupled in size in 4 months). Zcash Blockchain Size—Risks? - General - Zcash Community Forum

This proposal from our friends at Polygon Miden is the best proposal I’ve seen to combat this (it’s inspired by an old proposal from Vitalik). It’s definitely worth a read. And I reckon it’s worth implementing this approach in Aztec 3

.