Slashing/leaking in POS opens up the network to an attack vector that I can't wrap my head around. This attack is basic and common, but it's only possible in production and can't be tested for in development.

- Cryptocurrency holders of EOS, BTC, BCH, and ETC will DDOS Eth staking pools and nodes. They achieve short-term results in these attacks. These attacks are already common in cryptocurrency, but with the added benefit of slashing/leaking having an effect on people's coins, they will be a lot more common in ETH POS.
- Bagholders of ETH will want to maximize their ETH interest rate. They'll quietly DDOS a small percentage of nodes over a time period. As these nodes lose confidence in POS, they'll quit and won't stake again, leading to more returns for the bagholders in the long-term. This is especially true because the number of staking nodes is likely to rise up to a point where staking is unprofitable, so now if average users are also are being randomly DDOS'd and losing coins

, they'll be even less likely to stake.

This second bullet is basically the equivalent of Starbucks buying up 1,000 of cafes over these 10 years and cutting their prices. When no more cafes exist in an area (they've gone out of business), Starbucks raises their prices up to higher than what they were before they moved in.

More technically, imagine the following attack vector:

One of the many people with incentives to deliberately slash goes to a popular staking pool. They locate the ~25 IP addresses which stakers are supposed to connect to. They then run a prolonged, 7 day DDOS on these IP addresses. This causes a pretty large impact on the Ethereum network.

What worries me most

about this attack is [1] how cheap it is to repeatedly DDOS (e.g. versus printing ASICS), [2] how other POS/POW coins don't have this problem because they don't use slashing/leaking (these coins are already DDOSed often, without the benefit to the attacker that comes with slashing/leaking), and [3] how many wealthy and powerful people have the incentives to perform them. This attack really can be done in a lot of different ways other than DDOS, in the linked stackexchange post you'll find more. These types of attacks are only possible due to inactivity leaking in Eth's POS algorithm.

The attached post goes into more details on the long-term effects of slashing/leaking, specifically how over time, the structure incentivizes a single corporation to run the entire process protected by a propietary anti-DDOS structure.

ethereum.stackexchange.com

[

](https://ethereum.stackexchange.com/users/3172/nick-carraway)

Deliberate Slashing: Don't slashing and leaking incentivize DDOS attacks on smaller nodes? Won't this centralize POS more than POW, even?

proof-of-stake, network, casper, proof-of-work

asked by

nick carraway on 04:21PM - 01 Jan 19 UTC