I think this incident rises possibility for way more sophisticated and effective attacks

that can bring the network down.

It would be fantastic if Ethereum Foundation would create a network where people were allowed to experiment with bringing things down, and there would be some kind of bounty for reporting security problems.

One attack which I think is very real now and has never been tested, is a

Kamikaze type attack where several nodes start flooding the network with zillions of conflicting slashable attestations and block proposals. You then add to this a smarter attacker with some type of a reinforcing learning AI that maximizes harm, and the results can be catastrophic on the network as it is running today.

I actually filed several issues on Github before the ETH2 main net was launched, with very little response. It seems to me that no one ever tested the network under assumption of malicious agents, or at least I am not aware of any test network like this. I am not even talking about bounties, there is no playground network for people to try doing bad things to break the network just for fun.

PoS networks are supposed to be BFT resistant. This means that it is not enough to test that good clients work with each other and that the network does not stuck. It is important to test the network with bad guys actively attempting to do harm

.

The above analysis is fantastic but not sufficient imho. It does cover to a great degree, why good nodes ended up not working well and causing the finalization to stuck. There has to be another section in the analysis that assumes a set of intelligent bad guys intentionally attempting to disrupt finalization and liveliness of the network