It was interesting to read the paper

https://arxiv.org/pdf/2110.10086.pdf

It provides descriptions of attacks but does not make general conclusions and does not discuss the fact, whether the attacks are fixable at all.

The comment that I would like is very simple and I have been making it already for several years.

The consensus used in ETH2 has never had a proof of finite time finality. This means that one can prove that it is live, but one can not prove that it will actually finalize a block in finite time.

Moreover, there is a general argument that the attacker will always be able to keep the consensus from finalizing nomatter what the fix is.

The argument simply comes from the fact, that mathematically provable binary consensus algorithms known in this universe have n^2

behavior, and ETH2 is linear in n

.

Therefore, the only way to really fix ETH2 is to make it n^2

. Otherwise it is unfixable from the math point of view. There will always be another attack.

It may be that by continuing patching a fix after a fix after a fix one can end up with something that will work from an engineering point of view.

This will be security by obscurity.

But it will not be secure from the math point of view.