Description

Selfish mining is an important issue in the Nakamoto consensus such as Bitcoin and Eth 1.0. Eth 2.0 takes many effects to mitigate selfish mining, including proposer boost and honest reorgs. However, we find a new attack that utilizes these mitigations, thereby succeeding at a lower adversarial stake.

Background

Proposer Boost

To minimize an ex ante reorg attack and balancing attack, the proposer has a fork-choice “boost” equivalent to 40% of the full attestation weight. Importantly, this boost only lasts for the duration of the slot.

Honest Reorgs

In order to help push rational behavior (delaying the block publication) towards honest behavior (on-time publishing), honest reorg is implemented. It takes the proposer boost and allows honest proposers to use it to forcibly reorg blocks that have attestation weight below 20%.

[

fig1

3356×1619 67.2 KB

](https://ethresear.ch/uploads/default/original/2X/9/97f1f446791f2a934d474ed4a962d25b24d12bce.png)

Attack scenario

Assume that the proposer is malicious in slot i

and slot i+2

. And in slot i

and slot i+2

, \beta

stakes in a committee are adversarial. And the proposal boosting is 40\%

. The attack is as follows:

1. In slot i

, the malicious proposer delays the block i

til the attestation deadline. Only \gamma

percent of honest validators cast a vote on the delayed block i

. The rest 1-\gamma-\beta

percent of honest validators do not see block i

when they are voting. So they attest to block i+1

. The adversarial validators withhold their attestation.

1. Suppose \gamma < 20\%

, this means that the honest proposer releases the block i+1

upon block i-1

due to honest reorg implementation in slot i+1

. After that, the adversarial validators in slot i+1

vote on the delayed block i

while honest validators vote on the block i+1

.

1. In slot i+2

, the adversarial validators release the votes on block i

and propose a new block i+2

upon block i

. Because of the proposer boost, fork A has 40\%

weight.

[

fig2

3739×1659 130 KB

](https://ethresear.ch/uploads/default/original/2X/7/73c67b6d63978d09ed9e94a6a33e59184d82f06f.png)

Impact

According to the LMD-GHOST fork choice, chain A has a weight of \gamma +2\beta+40\%

while chain B has a weight of 1-\beta

. If \beta>14\%

, chain A has more weight than chain B and becomes the choice of LMD-GHOST. Thus block i+1

is an orphan and its proposer lost all profits in the consensus layer and execution layer. And the proposer of block i+2

receives extra rewards. And this attack succeeds at a lower adversarial stake.