Description

ETH consensus uses a pseudorandom number RANDAO to choose the attester and proposer roles in each epoch. However, this random number choice can cause a safety attack against Ethereum. This attack can finalize two conflict chains without violating the 1/3-slashable assumption. The basic idea of the attack is as follows:

[

figs1

1274×616 14.3 KB

](https://ethresear.ch/uploads/default/original/2X/c/c83d128a9af3b304d6ab83f5c82441d84e530776.png)

Attack scenario

Assumption

- Assume that the adversary has the ability for a short-time network partition. This is possible because the Ethereum consensus is in safety under the asynchronous model.
- Also we assume that 33% of total validators are adversarial.

Attack with Network Partition

First, we assume that the network partition lasts for 1 epoch. Notice that the assumption is strong, but this attack is easy to follow. The attack starts at an epoch when the last block proposer is adversarial. We denote this epoch as epoch 0 for simplicity. Notice that epoch 0 is not actual epoch 0 in reality.

1. During epoch 0, the adversary withholds all the attestations and the last block of epoch 0 (block 31).
2. At the beginning of epoch 1, the adversary split the honest validators into two parts, blue and purple. Each part has 33.5% of total validators. Then the adversary releases block 31 to purple but not to blue in epoch 1. So during epoch 1, the blue validators build the blue blocks upon block 30. And the purple validators build the purple blocks upon block 31.
3. The network gets well at the end of slot 64 (the first slot of epoch 2).

[

figs

1241×601 33.2 KB

](https://ethresear.ch/uploads/default/original/2X/d/d2cd6b452d7798a7749288a3fb791a0d1f959f17.png)

Analysis

At the beginning of epoch 2, the blue validators use the randao_reveal of block 0, block 1, …, block 30 and get seed_{\text{b}}

. The purple validators use the randao_reveak of block 0, block 1, …, block 30, block 31 and get seed_{\text{p}}

. These two seeds are different. So the blue validators and purple validators get different shuffles of validator indices. This leads that the blue votes are invalid to purple validators and also the purple votes are invalid to blue validators. So at the end of slot 64, in the view of purple validators, the purple chain gains more weight than the blue chain. The purple validators continue to build blocks on the purple chain. So does blue validators. Starting from epoch 2, the validators build two chains. And the messages of one part are invalid to another part. So the adversary can join in two parts. The adversary uses seed_{\text{b}}

to cast vote_{\text{b}}

on the blue chain and uses seed_{\text{p}}

to cast vote_{\text{p}}

on the purple chain. This double-vote action does not violate slashing condition 1 because vote_{\text{b}}

and vote_{\text{p}}

cannot both be valid for all validators. So both chains gain 66.5% votes and become finalized.

Attack without Network Partition

This attack use the delay of justification (SeeVoting Delay Attack) to replace the network partition. But we assume that the adversary has an new ability.

- The adversary can delay some honest attestations for some slots. This is possible because the Ethereum consensus is in safety under the asynchronous model.

We also assume that the last block proposer of epoch 0 is adversarial. In addition, we assume that block 34 is controlled by adversary. We denote \beta=\frac{1}{3}\times\frac{1}{32}\times total_stake

. The detail of attack is as follows:

1. During epoch 0, the adversary withhold all the attestations and block 31. The justification of epoch 0 is delayed to epoch 1. The block 31 contains enough attestations to justify epoch 0. The honest attestations in slot 31 is delayed by the adversary for 3 slots. So block 34 can contain these attestations to justify epoch 0.

2. In slot 32, the block 32 builds upon block 30 (denote as blue chain). The adversary withholds the attestations in slot 32. So the blue chain gains 2\beta

weight.

1. In slot 33, the block 31 is released. Because of the justification of epoch 0, block 33 build upon block 31 (denote as purple chain). The adversary also withhold the attestations in slot 33, so the purple chain gains 4\beta

weight.

1. In slot 34, the block 34 is proposed by the adversary upon blue chain. So blue chain also justify epoch 0. At that time, blue chain and purple chain both gain 4\beta

weight.

1. From slot 35 to slot 63, the adversary release some withheld attestations at proper time to maintain the balance of two chains. The adversary monitor the weight of two chains in real time, and release the attestations to some validator first to change its choice of heavies tree.

2. At slot 64 (the beginning of epoch 2), the adversary release some attestations to split the honest validators into two parts (blue and purple).

[

figs2

1240×476 17.2 KB

](https://ethresear.ch/uploads/default/original/2X/2/2c0d534836a29508e88dbd7c695ade1625bbbff6.png)

The analysis is same as the previous one.