Requesting for comment on this. #soft_fork

#bribery

#attacks

github.com

zack-bitcoin/amoveo/blob/a807dd26a5af156b8890474df7f709b0ddbe07cf/docs/other_blockchains/ethereum_casper_ffg.md

Review of Ethereum Casper FFG

I wrote a paper about why all PoS blockchains are vulnerable to soft fork bribery attacks https://github.com/zack-bitcoin/amoveo/blob/master/docs/other_blockchains/proof_of_stake.md

In general, any attempt to recover from a soft fork bribery attack will have one of these shortcomings: 1) we undo the history that occured during the soft fork bribery attack, enabling the attacker to do double-spends between that version of history, and the new version. 2) we don't undo the history that occured during the soft fork bribery attack, so there was a period of time during which the soft fork attack was successful, and the attacker could have profited during that time.

In this blog post https://ethresear.ch/t/responding-to-51-attacks-in-casper-ffg/6363 Vitalik talks about Casper FFG and tries to explain why it is secure against this kind of attack.

Finality Reversion

In the section of Vitalik's blog post titled "Finality Reversion", he explains why it is impossible to do a history rewrite attack, even if >50% of the validator stake is cooperating to attack.

Validator Censorship

This file has been truncated. show original

Edit:

I can attempt to summarize the information, although it is best to read all of it, however my concern was that this issue appeared to unresolved, and that the attack still seems well and truly possible.

Summary of the first article:

An attacker can theoretically (as ostensibly demonstrated in the proof) bribe validators of a PoS consensus system (including PoS blockchains like Casper FFG / Eth 2) with a small amount relative to the total amount of stake and market cap.

Some key snippets:

According to tragedy of the commons, the cost to bribe the validators to form a majority coalition and destroy the blockchain is:

LU = (how much the validators have to lock up)

V = (how many validators are there)

Bribe = LU / (2 * #V)

If there are 1000 validators, and the blockchain is worth $1 billion, and 90% of the value is staked, then the total cost to bribe >50% of the validators would be: ($1 billion) * (0.9) * (1/2) * (1/1000) => $450 000

So less than $1/2 million in bribes is sufficient to completely destroy a $1 billion PoS blockchain.