

I saw a discussion on Japanese twitter world.

And here is no such discussion so far (as far as I've seen) hence I post this summary of that discussion.

Problem and attack procedure

1. When "the sum of dapps price is far bigger than the sum of Ethereum price" scenario
2. Short-selling on dapps on DEX
3. Do the 51% attack on Casper PoS Ethereum, then make network paralyze
4. Make money

Solution

- Mitigation for excessive "mother-children ratio"(=ETH-dapps ratio)
- Discouragement of adversarial short-sell

Ambiguity, excuse, and help wanted

- How the community's thought?
- What is the current "mother-children ratio"?
- Indeed a PoW-based smart contract chain is weaker because mining machine cannot be a collateral, and reusable. (If that is ASIC poisoned chain, it can work as collateral fortunately 'ヾ)
- The mitigation for this issue is Casper PoS, because when the 51% attack happens, that 51% amount of collateral gonna be lost its value
- No simulation for short-sell profitability and 51% attack's cost, need feedback