There is one problem which has been bugging me recently. Let’s say I create a smart contract on which users can stake Ether in the same way Casper staking is done, and reward them slightly better than what they can earn from Casper staking. Wouldn’t an economically optimal behavior be moving to this new contract and increase their profit?

In this case, I am afraid the attacker can simply pay for the total amount of transaction fee for the whole network and halve the network security for a given period (+staking period, say Casper profit is 5% a year, doing this for half a year will require 2.5% of the stake amount). If the attacker pays for double of the fee amount, the security (i.e. total amount of deposit for PoS) will become 1/3, and so on.

I think this is a very similar issue to decentralized oracle - it seems to be impossible to obtain a safe decentralized data feed oracle mechanism which is independent of the value of the data feed (i.e. expected profit by faking the feed). In other words, if Ethereum starts to host valuable DApps whose operation requires staking some Ether, the security of the network would be affected by unwanted staking competition between the DApp and the network itself.

How do you think? Should DApps staking Ether be refrained from?