Not sure if it is appropriate for me to post this here, but…

Referring to https://flare.ghost.io/theflarenetwork/ and https://arxiv.org/abs/2001.00919 on how Proof of Stake security can be impaired/cannibalized by higher returns from DeFi lending, I wish to present my rebuttal here.

Tarun Chitra's argument is if return from DeFi lending is higher than return from staking, then capital would flow to such DeFi lending, causing reduced network security.

Flare shares the same argument while undermining the critically important relation of price = security.

My rebuttal:

1. Higher DeFi lending does not impair network security simply because capital flow between staking and lending will eventually reach a balance. As more capital switches from staking to lending, existing capital that continue to stake will earn a larger share of the staking pie. Eventually the return from staking will be equal to the return from lending, after risk-adjusted. Over the long term, I believe all DeFi lending return (and staking return) will normalize to around 7% average, disregarding over 100% annual return currently offered by DeFi lending that is simply fundamentally unsustainable.

2. The remaining leftover capital that continue to stake may still fully secure the network without any compromise, if the price of ETH is equivalent to (the total economic value of all assets tokenized on Ethereum) / (the number of ETH staked). In this case, it does not matter how much capital leaves staking in favor of lending, network security would still be preserved.

To quote Flare:

Taken to the logical endpoint, if smart contract networks using proof of stake were to become the ubiquitous method of doing business, the scale of diversion of capital required from other endeavors, just to secure the value built on these networks, would make the cost of commerce unfeasibly high. For this reason it is extremely unlikely to happen.

In my opinion, as long as a network (whatever the network it is) is used to secure the value built above it, the security in place must at least be worth as much as the value. Otherwise, imagine a network is used to secure some assets worth $1 trillion, but the instrument (be it coin, token, stablecoin, etc) used to secure the network is just worth $100 (as an extreme example to explain my point), then an arbitrage value of around $0.9999 trillion would be available for exploitation. Thus, for Flare to favor an instrument (Spark) which price is detached from security would be unwise.

Flare is at its core a new way of scaling smart contract platforms that does not link safety with the value of its token.

This is unwise. Something has to give. If it is not Spark, then it needs to be something else. Otherwise, arbitrage would exist. And such arbitrage would compromise the network security.

Question: What defect do you see from my rebuttal?