Let’s say we have n

shards, and s

ETH is being staked. If an attacker with s/3

ETH wants to corrupt a single shard, causing two conflicting blocks to be finalized, they only need to vote illegally on that particular shard. So the maximum penalty is s/3n

ETH, which seems rather insigificant for large n

.

How much trouble could a single-shard attack cause? If shards accepted crosslinks directly from other shards, then a single-shard attacker could create ETH “out of thin air” by yanking the same account to two different shards. As long as the attacker had an extra s/3n

ETH to fund a separate liquid account, the attack would be profitable.

My understanding is that, in the long term plan, all cross-shard communication would go through a Casper-based main chain. Is that right? That seems potentially better, but only if main chain committees are larger than shard committees. E.g. if the main chain committee consists of all registered validators, then the penalty for corrupting it would be s/3

ETH, which would be ideal. But such a large committee would present a scalability challenge.

Could you clarify what the long term plan is for main chain mechanics? I’m basically wondering if then penalty for a double spend attack would be on the order of s/3

ETH, or s/3n

ETH, or something in between.