Attack

Let’s assume that an attacker controls some proportion a

of validator deposits in the VMC, and some proportion b

of mining power in the main chain. Because the current [getEligibleProposer

method](https://github.com/ethereum/sharding/blob/develop/docs/doc.md#details-of-geteligibleproposer) is subject to blockhash grinding the attacker can make himself the eligible proposer on a shard (actually, several shards, depending on how fast the attacker can grind) with proportion a + (1 - a)*b

.

If we set a = b

(i.e. the attacker controls the same proportion of validator deposits and mining power) and solve for a + (1 - a)*a = 0.5

(i.e. solve for the attacker having controlling power) we get a = 0.292

. That is, an attacker controlling just 30% of the network can do 51% attacks on shards.

Defenses

One defense strategy is to use a “perfectly fair” validator sampling mechanism with no repetitions, e.g.see here. Another strategy is to improve the random number generator to something like RANDAO or Dfinity-style BLS random beacons.