One of the proposed frameworks for sharding is kown as Polyshard

which is introduced in this paper. In Polyshard, each validator verifies a coded combination of the blocks introduced by different shards, contributing to the security of all shards. In that way, each validator only needs to store one coded chain instead of raw chains of some or all shards. The interesting aspect of Polyshard is that the design of the encoding enables both throughput and security (the number of tolerable adversarial nodes) to scale linearly with the size of the network.

While Polyshard outlines an interesting approach to the scalability problem, we argue that it is vulnerable to some attacks. In particular, we have recognized a specific attack on Polyshard that causes only one of throughput and security to be able to scale linearly with network size. In this attack that we coin as the discrepancy attack

, shards controlled by the adversaries spread inconsistent blocks to different nodes in the network, in the very first step of Polyshard. Heavy communication load does not allow nodes to verify the consistency of blocks. The resulting discrepancy between nodes has detrimental effects in the subsequent steps of Polyshard, and changes the analytical results tremendously. Check out our paper here for detailed explanation and analysis of this attack.