

In previous post, Vitalik went over the manipulability of RANDAO [RNG exploitability analysis assuming pure RANDAO-based main chain](#) and [RANDAO beacon exploitability analysis, round 2](#).

Would applying something like LibSubmarine (<https://hackernoon.com/libsubmarine-temporarily-hide-transactions-on-ethereum-cheaply-6910191f46f2?gi=ffb1a94bc2a1>) decrease the influence of the last revealer having power over the final random number?