I'm interested in putting together a model for both attacker budgets and cost-of-reversion in the sub-finality environment[as discussed with Vitalik here](). Before I put too much work into it, does any analysis like this already exist? Especially given that we will want to parameterize by both total number of validators and participation levels (to get both reward levels and probabilities of being assigned proposals/attestations) as well as # of confirming blocks and attestations (respectively).

My first thoughts at a stab for attacker budget are: calculate the number of validators required to be assigned x consecutive block proposals within a 1 month window, PLUS y attestation chances during the x block period. Am I right that is minimal given that you can let the real network build an x block y attestation chain leading up to the period you control and then fork it off by disagreeing on the head immediately before the block you wish to orphan?

My first stab at a cost-of-reversion would be to add up the block rewards earned in a given number of confirming blocks, calculate the attestation rewards which would be lost if that fork is orphaned, and combine them. Does that seem right?