

- let  $\alpha(\kappa, n, \rho, \Delta) = 1 - (1 - p(\kappa))^{(1-\rho)n}$ . That is,  $\alpha$  is the probability that *some* honest player succeeds in mining a block in a round;
- let  $\beta(\kappa, n, \rho, \Delta) = \rho n p(\kappa)$ . That is  $\beta$  is the expected number blocks that an attacker can mine in a round.
- let  $\gamma(\kappa, n, \rho, \Delta) = \frac{\alpha}{1+\Delta\alpha}$ .  $\gamma$  is a “discounted” version of  $\alpha$  which takes into account the fact that messages sent by honest parties can be delayed by  $\Delta$  rounds and this may lead to honest players “redoing work”;  $\gamma$  corresponds to their “effective” mining power.