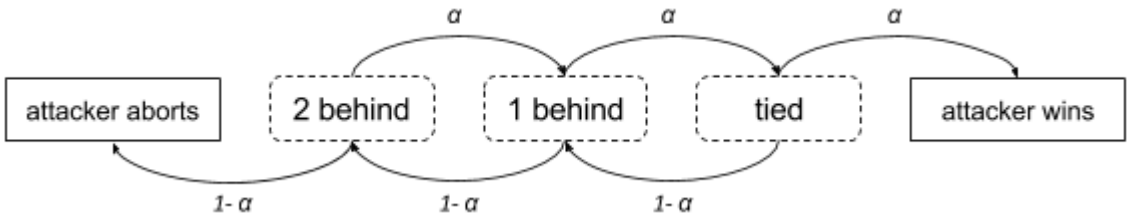
The Theory Behind Blockchains (Spring 19)
Recitation 6

Eliad Tsfadia

The following exercises are taken from the course "Cryptocurrencies and Decentralized Ledgers" by Joseph Bonneau.

1 Feather Forking

In class we learned about *feather forking*: a coalition of miners controlling a fraction α of the total mining power attempt to censor transactions by announcing: "if we see a block containing a transaction from our blacklist B, we will attempt to fork until we are 3 blocks behind the main chain." This strategy can be shown in a probabilistic state machine:



What is the probability that the censorship attack will succeed in terms of α?
Solution: For $i \in \{0, 1, 2\}$, let p_i be the probability that the attack succeed when the state is i blocks behind. It holds that

$$p_0 = \alpha + (1 - \alpha) \cdot p_1$$

$$p_1 = \alpha \cdot p_0 + (1 - \alpha) \cdot p_2$$

$$p_2 = \alpha \cdot p_1$$

Solving the above equations yields that $p_1 = \frac{\alpha^2}{1-2\alpha+2\alpha^2}$ (e.g., $\alpha = 0.25 \implies$ the attack succeed w.p. $p_1 = 0.1$).

2 Mining Pool Sabotage

Recall that mining pools enable individual miners to share risk and reward, lowering the variance of their earnings while keeping the same expected value. Participants repeatedly submit shares (blocks that are valid at a lower difficulty) to prove how much work they are doing. Whenever the pool finds a block, the coinbase from that block is split among the participants in proportion to the number of shares submitted. One risk is sabotage, in which a participant submits shares, but withholds full solutions if they are found.

Consider two pools, P_1 and P_2 with mining power α_1 and α_2, respectively. What will P_1's expected share of the total earnings be if it dedicates $\beta < \alpha_1$ power towards sabotaging P_2? Note that when P_1 finds a block it gets the entire coinbase. When P_2 finds a block, P_1 receives a fraction of the coinbase proportional to the number of shares P_1 generated while mining for P_2.

Solution: In the following, assume that the block discovery rate is always fixed (say 10 minutes), and let Gain_β be the expected fraction of the entire bitcoins that P_1 gains. First, note that $\text{Gain}_0 = \alpha_1$ (i.e., if P_1 does not try to sabotage P_2, then it just gains according to its mining power). For $\beta > 0$, note that P_2's total mining power is now $\alpha_2 + \beta$, but only α_2 is for finding a new block. Because β power is no longer used to find blocks, P_2's useful mining power, as a fraction of the entire network, is now $\alpha_2/(1-\beta)$. The expected gain of P_1 in this case can be expressed as follows:

$$\text{Gain}_\beta = \underbrace{\frac{\alpha_1 - \beta}{1-\beta}}_{\text{gain from pool P}_1} + \underbrace{\frac{\beta}{\beta+\alpha_2} \cdot \frac{\alpha_2}{1-\beta}}_{\text{gain from pool P}_2}$$

Using simple calculation it can be shown that for $\beta > 0$:

$$\text{Gain}_\beta > \alpha_1 \iff \beta < \frac{\alpha_1\alpha_2}{1-\alpha_1}.$$

For example: $\alpha_1 = 0.3$, $\alpha_2 = 0.4$ and $\beta = 0.1$ yields that $\text{Gain}_\beta \approx 0.311 > \alpha_1$.