CS269I: Exercise Set #7

Due by 11:59 PM on Wednesday, November 14, 2018

Instructions:

(1) You can work individually or in a pair. If you work in a pair, the two of you should submit a single write-up.

(2) Submission instructions: We are using Gradescope for the homework submissions. Go to www.gradescope.com to either login or create a new account. Use the course code MZZ2BV to register for CS269I. Only one person needs to submit the assignment. When submitting, please remember to add your partner's name (if any) in Gradescope.

(3) Please type your solutions if possible. We encourage you to use the LaTeX template provided on the course home page.

(4) Write convincingly but not excessively. You should be able to fit all of your solutions into two pages, if not less.

(5) Except where otherwise noted, you may refer to the course lecture notes and the specific supplementary readings listed on the course Web page *only*.

(6) You can discuss the exercises verbally at a high level with other groups. And of course, you are encouraged to contact the course staff (via Piazza or office hours) for additional help.

(7) If you discuss solution approaches with anyone outside of your group, you must list their names on the front page of your write-up.

(8) No late assignments will be accepted, but we will drop your lowest exercise set score.

Lecture 13 Exercises

Exercise 27

Recall the use of stake-based sampling in Ouroboros to pick a block creator in each time slot. Let s_i denote the current balance of user i, and consider the following randomized algorithm:

- For each user $i = 1, 2, \ldots, n$: (in arbitrary order)
  - Flip a biased coin with probability
    $$\frac{s_i}{\sum_{j=i}^{n} s_j}$$
    of "heads."
  - If the coin comes up "heads," deem user i the winner and halt.
  - Otherwise, continue.

Prove that the distribution of winners produced by this randomized algorithm matches want we want for a proof-of-stake blockchain protocol: for every user i,

$$\mathbf{Pr}[i \text{ wins}] = \frac{s_i}{\sum_{j=1}^{n} s_j}.$$

[Hint: induction on i.]

Exercise 28

Recall that a Sybil attack involves a single entity creating multiple identities to manipulate a system. Both proof-of-work and proof-of-state blockchain protocols are unaffected by Sybil attacks.

Is a Vickrey (or eBay) single-item auction vulnerable to a Sybil attack? Argue why not, or alternatively come up with a concrete attack that you could plausibly implement on eBay.

Lecture 14 Exercises

Exercise 29

Recall the recursive incentive scheme employed by the winning team of the DARPA "red balloons" challenge: the finder of a balloon receives $2,000, their recruiter $1,000, their recruiter's recruiter $500, and so on.

Suppose you join the competition. You have up to three friends whom you could recruit. Assume that none of your friends will participate unless you invite them. Assume that each of the four of you that participates has a 10% chance of finding a balloon, and that these four events are independent. To maximize your expected reward, how many of your friends should you recruit? Prove your answer.