Reichmann University: Blockchains and Cryptocurrencies

Exercise 2

Assigned: December 15, 2022 Due: December 29, 2022

General Instructions

How to Submit The homework exercise has two parts:

1. Question 1 requires you to write a formal proof, and its answer should be submitted via the course Moodle by uploading a PDF file. **The submitted homework must be typed** (not hand-written and scanned).

   You will receive a 2 point bonus for the exercise if your submission was prepared in LaTeX, and contains the LaTeX macro in a footnote. You can download a latex homework template to get you started. If you don't want to install latex locally, there are online latex editors such as Overleaf that you can use.

2. Questions 2 to 5 are coding questions and should be submitted via the Inginious Server.

Pair Submission You are encouraged to solve the **theory part** of this exercise in pairs. To register your pair, write your partner's name and inginious username at the top of the page you submit. When you solve in a pair, each member of the pair should submit the solution independently, but you and your partner may submit identical solutions.

Note that the *Inginious* part of the assignment should not be submitted in pairs (you are welcome to discuss solutions with your classmates, but don't copy code).

Homework Questions

1. (40 points) **(Byzantine Agreement in the Synchronous Model)** Prove that BA is impossible if at least $n/2$ nodes are corrupt, even in the synchronous model. In other words, unlike the BB abstraction, we need to assume honest majority to construct BA even under synchrony (This is exercise 19 in Elaine's book.)

2. (5 points) **(Byzantine Broadcast Upper Bound)** Solve the Byzantine Broadcast Upper Bound task on Inginious.

3. (5 points) **(Basic Blockchain Definitions)** Solve the Basic Blockchain Definitions task on Inginious.

4. (25 points) **(Attacking Simple Blockchains)** Solve the Bad (Simple) Blockchain task on Inginious.

   Due to popular demand, I have provided a testing framework that you can use offline in your favorite IDE. To use it, clone the repository: `https://vcs.ap.runi.ac.il/blockchain/hw2` (your Inginious credentials should work). Write your code in a new file named `student_code.py`.

   Note that submission is still via the Inginious server.

5. (25 points) **(Partial Synchrony)** Solve the Partial Synchrony task on Inginious (we solved part of this task in class).