COMS 6998-006 (Foundations of Blockchains): Homework #6

Due by 11:59 PM on Thursday, November 18, 2021

Instructions:

(1) Solutions are to be completed and submitted in pairs.

(2) We are using Gradescope for homework submissions. See the course home page for instructions, the late day policy, and the School of Engineering honor code.

(3) Please type your solutions if possible and we encourage you to use the LaTeX template provided on the Courseworks page.

(4) Write convincingly but not excessively. (We reserve the right to deduct points for egregiously bad or excessive writing.)

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

(6) You are not permitted to look up solutions to these problems on the Web. You should cite any outside sources that you used. All words should be your own. Submissions that violate these guidelines will (at best) be given zero credit, and may be treated as honor code violations.

(7) You can discuss the problems verbally at a high level with other pairs. And of course, you are encouraged to contact the course staff (via the discussion forum or office hours) for additional help.

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

(9) Some of these problems are difficult, so your group may not solve them all to completion. In this case, you can write up what you've got (subject to (4), above): partial proofs, lemmas, high-level ideas, counterexamples, and so on.

Problem 1

(25 points) In this problem you will learn about some of the differences between block rewards in Bitcoin and Ethereum, and the relevance of these differences to our selfish mining analysis in Lecture 10 and Homework #4. For parts (a)–(d), cite the source(s) you used to answer the question (just the URLs are fine).

(a) (4 points) What fraction of Bitcoin blocks are orphaned, on average? What about Ethereum blocks?

(b) (4 points) If the numbers in part (a) are different from each other, explain the main reason for the difference.

(c) (5 points) Explain how miner rewards are defined in Ethereum. (Be sure to include a description of "uncle rewards" and "nephew rewards.")

(d) (5 points) How was the longest chain defined in Ethereum's initial release? How is it defined in Ethereum today? What was wrong with the original definition?

(e) (7 points) Consider a simplified version of Ethereum, in which the only difference from Bitcoin is that a miner of an "uncle block" (an orphan block whose predecessor is on the longest chain) gets 50% credit (i.e., half the reward of a block on the longest chain). How would you revise the Markov chain and/or expressions (1) and (2) in Problem 5 of Homework #4 so that they faithfully capture selfish mining in this model? (Just describe the changes, don't redo any of the calculations.)

Problem 2

(10 points) Explore the Ethereum blockchain using a block explorer (such as `etherscan.io`). Include a screen shot of the weirdest block that you can find.[1] What's so weird about it, and what do you think caused it? Also, how are the changes introduced by EIP-1559 (Lecture 12) reflected in the block's description?

Problem 3

(10 points) Look up "feather forking" (and cite your source). What does this have to do with optimistic rollups in Ethereum (Lecture 18)?

Problem 4

(15 points) Recall that every Ethereum transaction includes a 65-byte signature by the sender; the sender address (which is only 20 bytes) can be easily extracted from the signature.

In a rollup, when L2 transaction data gets recorded in an L1 storage contract, do the transaction signatures need to be included, or are the sender addresses enough? Why or why not? Does the answer depend on whether it's an optimistic rollup (Lecture 18) or a validity rollup (Lecture 19)?

Problem 5

(15 points) Read up on BLS signatures (and cite your sources). Explain the potential relevance of BLS signatures to rollups, and give a back-of-the-envelope estimate as to how much they might decrease transaction fees.

Problem 6

(15 points) Recall that every Ethereum block includes a state root, which is the hash value at the root of a Merkle-Patricia tree that tracks Ethereum's global state (i.e., all Ethereum accounts) in a canonical way.

(a) (4 points) Explain why, given only a state root and an ordered list of transactions, it is computationally infeasible to compute the new state root (i.e., the one corresponding to the global state after all the transactions have been executed, starting from the global state encoded by the given state root).

(b) (11 points) Describe carefully the additional information necessary to compute the new state root.

[To answer fully, you may need to discuss some of the details of Ethereum's Merkle-Patricia trees.]

[1] The submission with the weirdest block of all will get 5 extra credit points.