COMS 4995-001 (Science of Blockchains): Homework #4

Due by 11:59 PM on Wednesday, February 26th, 2025

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.

Problem 1

(10 points) For this problem, you are tasked with exploring Etherscan (an Ethereum block explorer) and this Bitcoin block explorer. Your assignment is to look for "abnormal" transactions. As your answers, provide links to the transactions that you found in your pdf submission.

1. For Ethereum transactions, what's the highest gas price that you can find?
2. For Bitcoin transactions, what's the largest number of inputs and/or outputs that you can find?
3. For Ethereum transactions, what's the highest value that you can find?

For (a very modest amount of) extra credit, feel free to submit your candidates for the "weirdest" Bitcoin and/or Ethereum transactions out there, along with your best guess as to why these transactions were submitted.

Problem 2.

(15 points)

1. Take a look at the website http://evm.codes. This website contains a list of the opcodes for the Ethereum VM as well as the gas cost for each of these opcodes. Are there any instructions on the list that you would not expect to see in a traditional instruction set architecture (ISA)? For an example of what a "traditional" ISA might look like, take a look at the first page of this reference sheet for RISC-V: https://www.cs.sfu.ca/ ashriram/Courses/CS295/assets/notebooks/RISCV/RISCV_CARD.pdf.

2. Why do you think the opcodes that you identified are part of the EVM instruction set but uncommon in instruction sets that are meant to map fairly directly to physical machines?