CS 4501: Cryptocurrency Final Exam, spring 2023

Name ______________________________

You MUST write your e-mail ID on **EACH** page. And put your name on the top of this page, too.

If you are still writing when "pens down" is called, your exam will be ripped up and not graded. So please do that first. Sorry to have to be strict on this!

There are 6 pages to this exam. Once the exam starts, please make sure you have all the pages. Questions are worth different amounts of points.

Answers for the short-answer questions should not exceed about 20 words; if your answer is too long (say, more than 30 words), you will get a zero for that question!

This exam is CLOSED text book, closed-notes, closed-calculator, closed-cell phone, closed-computer, closed-neighbor, etc. Questions are worth different amounts, so be sure to look over all the questions and plan your time accordingly. Please sign the honor pledge below.

____

____

____

____

A world computer

The baseline of transactions

In ethereum, trust

Page 2: Auto-gradable questions

1. [3 points] A DEX, which uses CPAMM, has 4 BTC and 60 ETH. Somebody trades in 1 BTC. How many ETH do they get in return (ignoring fees)? Show your work, but put your final answer in the box provided.

2. [3 points] Consider the secp256k1 (aka $y^2 = x^3 + 7$) curve. Let $p = 43$, which means $o = 31$. Let $G = (25, 25)$. What is $(12, 12) \oplus (12, 31) \oplus (13, 22)$? You cannot use a calculator for this! Show your work, but put your final answer in the box provided.

3. [3 points] What is the running time of $OM(3)$ (i.e., oral messages with up to 3 traitors)? Express your answer as: $\Theta(\ldots)$, where you fill in the ellipsis part. Put your final answer in the box provided.

4. [3 points] - On a scale of 1-5, how much more or less likely are you to invest in cryptocurrency after this course, using the scale below? Put your final answer in the box provided.

   1. Much less likely
   2. Somewhat less likely
   3. About the same
   4. Somewhat more likely
   5. Much more likely

Page 3: Review and Stablecoins

5. [3 points] What are the contents of the pubKey script of a P2PKH transaction? We are looking for the specific opcodes and values, not a high-level English description.

6. [3 points] *Briefly*, what are the use(s) of a *nonce* in Ethereum?

7. [3 points] *Briefly*, what benefits do PATRICIA trees have over Merkle trees?

8. [3 points] The two most popular types of stablecoins are collateralized / centralized and collateralized / decentralized. Which is better? *Briefly*, why?

Page 4: Tokens, Consensus, and Scalability

9. [3 points] Name two valid uses for a NFT. Buying a stupid ape image (or any other image) is not one of them!

10. [3 points] What is the goal in the Byzantine Generals Problem?

11. [3 points] Briefly explain the characteristic(s) of layer 1 (on-chain) scalability enhancements.

12. [3 points] Briefly explain the characteristic(s) of layer 2 (off-chain) scalability enhancements.

Page 5: Mining and Applications

13. [3 points] What are the two types of staking? We are looking for the technical definition and the way it is more commonly used.

14. [3 points] List and *briefly* describe the four kinds of forks as they pertain to cryptocurrency.

15. [3 points] *Briefly,* why are there very few attempts at "traitorous" behavior with proof-of-stake coins?

16. [3 points] Briefly, what was the programming mistake that The ĐAO made?

Page 6: Scams

17. [3 points] Briefly explain one type of Solidity attack we studied in class today, but you can't use one that is an answer to another question on this exam.

18. [3 points] Briefly explain your favorite scam that we studied in class. You can't use the LUNA debacle.

19. [3 points] List one of the cryptocurrencies that we studied in class (other than LUNA) that you feel is sketchy, and *briefly* explain why it is sketchy.

20. [3 points] When, if ever, is it ethical to invest in – and use – cryptocurrency?