CS 4501: Cryptocurrency Final Exam, spring 2022

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 be brief – if the answer rambles on, or you are listing irrelevant information, points will be deducted.

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 crash reduces
Your expensive computer
To a simple stone.

Page 2: Stuff

1. [6 points] What is the biggest ethical dilemma facing cryptocurrencies today? How would you solve it? You should reference the ethical frameworks when answering this question.

2. [3 points] Describe what money laundering is, and give a realistic example that does not involve cryptocurrency.

3. [3 points] Give one *realistic* example of how you would improve Bitcoin's scalability *other* than the Lightning Network.

Page 3: Stuff

4. [3 points] How do you prevent 51% attacks?

5. [3 points] Describe the different types of blockchain "forks"

6. [3 points] What does an ECDSA private key represent? Meaning what mathematical properties or values are encoded in the private key?

7. [3 points] List three cryptocurrencies we've studied, other than Bitcoin and Ethereum, and one explain unique feature about them.

Page 4: Stuff

8. [3 points] Explain how the Oral Messages algorithm works in the Byzantine Generals Problem

9. [3 points] List three things that NFTs are useful for, other than selling artwork or images.

10. [3 points] What are PATRICIA trees and what benefits do they have?

Page 5: Stuff

11. [6 points] Explain the programming vulnerability that The DAO had, and how it was exploited.
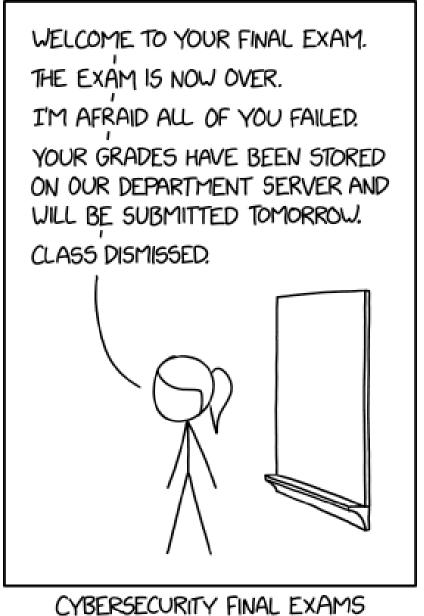
12. [3 points] What are a Homomorphic Hidings in zkSNARKs? Why are they important?

13. [3 points] If you were to design a new cryptocurrency based off of Ethereum, list three things you would change to improve its performance.

Page 6: Nothing to see here

This page unintentionally left blank.

xkcd # 2385