CS 4501: Cryptocurrency Exam 1, 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 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.

The Tao that is seen
Is not the true Tao,
until You bring fresh toner.

Page 2: Overview & Bitcoin

1. [3 points] *Briefly* describe the three physical types of currencies: commodity, representative, and fiat.

2. [3 points] *Briefly*, how do the *target* and *difficulty* relate to each other? This doesn't have to be a formula, but we are looking for the specific relationship between them, not a high-level overview of what they are.

3. [3 points] Given an nBits value of $0x1e123456$, what is the target? If you have any repeated digits in a straight in your answer, please briefly indicate how many so we don't have to count them all.

4. [3 points] *Briefly*, what is a UTXO and why do we care about them?

Page 3: Encryption

5. [3 points] *Briefly*, what property(ies) make RSA secure against cracking?

6. [3 points] *Briefly*, what property(ies) make ECDSA secure against cracking?

7. [3 points] *Briefly*, why is an ECDSA key pair quicker to generate than an RSA key pair?

8. [3 points] *Briefly*, what properties must a CSPRNG (Cryptographically Secure Pseudo-Random Number Generator) have?

Page 4: Bitcoin

9. [3 points] *Briefly*, what prevents a Bitcoin miner from just mining a block with no transactions so that s/he can keep all the reward?

10. [3 points] *Briefly*, what is a Bitcoin *witness*? Why is it necessary?

11. [3 points] *Briefly*, how is a Bitcoin transaction verified? This (brief!) explanation needs to show the purpose of the sigScript and the pubKey script.

12. [3 points] In English, *briefly* explain how a P2PKH transaction works. This question is looking for an English explanation of what the sigScript and pubKey script are doing.

Page 5: Mining

13. [3 points] *Briefly*, when discussing the current difficulty of a cryptocurrency, what is the difference between *ldiff* and *pdiff*?

14. [3 points] *Briefly*, what is a mining share?

15. [3 points] *Briefly*, what is staking?

16. [3 points] *Briefly*, what is the nothing-at-stake problem?

Page 6: Miscellaneous

17. [3 points] *Briefly*, how do you prevent 51% attacks from occurring?

18. [3 points] *Briefly*, why is the cross-chain atomic swap atomic? In other words, why can't one party obtain both funds?

19. [3 points] *Briefly*, is cryptocurrency mining allowed at UVA? Why or why not?

20. [3 points] Suggest a name for our cryptocurrency! As long as you put something here, you'll get full credit.