CS 4501: Cryptocurrency Midterm, fall 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.

_____

_____

_____

_____

Bitcoin price falls down

Hold the line! Trust Satoshi!

Tears fall, like your coins.

Page 2: Encryption

1. [3 points] *Briefly* describe how you compute an ECDSA key pair.

2. [3 points] *Briefly,* why are finite fields used in encryption, such as with ECDSA?

3. [3 points] *Briefly,* why does cryptocurrency wallet software have you write down (or memorize) 12 English words for your wallet?

4. [3 points] What is the general formula for an elliptic curve? Also, what is the formula for the secp256k1 curve discussed in class?

Page 3: Bitcoin

5. [3 points] What is the pubKey script for a P2PKH transaction?

6. [3 points] In a cross-chain atomic swap, give the transaction that both Alice and Bob broadcast to start the process.

7. [3 points] The Bitcoin Witness was created because of transaction malleability. *Briefly,* what is transaction malleability?

8. [3 points] *Briefly,* how is a Bitcoin invoice address computed?

Page 4: Mining

9. [3 points] *Briefly* explain how Bitcoin's target is adjusted.

10. [3 points] *Briefly,* what is staking? Is it legal in the US?

11. [3 points] *Briefly,* what is the nothing-at-stake-problem?

12. [3 points] Other than proof-of-work and proof-of-stake, list and *briefly* describe one other block certification mechanism.

Page 5: Ethereum & Solidity

13. [3 points] *Briefly,* how is an Ethereum contract's address determined?

14. [3 points] *Briefly,* how is the transaction fee computed for an Ethereum transaction?

15. [3 points] In Solidity, what are the different types of memory locations for a `string`, and *briefly* what do they mean?

16. [3 points] *Briefly,* how is a `view` and also a `pure` function different than a regular function in Solidity?

Page 6: Miscellaneous

17. [3 points] List and *briefly* describe the three types of (non-crypto) currencies.

18. [3 points] *Briefly,* what is the *coinbase*?

19. [3 points] Give a provably unspendable Bitcoin pubKey script, but you cannot use `OP_RETURN`. Assume the sigScript is the standard <sig> and <pubKey> of a P2PKH transaction.

20. [3 points] Should you buy an ASIC miner off of Amazon and start mining Bitcoin? *Briefly,* why or why not?