CS 4970: Cryptocurrency Midterm, spring 2026

Name _____

Be sure to write your name and e-mail ID on top of this page.

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.

"No B.S." rule: If you do not know the answer, you can write "No B.S." as the answer, and you will get a small amount of partial credit. Note that you have to write that in the answer spot (we don't care if you have the periods or not) – leaving it blank does not count.

_____

_____

_____

_____

Bitcoin's flying high,

then it crashes; bye-bye Lambo,

back to ramen life.

Page 2: Bitcoin

1. [3 points] *Briefly*, why are additional confirmations considered to increase the security of a Bitcoin transaction?

2. [3 points] *Briefly*, why might reusing Bitcoin addresses be considered bad practice?

3. [3 points] Suppose two transactions attempt to spend the same UTXO. *Briefly* explain how the network resolves this conflict.

4. [3 points] *Briefly*, why might a transaction remain unconfirmed for a long time?

Page 3: More Bitcoin

5. [3 points] List the fields in the bitcoin *header*; the order you list them does not matter.

6. [3 points] *Briefly*, what does the Bitcoin witness do, and how does it work?

7. [6 points] List the steps to determine a Bitcoin invoice address from the ECDSA *private* key.

Page 4: Encryption

8. [3 points] *Briefly*, if one could solve the elliptic curve discrete logarithm problem efficiently, how would one use that to attack a cryptocurrency?

9. [3 points] *Briefly*, what is/are the "hard" parts of ECDSA that one has to solve efficiently in order to "crack" it?

10. [3 points] *Briefly*, what is the purpose of the generator point G on an elliptic curve, and why is it necessary?

11. [3 points] *Briefly*, what problem does Ethereum gas pricing help prevent?

Page 5: Ethereum

12. [3 points] *Briefly*, how is the account nonce stored or computed in Ethereum?

13. [3 points] What is the formula to determine the cost, in US dollars, of an Ethereum transaction?

14. [3 points] *Briefly*, how does the Ethereum address checksum work? We are looking for a high-level overview, not the algorithm in pseudo-code.

15. [3 points] *Briefly*, what benefit do PATRICIA trees have over Fast Merkle trees?

Page 6: Miscellaneous

16. [3 points] *Briefly*, what is a *mining share*?

17. [3 points] If you are mining as part of a mining pool, the pool wants to ensure that, if you find a successful block (meaning whose hash is below the target), that the mining pool gets the block reward (to distribute to its members), and that you do not keep it for yourself. *Briefly*, how does the pool ensure that happens?

18. [3 points] *Briefly*, explain how the `nBits` fields encodes the target.

19. [3 points] *Briefly*, what is a *token* (as it applies to cryptocurrency)?