# CS 4501: Cryptocurrency Midterm, fall 2023

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.

Bitcoin price falls down

Hold the line! Trust Satoshi!

Tears fall, like your coins.

## Page 2: Encryption

1. [3 points] *Briefly,* why is ECDSA used in cryptocurrencies over RSA (or any other public key cryptosystem)?

Page 2 of 6

2. [3 points] Consider the secp256k1 curve ( $y^2 = x^3 + 7$ ) where p = 13; the order is o = 7. Perform the following operation:  $(7,8) \oplus (7,5) \oplus (11,5)$ .

3. [3 points] *Briefly,* what is a collision resistant hash?

4. [3 points] *Briefly,* what is a Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)?

#### Page 3: Bitcoin

5. [6 points] *Briefly*, how does one determine a Bitcoin invoice address? We are looking for a (*brief!*) listing of the steps here, not a high-level overview.

6. [3 points] *Briefly,* how is a Bitcoin transaction verified? (This question is asking about how the scripts are used to verify the transaction)

7. [3 points] Briefly, list two benefits that the Bitcoin Segregated Witness (segwit) provides

#### Page 4: Ethereum

8. [3 points] Briefly, what is special about PATRICIA trees, and why does Ethereum use them?

9. [3 points] *Briefly*, what is the full formula used to determine the cost (in USD) for an Ethereum transaction?

10. [3 points] Briefly, how is an owned Ethereum account's address determined?

11. [3 points] *Briefly,* how is a smart contract's address determined in Ethereum?

## Page 5: Miscellaneous

12. [3 points] *Briefly*, in Bitcoin, how does the *target* relate to the *difficulty*?

13. [3 points] List the parts of a P2PKH transaction. For the part(s) that are not opcodes, label EXACTLY what that part is.

14. [3 points] Don't you wish you had bought Bitcoin 10 years ago?

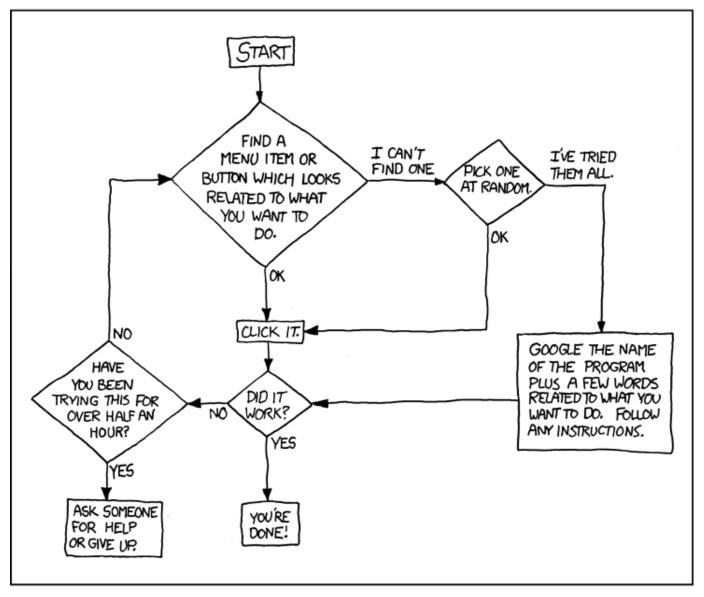
15. [3 points] Propose a name for our course cryptocurrency! But nothing that would get me in trouble, please.

Page 6: No questions here

This page unintentionally left unblank.

DEAR VARIOUS PARENTS, GRANDPARENTS, CO-WORKERS, AND OTHER "NOT COMPUTER PEOPLE."

WE DON'T MAGICALLY KNOW HOW TO DO EVERYTHING IN EVERY PROGRAM. WHEN WE HELP YOU, WE'RE USUALLY JUST DOING THIS:



PLEASE PRINT THIS FLOWCHART OUT AND TAPE IT NEAR YOUR SCREEN. CONGRATULATIONS; YOU'RE NOW THE LOCAL COMPUTER EXPERT!