CS 4501: Cryptocurrency Midterm, spring 2023

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 ECDSA keys are generated.

2. [3 points] *Briefly,* why is ECDSA used in cryptocurrencies instead of the more established RSA algorithm?

3. [3 points] *Briefly,* why do we use finite fields when computing elliptic curves for ECDSA?

4. [3 points] Consider the secp256k1 (aka $y^2 = x^3 + 7$) curve. Let $p = 43$, which means $o = 31$. Let $G = (25, 25)$. What is $(12, 12) \oplus (12, 31) \oplus (13, 22)$? You cannot use a calculator for this!

.

Page 3: Bitcoin

5. [3 points] What are the contents of the pubKey script of a P2PKH transaction?

6. [3 points] *Briefly,* in English, describe the main transaction of a cross-chain atomic swap (the "main" one is the one you had to implement in the homework).

7. [3 points] *Briefly,* what benefit(s) does the Bitcoin witness provide?

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

Page 4: Ethereum

9. [3 points] *Briefly,* what are the use(s) of a *nonce* in Ethereum?

10. [3 points] *Briefly,* how are Ethereum transaction fees computed in US dollars?

11. [3 points] *Briefly,* describe the three types of transactions in Ethereum.

12. [3 points] *Briefly,* what benefits do PATRICIA trees have over Merkle trees?

Page 5: Miscellaneous

13. [3 points] *Briefly,* why do cryptocurrency wallets use seed phrases?

14. [3 points] *Briefly,* what are the requirements for a Cryptographically Secure Pseudo-Random Number Generator?

15. [3 points] Should you buy a Bitcoin miner? *Briefly,* why or why not?

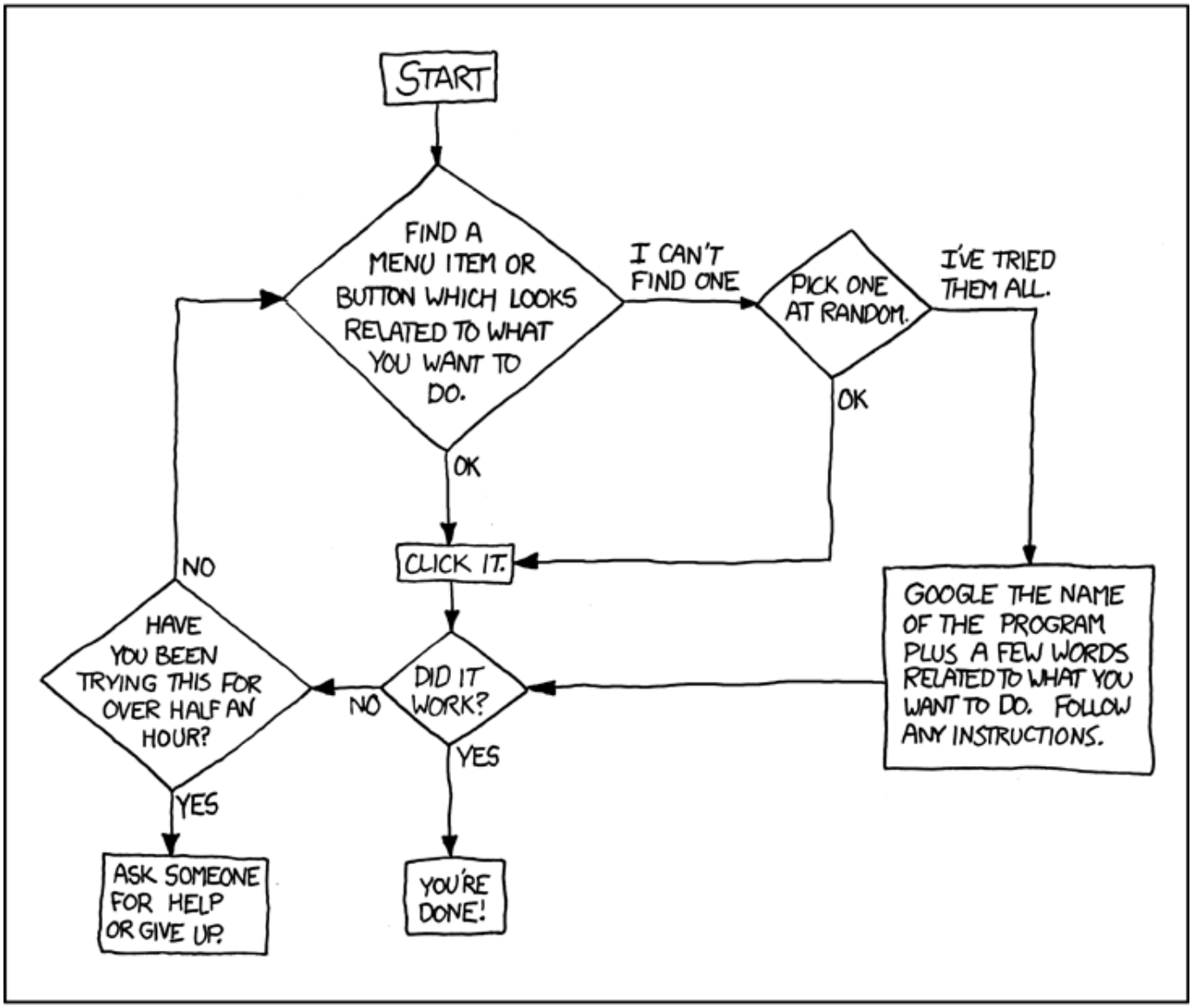
16. [3 points] Name our cryptocurrency! Suggest one (or more) viable names for our Ethereum-like cryptocurrency. More names do not get you more points. Just one (viable) name will get full credit.

Page 6: No questions here

This page unintentionally left blank.

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!

xkcd #627