CS 4501: Cryptocurrency Midterm, spring 2024

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.

_____

_____

_____

_____

Firewalls so mighty,

Like a sieve, they filter all,

Safety's not absolute.

Page 2: General

1. [3 points] list and *briefly* describe the four types of currencies.

2. [3 points] *Briefly,* how does the Bitcoin target relate to the difficulty?

3. [3 points] *Briefly,* how is the mining target encoded in the nBits value?

4. [3 points] *Briefly,* why are there no floating point numbers in cryptocurrencies?

Page 3: Encryption

5. [3 points] *Briefly,* what three things are needed for a good Cryptographically Secure Pseudo-Random Number Generator (CSPRNG)?

6. [3 points] *Briefly,* give one advantage of ECDSA over RSA (or any other general-purpose public key cryptosystem), and one disadvantage of ECDSA over RSA.

7. [3 points] *Briefly,* why is it important that the modulus p and the order o be prime when using ECDSA?

8. [3 points] The value of the base point G in the secp256k1 curve is quite large: each point is around 10^{63}. *Briefly,* how do you think they come up with that specific point?

Page 4: Bitcoin

9. [3 points] *Briefly,* what two problems did the Bitcoin Witness solve?

10. [3 points] *Briefly,* why is the P2PK (pay-to-public-key) transaction type not used anymore in Bitcoin? This question is ignoring any changes related to the Bitcoin Witness.

11. [3 points] *Briefly,* give two reasons why people believe that Satoshi Nakamoto is British.

12. [3 points] *Briefly,* explain how a Bitcoin invoice address is determined. Please ignore the checksum part of this algorithm – it's the rest of the algorithm that we want.

Page 5: Mining and Ethereum

13. [3 points] *Briefly,* give the two uses of the word "staking" as it relates to cryptocurrencies.

14. [3 points] *Briefly,* how does an Ethereum account address checksum work? We are looking for a high-level overview, not a description of the details of the algorithm.

15. [3 points] *Briefly,* how is an Ethereum contract address computed?

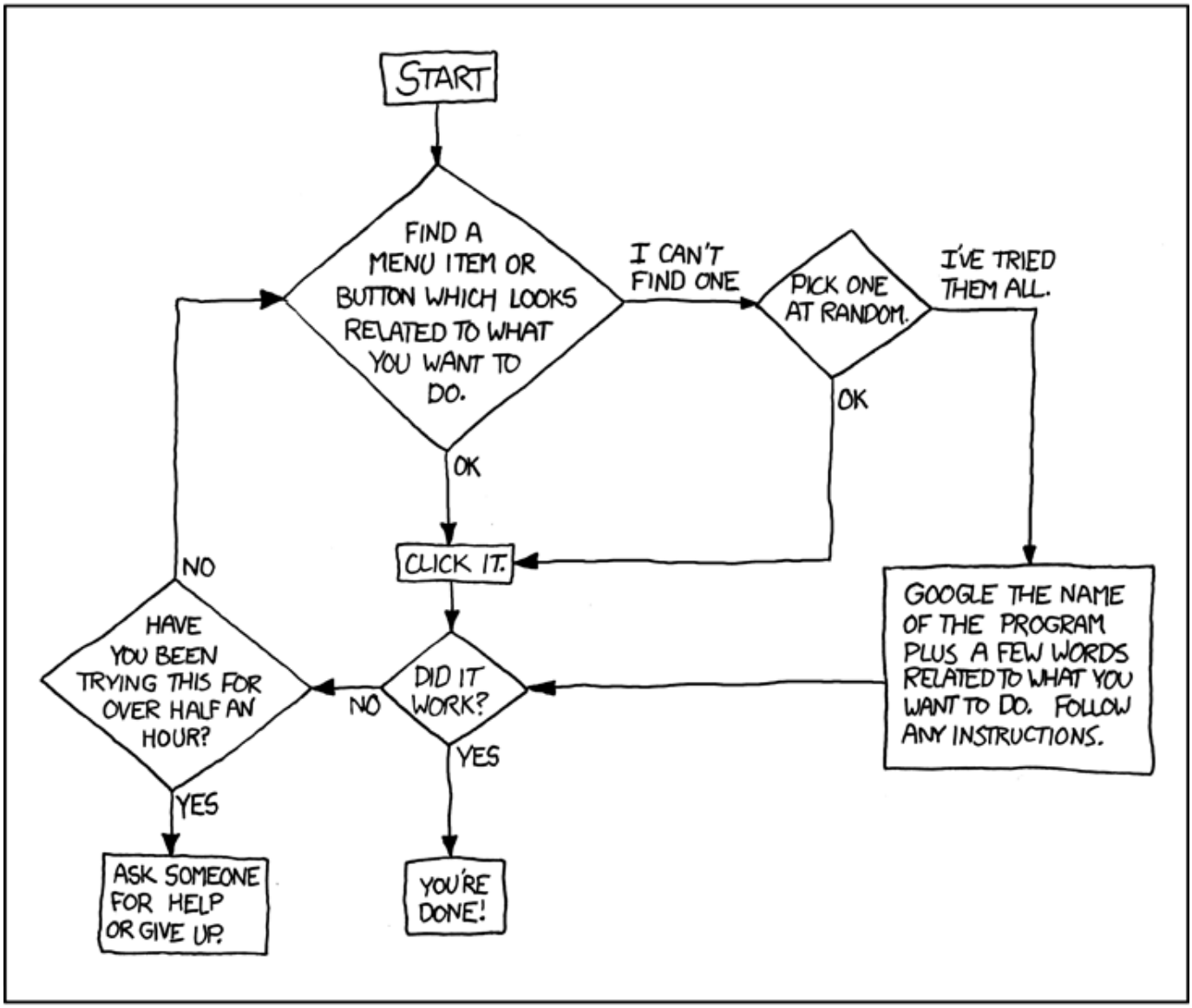
16. [3 points] *Briefly* describe how a 51% attack works

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!

xkcd #627