CS 4970: Cryptocurrency Midterm, spring 2025

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 8 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] Write a Bitcoin P2PKH script. If you don't remember a particular opcode, create an opcode name that makes it clear what that opcode is supposed to do.

2. [3 points] *Briefly,* list two benefits that the Bitcoin *witness* provides.

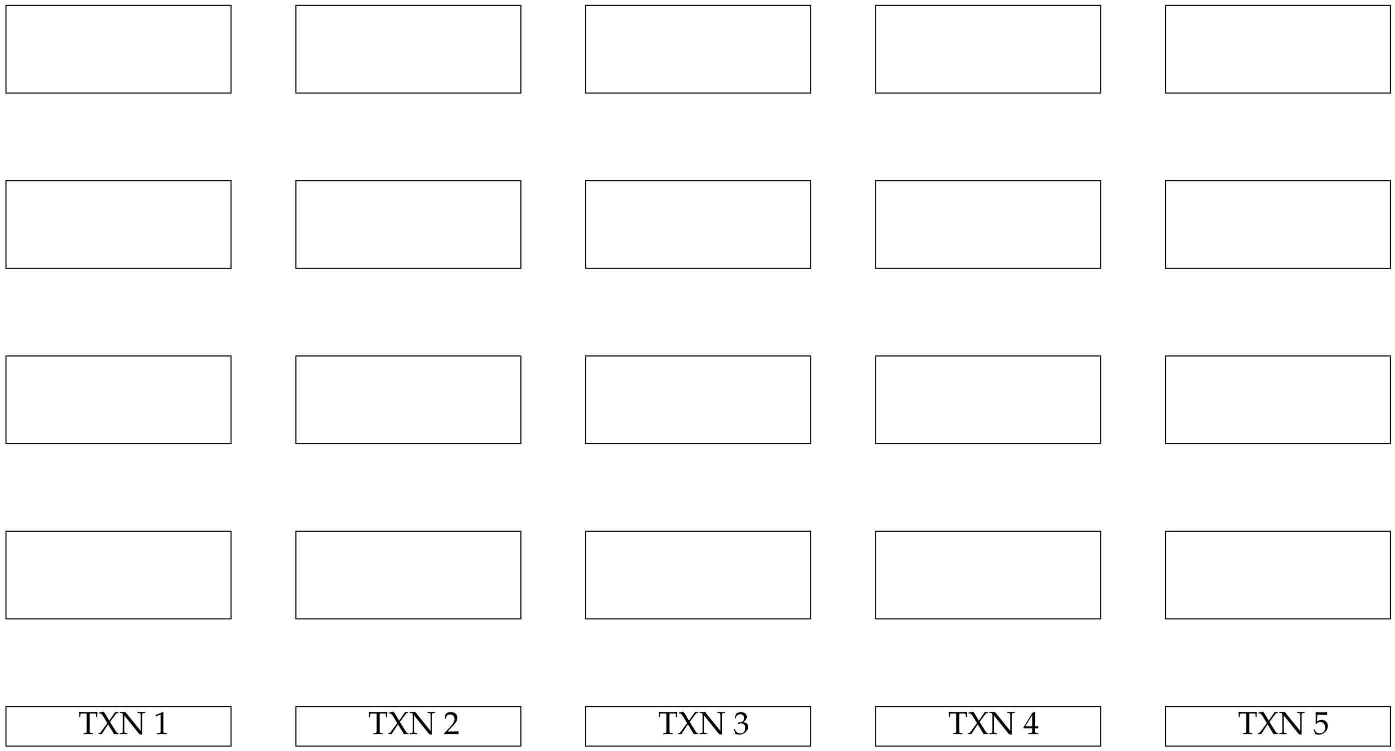
3. [3 points] Bitcoin has a number of "standard" transactions – P2PKH is one of them; the others all have acronyms of that form. List one other, and *briefly* describe it.

4. [3 points] How many transactions are in a typical Bitcoin block?

Page 3: More Bitcoin

5. [6 points] Consider a Bitcoin Merkle tree with 5 different transactions. Diagram the values in the Merkle tree nodes using the boxes below. Not all boxes are going to be used! You should draw lines between the parent and child nodes in the tree.

   We are looking for how the tree is constructed, and how the root hash is determined. You can use any syntax as long as we can reasonably understand what it means.



6. [3 points] *Briefly,* why does Bitcoin use base-58 encoding for the invoice addresses?

7. [3 points] When there is a digital signature in Bitcoin, *what* data is actually being signed?

Page 4: Encryption

8. [3 points] The secp256k1 curve comes with a number of values: a, b, G, p, and o. *Briefly* describe what each of these is.

9. [3 points] *Briefly,* give two reasons why ECDSA was chosen as the particular encryption method in Bitcoin and Ethereum.

10. [3 points] List the three things needed by a CSPRNG (computationally secure pseudorandom number generator).

11. [3 points] Draw what an elliptic curve looks like. We are looking for the values in the range of roughly -5 to 5; specifically: $(-5 \leq x \leq 5, -5 \leq y \leq 5)$. This should have the correct shape, but it doesn't have to be exact! Ideally you can draw secp256k1, but you can get partial credit if you draw another elliptic curve.

Page 5: Ethereum

12. [3 points] *Briefly,* how does an Ethereum address checksum work? We are looking for the high-level view here, not the low-level details

13. [3 points] *Briefly* define the following terms: ethereum, ether, wei

14. [3 points] What is the formula for gas cost, in USD, for an Ethereum transaction?

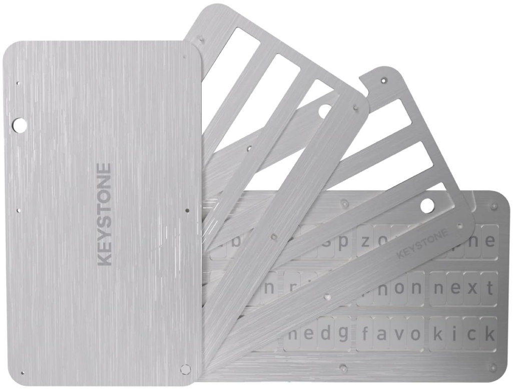
15. [3 points] *Briefly,* what is a token?

Page 6: Miscellaneous

16. [3 points] *Briefly,* what is the difference between the difficulty and the target?

17. [3 points] *Briefly,* how is the nbits field in Bitcoin encoded?

18. [3 points] *Briefly,* what is the point of one of these things? If the image is not clear, it can be put on the projector screen.



19. [3 points] *Briefly,* how do mining pools determine how much work you have contributed to the pool?

Page 7: Ethereum Reading Quiz

This is the Ethereum reading quiz, which we missed due to not having class because of a snow day.

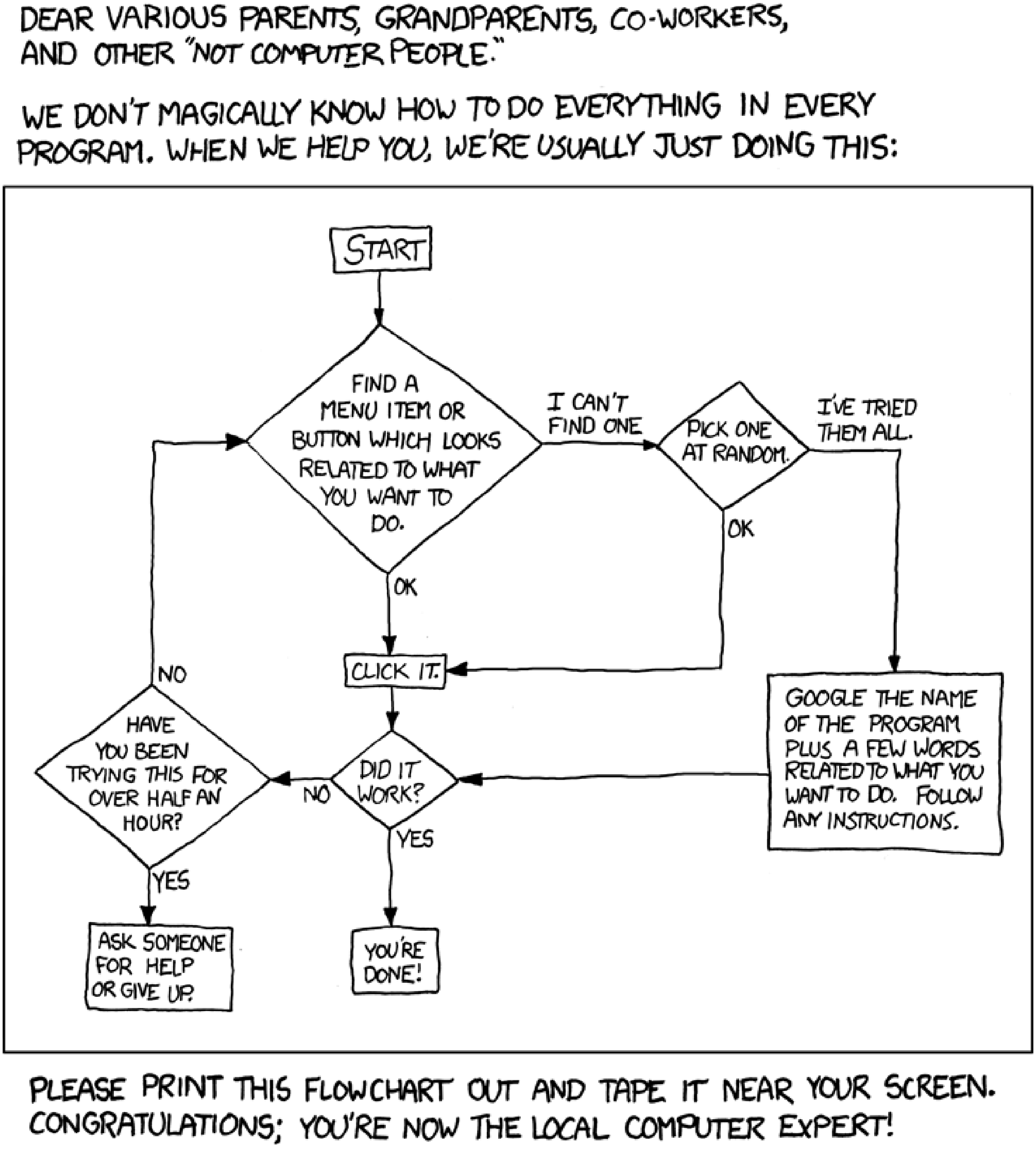
As with the rest of the exam, the ”No B.S.” rule applies.

The rest of the midterm is worth much more than this quiz, so if you are short on time, focus on the midterm first

1. [10 points] Describe one thing in the reading that was not discussed in lecture, and is not described in the Ethereum slide set. We are not looking for a long answer here – in fact, if it’s too long we will deduct points. We are just looking for a clear indication that you did the reading.

Page 8: 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:
START
FIND A MENU ITEM OR BUTTON WHICH LOOKS RELATED TO WHAT YOU WANT TO DO.
I CAN'T FIND ONE
PICK ONE AT RANDOM.
I'VE TRIED THEM ALL.
OK
OK
CLICK IT.
GOOGLE THE NAME OF THE PROGRAM PLUS A FEW WORDS RELATED TO WHAT YOU WANT TO DO. FOLLOW ANY INSTRUCTIONS.
DID IT WORK?
NO
HAVE YOU BEEN TRYING THIS FOR OVER HALF AN HOUR?
NO
YES
YES
ASK SOMEONE FOR HELP OR GIVE UP.
YOU'RE DONE!
PLEASE PRINT THIS FLOWCHART OUT AND TAPE IT NEAR YOUR SCREEN. CONGRATULATIONS; YOU'RE NOW THE LOCAL COMPUTER EXPERT!

xkcd #627