Quiz: Bitcoin Mining with Python

Due Feb 3 at 3:30pm **Points** 9 **Questions** 7 **Time Limit** None

Instructions

This is an individual quiz. Please first follow **these instructions** (https://app.box.com/embed_widget/s/aw3lvm29wz690ej7p9azfabvqyxpkw19?view=list&sort=name&direction=ASC&theme=dark) , and then answer the questions below. This quiz has unlimited time, and it is not proctored.

Attempt History

	Attempt	Time	Score
LATEST	Attempt 1	79 minutes	8 out of 9 *

* Some questions not yet graded

Score for this quiz: **8** out of 9 *
Submitted Feb 1 at 10:05pm
This attempt took 79 minutes.

Question 1 — 2 / 2 pts

What is the winning nonce (the nonce that makes the hash start with three leading zeros)?

- 1988
- 8495
- 451
- 12452

Correct!

Question 2

2 / 2 pts

What is the corresponding hash with the winning nonce?

- 000787d8ff144c502c7f5cffaafe2cc588d86079f9de88304c26b0cb99ce91c6
- Correct! 0009e766bc42829a78b16ea6fc5bf924c38284c487515a188d404648770046b2
- 000086057e5998a2bf58675a8fb405cca069fe783dc35091ff80f90a242bbd8fa
- 0006953de17e408fc4472261a48ea0f7ec58c2371b131a88a00c5bb479a5c9e3

Question 3

2 / 2 pts

Now we want to find a nonce that generates a blockheader hash with 4 leading zeros. What is the winning nonce.

- 102625
- Correct! 277704
- 900344
- 12899

Question 4

Not yet graded / 0 pts

Copy and paste the python code.

Your Answer:

```
import hashlib


trans_hash = hashlib.sha256(b"Cesare sends one bitcoin to
Shimon").hexdigest()
prev_hash =
'85738f8f9a7f1b04b5329c590ebcb9e425925c6d0984089c43a022de4f19c
281'
time = '2018-01-07 21:05:34'
bits = '3'
x = 0
search = 0
while search == 0:
  x += 1
  blockheader = trans_hash + ' ' + prev_hash + ' ' + time + ' ' + bits + ' ' +
str(x)
  newhash = hashlib.sha256(blockheader.encode()).hexdigest()
  if newhash[0:3] == '000':
    search = 1
print(newhash)
print(x)


trans_hash = hashlib.sha256(b"Cesare sends one bitcoin to
Shimon").hexdigest()
prev_hash =
'85738f8f9a7f1b04b5329c590ebcb9e425925c6d0984089c43a022de4f19c
281'
time = '2018-01-07 21:05:34'
bits = '3'
x = 0
search = 0
while search == 0:
  x += 1
```

```
  blockheader = trans_hash + ' ' + prev_hash + ' ' + time + ' ' + bits + ' ' +
str(x)
  newhash = hashlib.sha256(blockheader.encode()).hexdigest()
  if newhash[0:4] == '0000':
    search = 1
print(newhash)
print(x)
```

Question 5

1 / 1 pts

Suppose you have several opponents who have similar computational ability to you, and they all start with a nonce x = 0 and then try different numbers according to the ordering rule (0,1,2,3, ...). In order to compete against them, what might be you strategy?

Correct!

- (•) Start with a nonce x = 1
- ( ) Acquire 50% of the computing power of the network.
- ( ) Start with a nonce x = 0
- ( ) Use proof-of-stake.

By starting at x = 1, you are frontrunning all other miners. When your competitors mine x = 1, you already tried it and already know whether it works or not. In the meantime, you have already moved on to mine x = 2. You are practically guaranteed to win, unless the winning nonce is x = 0.

Question 6

1 / 1 pts

Suppose you happen to find that there is another smart guy who uses your strategy in the question above. What should you do? Suppose again that, each time you get a new strategy, some new smart guy enters the game and uses your newly-developed strategy, what will you do?

Correct!

- (selected) Always start using a nonce that is always one greater than what everybody else uses.
- Start with a nonce x = 1
- Acquire 50% of the computing power of the network.
- Start with a nonce x = 0

Question 7

0 / 1 pts

What might be miners' strategies of choosing numbers for trials in equilibrium?

- Acquire 50% of the computing power of the network.
- Always starts with x = 0

orrect Answer

- Choose random nonces.

ou Answered

- (selected) Try to front-run everybody else.

The reason why it is good to randomize the choice of nonce is that you do not want to be front-run by someone else who knows your nonce-selection strategy.

Quiz Score: **8** out of 9