Blockchain and Digital Currencies, 2019 Module 1

Midterm Exam 2019/10/24

Your name: ___________________________ Student ID: ___________________________

True False Questions:

1. (2 pts) __T__ A cryptographic hash function needs to be collision resistant and hiding.

2. (2 pts) __F__ Bitcoin transactions are absolutely secure and anonymous.

3. (2 pts) __F__ Private keys can be derived from public keys.

4. (2 pts) __T__ Miners collect transaction fees as their incentive to mine blocks.

5. (2 pts) __F__ A Bitcoin wallet needs to store the entire block chain to work properly.

Multiple Choice Questions:

Note: There may be more than one correct answer.

6. (3 pts) Ethereum has the following account types: _______
   a) Externally owned accounts
   b) Internally owned accounts
   c) Contract accounts
   d) Smart contract accounts

7. (3 pts) A Bitcoin transaction includes the following parts: _______
   a) Block header
   b) Metadata
   c) Inputs
   d) outputs

8. (3 pts) What is the minimum number of confirmations required to guarantee a Bitcoin transaction to be permanently recorded in the longest blockchain: _______
   a) 1
   b) 6
   c) 100
   d) None of the above

9. (3 pts) What are the main reasons for miners to provide proof-of-work when claiming validated blocks: _______
   a) To allow all miners to have a fair chance to get block reward

b) To encourage miners to work together in groups such as mining pools

c) To adjust the production rate of the blocks

d) To prevent Sybil and DoS attacks

10. (3 pts) Which of the followings are the characteristics of a Merkle Tree? _______

a) Binary Tree

b) Non-leaf nodes are hashes

c) Linked List

d) Search algorithm with a complexity of O(N), where N is the number of nodes included in the Merkle Tree

Short Answer Questions:

11. (3x2 pts) ***Bitcoin block reward calculation***

The total Bitcoin supply is around 21 × 10^6, that we learn in class is in fact an approximation. Anyway, we are going to derive this number. Please be reminded that (i) the block reward in the first stage was 50 Bitcoins and (ii) the block reward is halved every 210,000 blocks. Block rewards actually becomes zero when it goes below 1 × 10^{-8} (1 Satoshi), which is the smallest Bitcoin unit. However, we can assume that the reward can continue being halved infinitely.

(a) Using the facts and the assumption above, prove that the total Bitcoin supply is 21 × 10^6. The exact Bitcoin supply is 20999999.9769 (taking the reward actually becoming zero into consideration). So 21 × 10^6 is very close.

(b) The total Bitcoin in existence up to today is about 18 × 10^6. If Nakamoto designed the block reward in such a way that it begins with 100 Bitcoins (instead of 50) and the other conditions remain the same, what would be the supply up to today?

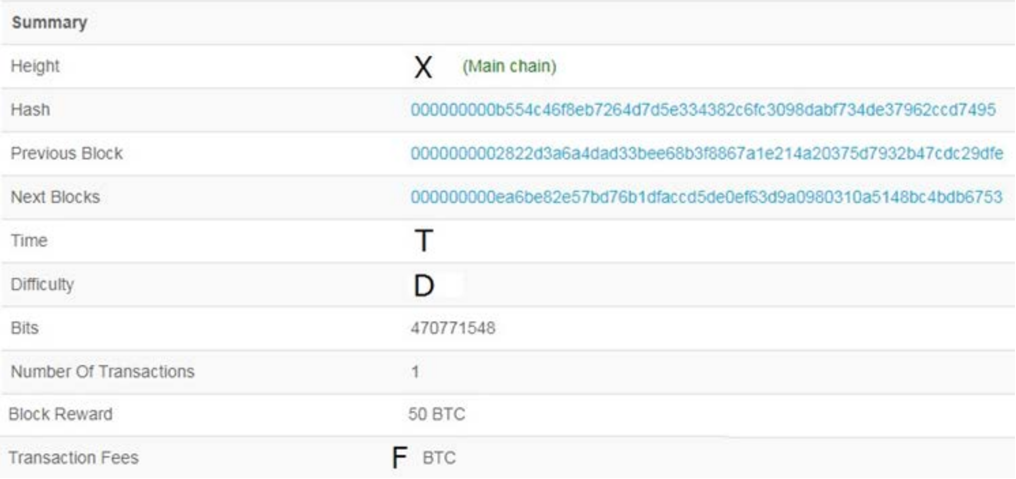
12. (2x3 pts) ***Understanding Bitcoin block***

Below is a summary of a block in the Bitcoin blockchain. Decide whether the following statements are True or False and briefly explain why.

(a) The block height **X** cannot be bigger than 210,000; F

(b) The mining time **T** is around the year 2016; F

(c) The transaction fee **F** must be zero. F



Summary	
Height	X (Main chain)
Hash	000000000b554c46f8eb7264d7d5e334382c6fc3098dabf734de37962ccd7495
Previous Block	000000002822d3a6a4dad33bee68b3f8867a1e214a20375d7932b47cdc29dfe
Next Blocks	00000000ea6be82e57bd76b1dfaccd5de0ef63d9a0980310a5148bc4bdb6753
Time	T
Difficulty	D
Bits	470771548
Number Of Transactions	1
Block Reward	50 BTC
Transaction Fees	F BTC

13. (6 pts) ***Public/private key cryptography***

Alice wants to send a message to Charlie, but she has to send the message to Bob first and then asks Bob to relay the message to Charlie. Alice does not want to reveal the message content to Bob and Charlie wants to be able to verify whether Bob changes the message.

Use the public/private key cryptography knowledge that we learned in class to design an algorithm to help Alice achieve her goal. Use a diagram for illustration if needed.

14. (3x2 pts) ***Miners***

Explain 3 key roles of miners for Bitcoin to work properly.

15. (8 pts) ***Bitcoin vs. Ethereum***

Explain the state machine abstractions of Bitcoin and Ethereum respectively and tell 3 major differences between Bitcoin and Ethereum.

16. (8 pts) ***Gas***

Gas plays an important role in the Ethereum and it is the unit in which all computation in Ethereum is priced. A transaction in Ethereum has two important fields, *gasLimit* and *gasPrice*.

Explain the definitions of these two fields and the importance of setting these two fields proper values.