Networks and Distributed Systems	**Homework 10: Bitcoin**
CS3700 Spring 2019	**January 10, 2019**

This homework is due at the beginning of class on April 17, 2019 and is worth 2% of your grade.

Name: _____

CCIS Username: _____

Problem	**Possible**	**Score**
1	25	
2	30	
3	15	
4	20	
Total	90	

1. In this homework, we'll be exploring actual Bitcoin data. We'll use the `https://blockchain.info/` web site, which allows us to interactively browse the blockchain. For the questions below, we'll be examining block number 351846 in the blockchain.

1a. How many transactions are in this block? (5 pts)

1b. How much in total did the miner who found this block receive for doing so? Hint: it's more than just the coinbase. (5 pts)

1c. Continue looking at block 351846. Locate the second transaction in this block (the one with transaction id `18b37c44...`). How many inputs and outputs are there in this transaction? What is the most likely explanation for why the recipients do not receive the same amount? (5 pts)

1d. To 6 decimal places, what is the total sum of the input for this transaction? What is the total sum of the output of this block? Why is there a difference? (5 pts)

1e. What are the first 6 characters of the recipient who received the difference between the input and output for this transaction? (5 pts)

2a. Locate block number 351833. What is odd about this block? Why do you think this occurred? (10 pts)

2b. What is the "nonce" value that the miner who found this block used? (5 pts)

2c. How "hard" was the block to find? On average, how many nonces would a miner have to try before finding a satisfactory nonce? (Hint: the "difficulty" listed on the page is not the answer. Instead, look at the number of leading zeroes of the hash. The answer requires doing some basic statistical calculations.) (5 pts)

2d. Look at all of the transactions that the miner who found that block has received. Roughly how much USD is this? How has this miner managed to win so many blocks? (10 pts)

3a. Locate the "genesis" block. How many BTC was this block worth? Why is this not the same as the previous blocks we've been looking at? (5 pts)

3b. What are the first 6 characters of the recipient of the coinbase transaction in this block? Have these funds been spent? (5 pts)

3c. Why does the genesis blocks not include any additional transactions? (5 pts)

4a. Suppose the Bitcoin developers released an update to the official Bitcoin client that had a bug. This bug caused these clients to produce blocks that all previous versions of the client (and all other client implementations) would find invalid. Suppose that 25% of the nodes in the network updated to the new client, and the other 75% stays on the older client. What would you expect to happen? (10 pts)

4b. Suppose instead that 75% of the clients switched to the new client and 25% stayed on the old client. What would happen in this case? (10 pts)