Cryptocurrencies Problem-set 2

1. Assumptions:
    a. The agent is rational, and cares about the value of bitcoin as opposed to just destroying the currency. The rationality of miners in common knowledge, which is to say everyone knows that everyone knows that everyone knows, etc. that miners are rational.
2. Given a probability of *q* that an attacker will gain the next block, how many blocks ahead must the honest nodes be to ensure there is a less than .1% the attacker catches up with the honest nodes.
3.

0.1	3
0.15	3
0.2	5
0.25	6
0.3	10
0.35	17
0.4	36
0.45	137

4.
    a. The cloud provider could be returning a copy of the same set of bytes-from data[j] instead of data[i] the way dropbox doesn't store duplicate files if multiple users store the same file.
    b. No, if the data at data[i] and data[j] are the same, and the user is using the same private, public key pair to encrypt, it will tell you that you wrote it, but not which index it is in.
5.
    a.
        i. Read
            1. Search through the database to find the data you are looking for.
        ii. Write
            1. Query the database to edit the value you want to write at data[i]
        iii. Verify
            1. If you want to verify whether the whole database remained the same, compare your local hash of the concatenation to the cloud hash for concatenation for differences.
    b.
        i. Write
            1. Constant. Simply go to the *i* specified.
        ii. Read
            1. Linear

a. Must iterate to a maximum of data[n-1] to find the appropriate data searched.

iii. Verify

1. Constant time to verify whether any of data[0]-data[n-1] has changed. Constant to verify an individual transaction.
    a. Use the public key to find the hash of the concatenation. Then compare that hash to your own to verify.

6.

a.

i. Read

1. Plug in all of the sub-tree hashes until you reach the node with two leaves.

ii. Write

1. Do the same process as reading, but then edit the leaf node, and then record the changes to the merkle hash state in your local machine.

iii. Verify

1. Do the same process as read, but the check the hash of the local data you want to verify with the hash of the data in the leaf node of the Merkle tree.

b.

i. Write

1. Log(n)

ii. Read

1. Log(n)

iii. Verify

1. Log(n)

7.

a. 21.6
b. .1*(number of minutes)*(a)

8. 144*(L/600 seconds)*a
    a. The block will get orphaned if it is discovered after another pool discovered the block, but before the other block was announced to the network due to latency
    b. 144 blocks in a day
    c. a is an individuals hashing power
9. 144*(1-a)
    a. a = hashing power of honest miners
    b. Any blocks mined by selfish miners will be withheld. It will only be revealed when the honest miners catch up to the selfish miners, and then announced at the exact same time due to the spy in the other pool. The number of blocks acquired by the selfish miners is 144*(1-a). If the selfish blocks are chosen by the network, it orphans all of the blocks mined by the honest nodes, which is the same number of

blocks as the selfish nodes. No matter whether the selfish or honest blocks are accepted, 144*(1-a) blocks are orphaned since either the selfish or the honest chains are orphaned.

10. Should returns from appreciated bitcoins be subject to capital gains tax?