Alishan Hassan (ah2xt)
CS4501 - Cryptocurrency
Problem Set 2

1) Satoshi makes the bold claim that it is more profitable for a greedy attacker with a majority of the mining power to play by the rules. This effectively means that it is more profitable to mine bitcoins than it is to steal back his old payments. Thus, Satoshi is assuming that the reward for mining would have a higher return on investment of electricity and CPU cycles than stealing old payments. Because there is going to be a finite number of bitcoins, it also assumes that any transaction fees in the future will have a higher return on investment than theft.

2) This means that the attacker is 340 blocks behind and the probability that he finds the next block is .45.

3) Used a simple C++ program.
Originally:
P < 0.001
q=0.10 z=5
q=0.15 z=8
q=0.20 z=11
q=0.25 z=15
q=0.30 z=24
q=0.35 z=41
q=0.40 z=89
q=0.45 z=340

P < 0.05
q=0.10 z=3
q=0.15 z=3
q=0.20 z=5
q=0.25 z=6
q=0.30 z=10
q=0.35 z=17
q=0.40 z=36
q=0.45 z=137

4) a. We cannot be sure that the content in data[i] is, in fact, at the position i because it could have moved.
b. For the same reason in part a, this isn't going to work. We have no way of verifying that the data didn't move before we read it back.

5) a. Write: Concatenates the new record, finds the hash, and writes to the database.
Read: Involves finding the concatenation of the of all of the records in the database as well as the hash of this concatenation.
Verify: Make sure local and computed hash math.
b. Both reading and writing scale linearly with the number of records, so we can call that O(n).

6) a. Write: Hash the new record and write it to wherever it belongs on the Merkle tree. Also need to rehash the parents of the new record until the root node of the Merkle tree is reached.
Read: Find the hash of the root node using the hashes for all the other elements of the Merkle tree.
Verify: Compare the root node's hash to the locally stored hash.

b. Writing now becomes O(log(n)), however reads become O(n*log(n)).

7) a. 144 blocks are found in a day (at a rate of 10 minutes/block). Thus, if α = .15, then 21.6 blocks will be found.

b. Number of blocks found = .015t, where t is the time used in minutes.

8) For using seconds as a unit, we find that .0016667 blocks are found every second. Thus, with a latency of L, as described in the problem statement, the number of orphaned blocks is .0016667L*α*(1-α)

9) When the mining pool is mining selfishly, then the number of blocks the pool finds is given by the equation:

$$\alpha^2\left(2+\frac{\alpha}{1-2\alpha}\right)$$

And the others are given by: $1 - \alpha^2$
So, now the number would be:

$$0.0016667\,L\left(\alpha^2\left(2+\frac{\alpha}{1-2\alpha}\right)\right)\left(1-\alpha^2\right)$$

10b) Towards the end of his life, Hal Finney received calls demanding an extortion fee in bitcoins. Because these calls were anonymous, and because it isn't inconceivable that criminals would use the semi-anonymity offered by bitcoins to extort bitcoins without leaving any personally identifiable traces, how can these criminals be tracked down?