Problem 1

Satoshi assumes that it is possible for a greedy attacker to assemble a majority of the nodes, that the greedy attacker values monetary value more than maliciously shutting down the bitcoin network, and that the value of bitcoin is based on mass trust of the integrity of the system.

Problem 2

At 45% in his example you need >340 confirmations for the attack to succeed less than 1/1000.

Problem 3

Q	Z
0.1	3
0.15	3
0.20	5
0.25	6
0.30	10
0.35	17
0.40	36
0.45	137

Problem 4

a. The problem is that the size of the private key to be sent with the merkle tree is too large and that matching the private key with the data requires information about the ith index.
b. Yes if the bytes of data I indicate the position we can be sure. Otherwise the private key will not match and the message will be an unintelligible string confirming a non-match.

Problem 5

a. It would verify the whole bitcoin chain and generate a new hash each time a new block is added. The new hash would represent the current state of the chain.
b. The cost of reading and writing would be that each time the records are read and verified all the previous records or n needs to be computed and that each time a new record is written n grows according to the size of the new record written.

Problem 6

a. The procedure for the system is that the node that needs to be verified is verified through the use of data of the pair of the node and the hash of the pair node to the parent pair. The computation for the hashes to the parent pair nodes will repeat recursively until it reaches the base node. To write it must be an even number of transactions and if it is odd a duplicate transaction is created to be paired with itself. If you have one child hash you

can only recreate the parent if you have the other child. You can read based off the information that is given to you and verify the information read is correct by tracing it back to the parent hash with the information requested from the server about the other children and parent hashes.

b. The cost of reading is low because it is read simply based on the information that is given. The cost writing is higher because information must be had about the total number of nodes currently need to be written. If odd a duplicate is created and if even it goes to the regular process of creating a parent node. Reading the database is simply based off of direct information given about the children node. However, reading is not the same as verification because verification needs the pair child node and all the other pair parent nodes to go back to the root node.

Problem 7

a. alpha = 0.15 fifteen percent of all blocks found in the day 1 per 10 minutes
   0.15 * 24*60/10 = 21.6 blocks
b. T Minutes/10 * hashing power percentage

Problem 8

Total amount of cycles per day * (1-hashingpower^2)*latency delay

Problem 9

Total amount of cycles per day * (hashingpower^2 * (2+(hashingpower/(1-2&hasingpower)))*latency delay

Problem 10B

How is Bitcoin taxed and what measures are in place to prevent money laundering through bitcoin?

Challenge 2

It impacts the analysis because once the latency is accounted for, the selfish miner would have to mine a third block and release all three blocks while taking into account that some nodes on the network will already have received a second block from the rest of the network. A new model would be to calculate the recent average time and release all three blocks in such a way such that it would propagate two blocks from the selfish miner so that after the current calculated mean time for a new block to be released has elapsed, there would still be two blocks propagated to all the nodes on the network.