Kienan Adams
PS2

1. First of all, Satoshi is assuming that the attacker actually cares about the Bitcoin network and is rational where money actually means something to them. There is the possibility that some central authority would just want to manipulate the system in the hopes of eventually causing it to lose all legitimacy. Additionally, he assumes that there isn't a way to subvert the system which isn't obvious to observers where the attack could be taking place without anyone realizing. Finally, he seems to assume that selfish mining isn't really a thing because selfish mining is essentially playing by the rules, just trying to manipulate the payout.

2. This means that it is almost entirely unlikely that an attacker with .45 of the mining power could catch up when 340 block behind.

3.
.10 z = 3
.15 z = 3
.20 z = 5
.25 z = 6
.30 z = 10
.35 z = 17
.40 z = 36
.45 z = 137

(In this case, I used the c code from the paper and just changed inputs)

4.

a. You could correctly sign the data but then the storage provider could mix it all up where the records aren't in proper order.

b. No, because writing doesn't provide any info about where it should be position-wise, only what it contained. The signature can match the data but that whole block might not be in the right place.

5.

a. Each time you update the database, create a new hash of all the entries and save that locally. Then when you read an entry from the database, make sure that the local hash value that is stored corresponds with the hash value of all the entries in the cloud's database.

b. Linear. Each time you add a new item, you have to get all items for the hash and that number of items to get will increase each time as well. Verifying requires all n entries.

6.

a. The write/read/verify procedure would probably be similar to the way transactions are verified. Each time we write a new entry, we create a new node in the merkle tree. Then when we read and verify, we only need logn number of data to verify, rather than needing all entries.

7.

a. There are about 6 x 24 = 144 blocks in a day. Therefore with .15 of the hashing power, I'd expect the mining pool to receive around 21 blocks.

b. $\frac{\text{alpha x 144}}{1440} \times t$

8.

$\frac{\text{alpha x 144}}{3600} \times L$

9.

If the mining pool were mining selfishly it would most likely have a much higher number of orphaned blocks. This is because every time it got behind the current chain it would have to dump the blocks that it had saved.

10B. What are your thoughts on New York's recent BitLicense regulations which have led to many companies leaving New York? On what level should regulation ideally come from?