Acacia Dai
Cryptocurrency – Problem Set 2

Problem 1. What are the assumptions necessary to support Satoshi's claim that it is more profitable for a greedy attacker with a majority of the mining power "to play by the rules"? (other than the assumption that the greedy attacker is a "he")

Assumptions include that other people would still want to be involved in Bitcoin and keep it going if one person controlled a majority of the computing power, even if that person was playing by the rules.

Problem 2. At the end of Section 11, Satoshi presents a table for $p < 0.001$, where it is listed "q=0.45 z=340". What does this mean in plain English, expressed in a short sentence?

An attacker has less than 0.01% chance of catching up from 340 blocks behind if they have a 45% chance of finding the next block.

Problem 3. For that same table, what would the *z* values be for $p < 0.05$ (instead of $p < 0.001$)?

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

```
int main() {
    double q = 0.1;
    for(int x = 0; x < 8; x++) {
        for(int z = 0; z < 140; z++) {
            if (AttackerSuccessProbability(q, z) < 0.05)
                cout << "q=" << q << " z=" << z << endl;

        }
        q += 0.05;
    }
}
```

Problem 7.
(a) If a mining pool has 15% (α = 0.15) of the total network hashing power, how many blocks is it expected to find in a day?

1 block per 10 minutes = 6 blocks per hour = 144 blocks per day
15% of 144 blocks = **21.6 blocks found by the mining pool per day**

(b) Obtain a general formula for expected number of blocks a mining pool with α fraction of the total hashing power should find in *t* minutes.

ExpectedBlocks = power * (.1 blocks / minute) * (minutes) = **(0.1)α*t* blocks**

Problem 8. Assuming all of the miners are honest, what is the expected number of orphaned blocks per day for an honest mining pool with hashing power α and latency *L* (as simplified above).

If we hold constant that a block will be found every 10 minutes
A pool with alpha = 0.15 has a 15% chance of finding that block within 10 minutes
The network with alpha = 0.85 has an 85% chance of finding that block within 10 minutes
The chance that both find a valid block within the same 10 minute span is 12.75%
The chance that that happens within L seconds of each other is 0.1275/600 seconds = x/L

So x = L(0.1275/600seconds)

Number of block discovery conflicts = X = **L (α(1- α) / 144)**

Problem 10B. In upcoming classes, we will have visits from a law professor (who also works for the State Department on international cyberlaw and promulgating the open Internet) and an FBI agent who works on criminals using bitcoin for ransom. Come up with at least one good question that you would like one of them to answer.

FBI Agent: Is it possible to use a Bitcoin Attack to give a criminal a false transaction for a ransom? Can former hackers be employed to do so?