Elizabeth Kukla
Cryptocurrency
Evans
6 October 2015

Problem Set 2

1.
The power necessary to rebuild the whole block chain from scratch and catch up necessary to steal your transactions back is so large that with that power you would be able to capture a large portion of the new blocks on the block chain and win the miner's reward of new bitcoin.
It also assumes the amount you would be stealing back from your past transactions is smaller than the amount of money you could gain through mining rewards. If you had millions of bitcoin in old transactions that assumption might not hold.

2.
The probability and attacker could catch up and reverse the transaction is less than 0.001 when he is 340 blocks behind and his probability of finding the next block is 0.45

3.
Z would be 2

4.
a) If the bytes of data don't indicate which index it came from you wouldn't know if they sent you the packet you wanted. All you could verify was that you uploaded the packet, not that it is the exact packet you are expecting to be a data[i].
b) So no, you can not be certain it is the same data item you wrote to data[i] because it's position in data is not recorded in the hash. All you would know it that you wrote it to some place in memory, but not necessarily the place you are currently examining.

5.
a)
Reading would mean pulling down all the files and concatenating and hashing them to make sure they match what you have stored and nothing has changed, writing would mean reconcatinating and hashing everything and storing the new hash.
b) the cost scales linearly which isn't great.

6.
a) read/write/verify would mean getting the hashes of the sibling files in the tree and the hashes of all the nodes above it to calculate the root hash and check it against the cloud storage.
b) log(n), the height of the tree

7.
a) You would expect them to find about 21 blocks per day.
14.76%
b) blocks in t minutes = $(144*\alpha/(1440)) * t$

8. abandoned blocks = $(144*\alpha/(1440))*(L/60)$

9.
You would expect more orphaned blocks when a pool is mining selfishly because it would reveal it’s blocks to make all the honest block abandon their now-useless work.

10b.
I would like to ask the lawyer what some of the implications would be if bitcoin were adopted in enterprise and how law codes would have to change regarding mergers and other corporate cash transactions that are currently regulated by laws. Presumably bitcoin would make it harder to monitor any of that.