Problem Set 2

Carter Hall | CS 4501 | 2015-10-09

Blockchain Consensus

1. The mining reward must be high enough that continuing to search for new blocks is, on average, more attractive than double-spending his/her existing coins. This is not a direct numeric comparison, as stealing from others is not a sustainable strategy, and will eventually damage the currency to the point that the attacker doesn't make money.

2. If an attacker controls 45% of the total hashing power, the probability that he/she could catch up from 340 blocks behind (and present the longest blockchain) is less than 0.001.

3. $p < 0.05$

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

Merkle Trees and Storage

4. Sign each record

- Verifying the signed files does not imply anything about the other files in the database unless you can verify the index of the file.
- Yes; it is impossible for the cloud storage company to alter the file and then sign it with your private key, so it must be the same.

5. Hash concatenation of all records

- Write: Download all existing records, concatenate them, append the new record to the end, hash the concatenation and save the hash locally (replacing the existing hash), upload the new record to the database.

Read: Download data[i] from the database.

Verify: To verify any data[i], download the entire database, concatenate all records, hash the concatenation, compare the hash to the locally stored hash.

- Reading is Theta(1), writing is Theta(n)

6. Merkle tree (assuming I am storing all the intermediate hashes locally)

- Write: Add a leaf to the tree, compute new required hashes using the previously stored hashes.

  Read: Download data[i] from the database

  Verify: Download the Merkle root from the database. Verify the desired item by downloading it and working towards the root, using the locally-stored intermediate hashes. Compare the newly-computed Merkle root to the one downloaded from the database.

- Reading is Theta(1), writing is Theta(lg(n))

Blockchain

7. Expected blocks per unit time

- 21.6 blocks
- 0.1 * alpha * t

8. 14.4 * alpha * L
9. 2 * 14.4 * alpha * L

Question

10. How did you get to work on bitcoin ransom cases with the FBI? How would a college student prepare for such a career?