Class 6: Hash Functions

Schedule

Tuesday, September 15 (8:29pm, tomorrow): Problem Set 1 due.

Wednesday, September 23: Check 2 (was originally scheduled for Monday, September 21)

Readings for next week (should be completed by Monday, September 21 at the latest, but earlier is better):

- Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, 2008. The is the original bitcoin paper, which is quite readable and historically interesting.
- *Chapter 6: The Bitcoin Network* and *Chapter 7: The Blockchain* from Andreas Antonopoulos' book.
- *Chapter 2: How Bitcoin Achieves Decentralization* and *Chapter 5: Bitcoin Mining* from Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder. *Bitcoin and Cryptocurrency Technologies*.

Notes

Why do we typically hash a message before signing it? What's wrong if we always signed the full message?

What are the properties we want in a cryptographically secure hash function?

What is the "birthday attack" in the context of a hash function?

Say you have 3000 distinct files in the "Documents" folder of our laptop. If you have SHA-256 hashes for each of them, do you expect any repeats? If we truncated the hash output to just 20 bits, how many repeats do you expect to see?

What is the advantage of using a Merkle tree as opposed to directly hashing the full string?