Problem Set 5

CSE 452 / CSE M552

June 7, 2017

Submit short, **typeset** (not plain text) answers to the following questions. Please work on this individually. You may not use skip days on this assignment.

Problem 1: Dynamo

Consider a cluster of 100 Dynamo nodes with the following parameters: N=3, W=3, R=3. Does this system provide strict consistency? If not, please provide an example execution where strict consistency is violated.

Problem 2: Bitcoin and Your Password

Instead of storing users' passwords in plaintext, websites usually store them hashed. That way, even if an attacker gets access to their database, users' passwords aren't leaked. Many websites still use SHA-256, though security experts suggest that it is better to use a memory-hard hash algorithm such as scrypt.

Recent blocks in the Bitcoin blockchain have 18 hexadecimal leading zeroes. With transaction fees, mining a Bitcoin block is worth about $40,000. Given this, to within an order of magnitude, how many potential passwords can you hash for one US penny?

Problem 3: Concepts and systems

Consider the following systems: Chubby, BigTable, GFS, Spanner, Dynamo, Bitcoin.

For each of the following concepts, give a (brief) example of how one of the above systems illustrates that concept. Do not use any system more than once.

1. RPC
2. Logging
3. Caching
4. Eventual consistency
5. State machine replication
6. Leases

Problem 4: Course evaluation

True or false: You have filled out the course evaluation.