**IS 651, Distributed Systems**

**Homework #5**

**Due May 8, 2020**

Q1. (30pt) What is a quorum? Explain why we can use quorum to build a correct consensus protocol for both crash quorum (e.g., Paxos) and Byzantine quorum (e.g., PBFT).

Q2. (30pt) Consider the PBFT protocol with 3f+1 nodes in total. You are an attacker who controls one node. Other failures are all benign (crash failures) and the total number of failures is fewer than f. Can you stop progress in the system (no one will agree on anything)? Can you cause an inconsistency?

Hint: you can differentiate between whether the node you control is the primary or the backups.

Q3. (40pt) Blockchains.

1. What’s the difference between permissionless and permissioned blockchains?
2. Why and how do permissionless blockchains solve the same problem of BFT (permissioned blockchain)?