**IS 651, Distributed Systems**

**Homework #5**

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).

Quorum is a number of nodes in the system. If we know a node collects votes from a quorum of nodes, all the correct nodes will reach a consensus in the end.

Key to correctness: there is at least ONE CORRECT node in common of two quorums.

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.

If the faulty node is the backup, it cannot stop progress or cause inconsistency.

If the faulty node is the primary, it can stop progress for a period of time (before every one notices that it’s faulty). But it cannot cause inconsistency in any cases.

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)?

Permissionless: everyone can participate

Permissioned: everyone knows the identity of each other but no one needs to trust anyone.

BFT – there is a leader that everyone agrees on. The leader proposes order of client requests. Everyone actively participates in the protocol all the time.

Permissionless – use PoW to select a leader that proposes the order of client requests. So it’s like a rotating leader protocol. Forking can happen, which means multiple leaders may exist at the same time.