NOC22-CS44: Blockchain and Its Applications
Assignment 6

Correct choices are highlighted in Yellow. Give partial marks for partially correct answers.

1. If there are 24 faulty nodes (crash fault) in asynchronous CFT, at least how many nodes needed to reach consensus
   a. 48
   b. 49
   c. 50
   d. 51

   Detailed Solution:
   2f + 1 = 2*24 + 1 = 48 + 1 = 49

2. In Paxos, a node can have only one role among the three roles at a time. True or False
   a. False
   b. True

   Detailed Solution:
   In typical paxos implementations, a single processor may play more than one role at the same time.

3. Can we reach a consensus when there is one commander, one good lieutenant, and one faulty lieutenant in a .Byzantine Generals Problem. Yes or No?
   a. Yes
   b. No

   Detailed Solution:
   One fault.
   Total nodes required = 3f + 1 = 3 + 1 = 4 . But we have 3 nodes.

4. If there are 24 faulty nodes in, at least how many nodes needed to reach consensus in the Byzantine Fault Tolerance (BFT) system.
   a. 72
   b. 73
   c. 48
   d. 49

   Detailed Solution:
   f = 24
   Total nodes required = 3f + 1 = 72 + 1 = 73

5. Which are the examples of the synchronous consensus techniques?
   a. RAFT
   b. PAXOS
   c. Byzantine General Model
   d. Practical Byzantine General Model

   Detailed Solution:
   RAFT, PAXOS, Byzantine General Model and PBFT , all are synchronous consensus techniques.

6. Suppose you execute your tasks distributedly from six different systems at six different locations. For maintaining the consensus among the systems, you are using the BFT model. You found that one system is permanently failed due to a hardware fault and another system is compromised by an attacker. Does your system correctly work at all?
   a. No
   b. Yes with the remaining nodes
   c. Yes with all the nodes

7. Which of the statements are true?
   a. Paxos is based on state-machine replication
   b. In Paxos, Proposers and Learners maintain a state of the running epochs
   c. In a Paxos, once a consensus is reached, Paxos cannot progress to another consensus
   d. Paxos works in two rounds

   Detailed Solution:
   In Paxos, Learners do not need to maintain a state of the running epochs. Therefore b is False.

8. State machine replication-based consensus is used over permissioned blockchains. Select the suitable reason(s)?
   a. The network is closed, and the nodes know each other, hence state replication is possible among the known nodes
   b. Not need to spend power, time, or bitcoin
   c. Machines can behave maliciously, hence consensus in required
   d. State machine replication-based consensus is not recommended to use over permissioned blockchains.

   Detailed Solution:
   A. and B. are true as nodes know each other and state machine replication does not need to spend power, time like in Proof of Work.
   C. is false because even if machines do not behave maliciously, consensus is required for crash faults.
   D. is false because it is recommended to use state machine replication based consensus over permissioned blockchains.

9. Which are the properties of an asynchronous consensus:
    a. Validity
    b. Agreement
    c. Termination
    d. Integrity

Detailed Solution:
All the options are correct.
Validity: If all correct process proposes the same value v, then any correct process decides v
Agreement: No two correct processes decide differently.
Termination: Every correct process eventually decides.
Integrity: If all the correct processes proposed the same value v, then any correct process must decide v. (Same as validity)

10. The following code snippet from paxos algorithm belongs to which phase?

```
is the ID the largest I have seen so far, max_id == N?
if yes
      reply with an ACCEPTED message & send ACCEPTED(ID, VALUE) to
all learners
if no
      do not respond (or respond with a "fail" message)
```

    a. PREPARE-PROMISE
    b. PROPOSE-ACCEPT

Detailed Solution:

Refer to Lecture 28 - Paxos. The steps in the code snipped belongs to the PROPOSE-ACCEPT phase of Paxos.