Sample Questions

1. What is the nonce and how is it used in mining?
   Answer:
   In Blockchain, mining is a process to validate transactions by solving a difficult mathematical puzzle called proof of work. Now, proof of work is the process to determine a number (nonce) along with a cryptographic hash algorithm to produce a hash value lower than a predefined target. The nonce is a random value that is used to vary the value of hash so that the final hash value meets the hash conditions.

2. In a system with a total of N processes and f faulty processes, what is the byzantine quorum system? Prove your answer.
   Answer:
   Every subset of the nodes with a size strictly larger than $(N + f)/2$ is a Byzantine quorum. Proof:
   We need to show that two Byzantine quorums always overlap in at least one correct process. Any Byzantine quorum might contain f Byzantine processes. Therefore, every Byzantine quorum contains **more than** $\frac{N+f}{2} - f = \frac{N-f}{2}$ correct processes. Following that, two disjoint Byzantine quorums together would have **more than** $\frac{N-f}{2} + \frac{N-f}{2} = N - f$ correct processes. But we know that there are at most $N - f$ correct processes. Therefore, there exists a correct process in both byzantine quorums.

3. Give an example of a pair of state-conflicting methods and explain why they are state-conflicting.
   Answer:
   In a set data structure, add and remove operations are state-conflicting. If both operations operate on one element, changing the order of the execution of the two operations results in different states:
   Starting from pre-state: σ, then doing add(1), remove(1) in sequence results in post-state: σ
   Starting from pre-state: σ, then doing remove(1), add(1) in sequence results in post-state: $\sigma \cup \{1\}$