CS 247: Principles of Distributed Computing
Time: 90 mins

Name and ID: _____

Instructor's name: _____

1. (30 points) Answer the following questions about the Bitcoin blockchain:
   (a) (5 points) Name the consensus mechanism that is used in this blockchain.
   Answer:
   Proof-of-Work
   (b) What is a 51% attack?
   Answer:
   In Blockchain, a 51% attack refers to a vulnerability where an individual or group of people controls the majority of the mining power (hash rate). This allows attackers to prevent new transactions from being confirmed. Further, they can double-spend the coins. In a 51% attack, smaller cryptocurrencies are being attacked.

2. (40 points) What is the amplification mechanism in the authenticated double-echo broadcast (Bracha) protocol? Explain why it is needed.
   Answer:
   When a process receives only f +1 READY messages but has not sent a READY message yet, it also sends a READY message. This step implements an amplification of the READY messages and is crucial for the totality property.
   The amplification step from f +1 to 2f +1 READY messages ensures the totality property. If some correct process bcr-delivers some m, then at least f +1 correct processes must have al-sent a READY message containing m. As these processes are correct, every correct process eventually al-sends a READY message with m by the amplification step or after receiving enough ECHO messages. In either case, every correct process eventually bcr-delivers m.

3. (30 points) What are the three conditions of a well-coordinated replicated execution? Briefly explain what each condition means.
   Answer:

   1. Local Permissibility: Every call must preserve the integrity when executed locally at each node.
   2. Conflict Synchronization: Conflicting calls must be synchronized with respect to each other to have the same total order across all the nodes.
   3. Dependency Preservation: Dependencies of calls must be tracked and checked before execution. In other word, the causal relation between dependent methods must be preserved.