

Assignment 3

Notes:

1 Write your answers in a new word document including your team number and members, and share it with our TA Caden before **03/05/2025, before the spring break.**

email: crh873@miami.edu.

2 No ChatGPT or any other generative AI (e.g., Calude or Copilot) are allowed for answering all the assignments. **Generative AI is only eligible for grammar editing and sentence improvements.**

Part 1: Multiple-Choice Questions (5 Questions. **Multiple Correct Answers**)

1. What are the advantages of using blockchain to store patient records in a healthcare system?

- A. Data cannot be altered, increasing security
- B. Patients can completely delete their medical records at any time
- C. Reduces single points of failure, preventing system crashes
- D. Transactions are verified through a consensus mechanism, ensuring data consistency

2. How does Byzantine Fault Tolerance (BFT) benefit medical data management?

- A. Ensures system agreement even if some nodes act maliciously
- B. Requires at least 51% of nodes to validate data before reaching consensus
- C. Prevents a single server from tampering with stored medical data
- D. Verifies data integrity by cross-checking multiple node confirmations

3. Why can a "51% attack" compromise the security of a blockchain network?

- A. Malicious nodes can double-spend transactions
- B. Honest nodes cannot detect when an attack is happening
- C. The attacker can modify historical transaction records
- D. If the attack fails, the system will automatically recover

4. In blockchain-based medical applications, what is the role of the Gossip protocol?

- A. Speeds up the distribution of block information across the network
- B. Ensures all nodes eventually reach data consistency
- C. Relies on a central server to control data transmission
- D. Helps share large-scale medical data more efficiently across hospitals

5. What are the main limitations of blockchain for healthcare data storage?

- A. High data storage costs
- B. Long transaction confirmation time, affecting real-time processing
- C. Allows unrestricted modification of historical records
- D. Not suitable for large-scale structured databases

Part 2: Scenario-Based Questions (5 Questions)

(Provide a detailed explanation based on blockchain and BFT concepts.)

6. Scenario: A hospital uses blockchain to store Electronic Health Records (EHR) to ensure patient data security. However, a patient is concerned that their medical history is permanently stored and cannot be deleted.

How would you explain blockchain's mechanism and possible solutions to the patient?

7. Scenario: A hospital network implements a BFT-based distributed database system. One server is hacked, and patient records are altered.

Explain how BFT prevents malicious modifications from affecting the entire system.

8. Scenario: A hospital allows Bitcoin payments for patient services. A patient claims they never completed a payment transaction and tries to reuse the same Bitcoin for another payment.

How does blockchain prevent this double-spending issue?