Quiz 5

- Honor Code: You must work completely independently on this assignment. Do not discuss the questions or answers with each other before the assignment is due. Any breach of the honor code will be handled per the University's policy on academic honesty.
- Follow the instructions very careful. Answers that do not conform to the instructions will not be given credit.
- Submit your answers through Blackboard as a PDF file
- A question may have multiple correct answers. You must select all possible correct answers.

1. Which of the following are limitations of building applications on top of Bitcoin?
    a. Transactions with complex locking scripts compromise the security of the Bitcoin protocol.
    b. The scripting language cannot support loops.
    c. A UTXO cannot maintain more than two states. It is either in the SPENT state or in the UNSPENT state.
    d. A UTXO script cannot decide to spend only a portion of the value of the UTXO. It must either spend the entire value of the UTXO or none of it.

2. Ethereum mitigates denial of service attacks by
    a. Requiring gas for each computational step a transaction executes.
    b. Requiring the IP address of the sender to be included in the transaction
    c. Requiring gas for each byte of data in a transaction.
    d. Requiring gas for each hop through the peer-to-peer network that the transaction makes.

3. Suppose an actor with externally-owned account A wants to send a transaction T with 100 gas to contract B. The actor anticipates that sending T would cause contract B to 1) initially consumes 30 gas, then 2) send a message M to contract C with 50 gas, and then 3) consumes an additional 40 gas. The actor also anticipates that the message M would cause contract C to consume 50 gas. What would be the effect on the Ethereum state if the actor does in fact send T to B?
    a. Transaction T has no effect on the state.
    b. 100 gas is subtracted from the actor's account.
    c. 100 gas is added to the miner's account.
    d. 30 gas is refunded to the actor's account.
    e. The effects of message M on in the internal state variables of contract C are stored in the blockchain.