Quiz 4

- 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
- You may use your BCT textbook only. Do not use any other resources.
- A question may have multiple correct answers. You must select all possible correct answers.

1. In a typical transaction
    a. There is one signature that covers all the inputs
    b. Each input contains a signature
    c. There is one signature that covers all the outputs
    d. Each output contains a signature

2. Bitcoin's script supports instructions whose effect is
    a. Adding two numbers
    b. Conditional execution (if/then)
    c. Looping
    d. Recursion
    e. Hashing

3. Alice is paying for a service using Bitcoin micropayments. If she simply disconnects at some point without notifying Bob and stops sending micropayments, what can Bob do?
    - Bob is out of luck. He doesn't earn any Bitcoins and must pursue legal recourse
    - Bob can redeem the maximum amount that Alice initially escrowed into a multisig address
    - Bob can redeem the latest micropayment transaction that Alice sent in the last time period before disconnecting, which matches the length of service she received
    - Bob can refuse to sign the refund transaction, so both Alice and Bob will end up losing Bitcoins, which will sit in the multisig escrow forever

    Bitcoin micropayments require the use of:

    a. Multisignature Transactions
    b. Proof of burn
    c. Time-locked transactions
    d. Pay-to-script-hash

4. Blocks contain a tree of transactions instead of a flat list because
    a. It results in smaller blocks
    b. It's easier to insert or delete new transactions while the block is being assembled
    c. It enables efficiently proving that a transaction is included in a block

Continues on next page…

5. If two conflicting transactions A → B and A → C are both broadcast almost simultaneously from different nodes, what determines which one will eventually end up in the block chain? Select all that apply.
    a. The transaction that reaches the majority of nodes first will win
    b. The transaction that was broadcast first will win
    c. The miner who finds the next block will likely resolve the tie by including one of the transactions in the block
    d. Each node has its own version of the block chain containing the transaction that it heard about first