1. What is the primary function of proof-of-work?

A. To validate transactions

B. To create new blocks

C. To secure the network

D. All of the above

ANS: B, C. Validation is done by digital signatures

2. What is the purpose of using hashing in proof-of-work

A. Compel miners to invest in computing power

B. Introducing parametric cost and profit

C. Properly authenticating the payer and receiver of funds.

D. All of the above

ANS: A,B. Authenticating is done by digital signatures.

3. Which of the following is a key drawback of PoW, often criticized for its environmental impact?

A. Centralization of power

B. Slow transaction speeds

C. High energy consumption

D. Vulnerability to 51% attacks

Answer: C. Discussed in the class. You can adjust the time of proof-of-work. The 6 confirmation is also not inherent for POW.

4. PoW is energy-intensive and computationally expensive. What is the main reason for this design?

A. To make the network more eco-friendly

B. To deter malicious actors from attacking the network

C. To encourage centralization

D. To speed up transaction validation

Answer: B. If PoW was not computationally and energy intensive anyone could propose arbitrary block and upend the whole consesnus mechanism.

5. A miner solved the PoW but included a double-spend transaction in the block

A. The miner will be penalized by other miners

B. The block is cancelled and the miner is banished from the network

C. The block is added and after only the miner agrees to remove the double-spend transactions

D. None of the above.

Answer: D. A blockchain is decentralized, no one can banish or penalize any node. If someone already won the hash puzzle and wants to remove a transaction it has to start calculating the hash from the beginning.

6. If the market price of Bitcoin suddenly drops massively, then

A. Miners will start leaving the network

B. Mining will stop until the price of the bitcoin goes up

C. Chances of 51% attack increases

D. The Bitcoin network is probably insecure and there is a chance the price of the bitcoin will drop further

Ans: A, C, D. If the price drops suddenly the mining process is not profitable anymore. Miners will start leaving the network leaving the network in the hand of dishonest miners. It disrupts the security and people will start leaving the network leading to the possibility of the price dropping further.

7. In PoW, what is the role of the nonce in the mining process?

A. It identifies the miner's public key.

B. It ensures transaction privacy.

C. It's a random number miners change to find a valid hash.

D. It verifies the authenticity of miners.

Answer: C. As explained in the class

8. In a Byzantine Fault Tolerant system, which of the following accurately describes the primary challenge the system is designed to overcome?

A. Synchronous communication between nodes.

B. Tolerance to nodes that may behave maliciously or arbitrarily.

C. Fast block propagation in a blockchain.

D. Elimination of network delays.

Answer: B. Discussed in class.

9. In a network, if the number if dishonest nodes (d) is $1<d<n/3$ where n is the number of nodes. Then,

A. Consensus is possible

B. Consensus is impossible

C. Achieving consensus depends if the message passing is asynchronous or synchronous

D. Incentive based consensus mechanism can help the system arrive at a consensus

ANS: C, D. It depends on if the message passing is Synchronous or asynchronous ref. Byzantine General's problem. Even in asynchronous incentive can solve the problem of consensus as $d<n/2$

10. If in the Bitcoin network, the hashrate suddenly drops to half of its initial value, then

A. The block generation is permanently delayed.

B. The Blockchain will immediately adjust the network rate to maintain the average block finding time of 10 minutes.

C. The blocks will be found with average time > 10 minutes

D. The blocks will be found with average time < 10 minutes

ANS: C. The nodes will adjust the difficulty when the two weeks deadline arrives. Till then the average block finding time is delayed.