Het Patel
CS 4301. 002
Professor Bhavani
02/09/2024

Bitcoin Basics Quiz 1

1) Proof of work is used to: **Establish Consensus because miners must solve complex puzzles to prove the validity of transactions between participants without a third-party authority.**

Not correct below :-

b. Match a private key to a public key → Part of cryptographic process in blockchain
c. Verify sender identity → done through digital signatures
d. Improve transaction performance → related to scalability

2) The following is NOT a benefit of a bitcoin based blockchain system: **Transaction speed is not a benefit of a bitcoin based blockchain system because it's a trade-off between decentralization and security.**

Below options not correct answers because all of them are beneficial to bitcoin based blockchain system.

a. Anonymity
b. Redundancy and fault tolerance
d. Removal of intermediaries

3) If the blockchain has "forked", leading to two competing chains, the bitcoin network will likely: **Pick the longer chain because the network typically chooses the longer chain as valid ones.**

Not correct below :-

b. Pick the shorter chain → represents minority of network's computational power
c. Choose randomly between the two → introduces the uncertainty and the undermine the security and reliability of networks
d. Bring in experts to make an informed decision → contradict the principles of decentralization and trustlessness that underpin the Bitcoin network.

4) The bitcoin network will NOT give the minors an incentive through which of the following mechanisms? **Payments proportional to time spent mining because there are transaction fees and fixed block rewards for miners, regardless of how long they have been mining.**

Not correct below :-

b. Transaction fees
c. A reward for successfully mining a block

are correct mechanisms through which miners are incentivized in the Bitcoin network.

5) For a bitcoin transaction, **the private key of the sender signs a hash containing the previous block and the recipient's public key because in a Bitcoin transaction, the sender uses their private key to create a digital signature, which is then verified using the sender's public key.**

Not correct below :-

b. The public key of the sender signs a hash containing the previous block and the recipient's private key → sender's private key is used for digital signature not recipient's

c. The private key of the sender signs a hash containing the previous block and the recipient's private key → recipient's private key shouldn't be involved in the signing process of a Bitcoin transaction

d. The public key of the sender signs a hash containing the previous block and the recipient's public key → recipient's public key is not involved in the signing process of a Bitcoin transaction

6) A double spend attack: **Is the case where a buyer attempts to use the same coins twice because the attacker tries to spend the same cryptocurrency coins more than once, exploiting a flaw in the network's consensus mechanism.**

Not correct below :-

a. Fools the buyer into spending twice as much → double spend attack involves using the same cryptocurrency coins twice, not deceiving the buyer into overspending.

c. Expends twice as many resources in an attempt to make a fork of the blockchain outpace the original chain → because it describes a 51% attack, not a double spend attack.

d. Causes other miner's to spend twice as many resources and therefore slows down mining progress → because it refers to the impact on other miners' resource expenditure, not the attacker's actions.