Eidgenössische Technische Hochschule Zürich
Swiss Federal Institute of Technology Zurich

Distributed Computing

Systems@ETH Zürich

Prof. T. Roscoe, Prof. R. Wattenhofer

Computer Systems

Quiz 6

Question 1

Which of the following statements is true?

a) Nash equilibria only exist in zero-sum games.

b) In a Nash equilibrium, two players can never increase both of their payoffs by collaborating.

c) Every Nash equilibrium maximizes the social payoff (or minimizes the social cost) of the players.

d) None of the above

Question 2

Which of the following statements best describes a dominant strategy in a game?

a) A strategy that results in the highest payoff regardless of what other players do.

b) A strategy that maximizes the collective payoff of all players.

c) A strategy that allows to beat all the other players (i.e., get a better payoff or a lower cost).

d) A strategy that depends entirely on the actions of the opponents.

Question 3

In a variation of the Prisoner's Dilemma, the total cost for mutual defection is decreased to match the total cost for unilateral defection. What happens to the Nash equilibrium?

a) Mutual cooperation becomes the only Nash equilibrium.

b) The Nash equilibrium remains mutual defection.

c) There are no Nash equilibria in this version.

d) Both mutual cooperation and mutual defection are Nash equilibria.

Question 4

Which of the following is NOT a necessary characteristic of the Prisoner's Dilemma in its classic form?

a) The game is designed so that rational and selfish players will choose to defect (snitch).

b) Both players have a dominant strategy that leads to mutual defection.

c) The game has a Nash equilibrium that is socially optimal.

d) Mutual cooperation yields a better outcome for both players than mutual defection.

Question 5

Consider a game where each strategy has some cost (as opposed to payoff). Under which scenario is the price of anarchy guaranteed to be strictly greater than 1?

a) When the game has only one Nash equilibrium.

b) When the social optimum is a Nash equilibrium.

c) When there are at least two Nash equilibria.

d) None of the above

Question 6

You play the following variation of rock-paper-scissors: you pay 1 if you lose (i.e., you gain -1), you gain 1 if you win, nothing happens if you draw with paper or scissors, but if you draw with rock, both players gain $x > 0$. Which of the following is TRUE?

a) For $x = 2$, it is a dominant strategy to always play rock.

b) For any $x > 0$, the best response to rock is to play paper.

c) There exists some $x > 0$ for which $PoA = OPoA = 1$.

d) For $x = 1$, any strategy is the best response to a player choosing each strategy with probability 1/3.

Question 7

An odd number n of friends live along a linear street, with x_i representing the position of i's house relative to the start of the street. They need to decide on a meeting point by reporting x'_i. Which of the following mechanisms is NOT truthful (i.e., allows some players to reduce their travel distance by misreporting $x'_i \neq x_i$?

a) They meet at the mean of the reported values x'_i.

b) They meet at the maximum of the reported values x'_i.

c) They meet at the median of the reported values x'_i.

d) They select j uniformly at random and meet at x'_j.

Question 8

Bitcoin's difficulty adjustment depends on which of the following?

a) Length of the blockchain.

b) Time taken to mine the last 2015 blocks.

c) Size of the UTXO set.

d) The increase in the number of mining pool operators (not miners).

Question 9

You're waiting for the next Bitcoin block. After waiting 8 minutes...

a) You'll likely wait another 10 minutes on average.

b) You'll likely get a block soon since the average time is 10 minutes.

c) If the mempool is nearly full, miners are incentivized to make block production faster. So, we will see a block sooner rather than later.

d) The difficulty adjustment will speed up block formation since the next block is overdue.

Question 10

Why does Bitcoin's core software intentionally lack an auto-update feature?

a) Auto-updates would introduce unacceptable latency in transaction processing since Bitcoin requires real-time validation.

b) Miners control the update process and prefer manual deployment.

c) The original codebase was designed to be technically immutable, making auto-updates impossible.

d) Node operators need to manually verify and choose which updates to install, preventing unwanted changes to Bitcoin's rules.

Question 11

How do Bitcoin nodes reach agreement on who owns which unspent transaction outputs (UTXO set)? Note: The UTXO set can be thought of crudely as "account balances" in Bitcoin.

a) Nodes use a variant of Practical Byzantine Fault Tolerance (PBFT) to validate the UTXO set.

b) Nodes don't need to agree on the UTXO set.

c) Nodes follow the chain with the most accumulated proof of work, and use that chain's UTXO set as canonical.

d) A master node validates and broadcasts the official UTXO set every 10 minutes.

Question 12

Which field in the Bitcoin block header allows nodes to verify proof of work without downloading the entire block?

a) The nonce field used by miners to find valid blocks.

b) The merkle-root field that represents all transactions in the block.

c) The difficulty target, which is encoded in scientific notation to save space.

d) The previous blockhash field that makes Bitcoin a blockchain.

Question 13

Which of these is FALSE regarding Bitcoin's genesis blockhash?

a) It is hardcoded in the Bitcoin source code.

b) It was generated entirely randomly by Satoshi Nakamoto.

c) It has a few zeroes in its prefix (when written in Hexadecimal notation).

d) It is valid as per the genesis block's proof-of-work difficulty parameter.

Question 14

Which of the following cryptographic primitives does Bitcoin's consensus NOT use?

a) Encryption

b) Digital signatures

c) Cryptographic hash functions

d) Zero-knowledge proofs

Question 15

How does a Bitcoin node know which other nodes to connect to?

a) The source code has a hard coded list of DNS servers (maintained by benevolent developers) that - when pinged - return a set of peers that a node can connect to.

b) If the node has connected to other peers in the past, those peers can be used again.

c) The user can specify node addresses as command line params.

d) All of the above.

Question 16

Alice has 1 UTXO of 4 BTC. She sends 3 BTC to Bob. Then Bob sends 2 BTC to Carol. Finally, Carol sends 1 BTC back to Alice. Assuming that all 3 try to be as efficient as possible, what is the minimum total number of UTXOs that exist after all these transactions are confirmed?