NPTEL Online Certification Courses

Indian Institute of Technology Kharagpur
Jan 2025

Course Name: Blockchain and its Applications (NOC25_CS08)

Assignment 4 - Week 4 (Jan 2025)

TYPE OF QUESTION: MCQ/MSQ

Number of questions: 10 **Total mark: 10 X 1 = 10**

QUESTION 1

What is a "fork" in the context of Bitcoin?

a) A change in the Bitcoin protocol that leads to the creation of a new version of the blockchain
b) A new type of cryptocurrency that does not rely on blockchain technology
c) A collaborative process for miners to resolve conflicts in the blockchain
d) None of the above

Answer: (a)

Detailed solution:
In the context of Bitcoin, a "fork" refers to a change in the protocol or rules of the network, which can result in the creation of a new version of the blockchain.
Please refer to the Week 4 Lecture 16.

QUESTION 2

Suppose a miner initially receives 100 bitcoins as a reward for successfully mining a block at time Jan, 2009. The reward for mining a block is halved approximately every four years (or after every 210,000 blocks). Based on this halving process, which of the following statements are correct? (Please note that once the reward is halved, it will remain the same until four years have been completed or after every 210,000 blocks.)

a) In Jan 2013, the miner will receive 50 bitcoins for adding a new block.
b) In Jan 2018, the miner will receive 25 bitcoins for adding a new block.
c) In Jan 2021, the miner will receive 12.5 bitcoins for adding a new block.
d) In Jan 2024, the miner will receive 6.25 bitcoins for adding a new block.

Answer: (a), (b), and (c)

Detailed solution:
The Bitcoin block reward halves approximately every 4 years (after 210,000 blocks). From Jan 2009 reward was 100 bitcoins(same for 2010, 2011, and 2012); By Jan 2013, the reward was 50 bitcoins(same for 2014, 2015, and 2016); by Jan 2018 it was 25 bitcoins(same for 2017, 2019, and 2020); and by Jan 2021 it was 12.5 bitcoins(same for 2022, 2023, and 2024). By Jan 2024, the halving to 6.25 bitcoins will not yet have occurred, making the last statement incorrect.

QUESTION 3

How does the Bitcoin network prevent double spending?

a) A centralized authority will be used to verify each transaction before it is added to the blockchain.
b) Relying on a proof-of-work consensus mechanism ensures that only one valid transaction is accepted.
c) All transactions are stored in a centralized database that tracks each Bitcoin's status.
d) By limiting Bitcoin transactions to one per user per day.

Answer: (b)

Detailed solution:

The proof-of-work consensus mechanism in Bitcoin prevents double-spending by requiring miners to solve cryptographic puzzles to add new blocks. This ensures transactions are verified by multiple miners and nodes, making it nearly impossible for double spending to occur.

QUESTION 4

Which of the following is a challenge of the permissionless model in blockchain?

a) Ensuring that all participants trust a central authority
b) Reaching agreement (consensus) across a decentralized network of participants without a trusted third-party
c) Limiting the number of participants to improve scalability
d) Preventing participants from accessing the blockchain

Answer: (b)

Detailed solution:
Please refer to the Week 4 Lecture 18.

QUESTION 5

Which of the following is not included in a block of a blockchain?

a) Transaction data
b) Hash
c) Timestamp
d) IP address of the miner

Answer: (d)

Detailed solution:

The **miner's IP address** is not included in a blockchain block. The other options—**transaction data**, **cryptographic hash**, and **timestamp**—are standard components of a blockchain block.

QUESTION 6

Which of the following is not a failure that blockchain tries to handle , as rather an attack that a blockchain can try to defend to ensure prevention?

a) Crash Fault
b) Double Spending
c) Byzantine Fault
d) Link Fault

Answer: (b)

Detailed solution:

Please refer to the Week 4 Lecture 18.

QUESTION 7

Which of the following best describes **Safety** and **Liveness** in Bitcoin?

a) **Safety** ensures transactions are irreversible, while **Liveness** ensures transactions are eventually added.
b) **Safety** guarantees quick transaction confirmation, while **Liveness** prevents forks.
c) **Safety** prevents double-spending, while **Liveness** speeds up block creation.
d) **Safety** ensures blocks are always valid, while **Liveness** ensures no transaction delays.

Answer: (a)

Detailed solution:
Safety ensures that once a transaction is confirmed, it cannot be reversed, preventing issues like double-spending. **Liveness** ensures that transactions will eventually be added to the blockchain, even if there are delays or forks.
Please refer to the Week 4 Lecture 19.

QUESTION 8

What is the main purpose of the **Proof of Work** (PoW) mechanism in Bitcoin?

a) To validate transactions with the need for a central authority.
b) To speed up transaction processing times by reducing the time needed to add new blocks.
c) To make it easier for miners to add new blocks without computational work.
d) To secure the network and prevent fraudulent transactions through computational difficulty.

Answer: (d)

Detailed solution:
Please refer to the Week 4 Lecture 19.

QUESTION 9

What is the correct order of events when adding a new block to the Bitcoin blockchain?

a) Block Mining → Block Propagation → Block Flooding → Transaction Flooding
b) Transaction Flooding → Block Mining → Block Propagation → Block Flooding
c) Transaction Flooding → Block Flooding → Block Propagation → Block Mining
d) Block Propagation → Block Mining → Block Flooding → Transaction Flooding

Answer: (b)

Detailed solution:
Please refer to the Week 4 Lecture 19.

QUESTION 10

Which of the following statements is incorrect regarding **Proof of Work (PoW)** in the context of forks, attacks, and the monopoly problem?

a) PoW forks can occur when two miners independently solve the puzzle at the same time, leading to a brief divergence in the blockchain.
b) While PoW encourages miners to follow the longest chain, it does not prevent attacks like 51% attacks, where malicious miners can control the blockchain.
c) The Monopoly Problem refers to a situation where a single miner or group controls a majority of the network's hashing power, undermining decentralization.
d) Proof of Work ensures complete decentralization by preventing any miner from controlling the majority of the hashing power.

Answer: (d)

Detailed solution:
Please refer to the Week 4 Lecture 20.