BRAINWARE UNIVERSITY

Term End Examination 2023-2024
Programme – MCA-2022
Course Name – Introduction to Blockchain Technology and Applications
Course Code - MCA403B
(Semester IV)

Full Marks : 60 **Time : 2:30 Hours**

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A

(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) List the attacks that involve creating multiple fake identities to control a network.

a) Sybil attack b) 51% attack
c) DDoS attack d) Brute force attack

(ii) What is Algorand?

a) Slow transaction processing b) Energy-intensive consensus
c) High scalability d) Centralized governance

(iii) Outline the concept of 51% attack.

a) Controlling the majority of network hash rate b) Duplicating private keys
c) Exploiting software bugs d) Launching a DDoS attack

(iv) How does Pseudo-anonymity differs from complete anonymity ?

a) Transparency b) Identity concealment
c) Centralized control d) Transaction speed

(v) Choose which of the following properties is NOT required from an atomic broadcast protocol?

a) Validity b) Uniform Agreement
c) Total Order d) Random Order

(vi) Decide what is the main purpose of a hash function?

a) To compress data into a fixed-size output. pseudo-anonymity offers partial concealment. b) To encrypt data for secure transmission.
c) To generate random numbers for cryptography. d) To create digital signatures for message authentication.

(vii) Select the use of zero-knowledge proof system be used in a real-world application.

a) To prove you are eligible to vote online without revealing your identity. b) To securely login to a website without sending your password. identity.

c) To verify the integrity of downloaded software without revealing its content.
d) All of these are possible applications.

(viii) What is the main purpose of a digital signature?

a) To encrypt data for secure transmission.
b) To compress data for storage efficiency.
c) To authenticate the origin and integrity of a message.
d) To generate random numbers for cryptographic protocols.

(ix) Identify the collision-resistant hash function be used in a secure file download system.

a) To encrypt the downloaded file before storing it locally.
b) To verify the integrity of the downloaded file before opening it.
c) To compress the file size for faster download speeds.
d) To generate a unique identifier for the downloaded file.

(x) What is the underlying technology that powers Bitcoin?

a) Artificial Intelligence
b) Blockchain
c) Quantum Computing
d) Cloud Computing

(xi) Estimate the role of the Ethereum Virtual Machine (EVM) in smart contract execution.

a) It stores smart contracts on the blockchain.
b) It provides a secure environment for running smart contract code.
c) It determines the transaction fees for smart contract interactions.
d) It allows users to directly modify smart contracts.

(xii) Infer the use of the Zk-SNARKs (Zero-knowledge Succinct Non-interactive Argument of Knowledge) in Zcash .

a) Faster block verification times.
b) Proof of transaction validity without revealing sensitive details.
c) Enabling direct communication between blockchain nodes.
d) Minting new cryptocurrency units.

(xiii) Outline the involvement of Selfish mining .

a) Miners withholding valid blocks to gain an unfair advantage in the network.
b) Upgrading mining hardware to increase processing power.
c) Collaborating with other miners to centralize control.
d) Utilizing renewable energy sources for mining operations.

(xiv) Infer the role of hash pointers that plays in maintaining data integrity,In the context of blockchain.

a) They ensure all transactions are reversible
b) They prevent unauthorized access to the blockchain
c) They provide a unique identifier for each block
d) They create a cryptographic link between blocks

(xv) List essential feature does digital cash offer in the realm of blockchain technology.

a) Anonymity and privacy
b) Centralized control by financial institutions
c) Inability to trace transaction history
d) Instantaneous transaction processing

Group-B

(Short Answer Type Questions) 3 x 5=15

2. What is the concept of Turing completeness in the context of smart contract languages? (3)
3. Explain the concept of permissioned blockchain and its use cases. (3)
4. Give an example of a decentralized digital cash system and explain how it operates without relying on a central authority. (3)
5. Discuss a novel scripting language feature for Bitcoin and justify its potential benefits. (3)
6. Explain the role of verifiable random functions in cryptographic systems. (3)

OR

Compare the security implications of public key cryptography versus symmetric key cryptography. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Identify the limitations of the fail-stop model in representing real-world scenarios with distributed systems. (5)
8. Explain the concept of a puzzle-friendly hash function and its role in cryptocurrency mining. (5)
9. Evaluate the statement: "Public key cryptography revolutionized secure communication in the digital age." (5)
10. Analyze the trade-offs between Proof-of-Work and Proof-of-Stake consensus mechanisms. (5)
11. Justify why understanding Bitcoin scripting language is valuable even if you're not a developer. (5)
12. Discuss the concept of smart contracts and their role on the Ethereum blockchain. (5)

OR

Develop various scenarios where smart contracts could be used. (5)

****