VIT Vellore Institute of Technology

Reg. No. : 20BCB1167

Final Assessment Test (FAT) - November/December 2023

Programme	**B.Tech.**	Semester	**FALL SEMESTER 2023 - 24**
Course Title	**BLOCKCHAIN AND CRYPTOCURRENCY TECHNOLOGIES**	Course Code	**CSE1006**
Faculty Name	**Prof. Prabakaran R**	Slot	**E1+TE1**
		Class Nbr	**CH2023240100188**
Time	**3 Hours**	Max. Marks	**100**

Section 1 (10 X 10 Marks)
Answer all questions

01. Imagine you are developing a new cryptocurrency based on the Proof of Work (PoW) consensus mechanism. Describe how you would design the incentive structure to encourage miners to participate in the network and secure transactions. Discuss the potential challenges you might face in balancing these incentives and ensuring the security and stability of your blockchain network. **[10]**

02. Assume that you are working as a system engineer in ABC Software development company, and you are developing a project with your team members for "HFCC BANK". The bank customer asked you to provide more security to the bank information and remove the central authority in the banking operation process. Suggest a suitable current technology to implement the customer's demand, List out the key components and processes that make up the structure of the proposed technology and Describe how they contribute to its security and decentralization. **[10]**

03. Construct a Merkle tree for the following data: 1, 2, 6, 7, 4, 5, 3, 9. **[10]**
a) The hashes are generated by summing the two adjacent nodes. (5 Marks)
b) Determine whether the following nodes 23 and 19 are members of the Merkle tree or not. (5 Marks)

04. Imagine you are designing a blockchain-based voting system where each vote is represented as a leaf node in a Merkle tree. The root of this Merkle tree is then stored in a blockchain block. Explain how the use of Merkle trees in this context provides security and transparency to the voting process, and How it can help detect any tampering with the votes. **[10]**

05. Assume mobile cost is 2000 BTC and a TV cost is also 2000 BTC. X has 2000 BTC only in his wallet and is attempting to use the same 2000 BTC to buy a phone and a TV from the Amazon website. What technologies does the online portal need to have in order to prevent this kind of purchase? Discuss in detail the technology behind bitcoin and how it efficiently addresses and prevents the aforementioned issue. **[10]**

06. Consider you are a Bitcoin miner. Discuss the step-by-step process you would follow when attempting to add a new block of transactions to the Bitcoin blockchain. Include details about how you select transactions, solve the proof-of-work puzzle, and compete with other miners in the network. Discuss the rewards and incentives you receive for successfully mining a block. Elaborate the role this plays in the security and integrity of the Bitcoin network. **[10]**

07. Mr.Alice wants to send 1 Bitcoin to Bob. Alice creates a transaction that specifies the amount and Bob's Bitcoin address, signs it with her private key, and broadcasts it to the network. [10]

a) Describe the role of a minor in adding multiple transactions into a block. (5 Marks)

b) Suggest a mechanism to overcome the double-spending attack for the transaction initiated by Alice. (5 Marks)

08. Create a special 'mint' transaction whose output 'address' is the cryptographic commitment of the zerocoin's serial number. The input of the mint transaction is a basecoin, which has now been spent on creating the zerocoin. [10]

a) Explain the role of the "mint" transaction in the ZeroCoin protocol, and how it differs from a typical cryptocurrency transaction. (5 Marks)

b) Describe the process for creating a new ZeroCoin using the "mint" transaction and explain why the output address is the cryptographic commitment of ZeroCoin's serial number. (5 Marks)

09. Imagine you're a cryptocurrency enthusiast who values privacy. You want to use a decentralized mixing service to enhance the privacy of your Bitcoin transactions. Describe the process you would follow to use a decentralized mixing service, How it works to obfuscate the origin of your coins and What potential challenges or risks you should be aware of when utilizing such services to maintain your privacy within the Bitcoin network. [10]

10. Assume that You are part of a group of friends who want to organize a secure multi-party lottery using Bitcoin as the platform. Describe the steps and technologies you would use to ensure the lottery's fairness, security, and transparency. Discuss how Bitcoin's blockchain and smart contracts can be utilized to guarantee that the lottery results are tamper-proof and that all participants have confidence in the integrity of the process. Also, consider the potential challenges and risks associated with such a venture and how they can be mitigated. [10]