Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 15-12-2025 **Time:** 1.00pm to 04.00pm

School: SOCSE	**Program:** B.Tech	
Course Code: CCS3412	**Course Name:** Blockchain Security	
Semester: V	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	CO1	CO2	CO3	CO4	CO5
Marks	26	36	38	-	-

Instructions:

(i) Read all questions carefully and answer accordingly.

(ii) Do not write anything on the question paper other than roll number.

Part A

Answer ALL the Questions. Each question carries 2marks. **10Q x 2M=20M**

1.	Define Blockchain technology.	**2 Marks**	**L1**	**CO1**
2.	State Byzantine generals Problem.	**2 Marks**	**L1**	**CO1**
3.	Define Block.	**2 Marks**	**L1**	**CO1**
4.	Define confidentiality in cryptography.	**2 Marks**	**L1**	**CO2**
5.	Define Stream ciphers.	**2 Marks**	**L1**	**CO2**
6.	Define Elliptic curve.	**2 Marks**	**L1**	**CO2**
7.	Define Bitcoin.	**2 Marks**	**L1**	**CO3**
8.	Define Deterministic Wallet.	**2 Marks**	**L1**	**CO3**
9.	List the methods of providing intial number of altcoins.	**2 Marks**	**L1**	**CO3**
10.	State Kimoto Gravity Well.	**2 Marks**	**L1**	**CO3**

Part B

Answer the Questions. **Total Marks 80M**

11.	**a.**	Describe the network view of a blockchain.	**10 Marks**	**L2**	**CO1**
	b.	List and explain different types of Blockchain.	**10 Marks**	**L2**	**CO1**
		Or			
12.	**a.**	Describe different types of network system.	**10 Marks**	**L2**	**CO1**
	b.	Explain how Arvind Narayanan's four-question framework helps determine the degree and method of decentralization in a blockchain-based system. Provide an example of how this framework could be applied to decentralizing an identity management system.	**10 Marks**	**L2**	**CO1**

13.	**a.**	Define Symmetric key cryptography. Describe different types of ciphers.	**10 Marks**	**L2**	**CO2**
	b.	Explain the working of ECC.	**10 Marks**	**L2**	**CO2**
		Or			
14.	**a.**	Explain the security properties of hash function. Describe the algorithm design of SHA-256.	**10 Marks**	**L2**	**CO2**
	b.	Define shared key cryptography. Explain the cryptographic services.	**10 Marks**	**L2**	**CO2**

15.	**a.**	Alice wants to send 1.5 Bitcoins to Bob through the Bitcoin blockchain network. Describe what happens from the moment Alice initiates the transaction until Bob successfully receives the Bitcoin in his wallet. Based on this scenario, explain the transaction life cycle in the blockchain network	**10 Marks**	**L2**	**CO3**
	b.	Discuss the role of digital keys and addresses in Bitcoin transactions.	**10 Marks**	**L2**	**CO3**
		Or			
16.	**a.**	An investor uses a blockchain-enabled trading platform to purchase 100 shares of a company through a smart contract-based system. The transaction passes through multiple stages — from order placement to final settlement all recorded on a distributed ledger. Discuss in detail how the key components of	**10 Marks**	**L2**	**CO3**

		the trade life cycle are managed within this blockchain-based environment.			
	b.	Analyze how the various attributes of the transaction within the blockchain environment work together.	**10 Marks**	**L3**	**CO3**

17.	**a.**	Describe the structure and operation of the Data Encryption Standard (DES).	**10 Marks**	**L2**	**CO2**
	b.	In a blockchain network such as Bitcoin, every transaction must be digitally signed to ensure that only the legitimate owner of the funds can authorize their transfer. The Elliptic Curve Digital Signature Algorithm (ECDSA) is widely used to provide this security. Explain in detail how the ECDSA algorithm is used in blockchain systems to ensure authentication, integrity, and non-repudiation of transactions. Describe each step involved in key generation, signature creation, and signature verification using ECDSA.	**10 Marks**	**L2**	**CO2**
Or					
18.	**a.**	Explain the concept of alternative coins and their evolution from Bitcoin.	**10 Marks**	**L2**	**CO3**
	b.	Describe how bitcoin payments are initiated.	**10 Marks**	**L2**	**CO3**