Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – December 2025

Date: 05-12-2025 **Time:** 01:00pm – 04:00pm

School: SOCSE	**Program:** B.Tech., IST	
Course Code: CSE3022	**Course Name:** CRYPTO CURRENCY TECHNOLOGY	
Semester: VII	**Max Marks**: 100	**Weightage**: 50%

CO – Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**26**	**24**	**26**	**24**	**-**

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.	Explain the role of a hash function in cryptocurrencies?	**2 Marks**	**L2**	**CO1**
2.	Discuss about collision-resistance?	**2 Marks**	**L2**	**CO1**
3.	Distinguish a hash pointer from a normal pointer?	**2 Marks**	**L2**	**CO1**
4.	Recognize a Bitcoin address and how is it linked to a public key?	**2 Marks**	**L2**	**CO2**
5.	Identify the three main digital signature algorithms?	**2 Marks**	**L2**	**CO2**
6.	Express in what way do HD wallets make key management easier to understand and handle	**2 Marks**	**L2**	**CO3**
7.	Explain how Bitcoin maintains a consistent block creation time even when mining power changes	**2 Marks**	**L2**	**CO3**
8.	Identify the difference between hot storage and cold storage?	**2 Marks**	**L2**	**CO3**
9.	Choose which method can be applied to prevent double-spending without a central authority?	**2 Marks**	**L3**	**CO4**
10.	Write about the concept which is applied when a car unlocks only after blockchain payment?	**2 Marks**	**L3**	**CO4**

Part B

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

11.	**a.**	Explain how cryptography supports the security and functioning of cryptocurrencies compared to traditional encryption uses.	**10 Marks**	**L2**	**CO1**
	b.	Explain why collision-resistance, hiding, and puzzle-friendliness are important properties of hash functions.	**10 Marks**	**L2**	**CO1**
		Or			
12.	**a.**	Describe how the Merkle–Damgård transform enables variable-length input processing and how SHA-256 applies it.	**10 Marks**	**L2**	**CO1**
	b.	Explain how hash pointers work and how they create tamper-evident blockchain logs.	**10 Marks**	**L2**	**CO1**

13.	**a.**	Describe how a blockchain built using hash pointers forms a tamper-evident log and why altering past blocks fails.	**10 Marks**	**L2**	**CO2**
	b.	Explain how digital signature schemes work and how the unforgeability game checks their security.	**10 Marks**	**L2**	**CO2**
		Or			
14.	**a.**	Explain how Bitcoin combines puzzles and secure timestamping and why this improves earlier systems.	**10 Marks**	**L2**	**CO2**
	b.	Distinguish cash-based and credit-based systems and relate them to modern online payments.	**10 Marks**	**L2**	**CO2**

15.	**a.**	Describe the structure of a Bitcoin block and how it ensures blockchain security.	**10 Marks**	**L2**	**CO3**
	b.	Explain hot vs cold storage and how exchanges combine them securely.	**10 Marks**	**L2**	**CO3**
		Or			
16.	**a.**	Explain how (k,n) secret sharing works and why it is more secure than single-key storage.	**10 Marks**	**L2**	**CO3**
	b.	Descrcibe PoR and PoL and explain how they prove exchange solvency.	**10 Marks**	**L2**	**CO3**

17.	**a.**	Demonstrate how blockchain, consensus, and digital signatures can be used to build a trustless ownership-tracking service.	**10 Marks**	**L3**	**CO4**

	b.	Apply smart property and smart contracts to automate property-title transfer once full payment is completed	**10 Marks**	**L3**	**CO4**
Or					
18.	**a.**	Use payment channels (e.g., Lightning) to support repeated micropayments efficiently.	**10 Marks**	**L3**	**CO4**
	b.	Demonstrate how interdependent transactions guarantee simultaneous payment and delivery of a digital license.	**10 Marks**	**L3**	**CO4**