



PRESIDENCY UNIVERSITY

BENGALURU

Roll No.																			
----------	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--	--

End - Term Examinations – December 2025

Date: 18 – 12- 2025

Time: 01:00pm – 04:00pm

School : SOCSE	Program : B.Tech. Computer Science and Engineering (Block Chain)		
Course Code : CBC3408	Course Name : AI Powered Fraud Detection in Block Chain		
Semester : VII	Max Marks : 100	Weightage : 50%	

CO - Levels	C01	C02	C03	C04	C05
Marks	24	24	26	26	

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.	How does a Sybil attack affect block chain networks?	2 Marks	L2	C01
2.	List the purposes of anti-fraud mechanisms in block chain.	2 Marks	L1	C01
3.	How does a decision tree help detect fraudulent transactions?	2 Marks	L2	C02
4.	What type of data is available in the Elliptic dataset?	2 Marks	L1	C02
5.	What is reentrancy vulnerability in Solidity?	2 Marks	L1	C03
6.	Define Hidden transfer restriction attack.	2 Marks	L1	C03
7.	What does a sudden burst in crypto wallet activity indicate?	2 Marks	L2	C03
8.	Write down the purpose of using Kibana in block chain fraud analysis.	2 Marks	L1	C04
9.	What is the significance of real-time alerts for crypto transactions?	2 Marks	L2	C04
10.	What is the purpose of API integration in crypto fraud monitoring?	2 Marks	L2	C04

Part B

Answer the Questions.

Total Marks 80M

11.	a.	<p>A global cryptocurrency exchange, CryptoTrust, has recently observed a surge in fraudulent transactions, including account takeovers, fake KYC profiles, and money-laundering attempts through rapid wallet-to-wallet transfers.</p> <p>The compliance team wants to integrate AI-driven fraud detection and improve its anti-fraud and AML/KYC mechanisms to meet international regulatory standards.</p> <p>As a blockchain forensics and AI analyst, you are assigned to design a fraud prevention strategy.</p> <p>(a) Explain how Artificial Intelligence can be used to detect fraud in crypto transactions.</p> <p>(b) Identify and describe three anti-fraud mechanisms that CryptoTrust can deploy to prevent future attacks.</p> <p>(c) The compliance team reports issues in verifying user identity during onboarding. Discuss the major AML/KYC challenges faced by exchanges and suggest how AI can help overcome them.</p> <p>(d) Design a high-level AI-based fraud detection framework integrating data sources, model components, and alerting systems for CryptoTrust. Illustrate the flow or explain step-by-step.</p>	20 Marks	L4	C01
Or					
12.	a.	Apply your understanding of block chain security to analyze different types of frauds in block chain networks and illustrate each with an appropriate use case.	20 Marks	L3	C01
13.	a.	Explain the role of unsupervised learning methods in data analysis.	10 Marks	L2	C02
	b.	Discuss the importance and challenges of using real-world block chain datasets.	10 Marks	L2	C02
Or					
14.	a.	Describe the workflow of an ML-based fraud detection system.	10 Marks	L2	C02
	b.	Describe the process of transaction feature engineering.	10 Marks	L2	C02
15.	a.	Evaluate the effectiveness of smart contract flow analysis techniques—Control Flow Graphs (CFG), data-flow analysis, and state-transition tracking—in detecting vulnerabilities, and justify which technique is most reliable for securing smart contracts.	20 Marks	L5	C03
Or					
16.	a.	Explain wallet profiling in block chain forensics.	10 Marks	L2	C03
	b.	Analyze the structure and working of honeypot smart contracts. Examine the detection methods and tools used to identify such attacks, and analyze a real-world honeypot case.	10 Marks	L4	C03
17.	a.	Explain the architecture of a real-time fraud detection and visualization system using big data analytics.	10 Marks	L2	C04

	b.	Explain the architecture of a stream analytics framework for fraud detection.	10 Marks	L2	CO4
Or					
18.	a.	Illustrate the key technical, architectural, and operational challenges in building scalable and accurate real-time fraud analytics systems. Apply appropriate examples, workflows, and diagrams to explain how these challenges influence detection accuracy, latency, and overall system performance.	20 Marks	L3	CO4