Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

End - Term Examinations – May/June 2026

Date: 18-05-2026 **Time:** 01:00pm – 04:00pm

School: SOCSE (Spl. Div)	**Program:** B. Tech-CSE(Blockchain)	
Course Code: CBC2504	**Course Name:** Blockchain Security and Performance	
Semester: VI	**Max Marks**: 100	**Weightage**: 50%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**25**	**25**	**25**	**25**	**-**

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.	State one reason why open participation makes Sybil resistance difficult in permissionless blockchains.	**2 Marks**	**L2**	**CO1**
2.	How can an Eclipse attack help an attacker attempt a payment fraud against a lightly connected client?	**2 Marks**	**L2**	**CO1**
3.	What is reentrancy? Name one standard defense used in Solidity.	**2 Marks**	**L2**	**CO2**
4.	Why is tx.origin unsafe for authorization?	**2 Marks**	**L2**	**CO2**
5.	Mention one limitation of relying only on automated smart contract auditing tools.	**2 Marks**	**L3**	**CO2**
6.	A blockchain confirms 900 transactions in 45 seconds. Compute throughput in tx/s.	**2 Marks**	**L3**	**CO3**
7.	Propagation delay is 6 seconds and block interval is 24 seconds. Compute the fraction of the interval consumed by propagation as a percentage.	**2 Marks**	**L3**	**CO3**
8.	A rollup batch costs 0.018 ETH and includes 1,500 transactions. Compute the cost per transaction in ETH.	**2 Marks**	**L3**	**CO4**
9.	A chain has 12 shards, each at 100 tx/s, with 15% coordination overhead. Compute net throughput.	**2 Marks**	**L3**	**CO4**
10.	An MPC protocol runs for 4 rounds with 6 parties, where each unordered pair exchanges 2 messages per round. Compute the total number of messages.	**2 Marks**	**L3**	**CO4**

Part B

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

11.	**a.**	Explain why blockchain threat models must include peer manipulation, consensus abuse, and delayed network visibility.	**6 Marks**	**L2**	**CO1**
	b.	A peer list contains 120 identities, of which 36 are fake Sybil identities. If a wallet selects 5 peers uniformly at random, compute the expected number of Sybil peers selected.	**6 Marks**	**L3**	**CO1**
	c.	Analyse how resource-based admission such as PoW or PoS changes attacker cost compared with simple identity-based participation.	**8 Marks**	**L4**	**CO1**
		Or			
12.	**a.**	Explain how consensus vulnerabilities, delayed propagation, and confirmation policy together influence payment security.	**6 Marks**	**L2**	**CO1**
	b.	A merchant waits for 3 confirmations. If each block takes 12 minutes on average and the merchant experiences an extra 4-minute observation delay per confirmation, compute the apparent waiting time.	**6 Marks**	**L3**	**CO1**
	c.	Discuss whether longer confirmation depth always solves double-spending risk, especially under majority control or peer isolation.	**8 Marks**	**L4**	**CO1**

13.	**a.**	Explain the role of fallback or receive functions in classical reentrancy exploits.	**6 Marks**	**L2**	**CO2**
	b.	A vulnerable contract holds 30 ETH. An attacker has a recorded balance of 5 ETH and successfully reenters 2 extra times before the balance is cleared. Compute the total Ether withdrawn.	**6 Marks**	**L3**	**CO2**
	c.	Design a safer withdrawal mechanism using pull payments and explain why exploit depth no longer determines losses.	**8 Marks**	**L4**	**CO2**
		Or			
14.	**a.**	Explain transaction-order dependence and arithmetic wraparound, and connect them to incorrect financial outcomes in Ethereum contracts.	**6 Marks**	**L2**	**CO2**
	b.	A uint16 balance is 2. Without checks, 9 tokens are deducted. Compute the stored balance. Then a copied transaction raises gas from 25 gwei to 37 gwei. Identify who gets mined first if miners prefer higher gas price.	**6 Marks**	**L3**	**CO2**
	c.	Recommend contract-level design practices and audit steps that specifically target transaction-order dependence and arithmetic faults.	**8 Marks**	**L4**	**CO2**

15.	**a.**	A blockchain processes 1,440 transactions in 96 seconds. Compute throughput in tx/s.	**6 Marks**	**L3**	**CO3**
	b.	Latency samples are 9 s, 11 s, 15 s, 17 s, 18 s, and 20 s. Compute the average latency.	**6 Marks**	**L3**	**CO3**

	c.	If stale losses reduce nominal throughput by 8%, compute the effective throughput for a chain whose nominal throughput is 25 tx/s.	**8 Marks**	**L4**	**CO3**
		Or			
16.	**a.**	A block size is 3 MB and the average transaction size is 600 bytes. Estimate the maximum number of transactions per block.	**6 Marks**	**L3**	**CO3**
	b.	In 2 hours, ideal production at 15 seconds per block is 480 blocks. If only 450 appear on the canonical chain, compute the chain growth shortfall in blocks.	**6 Marks**	**L3**	**CO3**
	c.	Out of 500 discovered blocks, 35 become stale. Compute the stale rate and canonical chain quality.	**8 Marks**	**L4**	**CO3**

17.	**a.**	A rollup posts 2,400 transactions to Layer 1 at a total cost of 0.0216 ETH. Compute the fee per transaction in ETH.	**6 Marks**	**L3**	**CO4**
	b.	A sharded system has 6 shards at 210 tx/s each. If 12% of theoretical capacity is lost to coordination, compute net throughput.	**6 Marks**	**L3**	**CO4**
	c.	A cross-shard payment visits 4 shards. Each shard adds 3 seconds of verification delay and routing overhead adds 8 seconds. Compute the total delay.	**8 Marks**	**L4**	**CO4**
		Or			
18.	**a.**	In a DAG ledger, 96 blocks are issued in 8 minutes. If 18% are discarded during final ordering, compute the number of accepted blocks.	**6 Marks**	**L3**	**CO4**
	b.	A verifier checks 250 zero-knowledge proofs, each taking 32 ms. Compute the total verification time in seconds.	**6 Marks**	**L3**	**CO4**
	c.	A privacy pool has 1,200 deposits and analytics reduce the candidate set to 75. Compute the percentage reduction in anonymity set.	**8 Marks**	**L4**	**CO4**