Roll No.												

PRESIDENCY UNIVERSITY

BENGALURU

Mid - Term Examinations – MARCH 2026

Date: 10 – 03- 2026 **Time:** 02:00pm – 03:30pm

School : SOCSE	**Program:** B. Tech- Blockchain	
Course Code: CBC2504	**Course Name:** Blockchain Security & Performance	
Semester: VI	**Max Marks**: 50	**Weightage**: 25%

CO - Levels	**CO1**	**CO2**	**CO3**	**CO4**	**CO5**
Marks	**60**	**40**	**--**	**--**	**--**

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. **5Q x 2M=10M**

1	Define probabilistic finality in PoW using the idea of confirmations.	**2 Marks**	**L2**	**CO1**
2	Differentiate a Race attack and a Finney attack.	**2 Marks**	**L2**	**CO1**
3	State the three EVM data locations (stack, memory, storage) and identify which one persists across transactions.	**2 Marks**	**L2**	**CO2**
4	Explain how mining pool concentration can enable censorship/MEV via block-template control.	**2 Marks**	**L2**	**CO1**
5	Explain why tx.origin auth is unsafe.	**2 Marks**	**L2**	**CO2**

Part B

Answer the Questions. **Total Marks 40M**

6.	**a.**	Define a mining pool and a share.	**2 Marks**	**L2**	**CO1**
	b.	Differentiate PPS vs PPLNS payout schemes.	**4 Marks**	**L2**	**CO1**
	c.	Explain why the pool operator matters for security.	**4 Marks**	**L2**	**CO1**
		Or			
7.	**a.**	Describe the selfish-mining strategy.	**4 Marks**	**L2**	**CO1**
	b.	Explain why network propagation advantage (γ) affects when it becomes profitable.	**3 Marks**	**L2**	**CO1**
	c.	List three mitigations (protocol/network/ecosystem) and explain each one of them.	**3 Marks**	**L2**	**CO1**

8.	**a.**	Define a Sybil attack.	**4 Marks**	**L2**	**CO1**
	b.	List three defense families.	**4 Marks**	**L2**	**CO1**
	c.	Explain one limitation for any two defense families.	**2 Marks**	**L2**	**CO1**
		Or			
9.	**a.**	Define an eclipse attack.	**2 Marks**	**L2**	**CO1**
	b.	Describe address-table poisoning and connection monopolization	**4 Marks**	**L2**	**CO1**
	c.	List two best practices for arithmetic-heavy logic.	**4 Marks**	**L2**	**CO1**

10.	**a.**	Define reentrancy in EVM context.	**2 Marks**	**L2**	**CO2**
	b.	Explain what unchecked {} does and why it is risky.	**4 Marks**	**L2**	**CO2**
	c.	Describe the correct CEI-ordered withdraw flow in bullet steps.	**4 Marks**	**L2**	**CO2**
		Or			
11.	**a.**	Explain what delegate call implies about storage in a proxy.	**2 Marks**	**L2**	**CO2**
	b.	List two proxy failure modes and explain each briefly.	**3 Marks**	**L2**	**CO2**
	c.	Describe a sandwich attack in three steps.	**3 Marks**	**L2**	**CO2**
	d.	Describe why time locks + a separate pause guardian reduce risk.	**2 Marks**	**L2**	**CO2**

12.	**a.**	Explain why block timestamp and block hash are weak randomness sources.	**4 Marks**	**L2**	**CO2**
	b.	Differentiate property-based fuzzing vs invariant fuzzing.	**3 Marks**	**L2**	**CO2**
	c.	Explain why shrinking/minimization is important.	**3 Marks**	**L2**	**CO2**
Or					
13.	**a.**	Explain “nothing-at-stake”.	**3 Marks**	**L2**	**CO1**
	b.	Describe a short-range attack.	**4 Marks**	**L2**	**CO1**
	c.	List three vault invariants and describe each in one line.	**3 Marks**	**L2**	**CO1**