


Name:			
Enrolment No:			
<div><div>UPES</div><div>End Semester Examination, May 2025</div><div><div>Course: Industry Use Cases using Blockchain</div><div>Program: BT-CSE-VIII-I-MINOR</div><div>Course Code: CSBL4004P</div></div><div><div>Semester : VIII</div><div>Time : 03 hrs.</div><div>Max. Marks: 100</div></div></div>			
Instructions: Please attempt according to the time provided and given weightage. All questions are compulsory			
SECTION A (5Qx4M=20Marks)			
S. No.		Marks	CO
Q 1	Outline the potential benefits of using blockchain for digital identity management in government services.	4	CO3
Q 2	Briefly describe the role of the Cryptography layer in the Blockchain architecture. What specific cryptographic techniques are crucial for its security?	4	CO4
Q 3	Define a smart contract. How does it differ from traditional digital contracts in terms of reliability and enforcement?	4	CO1
Q 4	Outline the steps involved in the process of generating a public key and an Ethereum address from a private key. What cryptographic algorithm is used in this process?	4	CO3
Q 5	Explain the functionality of "software oracles." What is a potential challenge associated with relying solely on software oracles for data, and how can this challenge be mitigated?	4	CO1
SECTION B (4Qx10M= 40 Marks)			
Q 6	Consider a scenario where a smart contract on one blockchain needs to trigger a physical action by a device connected to a different blockchain. Discuss whether an "outbound oracle" is strictly necessary in this case. What role could an oracle play in ensuring the security and reliability of such cross-chain interactions involving physical devices or legacy systems?	2+3+5	CO4
Q 7	Describe the "Ricardian Contract Bowtie Model" by explaining how does a Ricardian contract aim to bridge the gap between legal language and computer-executable code? What are the types of semantics associated with a legal contract, and how does a Ricardian contract address them?	5+5	CO1
Q 8	Describe the "point doubling" operation on an elliptic curve. How does it differ geometrically from point addition? Provide a conceptual diagram to illustrate this operation.	10	CO3

Q 9	Elaborate on the working mechanism of an oracle in providing external data to a smart contract. Detail the steps involved, from the smart contract's request to the delivery of verified data, including the role of data sources and cryptographic proofs.	10	CO2
SECTION-C (2Qx20M=40 Marks)			
Q 10	a) Explain the characteristics of "Non-Fungible Tokens" (NFTs). How do they differ from fungible tokens? List and briefly describe the key characteristics of NFTs, providing an example to illustrate each characteristic. b) What are "stable tokens"? Explain their primary purpose and how they aim to achieve price stability. Describe the common mechanisms used to maintain the peg of stable tokens to traditional assets, providing examples of well-known stable tokens.	10+10	CO4
Q 11	Evaluate the security considerations for implementing blockchain solutions in various industries, focusing on privacy, access control, and smart contract vulnerabilities. Propose a comprehensive security framework for deploying blockchain applications in a sensitive sector like healthcare.	20	CO4