

**SECTION-A (10 Marks)**

Answer ALL questions

ALL questions carry EQUAL marks

(10 × 1 = 10)

| Module No. | Question No. | Question                                                                                                                                                                                                                                                                | K Level | CO  |
|------------|--------------|-------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----|
| 1          | 1            | A binary tree with hash pointers is known as a -----<br>a) B-Tree      b) B+ Tree      c) Merkle tree      d) Hash Tree                                                                                                                                                 | K1      | CO1 |
|            | 2            | Bitcoin uses a particular digital signature scheme called -----<br>a) Elliptic Curve Digital Signature Algorithm      b) RSA<br>c) DES      d) AES                                                                                                                      | K2      | CO1 |
| 2          | 3            | Select the online wallet service.<br>a) Coinbase      b) Bitcoin      c) Ethereum      d) Sybil                                                                                                                                                                         | K1      | CO2 |
|            | 4            | Select the decentralized system based on an open standard.<br>a) Indian Railways      b) Email<br>c) Airline Reservation      d) Bus Reservation                                                                                                                        | K2      | CO2 |
| 3          | 5            | ----- introduces new features in the bitcoin protocol that were previously considered invalid.<br>a) Soft Fork      b) Mutable Fork<br>c) Hard Fork      d) Immutable Fork                                                                                              | K1      | CO3 |
|            | 6            | ----- states that any non-reversible computation must use a minimum amount of energy<br>a) Landauer's principle      b) Mining Principle<br>c) Greham's Principle      d) Stefan's Principle                                                                            | K2      | CO3 |
| 4          | 7            | ----- means that if a user interacts with the system repeatedly, these different interactions should not be able to be tied to each other from the point of view of the adversary in consideration<br>a) Anonymity      b) unlinkability<br>c) Closure      d) Identity | K1      | CO4 |
|            | 8            | ZeroCash uses a cryptographic technique called -----<br>a) SHARKS      b) zk-SNARKS<br>c) Merkle Tree      d) SHA-256                                                                                                                                                   | K2      | CO4 |
| 5          | 9            | ----- is a specific effort by a specific state to introduce specific regulation of Bitcoin<br>a) New York State's BitLicense proposal<br>b) Tamilnadu's Cryptocurrency Proposal<br>c) California's Ethereum Proposal<br>d) Boston's Cryptocurrency Standard             | K1      | CO5 |
|            | 10           | A ----- is a data structure to which we can write new data, and that which once we've written data, is tamper-proof and available forever<br>a) Lottery      b) Append Only Log<br>c) Contract      d) Merkle Tree                                                      | K2      | CO5 |

Cont...

**SECTION - B (35 Marks)**

Answer ALL questions

ALL questions carry EQUAL Marks

(5 × 7 = 35)

| Module No. | Question No. | Question                                                                                                                                                | K Level | CO  |
|------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----|
| 1          | 11.a.        | Examine the use of Public keys as identities.                                                                                                           | K4      | CO1 |
|            |              | (OR)                                                                                                                                                    |         |     |
|            | 11.b.        | Analyze about Hash pointers and data structures.                                                                                                        |         |     |
| 2          | 12.a.        | Test for the soundness of the statement: "Bitcoin's decentralization is partly a technical mechanism and partly clever incentive engineering". Explain. | K4      | CO2 |
|            |              | (OR)                                                                                                                                                    |         |     |
|            | 12.b.        | Compare Hot and Cold storage.                                                                                                                           |         |     |
| 3          | 13.a.        | Explain the various Mining Strategies of Bit coin.                                                                                                      | K5      | CO3 |
|            |              | (OR)                                                                                                                                                    |         |     |
|            | 13.b.        | Interpret the various Applications of bitcoin Scripts.                                                                                                  |         |     |
| 4          | 14.a.        | Explain Decentralized Mixing.                                                                                                                           | K2      | CO4 |
|            |              | (OR)                                                                                                                                                    |         |     |
|            | 14.b.        | Explain the Basics of Anonymity.                                                                                                                        |         |     |
| 5          | 15.a.        | Identify the Anti Money Laundering (AML) rules that governments have imposed, especially in the US, that affect some Bitcoin-related businesses.        | K3      | CO5 |
|            |              | (OR)                                                                                                                                                    |         |     |
|            | 15.b.        | Identify the use of Bitcoin as public randomness source.                                                                                                |         |     |

**SECTION -C (30 Marks)**

Answer ANY THREE questions

ALL questions carry EQUAL Marks

(3 × 10 = 30)

| Module No. | Question No. | Question                                                                                                                                                | K Level | CO  |
|------------|--------------|---------------------------------------------------------------------------------------------------------------------------------------------------------|---------|-----|
| 1          | 16           | Explain the role of Digital Signatures.                                                                                                                 | K2      | CO1 |
| 2          | 17           | Examine the validity of the statement: "The key technical problem to solve in building a distributed e-cash system is achieving distributed consensus". | K4      | CO2 |
| 3          | 18           | Assess the energy usage of bitcoin and analyze its implications for both the currency and our planet.                                                   | K5      | CO3 |
| 4          | 19           | Analyze the statement: "ZeroCoin incorporates Anonymity at the protocol level".                                                                         | K4      | CO4 |
| 5          | 20           | Explain about the Roots of bitcoin.                                                                                                                     | K5      | CO5 |

Z-Z-Z END