Code : 100816

B.Tech 8th Semester Exam., 2022

(New Course)

BITCOIN AND CRYPTOCURRENCIES

Time : 3 hours *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

*(iv) Question No. **1** is compulsory.*

1. Choose the correct answer (any *seven*) : 2×7=14

(a) Encryption is

(i) putting data into code making it difficult to read or understand

(ii) jumbling data

(iii) a formal language

(iv) a secret way of writing programs

(b) ____ is not a property of hash function.

(i) Pre-image resistance

(ii) Compression

(iii) Fixed length output

(iv) None of the above

(c) ____ is a principle of data security.

(i) Confidentiality

(ii) Masquerading

(iii) Confusion

(iv) Diffusion

(d) Bitcoin is created by

(i) Saifedean Ammous

(ii) Satoshi Nakamoto

(iii) Vitalik Buterin

(iv) None of them

(e) The value of 3^{51} mod 5 is

(i) 1

(ii) 2

(iii) 3

(iv) 4

(f) A node in blockchain environment is

(i) a type of cryptocurrency

(ii) a blockchain

[✓ *(iii)* a computer on a blockchain network]

(iv) an exchange

(g) _____ is used to store cryptocurrency.

(i) Bank account

(ii) Floppy disk

(iii) Single central account

[✓ *(iv)* Wallet]

(h) A computer program that validates and process blockchain transaction is

(i) an adder

[✓ *(ii)* a miner]

(iii) a mixer

(iv) a manager

(i) A hot wallet is connected to Internet.

[✓ *(i)* True]

(ii) False

(iii) Depends on connectivity

(iv) Internet is not an issue for using wallet

(Turn Over)

(j) Hash functions are used in

(i) cryptocurrency

(ii) blockchain

(iii) cryptography

[✓ *(iv)* All of the above]

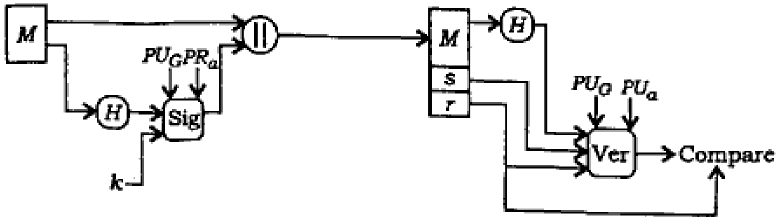
2. *(a)* Define encryption. Explain how encryption provides confidentiality. 7

(b) Differentiate between plaintext, cleartext and ciphertext with diagrams. 7

3. What do you mean by hashing? With the help of a neat diagram, explain SHA-256 algorithm. 14

4. Explain a bitcoin transaction with the help of a flowchart. 14

5. Explain the concept of signature shown in the following figure while providing the information about *M*, *H*, *k*, *Sig*, PU_G, PR_a, *s*, *r* : 14



(Continued)

6. Cryptocurrency transactions are recorded on a blockchain, which is generally public. At the same time, crypto trades are not necessarily linked to an identity, which provides a bit of anonymity for users.

   (a) What do you mean by anonymity or pseudo-anonymity? 7

   (b) Explain, with diagrams, how bitcoin enforces anonymity simultaneously with tracing feature. 7

7. *(a)* Define the role of Merkle tree in blockchain. 7

   (b) Explain, how a blockchain ledger works. 7

8. "Zerocoin is a blockchain and cryptocurrency privacy protocol made to address the lack of privacy features of bitcoin." In the context of the zerocoin, answer the following questions :

   (a) Explain how zerocoin ensures privacy. 7

   (b) Explain zerocash as an extension to zerocoin. 7

9. Write short notes on the following : 3½×4=14

   (a) Proof of work

   (b) Proof of stake

   (c) Mining incentive

   (d) Elliptic curve

★★★