VIT | Vidyalankar Institute of Technology
(Accredited A+ by NAAC)
(Autonomous Institute Affiliated to University of Mumbai)

Mid Semester Examination

Branch	Test Date	Semester	Div.	Roll No.	Student's Signature
CMPN.		VII	A and B	—	

Test No.	Subject
	Blockchain (Faculty MSE Solution)

Junior Supervisor's full signature with date :

Question No.	1	2	3	4	5	Total 30 / 40 / 50	Examiners Signature	Student's Sign After receiving the assessed answer sheet
Marks obtained								

Q. 1.

a. Blockchain.

Blockchain is defined as a distributed, replicated and peer-to-peer network of databases that allow multiple non-trusting parties to transact without a trusted intermediary & maintains an ever-growing, append-only, tamper-resistant list of time sequenced records.

b. Components of Blockchain

Node
Ledger
Wallet
Nonce
Hash.
Mining
Consensus protocol.

c. Challenges :-

1. Traditional db may be more suited to work faster & cheaper.
2. Stronger player can control the network
3. Significant computing power is required by miners
4. Risk of 51% attack.

d: Double spending problem

Double spending is spending the money more than once. Just as one can copy a digital file and send it to several people, it is possible to duplicate cryptocoin or token and reuse it.

e: Mining difficulty

It refers to the difficulty of solving the math puzzle and generating bitcoin.

The formula is,

Difficulty level = Difficulty Target / Current target

It influences the rate at which bitcoins are generated.

f: Altcoins

The cryptocurrency alternatives to the bitcoin are referred as 'Alternative Cryptocurrency Coin'. They come from a list of famous and durable cryptocurrencies like bitcoin, litecoin & ethereum.

g: Types of Cryptocurrency tokens:

1. Utility Tokens

Provide users with access to a product or a service.

2. Security Tokens

Represents equity in the company that issues the tokens.

h: Mining pool:

To counteract the huge time and energy consumption involved in transaction validation, some miners group together in mining pools to combine their mining resources for more efficiency & savings.

Q 2.

a. Different types of blockchain

	Public Blockchain	Private Blockchain	Consortium blockchain
Users.	Anonymous.	Known & trusted.	Known & trusted
Access.	Open	Fully restricted.	Selectively open.
N/w Type.	Decentralized.	Centralized.	Partially decentralized.
Operations.	Anyone can read, write & initiate	Pre-approved participants can read, initiate	Pre-approved participants can read, initiate.
Verification.	Anyone can take part in consensus.	Single validator.	Only privileged nodes.
Security:	Hashing	Distributed consensus	Distributed consensus.

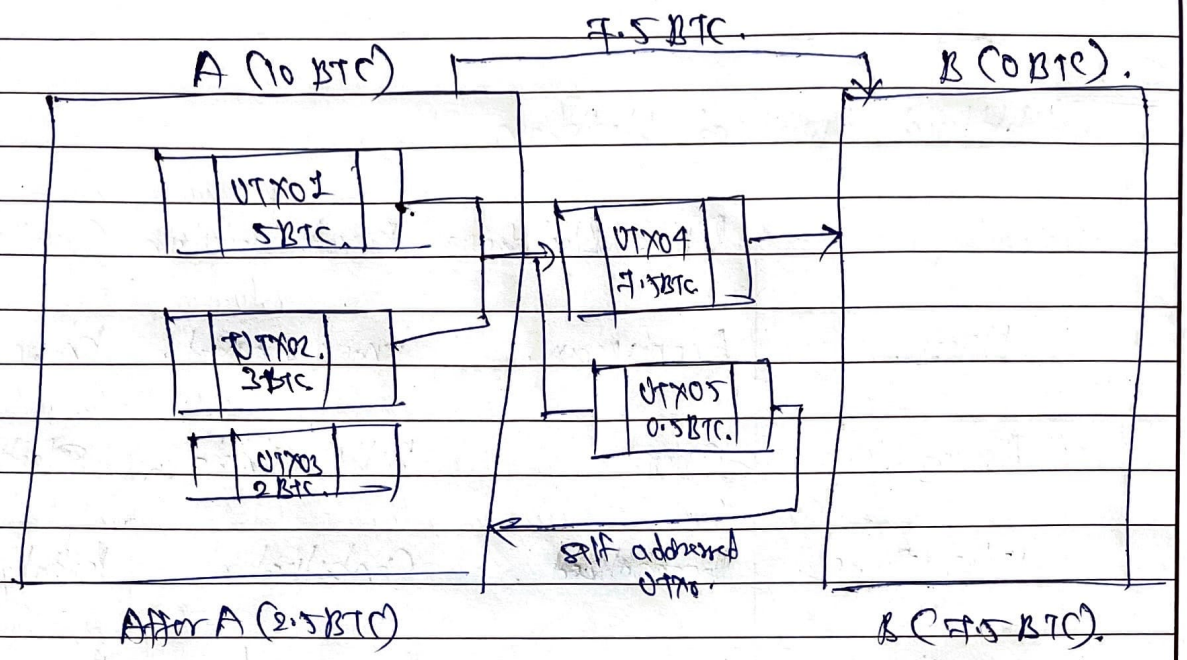
b. UTXO Model of bitcoin

An unspent transaction output (UTXO) is the technical term for the amount of digital currency that remains after a cryptocurrency transaction.

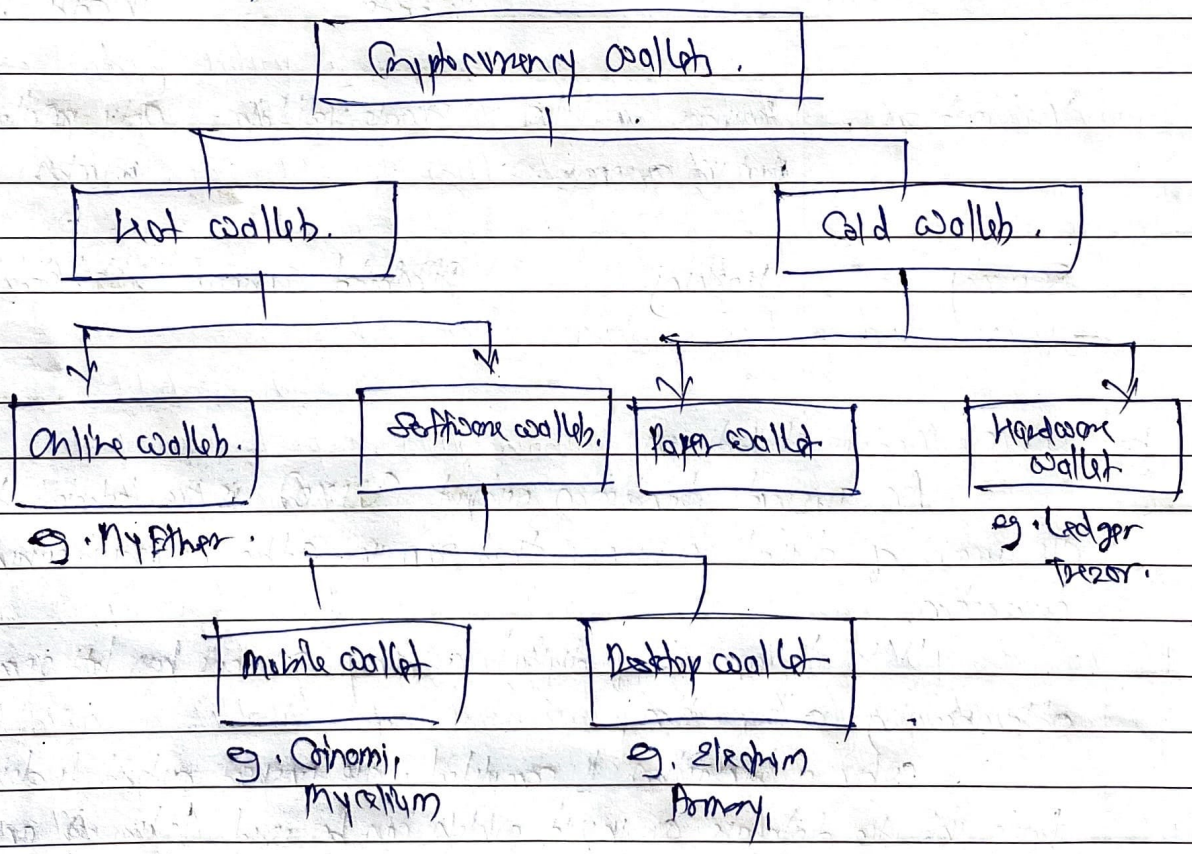
It is the amount of digital currency someone has left remaining after executing a transaction.

When a transaction is completed, the unspent output is deposited back into the database as input which can be used later for another transaction.

UTXOs are created through the consumption of existing UTXOs. Every bitcoin transaction is composed of inputs & outputs. Inputs consume an existing UTXO, while outputs create a new UTXO.



Q: Cryptocurrency wallets.



Hot wallet.

It is designed for online day-to-day transactions. It is connected to internet at all times.

Cold wallet

It is digital wallet that is not connected to the internet. Being offline they are more secure & used for long term storage of cryptocurrencies.

Q. 5.

a) Different types of consensus algorithms.

1. Proof-of-work.

The algorithm is used to confirm the transaction & creates a new block to the chain. In this algorithm, miners compete against each other to complete the transaction on the network.

2. Proof-of-elapsed time.

PoET follows a lottery system that spreads the chances of winning equally among participants, giving every node the same chance. It generates a random wait time for each node in the blockchain network. Each node must sleep for that duration.

3. Proof-of-stake

This selection algorithm of validators or forgers combines the quantity of stake (amount of cryptocurrency) with other factors. (like coin-age based selection, randomization process) to make the selection fair to everyone on the network.

4. Delegated Proof-of-stake

Just as in PoS, the delegates are responsible for validating transactions and maintaining the blockchain ledger. These elected delegates are called witnesses. The more the crypto-coins or tokens, the more the voting power.

5. Proof-of-Authority

These process is automated and does not require validators to continuous monitoring from computers. They own software allowing them to put transactions in block.

b. Bitcoin mining terminologies.

1. Block frequency
Bitcoin transactions are being registered into blockchain once in 10 minutes.

2. Industrial mining.
Some nodes, which do industrial-grade mining & connect to a massive set of computers & use complicated algo.

3. Mining pool
Some miners group together in mining pools to combine their mining resources for some efficiency & savings.

4. Halving policy.
The reward will be reduced to half for every four years. At last, in 2140 it will decrease to zero.

5. Block
Each block has 3 necessary informations namely -
Block header.
Hash of prev. block header
Merkle root

6. Orphaned block.
They are not part of main chain. They occur naturally when 2 different miners successfully mine at the same time.

7. Mempool
Mempool is the staging area for the transactions. A mempool can take around 10000 transactions at a time.

8. Block Propagation.

When a miner announces a block, the block needs to propagate to all the nodes in the n/w, using gossip protocol.

9. SEGWIT.

In the bitcoin, the segregation of the signature from the block is called as Segregated witness (SegWit). SegWit will be send separately in the n/w.

10. Nonce.

Nonce is a number that can be used just once in the cryptographic communication.