

Branch	Test Date	Semester	Div.	Roll No.	Student's Signature
CmpN.	10/10/2023	VII	A - 96B	10160100000000000000	

IA Test No.	Subject
02.	BLOCKCHAIN Faculty Solution.

Junior Supervisor's full signature with date :	Question No.	1	2	3	Total 20	Examiners Signature	Student's Sign After receiving the assessed answer sheet
03/05/2023	Marks obtained						

<u>Q1:</u>	<p>a. <u>1. Application Layer:</u> - Holds decentralized applications and user interface.</p> <p>b. <u>2. Smart contract Layer:</u> Contains the logic and code for executing contracts.</p> <p>c. <u>3. VM:</u> Executes smart contracts in a secured environment.</p> <p>d. <u>4. Consensus Layer:</u> Uses Proof of Stake to validate Tx and add blocks.</p> <p>e. <u>5. Network Layer:</u> Connects Ethereum nodes via P2P communication.</p> <p>f. <u>6. Data Layer:</u> Stores all BC data, including transaction & states.</p>
------------	---

↳ Architecture Components of hyperledger fabric :-
↳ Peer :-

Nodes that host ledgers and smart contracts.

↳ Orderer :-

Manages Tx order and delivers Tx batches to peers.

↳ Channel :-

Private subset for communication among specific node members.

↳ Ledger :-

Immutable record of all Tx within a channel.

↳ Chaincode :-

Smart contracts that define business logic.

↳ MSP :-

Manages identities and permissions of participants.

↳ Endorsement policy :-

Defines which peer signatures are required to validate a Tx.

↳ Fabric CA :-

Issues and manages certificates for identity verification.

↳ Bitcoin v/s Ethereum BC :-

Bitcoin.

Ethereum.

Tx mediation : Uses native Tx by specifying inputs & outputs. Include executing smart contracts or burnishing ethry.

Broadcasting

Tx broadcast to the network and propagated to all nodes.

Tx broadcast to the network & propagated to all nodes.

Validation: Miner validate Tx by validating or mining
PoW validate Tx by PoS.

Block creation: Valid Tx going into a block.
Valid Tx added in a block.

Confirmation: Tx is confirmed after included in a block.
Tx is confirmed after inclusion in a block.

Q.2.

gas ether (ETH).

- The native cryptocurrency of Ethereum (ether).
- Used to pay the Tx fees, computational services and incentivizing miners.

Smart Contracts:

- self-executing contracts with the terms of the agreement directly written into code.
- Automate and enforce the execution of contract terms without intermediaries.

3. EVM:

- A decentralized computing engine that executes smart contracts
- provide a runtime environment for smart contracts, letting them execute as intended across all nodes.

4. Nodes:

- Maintain the BC ledger, validate Tx, execute smart contracts and propagate data across the network.

5. Gas:

- Defining Tx fees and prevent abuse by requiring users to pay for each operation performed.

	Public BC.	Private BC.
Accessibility	Open to anyone	Restricted access -
Control	Decentralized	Centralized
Consensus	Proof of PoS.	PBFT or RAFT.
Speed	Slower.	Faster.
Transparency	Fully transparent	Limited transparency

Typical Use cases of private BC!

- Supply chain management
- Finance and Banking
- Healthcare
- Corporate Governance
- Real Estate

C. BFT.

- Ensures consensus in the system with some faulty or malicious nodes.
- Derived from the Byzantine Generals problem.

Implementation in Private BC:

I. PBFT

- Nodes agree on Tx via message exchange.
- Tolerate up to $\left(\frac{n-1}{3}\right)$ faulty nodes.

II. Hyperledger Fabric

- Uses PBFT-like consensus.
- Order, Endorsing peers and committing peers manage Tx flow.

3. Quantum

- Enterprise BC with PBFT - Replicated currency.
- Suitable for financial services needing secure, permissioned solutions.

Q. 3.

a. DeFi

- DeFi refers to a system of financial applications built on BC technology particularly Ethereum that operate without intermediaries like banks or brokers.
- Include decentralized exchanges, lending platforms, stablecoins and smart contracts.

Potential Impact on Traditional Financial Systems -

1. Disintermediation:

- Eliminates the need for traditional financial intermediaries, reducing costs and increasing efficiency.

2. Increased Accessibility

- Provides financial services to unbanked and underbanked populations globally.

3. Transparency

- Enhances transparency through public, immutable BC records.

4. Innovation

- Accelerates financial innovation by allowing anyone to create and deploy financial applications.

Advantages of DeFi

- 1. Lower costs: Reduces fees by removing intermediaries.
- 2. Accessibility: Provides financial services to anyone with internet access.

3. Transparency: offers clear & immutable tx records.

4. Control: gives users full control over their assets.

5. Interoperability: enables integration & interaction between different DLT applications.

b. Key characteristics of private BCs:

1. Controlled access:

- Only authorized participants can join and interact with the network.
- Ensures data privacy & compliance with regulatory requirements.

2. Enhanced privacy & data security:

- Transactions and data are visible only to authorized participants.
- Protects sensitive business information & maintains confidentiality.

3. High Performance:

- Optimized for fast tx processing and higher throughput.
- Suitable for high-volume and low-latency business operations.

4. Efficient consensus mechanism:

- Utilizes less resource-intensive consensus algorithms like PBFT or Raft.
- Reduces energy consumption &提高
increases efficiency.

5 Scalability:

- Can be scaled according to the needs of the enterprise.
- Supports the growth of business operations without compromising performance.

- Private BC controlled access, enhanced privacy, high performance, efficient consensus mechanism, strong governance, scalability, customization and regulatory compliance make them highly suitable for enterprise applications, existing supply chain and tailored solutions for business environments.