# BLOCK CHAIN TECHNOLOGY

## PROFESSIONAL ELECTIVE

## SEMESTER – FIFTH

***These important questions have been prepared using your previous exam papers (PYQs), verified concepts, and additional reference from trusted online academic sources.***
***For deeper understanding, please refer to your class notes as well.***



---

## 1️⃣ HIGH & LONG IMPORTANT QUESTIONS

These questions are structured for maximum weightage (Long Answer Type).

### Unit I & II: Fundamentals, Architecture & Consensus

1. Explain the evolution of digital money to **distributed ledgers** and describe the **Blockchain Architecture and Design** in detail. Include a discussion on its key **Design Primitives** (Protocols, Security, Permissions).

2. What is a **Hash Chain**? Explain how a **Hash Chain** leads to the formation of a **Block Chain**. Describe the function of the basic **crypto primitives: Hash and Digital Signature** in securing the Block Chain.
3. Define **Consensus Mechanism**. Elaborate on the working principle of **Proof of Work (PoW)** and discuss its key **requirements** and **scalability aspects** in Block Chain consensus protocols.

### Unit II & III: Permissioned Blockchains & Hyperledger Fabric

4. Differentiate between **Permissioned** and **Permissionless** Block Chains. Explain the **Design Goals** and the specific **Consensus Protocols** used for **Permissioned Block Chains**.
5. Explain the complete process of **Decomposing the Consensus Process** in a complex Block Chain system. Describe the key **components of Hyperledger Fabric** and their roles in achieving consensus.

6. What is **Chain Code** in Hyperledger Fabric? Explain the process of **Chain Code Design and Implementation**. Discuss the concept of **Hyperledger Fabric II** and its advancements.

**Unit IV & V: Applications & Security**

7. Elaborate on the various applications of **Block Chain in Financial Software and Systems (FSS)**. Discuss its specific roles in **Settlements, KYC (Know Your Customer), Capital Markets, and Insurance**.
8. Explain how Block Chain technology is transforming the **Trade/Supply Chain** sector. Detail its use cases for **Provenance of Goods, Visibility, Trade/Supply Chain Finance, and Invoice Management/Discounting**.
9. Discuss the critical role of **Block Chain for Government**. Detail its application in **Digital Identity, Land Records,** and managing **Public Distribution System / Social Welfare Systems**.
10. Describe the concepts of **Privacy and Security** on Block Chain. Explain the role of **Block Chain Cryptography** in maintaining the integrity and confidentiality of data within the ledger.

---

## 2️⃣ IMPORTANT & SHORT QUESTIONS (50–70% probability)

These questions are suitable for short descriptive or comparative answers.

1. **Differentiate** between **Block Chain** and **Distributed Ledger Technology (DLT)**.
2. Briefly explain the basic concept of **Digital Money** and how it is related to the need for distributed ledgers.
3. Define **Consensus** and **Privacy** as design primitives in Block Chain technology.
4. Write a short note on **Basic Consensus Mechanisms** (other than PoW) used in Block Chain.
5. What are the key **requirements** for a good consensus protocol?
6. Explain the problem of **Scalability** in Block Chain consensus protocols.
7. Define **Chain Code** (Smart Contracts) and state its primary functions in Hyperledger Fabric.

8. What is the significance of **KYC (Know Your Customer)** in the financial sector, and how does Block Chain help to improve it?
9. Explain the term **Provenance of Goods** in the context of a supply chain and Block Chain.
10. Briefly discuss the application of Block Chain in **Insurance**.

---

## 3️⃣ "AA BHI SAKTA HAI" QUESTIONS (20–30% probability)

These cover new, peripheral, or conceptual extension topics.

1. Describe the concept of **Permissions** in a Block Chain environment.
2. How does a **Digital Signature** ensure **non-repudiation** in a Block Chain transaction?
3. Briefly explain how Block Chain can be used for **Invoice Management/Discounting**.
4. Discuss the challenges faced by the government in **Record Keeping** and how Block Chain addresses them.
5. What is the **Double Spending** problem, and how does Block Chain solve it? (This is an indirect concept linked to digital money history).

**QUICK REVISE**

**UNIT I: Fundamentals & Design Primitives**

| Topic | Key Concepts |
|---|---|
| **History: Digital Money to DLT** | The evolution was driven by the need to solve the **Double Spending Problem** in digital cash, leading to decentralized systems (**Distributed Ledger Technology - DLT**). Blockchain is a specific type of DLT. |

| Topic | Key Concepts |
|---|---|
| **Design Primitives** | **Protocols:** Rules governing interaction. **Security:** Use of cryptography (Hashing/Signatures). **Consensus:** Agreement mechanism. **Permissions:** Who can participate (Permissioned vs. Permissionless). **Privacy:** Data visibility control. |
| **Blockchain Architecture** | A chain of **Blocks** connected by **Hashes**, secured cryptographically, and distributed across a peer-to-peer network. It is an **immutable** ledger. |

**Basic Crypto Primitives** Hash: A one-way function producing a fixed-size string (digest) from arbitrary data. Used for integrity. Signature: Verifies the authenticity and non-repudiation of a transaction/block.

**Hash Chain to Blockchain** Hash Chain (data > hash > next data > next hash) is the predecessor. Blockchain adds the concept of grouping transactions into a block, and each block header includes the hash of the previous block for linkage and tamper resistance.

**Basic Consensus** Mechanisms (like PoW, PoS) used to achieve agreement among distributed nodes on the validity of new transactions/blocks.

---

**UNIT II: Consensus Protocols & Permissioned Blockchains**

| Topic | Key Concepts |
|---|---|
| **Requirements for Consensus** | **Agreement:** All honest nodes agree on the same history. **Validity:** Only valid transactions are included. **Termination:** The process eventually stops and a decision is reached. **Fault Tolerance:** Ability to continue despite node failures. |

| Topic | Key Concepts |
|---|---|
| **Proof of Work (PoW)** | Requires miners to expend computational effort (solving a cryptographic puzzle) to propose the next block. It is resource-intensive but highly secure and decentralized (e.g., Bitcoin). |
| **Scalability Aspects** | PoW chains often have low throughput (slow transaction rate) and high latency due to block time and confirmation requirements. This is a major challenge for mass adoption. |
| **Permissioned Blockchains** | Networks where participants are known and authorized (e.g., Hyperledger Fabric). Access control mechanisms are built-in. |
| **Design Goals of Permissioned Chains** | High **Performance** (fast transactions), **Scalability**, **Identity Management**, and **Confidentiality** (data privacy between authorized parties). |
| **Consensus for Permissioned Chains** | Often use faster, deterministic algorithms like **PBFT (Practical Byzantine Fault Tolerance)** or **RAFT**, as they don't need to prevent unknown attackers. |

---

**UNIT III: Hyperledger Fabric**

| Topic | Key Concepts |
|---|---|
| **Decomposing Consensus** | Fabric separates the transaction workflow into three phases: **Endorsement** (simulating transaction and signing), **Ordering** (achieving agreement on transaction sequence), and **Validation/Commit** (checking policy and updating the ledger). |
| **Hyperledger Fabric Components** | **Peers** (maintain ledger and execute chaincode), **Ordering Service** (sequences transactions), **Certificate Authority (CA)** (manages identities), **Clients** (submit transactions). |

| Topic | Key Concepts |
|---|---|
| **Chain Code (Smart Contracts)** | Code that defines the assets and transaction logic. It is executed by the endorsing peers and governs interactions with the ledger state. |
| **Chain Code Design & Impl.** | Focuses on defining the asset structure, access control rules, and the functions (e.g., *createAsset*, *transferAsset*) that modify the ledger state. |
| **Hyperledger Fabric II** | Focuses on enhancements like Fabric Private Chaincode (FPC) and improved operational security/usability. |

---

**UNIT IV: Applications in FSS & Trade/Supply Chain**

| Topic | Key Concepts |
|---|---|
| **FSS: Settlements** | Faster and cheaper **cross-border payments** and interbank settlements by removing intermediaries. |
| **FSS: KYC** | Shared, verified digital identity record among financial institutions, reducing redundant background checks and costs. |
| **FSS: Capital Markets** | Streamlining trade processing, record-keeping, and security issuance (tokenization). |
| **FSS: Insurance** | Automating claims processing via **Smart Contracts**, combating fraud, and improving policy management. |
| **Trade/Supply Chain: Provenance** | Creating an immutable record of ownership and handling (the origin and journey of goods) to verify authenticity and track quality. |
| **Trade/Supply Chain: Visibility** | Real-time tracking of goods across multiple organizations, improving transparency and efficiency. |

| Topic | Key Concepts |
|---|---|
| **Trade/Supply Chain Finance** | Automating the financing process (e.g., letter of credit, invoice discounting) based on verified data on the chain. |

---

**UNIT V: Government & Cryptography**

| Topic | Key Concepts |
|---|---|
| **Govt: Digital Identity** | Creating tamper-proof, self-sovereign digital IDs controlled by the individual, simplifying access to services. |
| **Govt: Land Records** | Replacing paper-based, fraud-prone records with a secure, transparent, and immutable ledger of ownership. |
| **Govt: Public Distribution System (PDS)** | Tracking the flow of goods and funds to reduce leakage, improve transparency, and ensure subsidies reach the intended beneficiaries. |
| **Govt: Record Keeping** | Secure, auditable storage for inter-government entity data sharing and archival. |
| **Blockchain Cryptography** | Relies on **Hashing** (data integrity) and **Asymmetric Cryptography** (digital signatures for authentication/authorization) to secure transactions. |
| **Privacy and Security** | **Security** is achieved through cryptographic linkage and decentralization. **Privacy** is maintained through techniques like **zero-knowledge proofs (ZKPs)** or private channels (as in Fabric) to limit data visibility. |