BLOCK-CHAIN TECHNOLOGY
END-SEM QUESTIONS

1. What is Blockchain? Explain Features of Blockchain

Blockchain is a decentralized and distributed digital ledger technology that records transactions securely across a network of computers. Each transaction is grouped into a "block," which is linked to the previous block, forming a continuous and immutable "chain." This technology eliminates the need for intermediaries, ensuring transparency, security, and efficiency. Blockchain operates on a peer-to-peer (P2P) network, meaning no single entity has control over the system, making it highly resistant to fraud and manipulation. Transactions are verified using cryptographic techniques and consensus mechanisms, such as Proof of Work (PoW) or Proof of Stake (PoS).

Key Features of Blockchain:

1. **Decentralization** – Unlike traditional centralized systems, blockchain operates on a distributed network where every participant has access to the same data, reducing risks associated with single points of failure.
2. **Immutability** – Once data is recorded on the blockchain, it cannot be altered or deleted. This ensures data integrity and prevents fraud or unauthorized modifications.
3. **Transparency** – Transactions recorded on a public blockchain are visible to all network participants, promoting accountability and trust. Even in private blockchains, predefined participants can verify records.
4. **Security** – Blockchain uses cryptographic encryption to secure transactions. Each block is hashed and linked to the previous one, making it extremely difficult for hackers to alter the data without controlling the entire network.
5. **Consensus Mechanisms** – Transactions are validated using consensus algorithms like PoW, PoS, or Delegated Proof of Stake (DPoS), ensuring that only legitimate transactions are added to the blockchain.

2. Enlist Applications and Challenges of Blockchain

Blockchain technology is being adopted across various industries due to its transparency, security, and efficiency. It eliminates the need for intermediaries, reducing costs and increasing trust in digital transactions. From financial services to healthcare, blockchain is reshaping industries by offering decentralized and tamper-proof solutions. However, like any technology, blockchain also faces several challenges that limit its widespread adoption.

Applications of Blockchain:

1. **Cryptocurrency and Finance** – Blockchain is the backbone of cryptocurrencies like Bitcoin and Ethereum. It ensures secure and transparent financial transactions while enabling smart contracts that automate agreements without intermediaries.
2. **Supply Chain Management** – Blockchain enhances transparency by allowing businesses to track products from the point of origin to the end consumer, reducing fraud, theft, and inefficiencies.
3. **Healthcare** – Medical records stored on a blockchain can be securely shared between patients and healthcare providers, improving data security and patient privacy while preventing data breaches.
4. **Voting Systems** – Blockchain-based voting systems can prevent fraud, increase voter participation, and provide a tamper-proof election process with verifiable results.
5. **Identity Management** – Blockchain helps create decentralized digital identities, reducing identity theft and improving personal data security for online transactions and authentication.

Challenges of Blockchain:

1. **Scalability Issues** – Blockchains like Bitcoin and Ethereum struggle to handle large transaction volumes, leading to slow processing times and high fees.
2. **Energy Consumption** – PoW-based blockchains require extensive computational power, making them environmentally unsustainable and expensive to maintain.
3. **Regulatory and Legal Uncertainty** – Governments worldwide are still developing legal frameworks for blockchain, leading to uncertainty regarding compliance and adoption.
4. **Security Vulnerabilities** – While blockchain itself is secure, smart contracts and exchanges can have loopholes that hackers exploit, leading to financial losses.
5. **Integration Complexity** – Businesses face difficulties integrating blockchain with existing IT infrastructure, requiring significant investment and expertise.

3. Differentiate between Symmetric and Asymmetric cryptography

Cryptography is the practice of securing information through encryption techniques. There are two primary types of cryptography: **symmetric cryptography** and **asymmetric cryptography**. The key difference between them is the number of keys used for encryption and decryption.

Key Differences Between Symmetric and Asymmetric Cryptography:

Feature	Symmetric Cryptography	Asymmetric Cryptography
Keys Used	Uses a single key for both encryption and decryption.	Uses a pair of keys (public key for encryption and private key for decryption).
Speed	Faster as it requires less computational power.	Slower due to complex mathematical computations.
Security	Less secure because sharing the secret key increases risk.	More secure as private keys are never shared.
Example Algorithms	AES, DES, 3DES, Blowfish.	RSA, ECC, Diffie-Hellman, DSA.
Use Cases	Used for bulk data encryption, file transfers, and secure communication within trusted environments.	Used for secure online transactions, digital signatures, and key exchange mechanisms.

Key Points:

1. **Key Usage** – Symmetric cryptography uses one key, while asymmetric cryptography uses two keys.
2. **Speed and Performance** – Symmetric encryption is faster; asymmetric encryption is slower due to complex key management.
3. **Security Level** – Asymmetric encryption provides higher security since private keys are never shared.
4. **Use Cases** – Symmetric is used for fast, large-scale encryption; asymmetric is used for secure key exchange and authentication.
5. **Example Scenario** – AES encrypts a file quickly (symmetric), whereas RSA is used for secure email communication (asymmetric).

4. What is Cryptography. Explain in detail with suitable example.

Cryptography is the process of securing communication and data by converting it into an unreadable format (encryption) and then converting it back to its original form (decryption) using cryptographic keys. It ensures **confidentiality, integrity, authentication,** and **non-repudiation** in digital communication.

Types of Cryptography:

1. **Symmetric Cryptography** – Uses a single key for encryption and decryption. Example: **AES (Advanced Encryption Standard)** is used in banking transactions.
2. **Asymmetric Cryptography** – Uses a pair of keys: a public key (encryption) and a private key (decryption). Example: **RSA (Rivest-Shamir-Adleman)** secures online banking and email encryption.
3. **Hash Functions** – Converts data into a fixed-length hash value, ensuring integrity. Example: **SHA-256** secures Bitcoin transactions.

Example of Cryptography in Action:

Consider **email encryption** using asymmetric cryptography:

- Alice wants to send a secure message to Bob.
- She encrypts the message using Bob's **public key**.
- Bob decrypts it using his **private key**, ensuring that only he can read it.
- This method guarantees **secure communication** even if someone intercepts the message.

Key Points of Cryptography:

1. **Ensures Data Security** – Protects sensitive information from unauthorized access.
2. **Types of Cryptography** – Includes symmetric, asymmetric, and hash functions.
3. **Real-World Applications** – Used in online banking, digital signatures, and cryptocurrency.
4. **Encryption & Decryption** – Converts data into unreadable format and back to original.
5. **Example** – Email encryption using RSA ensures confidential communication

5. Differentiate between hard and soft fork

A **fork** in blockchain occurs when the network's rules are updated or changed, leading to a divergence in the blockchain. Forks can be classified into two types: **hard forks** and **soft forks**.

Feature	Hard Fork	Soft Fork
Definition	A permanent divergence in the blockchain where nodes must upgrade to the new rules to continue participation.	A backward-compatible upgrade where old nodes can still recognize new transactions.
Compatibility	Not compatible with previous versions; requires all participants to upgrade.	Compatible with older versions; only requires majority miners to upgrade.
Chain Splitting	Results in two separate blockchains if some users continue with the old rules.	Does not create a new chain; only updates existing blockchain rules.
Consensus Requirement	Requires the majority of the community to upgrade to the new version.	Can work with a minority of upgraded nodes while still supporting old ones.
Examples	Bitcoin Cash (BCH) split from Bitcoin (BTC) in 2017. Ethereum Classic (ETC) emerged after Ethereum (ETH) forked.	Segregated Witness (SegWit) upgrade in Bitcoin. Ethereum's London Upgrade.

Key Points:

1. **Hard Forks** create a new blockchain, whereas **Soft Forks** update rules without splitting the chain.
2. **Hard Forks** require all nodes to upgrade, while **Soft Forks** work with existing rules.
3. **Hard Forks** lead to potential cryptocurrency splits, while **Soft Forks** maintain a single blockchain.
4. **Examples:** Bitcoin Cash (Hard Fork) and SegWit in Bitcoin (Soft Fork).
5. **Use Cases:** Hard forks introduce major changes, while soft forks improve functionality without disruption.

6. What are the main stages in the blockchain transaction life cycle?

A **blockchain transaction life cycle** consists of multiple stages from transaction initiation to final confirmation. Each transaction undergoes validation, propagation, and settlement before becoming part of the blockchain.

Stages in the Blockchain Transaction Life Cycle:

1. **Transaction Creation:**
    - A user initiates a transaction by signing it with their private key.
    - The transaction includes sender, receiver, and amount details.
2. **Transaction Broadcast:**
    - The transaction is broadcasted to the blockchain network (nodes).
    - Nodes verify the transaction format and validity.
3. **Transaction Validation:**
    - Miners or validators check if the sender has sufficient balance.
    - The transaction must comply with network rules (consensus mechanisms like Proof of Work or Proof of Stake).
4. **Transaction Mining & Block Inclusion:**
    - The valid transaction is grouped into a block.
    - Miners compete to validate the block by solving cryptographic puzzles (PoW) or using staking mechanisms (PoS).
    - Once validated, the block is added to the blockchain.
5. **Block Confirmation & Finalization:**
    - The network confirms the block and transactions within it.
    - More confirmations strengthen the immutability of the transaction.
    - Transactions with multiple confirmations are considered final and irreversible.

Key Points:

1. **Transaction Initiation** – User creates and signs the transaction.
2. **Network Broadcast** – The transaction is sent to blockchain nodes for validation.
3. **Validation Process** – Nodes check transaction legitimacy and approve it.
4. **Mining & Block Inclusion** – Transactions are added to a block through consensus mechanisms.
5. **Final Confirmation** – Once validated, transactions become immutable.

7. What is the Genesis Block?

The **Genesis Block** is the very first block in a blockchain network. It serves as the foundation for all subsequent blocks and is hardcoded into the blockchain protocol. Unlike other blocks, the Genesis Block has no predecessor since it is the first entry in the blockchain ledger.

Characteristics of the Genesis Block:

1. **First Block of the Blockchain** – Every blockchain starts with a Genesis Block, which contains the initial transaction data.
2. **Hardcoded into Protocol** – Unlike regular blocks, it is pre-defined in the blockchain's source code.
3. **No Parent Block** – It does not reference any previous block since it is the first in the chain.
4. **Special Messages** – Some Genesis Blocks include messages or hidden text. For example, Bitcoin's Genesis Block includes a newspaper headline: *"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks."*
5. **Establishes the Blockchain's Initial Parameters** – Defines the initial mining rewards, difficulty level, and blockchain rules.

Example: Bitcoin's Genesis Block

- Created by **Satoshi Nakamoto** on **January 3, 2009**.
- Block height: **0**
- Block reward: **50 BTC (unspendable)**

Key Points:

1. **Genesis Block is the first block of any blockchain** and serves as the foundation.
2. **It has no parent block**, making it unique in the blockchain structure.
3. **Hardcoded into the blockchain's protocol** and cannot be altered.
4. **Bitcoin's Genesis Block contains a hidden message** referencing the 2008 financial crisis.
5. **Essential for blockchain initiation**, defining network rules and parameters.

8. What is the Ethereum Virtual Machine (EVM)?

The **Ethereum Virtual Machine (EVM)** is a decentralized runtime environment that executes smart contracts on the Ethereum blockchain. It is responsible for processing transactions, executing code, and maintaining the state of the Ethereum network. The EVM allows developers to deploy and run decentralized applications (**DApps**) in a secure and trustless manner.

Key Features of the Ethereum Virtual Machine (EVM):

1. **Turing-Complete Computation**
    - The EVM can execute any computational logic, enabling complex smart contract functionalities similar to traditional programming languages.
2. **Isolation and Security**
    - Each smart contract runs in a sandboxed environment, preventing malicious contracts from affecting the Ethereum network.
3. **Gas Mechanism for Cost Control**
    - Every computation on the EVM requires **gas**, a fee system that prevents network abuse and optimizes resource allocation.
4. **Platform Independence**
    - The EVM is independent of the underlying hardware and can run on any Ethereum node across different devices.
5. **State Management**
    - The EVM maintains a state of all accounts, smart contracts, and balances across the Ethereum blockchain.

Example of EVM Execution:

- When a user interacts with a **DeFi (Decentralized Finance) application**, the EVM processes the transaction, executes the smart contract logic, and updates the blockchain state accordingly.

9. Differentiate between DApps. Ethereum vs bitcoin

Ethereum and Bitcoin both support decentralized applications (**DApps**), but they differ in functionality, purpose, and blockchain structure.

Key Differences Between Ethereum and Bitcoin DApps

Feature	Ethereum	Bitcoin
Purpose	Designed for smart contracts and DApps.	Primarily used as a decentralized currency.
Smart Contracts	Supports complex smart contracts via the EVM.	Limited scripting with simple transaction-based functionality.
Programming Language	Uses Solidity, Vyper for DApp development.	Uses a simple scripting language (Bitcoin Script).
Flexibility	High flexibility for developing DeFi, NFTs, and DAOs.	Limited to payment-based applications.
Examples	Uniswap (DeFi), OpenSea (NFT marketplace), Aave (Lending protocol).	Lightning Network (Scalability), Bitcoin Ordinals (NFT-like inscriptions).

Key Points:

1. Ethereum supports full-fledged DApps, while Bitcoin primarily supports simple financial transactions.
2. Ethereum's EVM enables smart contracts, but Bitcoin's scripting is limited.
3. Ethereum uses Solidity for coding smart contracts, whereas Bitcoin has basic script-based functionality.
4. Ethereum enables DeFi, NFTs, and DAOs, while Bitcoin focuses on store-of-value applications.
5. Ethereum's DApps offer extensive use cases, whereas Bitcoin's DApps focus on scalability and payments.

10. Describe the key components of an Ethereum smart contract.

An **Ethereum smart contract** is a self-executing program that runs on the Ethereum blockchain. It eliminates intermediaries by enforcing agreements through code, ensuring transparency, security, and automation in blockchain transactions. Smart contracts operate within the **Ethereum Virtual Machine (EVM)** and follow rules defined in **Solidity** (Ethereum's programming language).

Key Components of an Ethereum Smart Contract:

1. **State Variables**
   - These store important contract-related data permanently on the blockchain.
   - Examples of stored data include user balances, ownership details, and contract-specific parameters.
2. **Functions**
   - Functions define the actions a smart contract can perform, such as transferring funds, updating records, or executing logic.
   - They allow users to interact with the contract, such as making payments or voting in a decentralized system.
3. **Modifiers**
   - Modifiers impose rules on functions to control their execution, ensuring that only authorized actions occur.
   - They are commonly used for access control, such as allowing only the contract owner to perform specific operations.
4. **Events**
   - Events provide a mechanism for smart contracts to log important activities, which external applications can track.
   - These logs enable decentralized applications (**DApps**) and blockchain explorers to notify users about contract actions, such as successful transactions.
5. **Constructor**
   - A constructor is a special function that initializes the smart contract when deployed.
   - It typically sets important values, such as the owner's address, initial balances, or predefined rules.

Key Points:

1. **State Variables store critical contract data on the blockchain.**
2. **Functions define contract behavior and allow user interaction.**
3. **Modifiers restrict function execution to ensure security and control.**
4. **Events help track contract activities and notify external applications.**
5. **Constructors initialize the contract when deployed, setting key parameters.**

11. How does blockchain facilitate cross-border payments?

Blockchain technology is revolutionizing **cross-border payments** by making transactions faster, cheaper, and more transparent. Traditional international payments rely on multiple intermediaries, leading to high fees, delays, and inefficiencies. Blockchain eliminates these intermediaries, enabling direct, near-instant transactions between parties worldwide.

How Blockchain Improves Cross-Border Payments:

1. **Faster Transactions**
    - Traditional bank transfers can take days due to clearinghouses and currency conversions.
    - Blockchain enables near-instant transactions by directly connecting senders and receivers without intermediaries.
2. **Lower Transaction Costs**
    - Banks and remittance services charge high fees for processing cross-border transactions.
    - Blockchain significantly reduces costs by removing middlemen and using cryptocurrencies with minimal transaction fees.
3. **Greater Transparency and Security**
    - Transactions are recorded on an immutable, transparent ledger accessible to all participants.
    - Smart contracts automate payments based on predefined conditions, reducing fraud and disputes.
4. **Financial Inclusion**
    - Many people in developing countries lack access to traditional banking services.Blockchain allows anyone with internet access to send and receive money without needing a bank account.
5. **Stablecoins and CBDCs**
    - Cryptocurrencies like **USDT (Tether)** and **CBDCs (Central Bank Digital Currencies)** provide stable, blockchain-based alternatives to volatile fiat currencies.
    - These digital assets enable seamless, borderless transactions without fluctuations in exchange rates.

12. Differentiate between Virtual reality, Augmented reality, Mixed reality.

Virtual Reality (VR), Augmented Reality (AR), and Mixed Reality (MR) are immersive technologies that enhance human interaction with digital environments. Each offers a unique way of blending the real and virtual worlds.

Key Differences:

Feature	Virtual Reality (VR)	Augmented Reality (AR)	Mixed Reality (MR)
Definition	A fully immersive digital experience replacing the real world.	Overlays digital content onto the real world.	Blends physical and digital elements interactively.
Interaction	Users are entirely inside a virtual world with no real-world interaction.	Users see and interact with both real and virtual elements.	Virtual objects integrate into the real world, reacting dynamically.
Device Required	VR headsets (Oculus, HTC Vive, PlayStation VR).	Smartphones, AR glasses (Google Lens, Microsoft HoloLens).	Advanced AR devices (HoloLens 2, Magic Leap).
Examples	VR gaming (Meta Quest), virtual tourism, training simulations.	AR filters (Snapchat, Instagram), Pokémon GO, digital manuals.	Interactive 3D models, collaborative workspaces, advanced gaming.

Key Points:

1. **VR** is a fully immersive experience where users enter a digital world.
2. **AR** enhances the real world by overlaying digital objects onto it.
3. **MR** allows digital elements to interact dynamically with the real world.
4. **VR requires headsets, while AR/MR can be accessed through glasses or mobile devices.**
5. **Applications range from gaming and training to healthcare and industrial simulations.**

13. Explain the concept of decentralized identity using blockchain.

Decentralized Identity (DID) is a blockchain-based system that allows individuals to control their digital identities without relying on centralized authorities like governments or corporations. It enhances privacy, security, and user control over personal data.

How Decentralized Identity Works:

1. **User-Owned Digital Identity**
    - Unlike traditional identity systems controlled by governments or companies, DID allows users to create and manage their digital identities on the blockchain.
    - Users receive a unique cryptographic identifier stored securely in a blockchain wallet.
2. **Eliminates Centralized Databases**
    - Traditional identity verification relies on centralized databases prone to hacking.
    - DID removes this risk by storing identity credentials on a decentralized ledger, reducing single points of failure.
3. **Verifiable Credentials**
    - Users receive cryptographic proofs (digital certificates) from trusted institutions like banks, universities, or governments.
    - These credentials can be verified instantly without exposing sensitive personal information.
4. **Selective Disclosure & Privacy**
    - DID enables users to share only necessary details (e.g., proving they are over 18 without revealing their birthdate).This enhances privacy and reduces the risk of identity theft.
5. **Use Cases in Web3 and Real World**
    - Secure login to decentralized applications (DApps) without passwords.
    - Digital passports, medical records, and financial credentials on the blockchain.
    - Enabling self-sovereign identity in sectors like finance, healthcare, and education

MCQs

1. What is the term applied for splits in a blockchain network?
   a. Mergers
   b. Divisions
   c. Forks
   d. None of above

2. Which trees are responsible for storing all transactions in a black through digital signatures of the complete set of transactions?

   a. Binary
   b. Merkel
   c. Red Black
   d. AVL

3. What are the advantages of blockchain technology?
   a. Security and Speed
   b. User control over data
   c. Cost-effective transactions
   d. All of the above

4. What are the important traits of blockchain technology?
   a. Decentralization
   b. Immutability
   c. Transparency
   d. All of the above

5. What can you find in the block of a blockchain?
   a. Timestamp
   b. Transaction Data
   c. Hash Point
   d. All of the above

6. What is the name of the first block in a blockchain?
   a. Genesis Block
   B. Origin Block
   c. Block One
   d. None of the above

7. In cryptography, what is cipher?
   a. algorithm for performing encryption and decryption
   b. Encrypted Message
   c. both algorithm for performing encryption and decryption and encrypted message
   d. Decrypted Message

8. In asymmetric key cryptography, the private key is kept by _____
   a. Sender
   b. Receiver
   c. Sender and Receiver
   d. All the connected devices to the network

9. Bitcoin is a cryptocurrency, which is an application of Blockchain.
   a. True
   b. False

10. Blockchain has ____ versions.
   a. 2
   b. 3
   c. 4
   d.5

11. What is a DApp?
   a. A type of cryptocurrency
   b. A condiment
   c. A type of blockchain
   d. A decentralized application

12. What powers the Ethereum Virtual Machine?
   a. Gas
   b. Ether
   c. Bitcoin
   d. Block Rewards