OVERVIEW OF BLOCKCHAIN

Basics of Blockchain Technology

OVERVIEW OF BLOCKCHAIN

UNIT 1

WHAT IS BLOCKCHAIN?

- - Blockchain is a distributed digital ledger that stores information in blocks linked together to form a chain.
- - Operates in a decentralized manner with no single entity controlling the data.
- - Ensures transparency and security through immutability.

CORE COMPONENTS OF BLOCKCHAIN

- Blocks: Contain data, a timestamp, and unique cryptographic hash; also include the previous block's hash.
- Chain: Sequence of blocks linked in a secure, chronological order.
- Nodes: Computers in the network that store copies of the blockchain.
- Consensus Mechanisms: Methods to validate transactions (e.g., Proof of Work, Proof of Stake).

KEY FEATURES OF BLOCKCHAIN

- Decentralization: Eliminates the need for intermediaries by distributing data across the network.
- Immutability: Once recorded, data cannot be altered or deleted.
- Transparency: Public blockchains allow participants to view all transactions.
- Security: Cryptographic algorithms protect against hacking and fraud.

HOW BLOCKCHAIN WORKS

1. Transaction Initiation: User requests a transaction (e.g., transferring funds).
2. Broadcast to Network: Transaction shared across the network for validation.
3. Validation: Nodes validate the transaction using consensus mechanisms.
4. Block Formation: Validated transactions are grouped into a block.
5. Block Addition: Block added to the blockchain in chronological order.
6. Update Across Nodes: Blockchain updated across all network nodes.

TYPES OF BLOCKCHAIN

- Public Blockchain: Open to anyone; no permissions required (e.g., Bitcoin, Ethereum).
- Private Blockchain: Access restricted to specific participants; used in businesses.
- Consortium Blockchain: Controlled by a group of organizations (e.g., banking sector).
- Hybrid Blockchain: Combines features of public and private blockchains.

ADVANTAGES OF BLOCKCHAIN

- Security: Cryptography ensures data integrity and prevents fraud.
- Transparency: All transactions are visible, fostering trust.
- Efficiency: Removes intermediaries, reducing costs and speeding up processes.
- Traceability: Allows end-to-end tracking of transactions, useful for supply chains.

APPLICATIONS OF BLOCKCHAIN

- 1. Cryptocurrency: Backbone of digital currencies like Bitcoin and Ethereum.
- 2. Supply Chain: Tracks goods from production to delivery.
- 3. Finance: Enables secure, fast, and low-cost cross-border payments.
- 4. Healthcare: Manages secure and interoperable patient records.
- 5. Voting Systems: Offers tamper-proof and transparent voting platforms.

WHY IS BLOCKCHAIN IMPORTANT?

- - Revolutionizes how data is recorded, shared, and secured.
- - Reduces reliance on central authorities, fostering trust.
- - Drives innovation and digital transformation across industries.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

1. Definition

Aspect	Blockchain	Distributed Database
Definition	A decentralized, immutable ledger that records transactions securely using cryptographic hashing.	A centralized or partially decentralized database distributed across multiple nodes, designed for efficient data storage and access.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

2. Architecture

Aspect	Blockchain	Distributed Database
Data Structure	Uses a linked list of blocks where each block is cryptographically linked to the previous block.	Uses relational or non-relational databases like SQL, NoSQL, or other database models.
Immutability	Data once written cannot be changed (immutable).	Data can be updated, modified, and deleted as needed.
Control	Operates in a decentralized manner with consensus protocols (PoW, PoS, etc.).	Often partially centralized or distributed, with a central controlling authority.
Storage	Every node stores the entire blockchain.	Data is partitioned among nodes for better efficiency.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

3. Data handling

Aspect	Blockchain	Distributed Database
Data Redundancy	High redundancy, as every node stores the full blockchain.	Data is distributed logically, with no full replication of all data across nodes.
Data Consistency	Uses eventual consistency (data consistency is guaranteed eventually) due to consensus algorithms.	Uses immediate consistency (data is immediately consistent after commit) in most cases.
Data Modification	Once written, data is immutable and cannot be changed.	Data can be edited, updated, or deleted.
Data Validation	Requires consensus from multiple nodes to validate new transactions.	No consensus is required; the central authority can approve changes.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

4. Consensus Mechanism

Aspect	Blockchain	Distributed Database
Mechanism	Uses **consensus protocols** (Proof of Work, Proof of Stake) to validate data.	No consensus mechanism is required as a central authority manages updates.
Fault Tolerance	Highly tolerant to node failures (Byzantine Fault Tolerance).	Depends on **replication and failover** strategies.
Trust	No central authority, hence requires trustless consensus.	Centralized or partially distributed authority, requiring users to **trust the system**.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

5. Security

Aspect	Blockchain	Distributed Database
Security	High security due to cryptography and hashing (SHA-256, etc.).	Security depends on access control, firewalls, and encryption.
Tamper Resistance	**Tamper-proof** due to immutability and consensus protocols.	Vulnerable to hacking, as central control allows data changes.
Anonymity	Anonymous or pseudonymous users can participate.	Users are authenticated, and their identity is known.
Attack Resistance	**Resistant to attacks** like DDoS or malicious changes.	Can be targeted by DDoS and SQL injection attacks.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

6. Usage

Aspect	Blockchain	Distributed Database
Use Cases	**Cryptocurrencies**, smart contracts, supply chain tracking, healthcare records, etc.	Enterprise databases, financial systems, CRM, inventory management, etc.
Primary Goal	To achieve **trustless, secure, and immutable transactions**.	To provide **high-speed access to data** and support data operations like CRUD.
Data Visibility	Data is public or private depending on permissioned or public blockchains.	Data is **restricted to certain users** and visible only with proper access rights.

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

7. Efficiency

Aspect	Blockchain	Distributed Database
Transaction Speed	Slow (due to mining, consensus, and validation).	Fast, as transactions are updated in real time.
Latency	High latency due to mining, hashing, and validation processes.	Low latency since updates are done instantly.
Scalability	Limited scalability due to the need for consensus.	Scalable, as additional servers/nodes increase capacity.
Throughput	Low throughput due to consensus (e.g., Bitcoin ~7 TPS).	High throughput (thousands of transactions per second).

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

8. Performance

Aspect	Blockchain	Distributed Database
Speed	Slow (depends on consensus, mining time, etc.).	**Fast** (queries, reads, and writes are much quicker).
Efficiency	Less efficient due to the redundancy of data storage.	Highly efficient, as only necessary data is stored and shared.
Energy Consumption	High (especially in Proof of Work systems).	Low energy consumption (no need for mining or consensus).

BLOCKCHAIN VS DISTRIBUTED TECHNOLOGY

9. Permission

Aspect	Blockchain	Distributed Database
Public/Private	Can be **public or permissioned** (private).	Typically **private or permissioned**.
Access Control	Can be **open (public) or restricted (private)**.	Uses **role-based access control** (RBAC) and other access controls.
User Participation	Anyone can participate in public blockchains.	Access limited to authenticated users.

WHEN TO USE

When to Use Blockchain?

- When immutability is required (like cryptocurrency or legal documents).
- When trust among parties is an issue (like supply chains, voting, or healthcare).
- When anonymity and privacy are crucial.

When to Use Distributed Databases?

- When high-speed processing is required (like financial transactions, banking, and inventory).
- When efficient querying and data analysis are needed.
- When strong data control and permissioning are required.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Blockchain technology plays a transformative role in digitalization, revolutionizing how data is stored, shared, and trusted. By enabling secure, transparent, and decentralized digital ecosystems, blockchain drives innovation in multiple industries. Here's a comprehensive analysis of the role of blockchain in the landscape of digitalization.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Decentralization and Elimination of Intermediaries

- **Traditional Approach**: Centralized systems like banks, payment gateways, and government authorities act as intermediaries for transactions and verifications.
- **Blockchain Approach**: Eliminates intermediaries by enabling peer-to-peer (P2P) transactions where trust is established through consensus protocols.
- **Impact**:
  - **Faster Transactions**: No delays caused by third-party approvals (like banks).
  - **Cost Reduction**: Eliminates fees charged by intermediaries.
  - **Example**: **Cryptocurrencies** (like Bitcoin, Ethereum) allow direct payments between users, bypassing financial institutions.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Data Security and Integrity

- **Traditional Approach**: Centralized databases are vulnerable to hacks, data breaches, and insider threats.
- **Blockchain Approach**: Data is stored using **cryptographic hashing** (like SHA-256), and every change is recorded as a new block, ensuring **immutability**.
- **Impact**:
  - **Tamper-Proof Records**: Once data is added, it cannot be altered.
  - **Auditability**: Entire transaction history is transparent and verifiable.
  - **Example**: **Supply Chain Management** systems use blockchain to track products from origin to destination, ensuring data integrity and product authenticity.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Enhanced Transparency and Trust

- **Traditional Approach**: Trust is established through contracts, legal systems, and third-party verifiers.
- **Blockchain Approach**: Data is transparent to all participants, as every participant has access to the same copy of the ledger.
- **Impact**:
  - **Accountability**: Every participant is accountable, as every transaction is traceable.
  - **Reduces Corruption**: Since all actions are recorded and public, corruption is difficult to hide.
  - **Example**: **Government Services** like land registration systems use blockchain to create tamper-proof property records, reducing disputes and fraud.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Smart Contracts and Automation

- **Traditional Approach**: Contracts are enforced manually through intermediaries, lawyers, or regulatory authorities.
- **Blockchain Approach**: **Smart contracts** are self-executing contracts with pre-defined rules and conditions written in code.
  - **Impact**:
  - **Automatic Execution**: Once conditions are met, contracts are executed automatically without intermediaries.
  - **Error Reduction**: Human errors are eliminated.
  - **Example**: **Insurance Claims**: Blockchain-powered insurance automates the claims process. When a claim is triggered (like flight delay), the smart contract releases payment automatically.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Tokenization of Assets

- **Traditional Approach**: Ownership of physical assets like real estate, art, and shares is represented by paper certificates.
- **Blockchain Approach**: Tokenization converts physical and digital assets into **digital tokens** stored on the blockchain.
  - **Impact**:
  - **Fractional Ownership**: Investors can own fractional shares of large assets (like real estate) without full ownership.
  - **Liquidity**: Assets become easily tradable, increasing liquidity.
  - **Example**: **Real Estate Tokenization** platforms allow investors to buy and sell portions of properties using blockchain-based tokens.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Digital Identity Management

- **Traditional Approach**: Identity verification is managed by third parties (governments, banks, and online platforms), requiring users to share personal information repeatedly.
- **Blockchain Approach**: **Decentralized Digital Identity** (DID) systems allow users to control and share their data selectively using blockchain.
  - **Impact**:
  - **Self-Sovereign Identity**: Users control their identity without relying on a third party.
  - **Data Privacy**: Users can share only relevant data, not the entire document.
  - **Example**: **DID Solutions** like Microsoft's ION project enable users to manage their digital identity, avoiding the need for repeated KYC processes.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Secure Payments and Digital Currencies

- **Traditional Approach**: Payments rely on financial institutions, SWIFT networks, and payment processors, resulting in high fees and delays.
- **Blockchain Approach**: **Cryptocurrencies** allow borderless, real-time payments without intermediaries.
  - **Impact**:
    - **Faster Settlements**: Payments are processed in minutes instead of days.
    - **Cost Reduction**: No intermediary fees for cross-border payments.
    - **Example**: **Remittances** through Bitcoin or **Stablecoins** (like USDC) allow fast, cheap, and borderless payments.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Supply Chain Traceability and Anti-Counterfeiting

- **Traditional Approach**: Supply chain tracking is managed manually, leading to mismanagement, fraud, and counterfeit goods.
- **Blockchain Approach**: Blockchain creates a **shared ledger** where every stakeholder (manufacturer, supplier, retailer, consumer) records data at each stage of the supply chain.
  - **Impact**:
  - **Product Authenticity**: Buyers can trace product origin, ensuring authenticity.
  - **Reduced Counterfeiting**: Tamper-proof records prevent fraud.
  - **Example**: **Walmart** uses blockchain to track food items, ensuring quality and quick recalls in case of contamination.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Role in Digital Governance

- **Traditional Approach**: Voting systems are paper-based or electronic but controlled by a central authority, making them prone to manipulation.
- **Blockchain Approach**: **Blockchain Voting** enables transparent and secure voting without central control.
  - **Impact**:
  - **Transparency**: Votes are immutable, verifiable, and cannot be changed.
  - **Prevents Vote Manipulation**: Every vote is securely recorded and validated by the network.
  - **Example**: **E-Voting Systems** in countries like Estonia leverage blockchain to ensure fair and transparent elections.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Role in Healthcare and Patient Data Management

- **Traditional Approach**: Patient health records are siloed across hospitals, clinics, and insurance providers.
- **Blockchain Approach**: Patient health records are stored on **decentralized ledgers**, accessible to healthcare providers with patient consent.
  - **Impact**:
    - **Interoperability**: Patient records are accessible across hospitals, doctors, and clinics.
    - **Data Privacy**: Patients control access to their own health data.
    - **Example**: **Healthcare Systems** like MediBloc use blockchain to ensure patients have complete control over their health records.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Audit and Compliance

- **Traditional Approach**: Auditing processes are manual, time-consuming, and subject to human error.
- **Blockchain Approach**: Blockchain creates **immutable audit trails**, enabling automatic audits and real-time verification.
  - **Impact**:
  - **Automatic Audits**: Each transaction is automatically logged, reducing human intervention.
  - **Real-Time Compliance**: Regulatory authorities can view and audit transactions in real-time.
  - **Example**: **Financial Audits** on blockchain ensure regulators have instant access to company financials.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

NFTs and Digital Art

- **Traditional Approach**: Digital art is distributed online without unique ownership, making it hard to prove authenticity.
- **Blockchain Approach**: Non-Fungible Tokens (NFTs) provide **proof of ownership** for digital art, music, videos, and collectibles.
  - **Impact**:
    - **Digital Ownership**: Artists can sell their art with proof of authenticity.
    - **Royalty Management**: Artists can receive royalties each time their digital art is sold.
    - **Example**: Platforms like **OpenSea** enable creators to sell unique NFTs, while buyers hold verifiable ownership.

ROLE OF BLOCKCHAIN IN THE LANDSCAPE OF DIGITALIZATION

Role in Emerging Technologies (IoT, AI)

- **Traditional Approach**: IoT devices are vulnerable to hacking, and AI models are controlled by large corporations.
- **Blockchain Approach**: Blockchain creates a **secure, decentralized network** for IoT devices to communicate securely.
  - **Impact**:
  - **Device Autonomy**: IoT devices can communicate and transact autonomously using smart contracts.
  - **Data Ownership**: Blockchain ensures data is owned and controlled by the device owner.
  - **Example: IoT Devices** in smart homes use blockchain to ensure device-to-device payments, secure communication, and enhanced privacy.

HASHING

WHAT IS HASH

- A **hash** is a fixed-length alphanumeric string (a sequence of letters and numbers) generated from an input of arbitrary length. The process of generating a hash is done through **cryptographic hash functions**.
- **Example of a Hash (using SHA-256)**
  - **Input:** "Blockchain Technology"
  - **Output (Hash):**
  - `2c26b46b68ffc68ff99b453c1d30413413422c66e993b6f752c2207c03aee34e`

HASHING

Key Characteristics of a Cryptographic Hash Function

Characteristic	Description
Deterministic	The same input will always produce the same hash.
Fixed Size	Regardless of input size, the output hash has a fixed length.
Pre-image Resistance	It's impossible to determine the input from the output hash.
Collision Resistance	No two different inputs should produce the same hash.
Avalanche Effect	A small change in the input drastically changes the output.
Efficiency	The function must compute the hash quickly and efficiently.

HASHING

Key Characteristics of a Cryptographic Hash Function

Characteristic	Description
Deterministic	The same input will always produce the same hash.
Fixed Size	Regardless of input size, the output hash has a fixed length.
Pre-image Resistance	It's impossible to determine the input from the output hash.
Collision Resistance	No two different inputs should produce the same hash.
Avalanche Effect	A small change in the input drastically changes the output.
Efficiency	The function must compute the hash quickly and efficiently.

HASHING

Role of Hashing in Blockchain

- Hashing plays a critical role in **securing blockchain transactions** and ensuring the integrity of the entire system. Below are some of the most important roles of hashing in blockchain.
- **Block Hashing**
- Every block in the blockchain contains a **block header** that includes the hash of the previous block.
- This hash links the current block to the previous block, forming a **chain of blocks**.
- If a hacker tries to modify the content of a block, the hash of that block changes, invalidating the hashes of all subsequent blocks.

HASHING

Role of Hashing in Blockchain

- **How It Works:**
- Data in the block (like transactions, timestamp, and nonce) is hashed using a hash function (like SHA-256).
- The resulting hash serves as a unique "digital fingerprint" for that block.
- The hash of the current block is stored in the next block, creating a link between them.
- **Impact:**
- **Tamper-Proof**: If any information in a block is changed, the hash changes, making it easy to detect tampering.
- **Immutability**: It becomes computationally infeasible to modify the data in previous blocks.

HASHING

Proof of Work (PoW)

- In Proof of Work (PoW) blockchains like Bitcoin, miners must find a hash value that satisfies a specific condition (e.g., a hash that starts with a certain number of zeros).
- This process is called **mining**, and the hash must be less than or equal to a "target value" set by the network.
- Miners keep changing the **nonce** (a random number) in the block until they generate a hash that meets the target.

HASHING

Proof of Work (PoW)

- **How It Works:**
- The miner combines the **block data** with a random **nonce**.
- The combined data is hashed using SHA-256.
- If the resulting hash meets the target (e.g., starts with "0000"), the miner is rewarded, and the block is added to the blockchain.
- **Impact:**
- **Security**: It is computationally expensive to find the correct hash, deterring attackers.
- **Decentralization**: Mining is distributed across multiple miners, ensuring no single entity controls the system.

HASHING

Transaction Verification

- Each transaction in a block is hashed before being included in the block.
- **Digital Signatures** are created by hashing the transaction data and encrypting it using the sender's private key.
- This ensures the transaction is **tamper-proof** and can be verified by any node on the blockchain using the sender's public key.
- **Impact:**
- **Authentication**: Ensures only the owner of the private key can sign transactions.
- **Integrity**: If the transaction data changes, the hash changes, making it easy to detect fraud.

HASHING

Types of Hash Functions Used in Blockchain

- Several hashing algorithms are used in blockchain technology, but the most popular is **SHA-256** (used in Bitcoin) and **Keccak-256** (used in Ethereum).

Hash Function	Hash Length	Used In	Description
SHA-256	256 bits	Bitcoin, Litecoin	Most widely used in blockchains.
Keccak-256	256 bits	Ethereum	Used in Ethereum for hashing.
SHA-3	256 bits	Advanced Projects	Next-generation hashing method.
RIPEMD-160	160 bits	Bitcoin Addresses	Used for creating wallet addresses.

HASHING

Why Hashing is Essential in Blockchain?

Use Case	How Hashing Helps
Data Integrity	Any change in the block data alters the hash.
Security	Blocks are linked using cryptographic hashes.
Immutability	Data once written cannot be changed.
Authentication	Transactions are signed and verified via hashing.
Proof of Work (PoW)	Mining requires hashing to generate a block.
Tamper Detection	If a hacker modifies any data, the hash changes.

HASHING

Example of Hashing in Blockchain

Imagine a **block** in the blockchain with the following information:

Step 1: The following data is concatenated:

```
Transaction details + 2024-12-13 + 0000abc123 + 10245
```

Step 2: The SHA-256 hash function is applied:

Hash:

```
00c23a6f5c6d58c812b6725b4c9b3a1095cc2bce78a12f23d918b
4676a5d96d2
```

Step 3: The resulting hash becomes the **identifier for the block** and is stored in the header of the next block.

If any data in this block changes, the hash will be completely different, and this change will propagate through the entire chain, making tampering **impossible**.

Field	Value
Data	Transaction details
Timestamp	2024-12-13
Previous Hash	0000abc123
Nonce	10245
Field	Value
Data	Transaction details

HASHING

Real-World Applications of Hashing in Blockchain

Imagine a **block** in the blockchain with the following information:

Application	Description
Cryptocurrency	Used in mining, hashing transactions, and proof of work.
Supply Chain	Tracks and verifies product movement.
Digital Identity	Used for user authentication.
Smart Contracts	Contract details are hashed to ensure immutability.
Healthcare	Stores patient records securely.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

Public Key Cryptosystems (PKC) play a fundamental role in **blockchain technology** by enabling **secure communication, digital signatures, and user authentication**. Public key cryptosystems use a pair of cryptographic keys — a **public key** and a **private key** — to ensure secure interactions in decentralized blockchain networks.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

What is a Public Key Cryptosystem?

A **Public Key Cryptosystem** (also known as **Asymmetric Cryptography**) uses a pair of keys:

- **Public Key**: This key is shared with everyone and is used to encrypt data.
- **Private Key**: This key is kept secret by the user and is used to decrypt data or sign transactions.

Unlike **symmetric cryptography** (which uses a single key for both encryption and decryption), asymmetric cryptography uses two keys, making it more secure and ideal for blockchain applications.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

Key Concepts of Public Key Cryptosystems

Concept	Explanation
Key Pair	Each user has a unique pair of keys — one public and one private.
Encryption	Data is encrypted using the recipient's public key and can only be decrypted using their private key.
Digital Signatures	Data is "signed" with the sender's private key, and anyone with the public key can verify the sender's identity.
Non-repudiation	Since only the private key owner can sign transactions, users cannot deny their actions.
Authentication	Ensures the identity of the user sending or receiving data.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

How Public Key Cryptosystems Work in Blockchain

To understand how public key cryptosystems work, it's essential to understand how **keys are generated and used**.

1. Key Generation

- Each participant in the blockchain generates a pair of keys (public key and private key) using cryptographic algorithms like **Elliptic Curve Cryptography (ECC)** or **RSA**.
- The public key is shared with the world, while the private key is stored securely with the user.

2. Encryption and Decryption

- When someone wants to send a secure message to a user, they encrypt the message using the user's **public key**.
- The message can only be decrypted by the user's **private key**.

3. Digital Signatures

- To prove the authenticity of a message or transaction, the sender **signs** it using their **private key**.
- The recipient can verify the signature using the sender's **public key**.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

KEY FUNCTIONS OF PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN

1. Secure User Identity and Wallets

- Each user on the blockchain is identified by their **public key** (like an address) and controls their wallet using their **private key**.
- **Public Key = Wallet Address**: The public key is used to generate the wallet address.
- **Private Key = Access Key**: The private key is required to authorize transactions from the wallet.

  Example: If Alice wants to receive cryptocurrency, she shares her **wallet address** (derived from her public key). To spend or transfer funds, Alice must use her **private key** to sign the transaction.

Impact:

- Users remain **pseudonymous** because only the wallet address is visible on the blockchain.
- Users maintain complete control over their funds and identity since only they have access to their private keys.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

KEY FUNCTIONS OF PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN

2. Digital Signatures for Transaction Authentication

- When users create a transaction, they must **sign the transaction** using their **private key**.
- This digital signature proves that the transaction was created and authorized by the wallet owner.

How It Works:

- User creates a transaction (like sending cryptocurrency).
- The transaction data is hashed using a hash function (like SHA-256).
- The hashed transaction is encrypted using the **private key**, creating a **digital signature**.
- Miners and nodes verify the signature using the user's **public key**.

Impact:

- **Non-repudiation**: The user cannot deny authorizing the transaction since it is signed using their private key.
- **Security**: No one can forge a user's signature because only the private key owner can create it.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

KEY FUNCTIONS OF PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN

3. Data Integrity and Tamper Detection

- Public key cryptography ensures that **block data is immutable.**
- Each block contains a cryptographic hash, and the data in the block is signed using a key.
- If any data in the block is modified, the hash changes, and the signature is no longer valid.

How It Works:

- When data is added to the blockchain, a cryptographic hash is created.
- This hash, along with a signature, ensures the data's integrity.
- If anyone attempts to modify the data, the hash changes, and other nodes reject the modified block.

Impact:

- Ensures **immutability** of records in the blockchain.
- Detects tampering and prevents fraudulent changes to the blockchain.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

KEY FUNCTIONS OF PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN

4. Generating Wallet Addresses

- A user's **public key** is hashed to generate a **wallet address**.
- **Wallet Address ≠ Public Key**, but it is derived from the public key.
- The most common hashing algorithms for generating wallet addresses are **SHA-256** and **RIPEMD-160**.

How It Works:

- The public key is hashed using SHA-256.
- The output of SHA-256 is further hashed using RIPEMD-160.
- This result is used to generate the wallet address.

Impact:

- Users can share their wallet address (not their public key) to receive funds.
- Even if someone knows the wallet address, they cannot determine the public key or private key.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

KEY FUNCTIONS OF PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN

5. Encryption of Sensitive Data

- Blockchain systems may use public key cryptography to **encrypt private messages and data**.
- For example, in private blockchains, sensitive data (like medical records) is encrypted using **public keys** so that only the intended recipient (with the private key) can decrypt it.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

Cryptographic Algorithms Used in Blockchain

Blockchain systems use a combination of **asymmetric cryptography (for public-private keys)** and **symmetric cryptography (for encrypting data)**. Here are some key algorithms used:

Algorithm	Type	Purpose	Blockchain Used
RSA	Asymmetric	Public Key Encryption	Early cryptosystems
Elliptic Curve (ECC)	Asymmetric	Digital Signatures, Wallets	Bitcoin, Ethereum
ECDSA	Asymmetric	Digital Signatures	Bitcoin, Ethereum
SHA-256	Hash Function	Hashing Transactions	Bitcoin, Litecoin
RIPEMD-160	Hash Function	Generating Wallet Addresses	Bitcoin, Ethereum

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

Benefits of Public Key Cryptosystems in Blockchain

Benefit	Explanation
Decentralization	No central authority required for identity or security.
Authentication	Users prove their identity using private keys.
Integrity	Data integrity is preserved as blockchain data is immutable.
Privacy	Users remain pseudonymous by sharing only wallet addresses.
Security	Data encryption and digital signatures ensure transaction security.
Immutability	Cryptography ensures that blockchain data cannot be altered.

PUBLIC KEY CRYPTOSYSTEMS IN BLOCKCHAIN TECHNOLOGY

Challenges of Public Key Cryptosystems in Blockchain

Challenge	Description
Key Management	If users lose their private key, they lose access to their wallet.
Quantum Computing	Future quantum computers may break current cryptographic algorithms.
User Error	Users who accidentally share their private keys lose control over their funds.
Computational Cost	Generating and verifying signatures can be computationally expensive.

HASH PUZZLES

What Are Hash Puzzles in Blockchain Technology?

A **hash puzzle** is a cryptographic challenge where participants must find a solution to a specific problem involving a hash function. In the context of blockchain technology, hash puzzles are an integral part of **Proof of Work (PoW)** systems, where miners solve these puzzles to add new blocks to the blockchain.

Hash puzzles are designed to be computationally intensive, requiring miners to expend significant computational effort. However, verifying the solution is quick and easy for other nodes on the network. This ensures the integrity and security of the blockchain.

HASH PUZZLES

1. How Hash Puzzles Work in Blockchain

In a blockchain, hash puzzles are used as part of the **block mining process**. Here's how they work step by step:

- **Data Compilation**: Miners collect transactions and compile them into a block.
- **Hash Function Application**: The miner hashes the block's data along with a random number called a **nonce** using a cryptographic hash function (e.g., SHA-256).
- **Target Matching**: The miner adjusts the nonce until the resulting hash meets a predefined condition, such as starting with a certain number of zeros.
- **Puzzle Solution**: Once a valid hash is found, the puzzle is considered solved, and the block is added to the blockchain.
- **Verification**: Other nodes in the network can quickly verify the solution by rehashing the block data and checking the result against the target.

HASH PUZZLES

2. Characteristics of Hash Puzzles

- **Asymmetry**: Solving the puzzle is computationally intensive, but verifying the solution is quick and simple.
- **Difficulty Adjustment**: The blockchain dynamically adjusts the difficulty of the puzzle to maintain a consistent block generation time (e.g., ~10 minutes for Bitcoin).
- **Randomness**: The puzzle's randomness ensures that no miner can predict the solution, maintaining fairness.
- **Security**: Hash puzzles prevent malicious actors from easily tampering with the blockchain.

HASH PUZZLES

3. Example of a Hash Puzzle

- In the **Bitcoin blockchain**, the hash puzzle requires miners to find a hash that starts with a specific number of leading zeros.
- **Example:**
  - Block data: `"Transaction data" + Timestamp + Nonce`
  - Hash function: SHA-256
  - Target: A hash that starts with "0000".
- Process:
  - The miner varies the nonce (e.g., 1, 2, 3...) and hashes the block data.
  - For each nonce, the miner calculates
  - CODE: Hash = SHA-256(Block data + Nonce)
  - The miner stops when the hash satisfies the target condition (e.g., starts with "0000").

HASH PUZZLES

4. Importance of Hash Puzzles in Blockchain

- Hash puzzles serve several critical purposes in blockchain technology:
- **Ensuring Security**
  - The computational effort required to solve a hash puzzle makes it prohibitively expensive for attackers to modify past blocks.
  - The immutability of the blockchain is upheld, as changing a single block would require solving the puzzle for all subsequent blocks.
- **Decentralization**
  - Any participant (miner) with sufficient computational resources can attempt to solve the puzzle, ensuring no central authority controls the network.
- **Consensus Mechanism**
  - By solving hash puzzles, miners prove they have expended computational effort, allowing the network to reach consensus on the state of the blockchain.

HASH PUZZLES

4. Importance of Hash Puzzles in Blockchain

- Hash puzzles serve several critical purposes in blockchain technology:
- **Incentive for Miners**
  - Solving the hash puzzle earns the miner a **block reward** (e.g., new cryptocurrency coins) and transaction fees, incentivizing participation in securing the network.

HASH PUZZLES

5. Difficulty Adjustment in Hash Puzzles

- To maintain a consistent block time, blockchains dynamically adjust the difficulty of hash puzzles based on network conditions:
  - If blocks are being mined too quickly, the target is adjusted to make puzzles harder (e.g., requiring more leading zeros).
  - If blocks are being mined too slowly, the target is adjusted to make puzzles easier.

HASH PUZZLES

6. Advantages and Disadvantages of Hash Puzzles

- **Advantages**
  - **Security**: Prevents tampering and double-spending.
  - **Decentralization**: Enables a trustless and distributed consensus mechanism.
  - **Fairness**: Ensures no single miner or group can dominate the system.
- **Disadvantages**
  - **Energy Consumption**: Solving hash puzzles requires significant computational power and electricity.
  - **Scalability**: As network usage grows, solving puzzles can become more resource-intensive.
  - **Specialized Hardware**: Over time, mining has become dominated by powerful ASIC devices, reducing accessibility for casual participants.

HASH PUZZLES

7. Real-World Applications of Hash Puzzles

- Hash puzzles are not limited to blockchains and have broader applications:
- **Blockchain Mining**: Integral to cryptocurrencies like Bitcoin, Litecoin, and Ethereum (before transitioning to Proof of Stake).
- **Cryptographic Security**: Used in securing data transmission and digital signatures.
- **CAPTCHA Systems**: Similar concepts are used in challenges to differentiate humans from bots.
- **Proof-of-Work Systems**: Beyond blockchains, they are used in spam prevention and email security.

HASHES AS ADDRESSES

Hashes as Addresses in Blockchain Technology

- In blockchain technology, **hashes are used to create addresses** that uniquely identify entities such as wallets, transactions, or blocks. These addresses serve as a critical part of the system, enabling secure, efficient, and pseudonymous identification of participants and resources in a decentralized network.

HASHES AS ADDRESSES

1. What is a Hash Address?

- A **hash address** is a unique alphanumeric string generated using cryptographic hash functions (e.g., SHA-256, RIPEMD-160). These addresses represent:
- **Wallet Addresses**: Identifiers for users to send or receive cryptocurrency.
- **Transaction Identifiers (TxID)**: Unique IDs for blockchain transactions.
- **Block Identifiers**: Unique hashes that link blocks in the blockchain

HASHES AS ADDRESSES

2. How Hashes are Used to Create Addresses

- **1. Wallet Addresses**
  - A **wallet address** is derived from a user's **public key** using cryptographic hash functions. The process ensures:
  - **Uniqueness**: Every address is unique and tied to a specific public key.
  - **Security**: Even if someone knows the address, they cannot reverse-engineer the private key.

HASHES AS ADDRESSES

2. How Hashes are Used to Create Addresses

- **Steps to Create a Wallet Address:**
- **Generate a Key Pair**:
  - Public Key: Shared with others.
  - Private Key: Kept secret for signing transactions.
- **Hash the Public Key**:
  - The public key is hashed using **SHA-256.**
- **Apply RIPEMD-160**:
  - The SHA-256 output is further hashed using **RIPEMD-160** to shorten it.
- **Add Checksum and Prefix**:
  - A checksum (hash of the hash) and network-specific prefix (e.g., Bitcoin addresses start with 1) are added.
- **Encode the Address**:
  - The result is encoded using Base58 to create the final address.

HASHES AS ADDRESSES

2. How Hashes are Used to Create Addresses

- **Steps to Create a Wallet Address:**
- **Generate a Key Pair**:
  - Public Key: Shared with others.
  - Private Key: Kept secret for signing transactions.
- **Hash the Public Key**:
  - The public key is hashed using **SHA-256.**
- **Apply RIPEMD-160**:
  - The SHA-256 output is further hashed using **RIPEMD-160** to shorten it.
- **Add Checksum and Prefix**:
  - A checksum (hash of the hash) and network-specific prefix (e.g., Bitcoin addresses start with 1) are added.
- **Encode the Address**:
  - The result is encoded using Base58 to create the final address.

HASHES AS ADDRESSES

2. How Hashes are Used to Create Addresses

2. Transaction Identifiers (TxID)

- Each transaction in the blockchain has a unique **hash** called a **Transaction ID (TxID)**.
- **How It Works:**
  - Combine the transaction data (sender, recipient, amount, timestamp).
  - Apply a cryptographic hash function (e.g., SHA-256).
  - The resulting hash is the TxID.
- **Example**:
  - **Input Data**: `{from: Alice, to: Bob, amount: 1 BTC, timestamp: 2025-01-14}`
  - **TxID**: `3b7c3ba1d2f6c8...`
  - The TxID acts as a unique identifier for the transaction, enabling easy tracking and verification.

HASHES AS ADDRESSES

2. How Hashes are Used to Create Addresses

3. Block Identifiers

Each block in the blockchain is identified by a **block hash**. The block hash links blocks together and ensures immutability.

How It Works:

- The **block header** (previous block hash, Merkle root, timestamp, nonce) is hashed using SHA-256.
- The resulting hash is stored in the next block's header, creating a chain.

Example:

- **Block Data**: `{previous_hash: abc123..., Merkle_root: 987xyz..., nonce: 12345}`
- **Block Hash**: `00000000abc1d...`

HASHES AS ADDRESSES

3. Benefits of Using Hashes as Addresses

1. Security

- Cryptographic hash functions ensure that addresses are tamper-proof and secure.
- It is computationally infeasible to reverse-engineer a private key from a hash address.

2. Uniqueness

- Hashes provide unique identifiers for wallets, transactions, and blocks, avoiding conflicts.

3. Privacy

- Users remain pseudonymous as only their wallet address is visible, not their identity.

4. Efficiency

- Shortened addresses (e.g., RIPEMD-160 output) reduce storage requirements and improve processing speed.

CONSENSUS ALGORITHMS

What is a Consensus Algorithm?

A **consensus algorithm** is a mechanism that ensures all nodes in a blockchain network reach a common agreement on the state of the distributed ledger. It guarantees:

- **Consistency**: All nodes agree on the same version of the blockchain.
- **Trustlessness**: No need for a central authority; trust is established through the algorithm.
- **Fault Tolerance**: The system remains operational even if some nodes fail or act maliciously.

CONSENSUS ALGORITHMS

Consensus algorithms are the foundation of blockchain technology, enabling decentralized networks to function securely and reliably. The choice of algorithm depends on the blockchain's goals:

- **PoW**: High security and decentralization for public blockchains.
- **PoS**: Energy-efficient and faster for scalable applications.
- **PBFT**: Suitable for private, permissioned blockchains.

The evolution of consensus algorithms continues as blockchain technology aims to balance **scalability, security, and decentralization**.

CONSENSUS ALGORITHMS

2. Importance of Consensus in Blockchain

Consensus algorithms are critical because blockchains operate in **decentralized environments**, where:

- **Nodes may not trust each other**.
- There is a risk of **double-spending** (spending the same cryptocurrency twice).
- Participants must agree on the order and validity of transactions.

CONSENSUS ALGORITHMS

3. Common Consensus Algorithms in Blockchain

1. Proof of Work (PoW)
2. Proof of Stake (PoS)
3. Delegated Proof of Stake (DPoS)
4. Proof of Authority (PoA)
5. Practical Byzantine Fault Tolerance (PBFT)
6. Proof of Burn (PoB)
7. Proof of Elapsed Time (PoET)
8. Hybrid Consensus

CONSENSUS ALGORITHMS

1. Proof of Work (PoW)

Description: Miners compete to solve a complex cryptographic puzzle, where the first to solve it gets to add the next block and is rewarded.

- **How It Works**:
  - Miners solve a hash puzzle by varying a **nonce** until the block's hash meets the target condition.
  - The block is broadcasted to the network for validation.
  - Other nodes verify the solution and accept the block if valid.
- **Features**:
  - Computationally intensive.
  - High energy consumption.
- **Examples**:
  - Bitcoin, Litecoin.
- **Advantages**:
  - High security.
  - Decentralized and trustless.
- **Disadvantages**:
  - Inefficient energy usage.
  - Low transaction throughput.

CONSENSUS ALGORITHMS

2. Proof of Stake (PoS)

Description: Validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral.

- **How It Works**:
  - Validators lock up a portion of their cryptocurrency as a stake.
  - The network randomly selects a validator to propose the next block.
  - Other validators verify the block.
- **Features**:
  - Energy-efficient compared to PoW.
  - Incentivizes long-term participation.
- **Examples**:
  - Ethereum 2.0, Cardano, Solana.
- **Advantages**:
  - Low energy consumption.
  - Faster transaction processing.
- **Disadvantages**:
  - Wealth concentration (more coins = higher chances of selection).

CONSENSUS ALGORITHMS

3. Delegated Proof of Stake (DPoS)

Description: Users vote for a small group of delegates who are responsible for validating transactions and creating blocks.

- **How It Works**:
  - Stakeholders vote for delegates using their tokens.
  - Delegates take turns producing blocks.
  - Misbehaving delegates can be voted out.
- **Features**:
  - Governance-driven system.
  - High transaction throughput.
- **Examples**:
  - EOS, Tron.
- **Advantages**:
  - Scalable and efficient.
  - Democratic decision-making.
- **Disadvantages**:
  - Potential for centralization (small group of delegates).

CONSENSUS ALGORITHMS

4. Proof of Authority (PoA)

Description: A limited number of trusted validators are pre-approved to validate transactions and create blocks.

- **How It Works**:
  - Validators are selected based on their reputation and trustworthiness.
  - They take turns validating transactions and adding blocks.
- **Features**:
  - High efficiency and scalability.
  - Suitable for private or consortium blockchains.
- **Examples**:
  - VeChain, Binance Smart Chain.
- **Advantages**:
  - Fast transaction speeds.
  - Low energy consumption.
- **Disadvantages**:
  - Centralized trust in validators.

CONSENSUS ALGORITHMS

5. Practical Byzantine Fault Tolerance (PBFT)

Description: Nodes communicate with each other to agree on the state of the blockchain, tolerating malicious or faulty nodes.

- **How It Works**:
  - A primary node proposes a block.
  - Other nodes validate the block and broadcast their votes.
  - Consensus is reached when a majority (e.g., two-thirds) agree.
- **Features**:
  - Tolerates up to one-third of malicious nodes.
  - High fault tolerance.
- **Examples**:
  - Hyperledger Fabric.
- **Advantages**:
  - Fast finality.
  - High security in closed networks.
- **Disadvantages**:
  - Not scalable for large public networks.

CONSENSUS ALGORITHMS

6. Proof of Burn (PoB)

Description: Validators "burn" (destroy) coins by sending them to an irretrievable address to gain the right to mine or validate blocks.

- **How It Works**:
  - Validators burn coins as proof of commitment.
  - The network selects validators based on the amount burned.
- **Features**:
  - Reduces energy waste compared to PoW.
  - Incentivizes long-term participation.
- **Examples**:
  - Slimcoin.
- **Advantages**:
  - Environmentally friendly.
  - Prevents spam attacks.
- **Disadvantages**:
  - Coin destruction can be wasteful.

CONSENSUS ALGORITHMS

7. Proof of Elapsed Time (PoET)

Description: Nodes wait for a randomly assigned time before creating a block, and the node with the shortest wait time wins.

- **How It Works**:
  - Each node generates a random wait time using trusted hardware.
  - The node with the shortest wait time creates the block.
- **Features**:
  - Low energy consumption.
  - Fair selection process.
- **Examples**:
  - Hyperledger Sawtooth.
- **Advantages**:
  - Efficient and fair.
  - Energy-efficient.
- **Disadvantages**:
  - Relies on trusted hardware (e.g., Intel SGX).

CONSENSUS ALGORITHMS

8. Hybrid Consensus

Description: Combines multiple consensus mechanisms (e.g., PoW + PoS) to balance security, scalability, and decentralization.

- **Examples**:
  - Decred (PoW + PoS).

CONSENSUS ALGORITHMS

4. Comparison of Consensus Algorithms

Algorithm	Energy Efficiency	Scalability	Decentralization	Security	Examples
Proof of Work	Low	Low	High	Very High	Bitcoin, Litecoin
Proof of Stake	High	Medium	Medium	High	Ethereum 2.0, Cardano
Delegated PoS	High	High	Low	Medium	EOS, Tron
Proof of Authority	Very High	Very High	Low	Medium	VeChain, BSC
PBFT	High	Low	Medium	High	Hyperledger Fabric
Proof of Burn	High	Medium	Medium	High	Slimcoin
PoET	Very High	High	Medium	Medium	Hyperledger Sawtooth

CONSENSUS ALGORITHMS

5. Challenges of Consensus Algorithms

- **Energy Consumption**: PoW systems consume enormous amounts of energy.
- **Centralization Risks**: PoS and DPoS systems can concentrate power among wealthy or voted entities.
- **Scalability**: Many algorithms struggle to scale for high transaction volumes.
- **Security**: Some algorithms are vulnerable to attacks (e.g., 51% attack in PoW).

OVERVIEW OF BLOCKCHAIN

UNIT 2

BITCOIN CRYPTOCURRENCY

1. What is Bitcoin Mining?

Bitcoin mining is the process of validating transactions and adding new blocks to the **Bitcoin blockchain** by solving complex cryptographic puzzles. It plays a crucial role in maintaining the security, decentralization, and integrity of the Bitcoin network.

Mining involves:

- **Solving a cryptographic puzzle** using computational power.
- **Verifying Bitcoin transactions** to prevent double-spending.
- **Adding new blocks** to the blockchain.
- **Earning Bitcoin rewards** as an incentive for miners.

BITCOIN CRYPTOCURRENCY

2. Why is Bitcoin Mining Important?

Bitcoin mining is essential for the **security and decentralization** of the network. Its key functions include:

- **Transaction Verification**: Ensures that Bitcoin transactions are legitimate and prevents fraudulent activities.
- **Network Security**: Protects against attacks by requiring computational effort to add blocks.
- **Decentralization**: Eliminates the need for a central authority by distributing control among miners.
- **New Bitcoin Creation**: Introduces new Bitcoin into circulation as block rewards.
- **Preventing Double-Spending**: Ensures that each Bitcoin can only be spent once.

BITCOIN CRYPTOCURRENCY

BITCOIN CRYPTOCURRENCY

3. How Bitcoin Mining Works

Bitcoin mining follows the **Proof of Work (PoW)** consensus mechanism. The process involves the following steps:

Step 1: Transaction Broadcast

- Bitcoin users initiate transactions.
- Transactions are broadcasted to the Bitcoin network and collected in a **mempool**.

BITCOIN CRYPTOCURRENCY

3. How Bitcoin Mining Works

Step 2: Creating a New Block

- Miners collect pending transactions and form a **candidate block**.
- A block contains:
  - Transaction data
  - Timestamp
  - Previous block hash
  - Nonce (a random number)
  - Merkle root (hash of all transactions in the block)

BITCOIN CRYPTOCURRENCY

3. How Bitcoin Mining Works

Step 3: Proof of Work (PoW) - Solving the Cryptographic Puzzle

- Miners compete to find a **valid hash** that meets the network's difficulty target.
- The hash must be **less than or equal to** a target value (e.g., starting with a certain number of zeros).
- Miners vary the **nonce** and repeatedly hash the block header until they find a valid solution.

BITCOIN CRYPTOCURRENCY

3. How Bitcoin Mining Works

Step 4: Block Validation and Addition to the Blockchain

- The first miner to find a valid hash broadcasts it to the network.
- Other nodes verify the solution.
- If the solution is correct, the new block is added to the blockchain.

BITCOIN CRYPTOCURRENCY

3. How Bitcoin Mining Works

Step 5: Reward Distribution

- The successful miner receives a **block reward** (newly minted Bitcoin) plus **transaction fees** from included transactions.