UNIT 2 BLOCKCHAIN

1. Public-Key Cryptography:

- Based on the principle of mathematical one-way functions.
- Uses two different keys: a public key and a private key.
- The public key is used for encryption, while the private key is used for decryption.
- Enables secure communication and data exchange over insecure channels.
- Widely used in digital signatures, encryption, and key exchange protocols.
- Relies on the computational difficulty of certain mathematical problems, such as integer factorization or discrete logarithms.
- Popular algorithms include RSA, Diffie-Hellman, and Elliptic Curve Cryptography (ECC).
- Allows for non-repudiation, ensuring that the sender cannot deny having sent the message.
- Provides authentication, ensuring that the message originated from the claimed sender.
- Enables key distribution and management without the need for a secure channel.

2. Public Key and Private Key Combinations in Blockchain Security:

- Blockchain uses public-key cryptography for secure transactions and data integrity.
- Each user has a unique pair of public and private keys.
- The public key is derived from the private key and serves as the user's address on the blockchain.
- Transactions are digitally signed using the user's private key, ensuring authentication and non-repudiation.
- Signed transactions are broadcast to the network and verified using the corresponding public key.
- Private keys must be kept secure and never shared, as they control access to the user's blockchain assets.
- If a private key is lost or compromised, the associated assets become inaccessible.
- Public keys can be safely shared and used to receive transactions.

- Key management and secure storage of private keys are crucial for blockchain security.
- Multi-signature wallets and hardware wallets provide additional security for private key storage.

3. Hashing:

- Hashing is the process of mapping data of arbitrary size to a fixed-size output, called a hash or digest.
- Cryptographic hash functions are one-way functions, making it computationally infeasible to reconstruct the original data from the hash.
- Hash functions are deterministic, meaning that the same input will always produce the same output hash.
- Even a slight change in the input data results in a completely different hash value.
- Hashes are used for data integrity verification, digital signatures, and secure password storage.
- Popular hash functions include SHA-256, SHA-3, and BLAKE2.
- Blockchain uses hashing to link blocks together and ensure data integrity.
- Each block contains the hash of the previous block, forming an immutable chain.
- Modifying data in a previous block would invalidate all subsequent blocks due to the hash chain.
- Hash functions play a critical role in the consensus mechanisms of blockchains, ensuring tamper-resistance and transparency.

4. Transaction Integrity:

- Transaction integrity is crucial for maintaining the security and trust in blockchain systems.
- Digital signatures using public-key cryptography ensure transaction authenticity and non-repudiation.
- Transactions are broadcast to the network and verified by all nodes before being included in a block.
- Each transaction includes the sender's public key, ensuring that only the owner with the corresponding private key could have initiated the transaction.

- Transactions are hashed and included in a Merkle tree structure within each block.
- The Merkle root hash represents all transactions in the block and is included in the block header.
- Any modification to a transaction would result in a different Merkle root hash, invalidating the block and all subsequent blocks.
- Transaction integrity is maintained through the immutable and tamper-evident nature of the blockchain.
- Double-spending is prevented by the consensus mechanism and the shared ledger maintained by all nodes.
- Transaction integrity is essential for ensuring the reliability and trustworthiness of blockchain-based systems.

5. Securing Blockchain:

- Blockchain security relies on a combination of cryptographic techniques, decentralization, and consensus mechanisms.
- Public-key cryptography and digital signatures ensure secure transactions and user authentication.
- Hashing and Merkle trees provide data integrity and tamper-resistance.
- Decentralization and distributed consensus mechanisms prevent single points of failure or control.
- Proof-of-Work (PoW) and Proof-of-Stake (PoS) are popular consensus algorithms that secure the blockchain network.
- Node diversity and geographical distribution increase the resilience and security of the network.
- Smart contract security is crucial to prevent vulnerabilities and ensure the integrity of decentralized applications (DApps).
- Secure key management and storage are essential for protecting user assets and maintaining control over blockchain addresses.
- Blockchain networks should implement robust access control mechanisms and permissions management.
- Continuous monitoring, auditing, and security updates are necessary to address emerging threats and vulnerabilities.