Blockchain Technology – Exam Notes

Benefits and Limitations of Blockchain

Benefits: Decentralization, Transparency, Security, Traceability, Reduced costs.
Limitations: High energy use, Scalability issues, Data immutability, High storage needs.

Role of Cryptography in Blockchain Transactions

Hashing for immutability, Digital Signatures for authenticity, Encryption for confidentiality, Verification of transactions.

Hyperledger & Hyperledger Fabric

Hyperledger: Open-source blockchain by Linux Foundation.
Hyperledger Fabric: Framework with permissioned blockchain, channels, modular design. Used in supply chain, banking, healthcare.

Digital Money

Money in electronic form.
Examples: Cryptocurrencies (Bitcoin, Ethereum), CBDCs (e-rupee), Mobile wallets (Paytm, Google Pay), Online banking.

Blockchain – Centralized, Decentralized, Distributed

Blockchain: Distributed ledger linking blocks with cryptographic hashes.
Centralized: Single authority controls data.
Decentralized: Multiple nodes share control.
Distributed: Data stored across many nodes for redundancy.

Hashing & SHA-256

Hashing: Converts input into fixed-length hash.
SHA-256: Produces 256-bit hash, irreversible, deterministic, collision-resistant.
Example: 'Hello' → 185f8db32271fe25f561a6fc938b2e264306ec304eda518007d1764826381969

Public-Key Cryptography

Uses public & private keys.
Encryption with public key, decryption with private key.
Digital signatures: sender signs with private key, verified with public key.
Applications: Secure transactions, identity verification.

Smart Contracts – Applications, Advantages & Disadvantages

Smart Contracts: Self-executing contracts on blockchain.
Applications: Finance, Supply chain, Real estate, Insurance.

Advantages: No intermediaries, Transparent, Fast & cost-effective.
Disadvantages: Code bugs irreversible, Legal issues, Security risks.

Ethereum Virtual Machine (EVM)

Runtime environment for Ethereum smart contracts.
Turing complete, executes bytecode, ensures consensus across nodes.

Bitcoin – Working Mechanism

First cryptocurrency.
Block = Header (previous hash, Merkle root, timestamp, nonce) + Body (transactions).
Process: User signs transaction → broadcast → miners validate with Proof-of-Work → block added.

Consensus Mechanism (PoW vs PoS)

PoW: Miners solve puzzles, secure but energy-intensive.
PoS: Validators chosen by stake, energy-efficient.

Digital Signatures in Blockchain

Authenticate sender's identity.
Example: Alice signs Bitcoin transaction with private key, verified by public key.

Merkle Trees

Binary tree of hashes.
Leaves = transaction hashes, non-leaves = hash of children.
Root hash = represents all transactions in block.