Question No. 1.

Differentiate between any Bitcoin and Ethereum in terms of their design features e.g., cryptography, block size, consensus algorithms etc.

Bitcoin vs. Ethereum: Design Features Comparison

Feature	Bitcoin	Ethereum
Purpose	Digital currency for peer-to-peer transactions	Decentralized platform for smart contracts and DApps
Consensus Algorithm	Proof of Work (PoW) using SHA-256	Initially PoW, transitioned to Proof of Stake (PoS) with Ethereum 2.0
Block Time	~10 minutes	~12–15 seconds
Block Size	1 MB per block	Flexible block size based on gas limit
Cryptographic Algorithm	SHA-256	Keccak-256 (SHA-3 variant)
Smart Contract Capability	Limited scripting functionality	Supports Turing-complete smart contracts via EVM
Transaction Fees	Based on transaction size and network congestion	Dynamic gas fee model based on computational complexity and network demand
Development Focus	Secure and decentralized store of value	World computer supporting decentralized applications and DeFi

Reference:

Investopedia - Bitcoin vs. Ethereum

Question No. 2.

What is meant by double-spending problem and how it is addressed by the blockchain technology?

The double-spending problem occurs when a digital currency is spent more than once due to the ease of copying digital information. Unlike physical cash, digital currencies require a mechanism to prevent fraudulent duplication.

How Blockchain Prevents Double-Spending

1. **Decentralized Ledger:**
   - Blockchain records all transactions publicly, making fraud difficult.
2. **Consensus Mechanism:**
   - Algorithms like Proof of Work (PoW) or Proof of Stake (PoS) validate transactions before adding them to the blockchain.
3. **Cryptographic Security:**
   - Each block links to the previous one, making alterations nearly impossible.
4. **Transaction Confirmation:**
   - Multiple confirmations ensure a transaction is legitimate and irreversible.
5. **Mining Process:**
   - Miners verify transactions, preventing duplication and ensuring integrity.

Conclusion

Blockchain prevents double-spending using decentralization, cryptographic security, and consensus mechanisms, ensuring secure and transparent digital transactions.

Reference:

Investopedia - Double-Spending