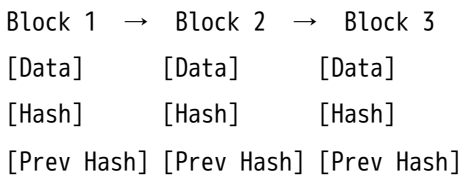
Blockchain Unit-1: Important Questions Detailed Exam Answers

1. Blockchain Features ⭐

Definition

Blockchain is a **decentralized and distributed digital ledger** that stores data in blocks connected using cryptographic hashes.

Diagram



Main Features

Feature	Explanation
Decentralization	No single authority controls the system
Distributed Ledger	Same copy of data is stored on many computers
Transparency	Transactions can be verified by participants
Immutability	Once data is added, it is very difficult to change
Security	Uses hashing, cryptography and digital signatures
Consensus	All nodes agree before adding a new block

Real-Life Example

Like a shared register where every student has the same copy. If one student changes something secretly, others can detect it.

Conclusion

Blockchain is secure, transparent and tamper-resistant, so it is used in cryptocurrency, banking, supply chain and smart contracts.

---

2. Bitcoin Working ⭐

Definition

Bitcoin is the first decentralized cryptocurrency that uses blockchain for secure peer-to-peer digital payments.

Diagram

```
Sender → Transaction → Bitcoin Network → Verification → Block → Blockchain → Receiver
```

Working Steps

1. **Transaction Creation**
   A user creates a transaction to send Bitcoin to another user.
2. **Broadcasting**
   Transaction is sent to the Bitcoin network.
3. **Verification**
   Network nodes check sender balance and digital signature.
4. **Mining**
   Miners solve a mathematical puzzle using Proof of Work.
5. **Block Creation**
   Verified transactions are added into a block.

6. **Block Added to Blockchain**

   After consensus, block becomes permanent part of blockchain.

Advantages

- No bank required
- Secure transactions
- Global transfer possible
- Transparent public ledger

Disadvantages

- Price changes quickly
- High energy consumption
- Transaction speed can be slow

Conclusion

Bitcoin proves that digital money can work without banks using blockchain and cryptographic security.

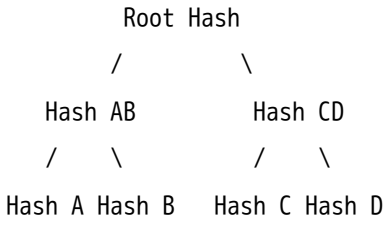
---

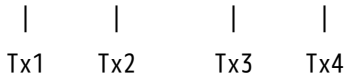
3. Merkle Tree ⭐

Definition

Merkle Tree is a tree-like data structure used in blockchain to verify transactions efficiently using hash values.

Diagram





Easy Explanation

Instead of checking all transactions one by one, blockchain checks only hash paths. This makes verification fast.

Working

1. Each transaction is converted into a hash.
2. Two transaction hashes are combined and hashed again.
3. This continues until one final hash is formed.
4. Final hash is called **Merkle Root**.

Advantages

- Fast transaction verification
- Saves storage
- Detects tampering easily
- Used in Bitcoin blocks

Conclusion

Merkle Tree improves blockchain efficiency and security by verifying large numbers of transactions quickly.

---

4. Hash Function ⭐

Definition

A cryptographic hash function converts input data into a fixed-size output called a hash value.

Example

```
Input: Hello
Hash: 185f8db32271fe25...

Input: hello
Hash: 2cf24dba5fb0a...
```

Small change in input creates a completely different hash.

Properties of Hash Function

Property	Meaning
Deterministic	Same input always gives same hash
Fixed Length	Output size remains fixed
Fast Computation	Hash is quickly generated
One-Way	Original data cannot be found from hash
Collision Resistant	Two inputs should not give same hash
Avalanche Effect	Small input change creates big output change

Use in Blockchain

- Links blocks
- Detects tampering
- Creates Merkle Tree
- Secures transactions

Conclusion

Hash function acts as a digital fingerprint and makes blockchain tamper-resistant.

---

5. Public vs Private Blockchain ⭐

Difference Table

Basis	Public Blockchain	Private Blockchain
Access	Open to everyone	Restricted users only
Control	Decentralized	Controlled by organization
Speed	Slower	Faster
Transparency	Very high	Limited
Security	Strong due to many nodes	Controlled security
Example	Bitcoin, Ethereum	Hyperledger, banking blockchain

Public Blockchain

A public blockchain allows anyone to join, read, write and verify transactions.

Private Blockchain

A private blockchain allows only selected and authorized users to participate.

Diagram

```
Public Blockchain:
Anyone → Join → Verify → Add Transactions

Private Blockchain:
Authorized User → Permission → Access Network
```

Conclusion

Public blockchain is best for open systems like cryptocurrency, while private blockchain is best for business and banking applications.

---

6. Smart Contracts ⭐

Definition

Smart contract is a self-executing digital contract where conditions are written in code and executed automatically.

Diagram

```
Condition Satisfied → Smart Contract Executes → Result Generated
```

Example

If payment is successful, then ticket is automatically booked.

```
IF payment received
THEN issue ticket
```

Features

- Automatic execution
- No middleman
- Secure
- Transparent
- Time-saving

Applications

- Insurance claim
- Banking
- Real estate
- Supply chain
- Online voting

Advantages

- Reduces cost
- Avoids fraud
- Fast processing
- No third-party dependency

Disadvantages

- Coding error can cause loss
- Difficult to change after deployment
- Legal acceptance is still developing

Conclusion

Smart contracts make agreements automatic, secure and trustworthy without middlemen.

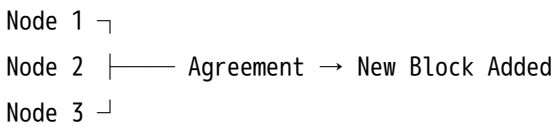
---

7. Distributed Consensus ⭐

Definition

Distributed consensus is a process where all nodes in a blockchain network agree on the same valid transaction or block.

Diagram



Need of Consensus

Blockchain has no central authority, so nodes must agree before adding data.

Popular Consensus Mechanisms

Mechanism	Explanation
Proof of Work	Miners solve puzzle
Proof of Stake	Validator selected based on stake
Practical Byzantine Fault Tolerance	Nodes vote to reach agreement

Advantages

- Prevents fraud
- Avoids double spending
- Maintains trust
- Keeps all copies same

Conclusion

Consensus is the heart of blockchain because it allows trust in a decentralized network.

---

8. Digital Signature ⭐

Definition

Digital signature is a cryptographic method used to prove the identity of sender and ensure message integrity.

Diagram

```
Sender:
Message + Private Key → Digital Signature

Receiver:
Message + Signature + Public Key → Verification
```

Working

1. Sender creates message.
2. Sender signs message using private key.
3. Receiver verifies signature using sender’s public key.
4. If verification succeeds, message is genuine.

Provides

Security Property	Meaning
Authentication	Sender is real
Integrity	Message not changed
Non-repudiation	Sender cannot deny sending

Conclusion

Digital signature is very important in blockchain because it verifies ownership and prevents fake transactions.

---

9. Security Aspects of Blockchain ⭐

Main Security Techniques

Technique	Role
Hashing	Protects block data
Digital Signature	Verifies sender
Public Key Cryptography	Secures identity
Consensus	Prevents fake blocks
Decentralization	Removes single point failure

Common Attacks

Attack	Meaning
51% Attack	Attacker controls majority network power
Double Spending	Same cryptocurrency spent twice

Attack	Meaning
Sybil Attack	One attacker creates many fake identities
Smart Contract Bugs	Coding errors in contract

Diagram

```
Hashing + Digital Signature + Consensus + Decentralization
                          ↓
                Secure Blockchain
```

Conclusion

Blockchain is secure because it combines cryptography, consensus and decentralization.

---

10. Public Key Cryptography ⭐

Definition

Public key cryptography is an encryption technique that uses two keys: public key and private key.

Keys

Key	Use
Public Key	Shared with everyone
Private Key	Kept secret by owner

Diagram

```
Public Key  → Used for encryption / verification
Private Key → Used for decryption / signing
```

Example

In blockchain, a user signs a transaction using private key, and others verify it using public key.

Advantages

- Secure communication
- Supports digital signature
- No need to share private key
- Useful in blockchain wallets

Conclusion

Public key cryptography protects blockchain users and ensures secure transactions.

---

11. Permissioned Blockchain ⭐

Definition

Permissioned blockchain is a blockchain where only authorized users can join and perform activities.

Features

- Controlled access
- Faster transaction speed
- Better privacy
- Suitable for organizations

Example

Banks using blockchain for internal transaction records.

Diagram

```
User Request → Permission Check → Access Granted → Blockchain Network
```

Advantages

- High privacy
- Faster performance
- Better management
- Suitable for business use

Disadvantages

- Less decentralized
- Controlled by authority
- Less transparent than public blockchain

Conclusion

Permissioned blockchain is useful where privacy, speed and control are more important than full decentralization.

---

12. Hash Pointer ⭐

Definition

Hash pointer is a pointer that stores the address of data along with the hash of that data.

Diagram

```
Hash Pointer
   |
   |---- Address of Data
   |---- Hash of Data
```

Use in Blockchain

Each block contains hash pointer to previous block.

```
Block 2 → Hash Pointer → Block 1
Block 3 → Hash Pointer → Block 2
```

Advantage

If previous block data changes, hash changes immediately. This helps detect tampering.

Conclusion

Hash pointer connects blocks securely and makes blockchain immutable.

---

13. Cryptocurrency Basics ⭐

Definition

Cryptocurrency is a digital currency secured by cryptography and operated on blockchain.

Examples

- Bitcoin
- Ethereum
- Litecoin

Features

- Digital form
- Decentralized
- Secure

- Peer-to-peer transfer
- Based on blockchain

Difference Between Cryptocurrency and Blockchain

Blockchain	Cryptocurrency
Technology	Application of technology
Stores records	Used as digital money
Example: Ethereum blockchain	Example: Ether coin

Conclusion

Cryptocurrency is one of the most popular applications of blockchain technology.

⭐ Best 7-Mark Answer Structure

```
1. Definition
2. Diagram
3. Explanation / Working
4. Features
5. Advantages / Applications
6. Conclusion
```

⭐ Best 14-Mark Answer Structure

```
1. Introduction
2. Definition
3. Neat diagram
4. Detailed working
5. Important features
```

6. Advantages
7. Disadvantages
8. Applications
9. Conclusion

🔥 Last Night Priority Order

1. Blockchain features
2. Bitcoin working
3. Hash function
4. Merkle Tree
5. Public vs Private Blockchain
6. Smart Contracts
7. Digital Signature
8. Distributed Consensus
9. Public Key Cryptography
10. Permissioned Blockchain