UNIT–2 : Understanding Blockchain with Cryptocurrency (Bitcoin)

⭐ Introduction to Bitcoin and Blockchain

Definition

Bitcoin is a decentralized digital cryptocurrency that works on Blockchain technology.

Blockchain is a distributed ledger that stores Bitcoin transactions securely in blocks.

Easy Explanation

Normally banks manage money transfers.

But in Bitcoin:

- No bank exists
- No central authority exists
- Computers around the world verify transactions

Blockchain keeps all records permanently.

Real-Life Example

Suppose:

- A sends ₹500 to B using UPI
- Bank verifies transaction

In Bitcoin:

- Network computers verify transaction instead of bank

⭐ Relationship Between Bitcoin and Blockchain

```
Blockchain = Technology
Bitcoin = Application of Blockchain
```

⭐ Creation of Coins (Bitcoin Mining)

Definition

Creation of new bitcoins is called Bitcoin Mining.

Miners solve complex mathematical problems and receive bitcoins as reward.

Easy Explanation

Mining means:

- Computers solve puzzles
- After solving puzzle:
  - New block added
  - Miner gets reward

Diagram

```
Transactions → Verification → Puzzle Solving → New Block → Reward
```

Mining Reward

Earlier:

- 50 BTC per block

Now:

- Reward decreases after fixed intervals (Halving)

Advantages

- Maintains network security
- Creates new coins
- Verifies transactions

Disadvantages

- High electricity consumption
- Requires expensive hardware

Conclusion

Mining is the backbone of Bitcoin because it secures the blockchain and generates new bitcoins.

⭐ Payments and Double Spending

Definition

Double spending means spending the same cryptocurrency more than once.

Easy Explanation

Digital currency can be copied easily.

Problem:

- A sends same Bitcoin to two people simultaneously.

Blockchain prevents this fraud using consensus and verification.

Example

```
A has 1 Bitcoin

A sends same Bitcoin to:
→ B
→ C

This is Double Spending
```

Prevention of Double Spending

Blockchain prevents this by:

- Transaction verification
- Consensus mechanism
- Timestamping
- Proof of Work

Diagram

```
Transaction → Verification → Consensus → Valid Transaction
```

Advantages of Prevention

- Stops fraud
- Ensures trust
- Secures digital payments

Conclusion

Double spending problem is solved using blockchain verification and consensus algorithms.

⭐ Bitcoin Scripts

Definition

Bitcoin Script is a simple programming language used in Bitcoin transactions.

Easy Explanation

It defines:

- Rules for spending bitcoins
- Conditions for transaction validation

Example

```
IF signature valid
THEN release payment
```

Features

Feature	Description
Stack-based	Uses stack operations
Simple	Limited instructions
Secure	Prevents malicious code

Uses

- Multi-signature transactions
- Smart contracts
- Payment validation

Advantages

- Secure transactions
- Flexible payment conditions

Disadvantages

- Limited functionality
- Less powerful than Ethereum smart contracts

Conclusion

Bitcoin Script controls how bitcoins can be spent securely.

⭐ Bitcoin P2P Network

Definition

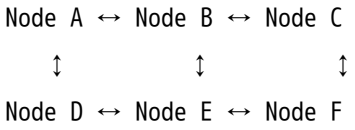
Bitcoin works on a Peer-to-Peer (P2P) network where computers communicate directly without central server.

Easy Explanation

In P2P:

- Every node is equal
- No central authority exists
- Nodes share transaction information directly

Diagram



Features

- Decentralized
- Distributed
- Fault tolerant
- Secure

Advantages

- No central failure
- High transparency
- Better security

Disadvantages

- Slower communication sometimes
- Large bandwidth usage

Conclusion

Bitcoin P2P network allows decentralized communication and transaction sharing.

⭐ Transaction in Bitcoin Network

Definition

Bitcoin transaction means transfer of bitcoins from one user to another.

Transaction Process

Step 1: Transaction Creation

Sender creates transaction.

Step 2: Digital Signature

Sender signs transaction using private key.

Step 3: Broadcasting

Transaction sent to network.

Step 4: Verification

Nodes verify transaction.

Step 5: Block Addition

Verified transaction added to block.

Step 6: Confirmation

Block added into blockchain.

Diagram

```
Sender
   ↓
Transaction Creation
   ↓
Broadcast to Network
   ↓
Verification
   ↓
Block Creation
   ↓
Blockchain
```

Advantages

- Secure
- Transparent

- Immutable

Conclusion

Bitcoin transactions are verified and permanently stored using blockchain.

⭐ Block Mining

Definition

Block mining is the process of validating transactions and adding new blocks to blockchain.

Easy Explanation

Miners:

- Collect transactions
- Solve mathematical puzzle
- Add block to blockchain

Mining Process

1. Transactions collected
2. Block created
3. Puzzle solved
4. Consensus achieved
5. Block added
6. Reward received

Diagram

```
Transactions → Block → Puzzle → Solution → Blockchain
```

Types of Mining

Type	Description
CPU Mining	Uses processor
GPU Mining	Uses graphics card
ASIC Mining	Uses special hardware
Cloud Mining	Mining through online service

Advantages

- Network security
- Transaction verification

Disadvantages

- Energy consumption
- Expensive hardware

Conclusion

Mining maintains blockchain security and creates trust in Bitcoin network.

⭐ Block Propagation and Block Relay

Definition

Block propagation is the process of spreading newly mined blocks across the Bitcoin network.

Easy Explanation

When miner creates block:

- It sends block to nearby nodes
- Those nodes forward it further
- Entire network gets updated

Diagram

```
Miner → Node A → Node B → Node C
```

Importance

- Keeps blockchain synchronized
- Prevents conflicts
- Maintains consistency

Conclusion

Block relay ensures all nodes maintain same blockchain copy.

UNIT–2 PART–2 : Working with Consensus in Bitcoin

⭐ Distributed Consensus in Open Environment

Definition

Distributed consensus means all nodes agree on one valid blockchain state without central authority.

Easy Explanation

Since blockchain is public:

- Anyone can join
- Nodes may not trust each other

Consensus ensures everyone agrees on valid transactions.

Need of Consensus

- Prevent fraud
- Avoid double spending
- Maintain trust

Conclusion

Consensus is essential for decentralized blockchain systems.

⭐ Consensus in Bitcoin Network

Definition

Bitcoin uses Proof of Work consensus mechanism to agree on valid blocks.

Working

1. Miner creates block
2. Miner solves puzzle
3. Other nodes verify solution
4. Block accepted by majority

Diagram

```
Miner → Solve Puzzle → Verification → Block Accepted
```

Advantages

- Strong security
- Prevents fake blocks

Conclusion

Consensus ensures all nodes maintain same valid blockchain.

⭐ Proof of Work (PoW)

Definition

Proof of Work is a consensus mechanism where miners solve difficult mathematical puzzles.

Easy Explanation

Computers compete to solve puzzle.

Winner:

- Adds block
- Gets reward

Diagram

```
Miner → Solve Hash Puzzle → Add Block → Reward
```

Advantages

- Very secure
- Prevents attacks

Disadvantages

- High energy use
- Slow process

Conclusion

PoW provides security but consumes large computational power.

⭐ HashCash PoW

Definition

HashCash is the original Proof of Work system used to reduce spam and later adopted in Bitcoin.

Working

- System finds hash with specific number of leading zeros.

Example:

```
00000ABCD123...
```

Importance

- Foundation of Bitcoin mining
- Makes mining difficult

⭐ Bitcoin PoW

Definition

Bitcoin PoW uses SHA-256 hashing algorithm for mining blocks.

Working

Miner repeatedly changes nonce value until valid hash is found.

Diagram

```
Block Data + Nonce → SHA-256 Hash
```

Goal

Find hash smaller than target value.

⭐ Attacks on PoW and Monopoly Problem

1. 51% Attack

Definition

If attacker controls more than 50% mining power, it can manipulate blockchain.

Effects

- Double spending
- Block manipulation
- Transaction reversal

---

2. Monopoly Problem

Definition

Large mining pools may dominate mining process.

Problems

- Centralization
- Reduced fairness
- Security risk

Conclusion

PoW is secure but large mining power concentration can create risks.

⭐ Proof of Stake (PoS)

Definition

PoS selects validators based on amount of cryptocurrency they own.

Easy Explanation

More coins = Higher chance to validate block.

Advantages

- Low energy consumption
- Faster than PoW

Disadvantages

- Rich users get more power

Conclusion

PoS is energy-efficient alternative to PoW.

⭐ Proof of Burn (PoB)

Definition

Users permanently destroy coins to gain mining rights.

Easy Explanation

Burning coins shows commitment to network.

Advantage

- Saves energy

Disadvantage

- Permanent loss of coins

⭐ Proof of Elapsed Time (PoET)

Definition

PoET selects miner randomly after waiting for random time.

Working

- Every node waits random time
- Shortest waiting node wins

Advantages

- Low energy consumption
- Fair selection

Used In

Hyperledger Sawtooth

⭐ Life of a Bitcoin Miner

Steps

1. Receive transactions
2. Verify transactions
3. Create block
4. Solve puzzle
5. Broadcast block
6. Receive reward

Diagram

```
Transactions → Verification → Mining → Block → Reward
```

⭐ Mining Difficulty

Definition

Mining difficulty controls how hard it is to mine a block.

Easy Explanation

If miners increase:

- Difficulty increases

If miners decrease:

- Difficulty decreases

Purpose

Maintain average block creation time (~10 minutes).

⭐ Mining Pool

Definition

Mining pool is a group of miners combining computational power together.

Easy Explanation

Instead of mining alone:

- Miners work together

- Share rewards

Advantages

- Higher success chance
- Stable income

Disadvantages

- Centralization risk

🔥 MOST IMPORTANT QUESTIONS

⭐ 7-Mark Questions

1. Explain Bitcoin P2P Network.
2. Explain Bitcoin transaction process.
3. Explain Proof of Work.
4. Explain Mining Difficulty.
5. Explain Mining Pool.
6. Explain Double Spending problem.
7. Explain Bitcoin Scripts.
8. Explain Proof of Stake.
9. Explain Block Mining.
10. Explain Block Propagation.

⭐ 14-Mark Questions

1. Explain Bitcoin architecture and working in detail.

2. Explain transaction processing in Bitcoin network.
3. Explain Proof of Work with mining process.
4. Explain attacks on PoW and monopoly problem.
5. Explain different consensus mechanisms.
6. Explain distributed consensus in open environment.
7. Explain Bitcoin mining and mining difficulty.
8. Explain Bitcoin P2P network with diagram.

🎯 PYQ-Based Expected Questions

⭐ Very Important

- Bitcoin transaction processing
- Proof of Work
- Mining
- Double Spending
- Consensus
- Bitcoin P2P Network

⭐ High Probability

- Mining Pool
- Mining Difficulty
- PoS vs PoW
- Block propagation

⭐ Medium Probability

- Proof of Burn
- Proof of Elapsed Time
- Bitcoin Scripts

⚡ One-Night Revision Notes

Topic	Keyword
Bitcoin	Cryptocurrency
PoW	Mining Puzzle
Mining	Block Validation
PoS	Stake-based Validation
Double Spending	Fraud Prevention
Consensus	Agreement
Mining Pool	Group Mining

📌 Smart Study Plan

First Priority

✅ Bitcoin Working
✅ Transactions
✅ Proof of Work
✅ Mining

Second Priority

✅ Consensus
✅ Double Spending
✅ Mining Pool
✅ Mining Difficulty

Last Revision

✅ Definitions
✅ Diagrams
✅ Advantages
✅ PYQs

🧠 Golden Exam Writing Trick

For every blockchain answer:

```
Definition
↓
Diagram
↓
Working Steps
↓
Advantages
↓
Applications
↓
Conclusion
```

This structure gives maximum marks in RGPV exams.