Blockchain Unit-2: PYQ-Based Ready-to-Write Answers

1. Bitcoin Transaction Processing ⭐

Introduction

Bitcoin transaction processing means transferring bitcoin from one user to another without any bank. It is verified by network nodes and miners.

Definition

Bitcoin transaction processing is the process of creating, verifying, broadcasting and adding a Bitcoin transaction into the blockchain.

Why It Is Needed

It is needed to:

- Transfer bitcoin securely
- Prevent fraud
- Prevent double spending
- Maintain public ledger

Working / Steps

1. **Transaction Creation**
   Sender creates a transaction using wallet.
2. **Digital Signature**
   Sender signs transaction using private key.
3. **Broadcasting**
   Transaction is sent to Bitcoin P2P network.

4. **Verification by Nodes**

   Nodes check:

   - Sender balance
   - Valid digital signature
   - Transaction format

5. **Mining**

   Miners collect valid transactions into a block.

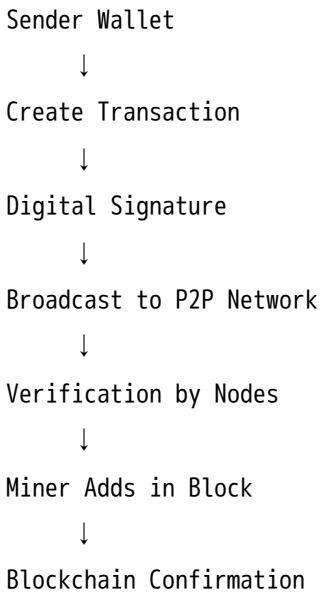
6. **Block Added to Blockchain**

   Miner solves Proof of Work puzzle and adds block.

7. **Confirmation**

   Transaction becomes confirmed after block addition.

Diagram



Real-Life Analogy

Like UPI payment, but instead of bank verification, Bitcoin network verifies payment.

Advantages

- No bank required
- Secure
- Transparent
- Permanent record

Disadvantages

- Slower than UPI
- Transaction fee may vary
- Requires internet

Important Keywords

Digital Signature, P2P Network, Miner, Verification, Blockchain, Confirmation

Conclusion

Bitcoin transaction processing allows secure peer-to-peer digital payment without central authority.

---

2. Proof of Work (PoW) ⭐

Definition

Proof of Work is a consensus mechanism where miners solve a difficult mathematical puzzle to add a new block to blockchain.

Easy Explanation

Miners compete to find a correct hash. The first miner who finds it gets chance to add block and receive reward.

Why It Is Needed

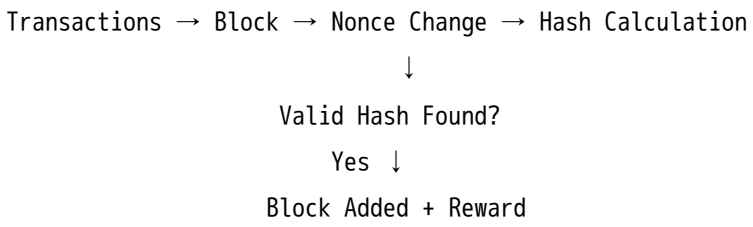
PoW is needed to:

- Secure blockchain
- Prevent fake blocks
- Prevent double spending
- Make attack expensive

Working

1. Miner collects transactions.
2. Miner creates candidate block.
3. Miner changes nonce again and again.
4. Hash is calculated.
5. If hash satisfies target, block is valid.
6. Other nodes verify block.
7. Block is added to blockchain.

Diagram



Example

Bitcoin uses SHA-256 hashing in Proof of Work.

Advantages

- Very secure
- Prevents fraud
- Fully decentralized
- Tested in Bitcoin

Disadvantages

- High electricity consumption
- Expensive hardware
- Slow process

Important Keywords

Nonce, Hash, Target, Miner, SHA-256, Consensus, Block Reward

Conclusion

Proof of Work gives strong security to Bitcoin but consumes high computation power.

---

3. Mining ⭐

Definition

Mining is the process of validating transactions and adding new blocks to the blockchain by solving Proof of Work puzzle.

Easy Explanation

Miners are like accountants of Bitcoin network. They verify transactions and maintain blockchain.

Why It Is Needed

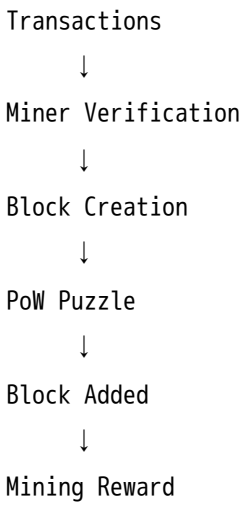
Mining is needed for:

- Transaction verification
- New block creation
- Bitcoin creation
- Network security

Mining Process

1. Miner receives transactions.
2. Miner verifies transactions.
3. Miner creates block.
4. Miner solves PoW puzzle.
5. Miner broadcasts block.
6. Network verifies block.
7. Miner receives reward.

Diagram



Types of Mining

Type	Explanation
CPU Mining	Mining using processor
GPU Mining	Mining using graphics card
ASIC Mining	Special mining hardware
Cloud Mining	Mining through rented online power
Pool Mining	Group of miners work together

Advantages

- Secures Bitcoin network

- Validates transactions
- Creates new bitcoins

Disadvantages

- High cost
- High electricity use
- Hardware requirement

Conclusion

Mining is the backbone of Bitcoin because it verifies transactions and maintains blockchain trust.

---

4. Double Spending ⭐

Definition

Double spending means using the same digital currency more than once.

Easy Explanation

Since digital money is data, a dishonest user may try to copy and spend same bitcoin twice.

Example

```
A has 1 BTC

A sends 1 BTC to B
A also sends same 1 BTC to C

This is Double Spending
```

Why It Is Dangerous

- Creates fake money
- Breaks trust
- Makes cryptocurrency useless

How Blockchain Prevents It

1. Every transaction is broadcasted publicly.
2. Nodes verify previous ownership.
3. Miners add only valid transaction.
4. Consensus accepts one valid chain.
5. Invalid duplicate transaction is rejected.

Diagram

```
Same Bitcoin → Two Transactions
        ↓
Network Verification
        ↓
Only First Valid Transaction Accepted
        ↓
Duplicate Rejected
```

Important Keywords

Fraud, Duplicate Spending, Verification, Consensus, Blockchain Ledger

Conclusion

Blockchain prevents double spending using public verification, mining and consensus.

---

5. Consensus ⭐

Definition

Consensus is the process by which all nodes in a blockchain agree on the valid state of blockchain.

Easy Explanation

Since there is no bank or central authority, all computers must agree before accepting a block.

Why It Is Needed

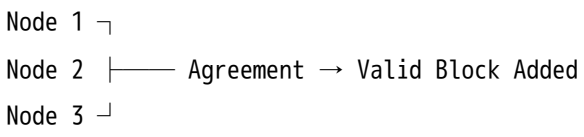
Consensus is needed to:

- Maintain same ledger copy
- Prevent fake transactions
- Prevent double spending
- Build trust

Working

1. Transaction is created.
2. Transaction is broadcasted.
3. Nodes verify transaction.
4. Miners create block.
5. Consensus mechanism checks validity.
6. Valid block is accepted by network.

Diagram



Types of Consensus

Consensus	Basic Idea
PoW	Solve puzzle
PoS	Stake-based validation
PoB	Burn coins
PoET	Random waiting time

Advantages

- Trust without central authority
- Prevents fraud
- Maintains blockchain consistency

Conclusion

Consensus is the heart of blockchain because it allows decentralized systems to work securely.

---

6. Bitcoin P2P Network ⭐

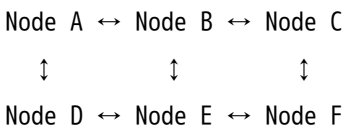
Definition

Bitcoin P2P network is a decentralized network where nodes communicate directly without central server.

Easy Explanation

In Bitcoin, every computer can connect with other computers and share transactions and blocks.

Diagram



Working

1. User creates transaction.
2. Wallet sends it to nearby node.
3. Node verifies and forwards it.
4. Other nodes receive transaction.
5. Miners include it in block.
6. New block is shared in network.

Advantages

- No central server
- Fault tolerant
- Transparent
- Difficult to shut down

Disadvantages

- Network delay
- High bandwidth
- Duplicate messages possible

Applications

- Bitcoin transaction sharing
- Block propagation
- Decentralized communication

Important Keywords

Peer-to-Peer, Node, Decentralized Network, Broadcast, Relay

Conclusion

Bitcoin P2P network allows direct communication between nodes and removes need of central authority.

---

7. Mining Pool ⭐

Definition

Mining pool is a group of miners who combine their computational power to mine blocks and share rewards.

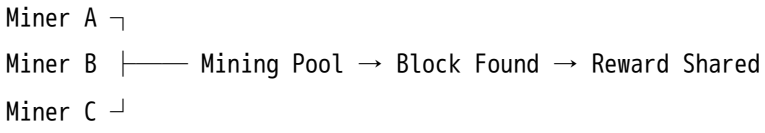
Easy Explanation

Mining alone is difficult. So miners work together like a team and divide reward.

Working

1. Many miners join a pool.
2. Pool assigns work.
3. Miners solve parts of puzzle.
4. If pool finds block, reward is received.
5. Reward is shared according to contribution.

Diagram



Advantages

- Higher chance of earning reward
- Stable income
- Useful for small miners

Disadvantages

- Centralization risk

- Pool fee
- Large pools may dominate network

Conclusion

Mining pool improves earning chances but may create centralization problem.

---

8. Mining Difficulty ⭐

Definition

Mining difficulty is a measure of how hard it is to find a valid hash for mining a block.

Easy Explanation

If more miners join, blocks may be mined faster. To control this, Bitcoin increases difficulty.

Why It Is Needed

Bitcoin tries to maintain average block time of about 10 minutes.

Working

```
More Miners → More Hash Power → Difficulty Increases
Less Miners → Less Hash Power → Difficulty Decreases
```

Diagram

```
Hash Power Changes
        ↓
Difficulty Adjustment
        ↓
Block Time Maintained
```

Advantages

- Controls block creation speed
- Maintains network stability
- Prevents too many coins creation

Disadvantages

- Mining becomes expensive
- Small miners struggle

Important Keywords

Hash Rate, Target, Difficulty Adjustment, Block Time

Conclusion

Mining difficulty keeps Bitcoin block generation stable and controls coin creation.

---

9. PoS vs PoW ⭐

Basis	Proof of Work	Proof of Stake
Full Form	Proof of Work	Proof of Stake
Selection	Based on computation power	Based on coin stake
Energy Use	Very high	Low
Hardware	Expensive mining hardware	No special mining hardware
Speed	Slower	Faster
Security	Very strong	Depends on stake distribution
Reward	Mining reward	Validator reward
Example	Bitcoin	Ethereum 2.0

PoW Explanation

Miners solve mathematical puzzles to validate blocks.

PoS Explanation

Validators are selected based on the amount of cryptocurrency they lock as stake.

Which is Better?

- **PoW** is better for strong security and decentralization.
- **PoS** is better for energy saving and faster processing.

Conclusion

PoW uses computational power, while PoS uses ownership stake to validate blockchain transactions.

---

10. Block Propagation ⭐

Definition

Block propagation is the process of spreading a newly mined block across the blockchain network.

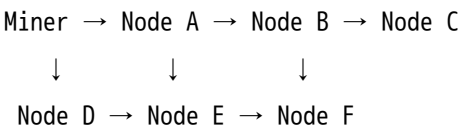
Easy Explanation

When a miner finds a valid block, it sends that block to other nodes. Then nodes forward it further.

Working

1. Miner mines new block.
2. Miner broadcasts block.
3. Nearby nodes receive block.
4. Nodes verify block.
5. Verified block is forwarded.
6. Network updates blockchain.

Diagram



Why It Is Needed

- Keeps all nodes updated
- Maintains same blockchain copy
- Reduces conflicts

Advantages

- Synchronization
- Fast network update
- Trust maintenance

Disadvantages

- Delay may cause temporary forks
- Bandwidth usage

Conclusion

Block propagation helps the Bitcoin network share new blocks and maintain a common blockchain.

---

11. Proof of Burn ⭐

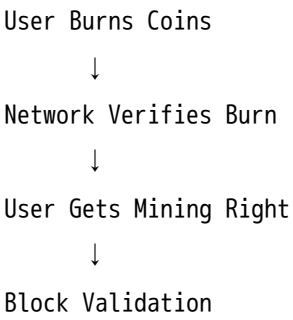
Definition

Proof of Burn is a consensus mechanism where users destroy coins permanently to get mining or validation rights.

Easy Explanation

Burning coins means sending them to an unusable address. This proves commitment to the network.

Working



Advantages

- Less energy use than PoW
- Shows serious participation
- Reduces coin supply

Disadvantages

- Coins are permanently lost
- Rich users may dominate
- Less popular than PoW/PoS

Conclusion

Proof of Burn is an alternative consensus mechanism where users sacrifice coins to gain network rights.

---

12. Proof of Elapsed Time (PoET) ⭐

Definition

Proof of Elapsed Time is a consensus mechanism where each node waits for a random time, and the node with shortest waiting time creates the block.

Easy Explanation

It is like a lucky draw where every node waits randomly. The node whose timer finishes first gets chance to add block.

Working

1. Each node gets random waiting time.
2. Nodes wait silently.
3. Node with shortest time wakes first.
4. It creates new block.
5. Other nodes verify it.

Diagram

```
Node A waits 20 sec
Node B waits 8 sec  → Wins
Node C waits 15 sec
```

Advantages

- Low energy consumption
- Fair selection
- Faster than PoW

Disadvantages

- Needs trusted hardware
- Mostly used in permissioned blockchain

Example

Hyperledger Sawtooth uses PoET.

Conclusion

PoET saves energy by selecting block creator through random waiting time instead of heavy computation.

---

13. Bitcoin Script ⭐

Definition

Bitcoin Script is a simple scripting language used to define conditions for spending bitcoins.

Easy Explanation

Bitcoin Script decides whether a transaction is valid or not. It checks signatures and conditions.

Example

```
IF digital signature is valid
THEN payment is allowed
ELSE transaction rejected
```

Why It Is Needed

It is needed for:

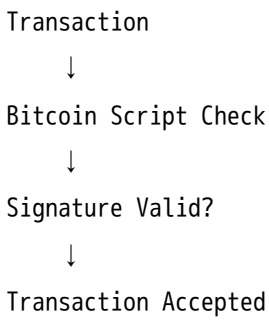
- Transaction validation
- Ownership checking

- Multi-signature payments
- Basic smart contracts

Working

1. Sender creates transaction.
2. Script contains spending condition.
3. Receiver or network checks script.
4. If condition is true, transaction becomes valid.

Diagram



Features

Feature	Explanation
Stack-based	Uses stack operations
Simple	Limited commands
Secure	Prevents complex attacks
Not Turing complete	Avoids infinite loops

Advantages

- Secure transaction rules
- Supports multi-signature
- Simple and reliable

Disadvantages

- Limited features
- Not as powerful as Ethereum smart contracts

Conclusion

Bitcoin Script is used to control and verify Bitcoin transactions securely.

🔥 Most Important 7-Mark Questions

1. Explain Bitcoin transaction processing.
2. Explain Proof of Work.
3. What is mining? Explain mining process.
4. Explain double spending problem.
5. Explain consensus in Bitcoin.
6. Explain Bitcoin P2P network.
7. Explain mining pool.
8. Explain mining difficulty.
9. Differentiate PoW and PoS.
10. Explain block propagation.
11. Explain Proof of Burn.
12. Explain Proof of Elapsed Time.
13. Explain Bitcoin Script.

⭐ Most Important 14-Mark Questions

1. Explain Bitcoin transaction processing with neat diagram.
2. Explain Proof of Work and mining process in detail.
3. Explain consensus mechanisms: PoW, PoS, PoB and PoET.
4. Explain Bitcoin P2P network and block propagation.
5. Explain double spending problem and how blockchain prevents it.

6. Explain mining, mining difficulty and mining pool.
7. Compare Proof of Work and Proof of Stake in detail.
8. Explain Bitcoin Script and transaction validation.

🎯 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 Script

⚡ One-Night Revision Notes

```
Bitcoin Transaction = Create → Sign → Broadcast → Verify → Mine → Confirm

PoW = Puzzle solving by miners

Mining = Verify transactions + Add block + Get reward

Double Spending = Same coin spent twice

Consensus = Agreement between nodes

P2P Network = Direct node-to-node communication

Mining Pool = Group mining

Mining Difficulty = Hardness of finding valid hash

Block Propagation = Sharing new block in network
```

📌 Smart Study Plan

First Priority

Study these first:

1. Bitcoin Transaction Processing
2. Proof of Work
3. Mining
4. Double Spending
5. Consensus

Second Priority

Then study:

1. Bitcoin P2P Network

2. Mining Pool
3. Mining Difficulty
4. PoW vs PoS

Last Priority

Revise:

1. Block Propagation
2. Proof of Burn
3. Proof of Elapsed Time
4. Bitcoin Script

🧠 Memory Tricks

Bitcoin Transaction Flow

```
Create → Sign → Broadcast → Verify → Mine → Confirm
```

Mining Flow

```
Collect → Verify → Puzzle → Block → Reward
```

Consensus Meaning

```
Many Nodes + Same Decision = Consensus
```

PoW vs PoS

```
PoW = Work Power
PoS = Stake Power
```

Double Spending

```
One Coin → Two Payments = Fraud
Blockchain → Only One Accepted
```

✅ Final Exam Tip

For every answer, write in this order:

```
Definition
↓
Need
↓
Diagram
↓
Working Steps
↓
Advantages
↓
Disadvantages
↓
Applications
```

↓

Conclusion

This format will help you write long and scoring RGPV answers.