MINI TASK – 1

Theoretical Part

1. ## Blockchain Basics

Ques1) Define blockchain in your own words (100–150 words).

Ans – A blockchain is like a digital ledger or notebook that everyone in a network can see and add to, but no one can erase or change what's already written. Imagine a group of friends keeping track of who owes whom money by writing it down together in a shared notebook. Each time someone pays or receives money, the group writes a new page. Once a page is added, everyone checks and agrees it's correct, and it's locked in place so no one can go back and change it. This way, everyone trusts the record because it's transparent and can't be messed with. Blockchains use special math and computers to keep everything secure and honest, making them really useful for things like digital money (like Bitcoin), contracts, or tracking important information. In short, it's a way for people to share and trust information online without needing a middleman.

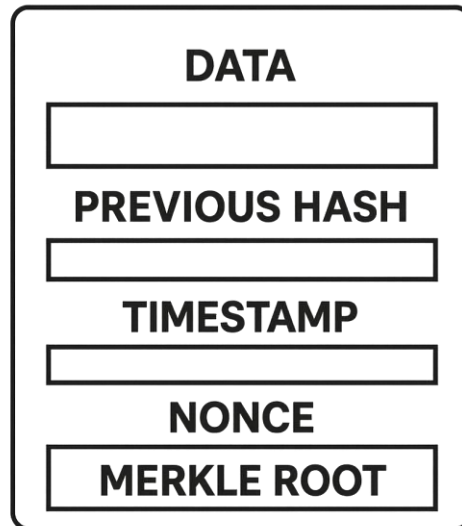Ques-2) List 2 real-life use cases (e.g., supply chain, digital identity).

Ans- The 2 real life use cases are:

1. Banking Industry – Here the Blockchain can be used in banking industry so that the transaction can be more secured and transparent and due to the presence of Blockchain technology it becomes utterly impossible for the hackers to hack someone's account.

2. Voting – Blockchain can be used in voting also and the population of India is huge and its very difficult to get vote of all people and if it becomes online then the frauds with voting will increase more so we can introduce blockchain and due to the characteristics of blockchain we can make voting online and also can minimize double voting which is a common problem in India

2. **Block Anatomy**

Ques 1) Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root

Ans -

```
┌─────────────────────────┐
│           DATA          │
│  ┌───────────────────┐  │
│  │                   │  │
│  └───────────────────┘  │
│      PREVIOUS HASH      │
│  ┌───────────────────┐  │
│  │                   │  │
│  └───────────────────┘  │
│        TIMESTAMP        │
│  ┌───────────────────┐  │
│  │                   │  │
│  └───────────────────┘  │
│          NONCE          │
│  ┌───────────────────┐  │
│  │    MERKLE ROOT    │  │
│  └───────────────────┘  │
└─────────────────────────┘
```

Ques 2) Briefly explain with an example how the Merkle root helps verify data integrity.

Ans - The Merkle Root is a single hash that summarizes all transactions in a block. If someone tries to change even one transaction, the Merkle root will change. For example, if a block has transactions A, B, C, and D, altering C will cause the Merkle root to be different. This makes it easy to check if any data in the block has been tampered with.

3. **Consensus Conceptualization**

Ques1) What is Proof of Work and why does it require energy?

Ans – Proof of work (POS) is a consensus mechanism where the participants called the miners solve complex math puzzle to validate transactions and add new block to the chain. The first one to solve the puzzle get to validation the transaction and add it to the block, solving these puzzles requires powerful computers running constantly, and this computational effort uses a lot of electricity. The energy cost acts as a security feature, making it expensive for anyone to cheat or attack the network.

Ques 2) what is Proof of Stake and how does it differ?

Ans – Proof of Stake (PoS) is a blockchain consensus mechanism where validators are chosen to verify transactions and create new blocks based on how many coins they hold and "stake" (lock up) as collateral. Unlike Proof of Work, which relies on miners solving complex puzzles using lots of energy, PoS selects validators randomly or based on their stake,

making it much more energy-efficient Validators have a financial incentive to act honestly, as they can lose their staked coins if they try to cheat. This approach helps keep the network secure while reducing the environmental impact compared to PoW.

Ques 3) What is Delegated Proof of Stake and how are validators selected?

Ans - Delegated Proof of Stake (DPoS) works like voting for a team to run the blockchain. People who own tokens get to pick a few trusted members (called delegates) to make sure all transactions are correct and new blocks are added. The more tokens you have, the more your vote counts, and you can change your vote anytime if you don't like how a delegate is doing. This keeps things running smoothly and fairly, and it's usually much faster than other methods.