Mini Task 1

Theoretical Part:

1. **Blockchain Basics:**

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

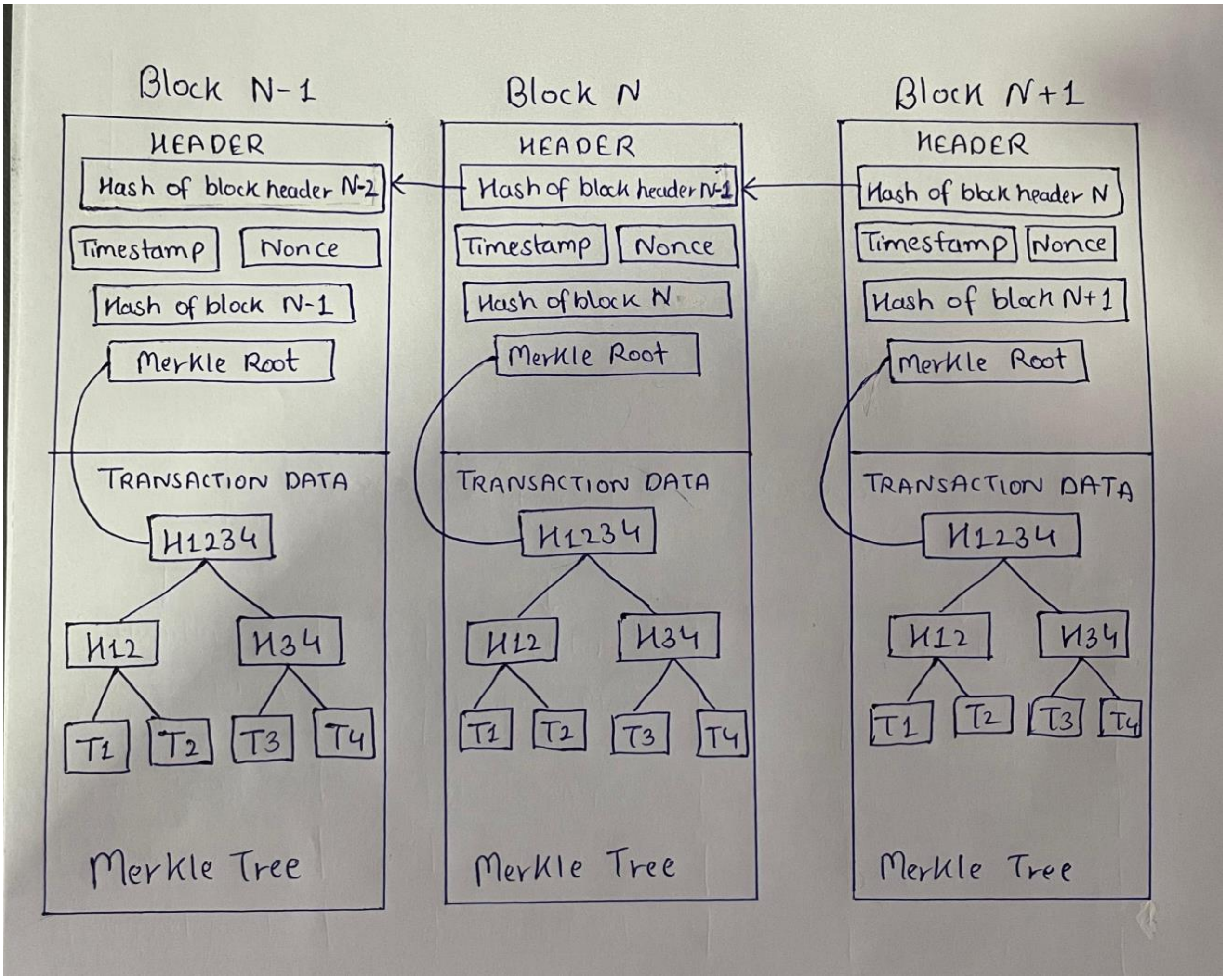
- A blockchain is a public, decentralized ledger that records all transactions made in a network like Bitcoin.
- It grows continuously as new blocks of verified transactions are added approximately every 10 minutes by miners.
- Each block is added in a chronological order, forming an unbroken chain of data.
- Every node (computer) in the network keeps a full copy of the blockchain, making the system transparent and secure.
- From the first block (genesis block) to the latest one, all data about transactions, wallet addresses, and balances are stored permanently.
- The true innovation of blockchain lies in its ability to build trust without relying on third parties such as banks.
- It supports peer-to-peer transactions globally, with use cases beyond cryptocurrency including asset tracking, voting, contracts, and more making it a powerful tool for creating a decentralized and secure digital world.
- Blockchain is already cash for the Internet, a digital payment system, and it may become the "Internet of Money," connecting finances in the way that the Internet of Things (IoT) connects machines.

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

- Money Transfers: Blockchain allows fast, secure, and low-cost money transfers by removing intermediaries like banks. For example, a person in the United States can send money to a relative in the Dominican Republic within minutes, saving on fees and time compared to traditional bank transfers.
- Real Estate Transactions: Buying or selling property often involves a lot of paperwork and verification steps. Blockchain technology can streamline the real estate process by securely storing and verifying personal information and ownership records, leading to faster and more secure transactions with less paperwork.
- Supply chain and logistics tracking Keeping track of articles as they traverse a supply chain network can help supply chain and logistics departments work better together. If all the data is stored on a blockchain network then it can't be modified and it can be accessed easily by the relevant parties.

2. **Block Anatomy:**

- **Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.**



Block Header:

- Each block contains a **header** with:
  - Hash of the previous block's header → links blocks in chronological order.
  - Timestamp → when the block was created.
  - Nonce → used in Proof of Work.
  - Merkle Root → top hash of all transactions in the block.

Transaction Data:

- Each block stores multiple transactions.
- These are organized in a **Merkle Tree**, where:
  - Transaction hashes (T1–T4) are combined into H12, H34, and finally H1234 (Merkle Root).
  - If **any transaction is altered**, the Merkle Root changes, making tampering obvious.

Blockchain Linkage:

- Each block points to the hash of the **previous block's header**, ensuring no block can be changed without affecting the rest of the chain.

o Briefly explain with an example how the Merkle root helps verify data integrity.

- A Merkle tree organizes blockchain transactions into a tree like structure where each leaf node is a transaction hash, and parent nodes are hashes of their child nodes.
- This hierarchy helps efficiently verify large amounts of data by allowing quick checks of specific transactions without needing to review the entire blockchain.
- If even a tiny part of transaction changes, the root hash at the top of the tree will change, ensuring data integrity.
- The Merkle root acts like a digital fingerprint for a group of records.
- Even if one item changes, the fingerprint (root) changes—making it perfect for ensuring data integrity in blockchain system.
- For example, Imagine an e-commerce company like **Amazon** is delivering 4 packages to customers:

- **Package A**: Order #1001
- **Package B**: Order #1002
- **Package C**: Order #1003
- **Package D**: Order #1004

Before dispatching, Amazon creates a Merkle Tree using the data (e.g., order ID, customer name, delivery address) of each package.

1. First, hash each package's data:

   H_A = hash(Package A info)
   H_B = hash(Package B info)
   H_C = hash(Package C info)
   H_D = hash(Package D info)

2. Combine and hash:

   H_AB = hash(H_A + H_B)
   H_CD = hash(H_C + H_D)

3. Final Merkle root:

   Merkle_Root = hash(H_AB + H_CD)

Now, let's say a customer claims **Package B** was tampered with. The delivery manager doesn't need to recheck all packages. They can:

- Re-hash Package B's data (H_B)
- Request H_A (sibling hash) and H_CD (hash of the other pair)
- Recalculate Merkle_Root and compare it with the original

If the root **matches**, Package B was **not altered**.
If it **differs**, then **Package B has been tampered with**.

3. Consensus Conceptualization

○ Explain in brief (4–5 sentences each):

- **What is Proof of Work and why does it require energy?**

- Proof of Work (PoW) is a consensus mechanism used in blockchains like Bitcoin where computers (called nodes or miners) compete to solve a complex mathematical puzzle.
- The first one to solve it gets to add the next block of transactions to the blockchain and earns a reward.
- This process is secure because it's very hard to solve but easy for others to verify.
- However, solving the puzzle needs a lot of computing power, which consumes a large amount of electricity. That's why PoW is considered energy-intensive.
- For example – Bitcoin - Imagine a school contest where every student has to solve a very tough math puzzle. The first student to solve it wins a prize and gets to write the answer on the school board. This is like PoW — every miner competes to solve a complex puzzle, and the winner adds the next block to the blockchain. It uses a lot of energy because many students (computers) are working hard at the same time.

- **What is Proof of Stake and how does it differ?**

- Proof of Stake (PoS) is a more energy-efficient alternative to Proof of Work.
- Instead of using computing power, validators are chosen to add new blocks based on how much cryptocurrency they "stake" or lock up.
- The more coins someone holds, the higher their chances of being selected.
- This system avoids the need for high energy consumption, making it eco-friendlier than PoW. However, it can favor the wealthy since those with more coins have more influence.
- For example - Ethereum 2.0 - Now imagine a class where students don't compete, but instead, the teacher chooses one student to write on the board based on how many tokens they hold. If a student

has more tokens (stake), they're more likely to be chosen. This is like PoS — no energy-intensive puzzle solving, just selection based on how much you've invested.

- **What is Delegated Proof of Stake and how are validators selected?**

- Delegated Proof of Stake (DPoS) is a version of Proof of Stake where coin holders vote for a small group of trusted people called "delegates" or "validators."
- These selected validators are responsible for verifying transactions and creating new blocks.
- The voting is continuous, so if a validator acts dishonestly, they can be replaced by another.
- This system is much faster and more scalable than regular PoS and PoW. It relies on trust and reputation, making community participation very important.
- For example - Think of a school election where students vote for a few class leaders who are trusted to write on the board. These elected leaders can be replaced anytime if they don't perform well. That's DPoS — coin holders vote for a limited number of validators to maintain the network. It's faster and more democratic, but it depends on trust and active voting.