Blockseblock :Internship

Mini Task 1

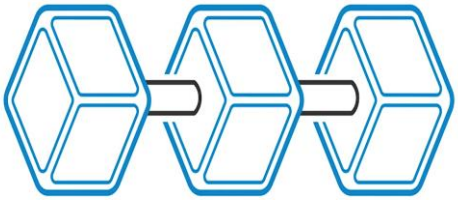
Name: Akshit G Rana

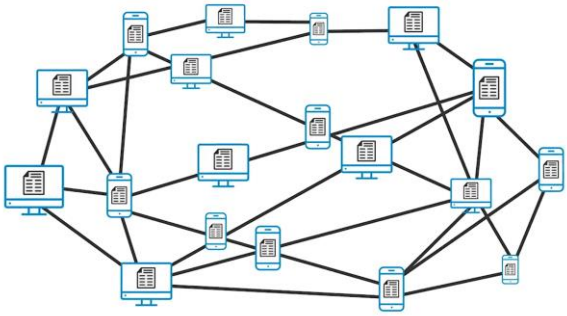
Theoretical Part:

1.Blockchain Basics

Q1. Define blockchain in your own words (100–150 words).

Big banks and some governments are using blockchains to revolutionize how they store information and conduct transactions. There are many reasons to do this, including faster speed, lower costs, greater security, and fewer errors. A blockchain also eliminates central points of attack and failure. None of these reasons requires cryptocurrency per se. However, many important blockchains are based on Satoshi Nakamoto's Bitcoin model, and here's how they work. Bitcoin or other digital currency isn't saved in a file somewhere. Instead it's represented by transactions recorded on a blockchain. Let us easily understand this by a visual representation :





Think of it as a global spreadsheet or ledger. Each Bitcoin transaction entered on it is verified by a large peer-to-peer network. Each blockchain is distributed. That means it runs on computers provided by volunteers around the world. It also means there's no central database to hack. It doesn't mean all distributed ledgers are blockchains. A distributed ledger is a database existing in many places with many people using it. Not all distributed ledgers have the encryption and verification standards of a blockchain. A blockchain is a specific type of distributed ledger, just as a square is a specific type of rectangle. The blockchain is public, it's **open-source code, it's a protocol, not a product**. Anyone can view it at any time because it's located on the network, not inside a single institution. The blockchain has heavy duty encryption, using **public** and **private keys**. Think of it like the two key system to access a safety deposit box. Unlike Target or Home Depot, there are no weak firewalls to attack. Unlike at Morgan Stanley or the US Federal Government, there are no untrustworthy staffers to steal secrets. Every 10 minutes, like the heartbeat of the Internet, all transactions conducted on the Bitcoin network are verified, cleared, and stored in a block. The block is linked to the preceding block and to the block before it, creating a chain of blocks. Each block must refer to the preceding block to be valid. The structure permanently timestamps, and stores exchanges of value, and it prevents anyone from altering the ledger. This validation process makes theft impossible by any practical measure. If you wanted to steal a bitcoin, you'd have to rewrite the coins' entire history on the block chain. What's more, you'd have to do it without being detected by millions of other people working on it. Well, that's practically impossible.

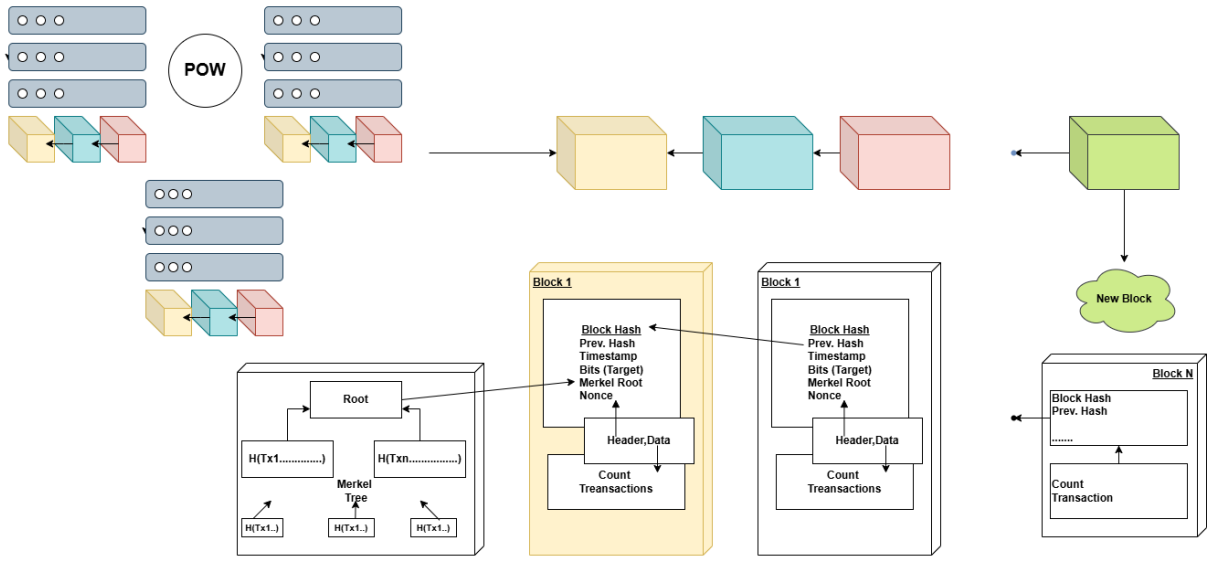
Q2. List 2 real-life use cases (e.g., supply chain, digital identity).

Supply Chain Tracking: Blockchain can be used to track the origins and movement of every ingredient in our meals. By using blockchain, each step of a product's journey (e.g., from farm to supermarket) is permanently and securely recorded, ensuring transparency and reducing the risk of fraud.

Digital Identity Verification: Blockchain can be used to record and verify important personal documents, such as birth and death certificates, marriage licenses, and educational degrees. By storing this data on a blockchain, it becomes tamper-proof, secure, and easily verifiable by authorized parties.

2.Block Anatomy

Q1. Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.



Block showing: data, previous hash, timestamp, nonce, and Merkle root.

by Akshit G Rana

Q2. Briefly explain with an example how the Merkle root helps verify data integrity.

Ans.: The Merkle root is the top hash of a Merkle tree, a binary tree of hashes. It allows efficient and secure verification of the contents of large datasets. When you store transactions in a blockchain block, each transaction is hashed. These hashes are then paired and hashed again, forming the next level of the tree. This process repeats until you get a single root hash — the Merkle root**.**

Suppose we have four transactions: Tx1, Tx2, Tx3, and Tx4.

First, we compute the hashes of each transaction:

- H1 = hash(Tx1)
- H2 = hash(Tx2)
- H3 = hash(Tx3)

- H4 = hash(Tx4)
- Then, we combine these in pairs and compute their hashes to get the next level:
- H12 = hash(H1 + H2)
- H34 = hash(H3 + H4)

Finally, we compute the Merkle root:

- Merkle Root = hash(H12 + H34)

This Merkle root is stored in the block header.Now, imagine someone tries to modify Tx3. The hash of Tx3 (H3) will change, so H34 will also change, and eventually, the Merkle root will not match the original value.When a node wants to verify that Tx3 is part of the block and hasn't been tampered with, it only needs to check the path:
H3 → H34 → Merkle Root
rather than re-checking every transaction.If the hashes along this path don't match what's in the block header, the node knows that Tx3 has been modified, and the block's data integrity has been compromised.

Consensus Conceptualization
Explain in brief (4–5 sentences each):
Q1.What is proof of Work and why does it need energy ?

Ans.: Proof of Work is a way to keep the blockchain safe by making computers solve very hard puzzles. This takes a lot of computer power and electricity. The first computer to solve the puzzle adds a new block to the blockchain and gets a reward. All this energy makes it very hard for anyone to cheat.

Q2.What is Proof of Stake and how does it differ?
Ans.: Proof of Stake doesn't use puzzles or a lot of energy. Instead, people who own a lot of the blockchain's coins can "lock up" some coins to show they care about the network. The system then chooses who gets to add the next block based on how much they have locked up. This saves energy and is faster than Proof of Work.

Q3.What is Delegated Proof of Stake and how are validators selected?

Ans.: In Delegated Proof of Stake, people vote for a few trusted computers to add blocks. Only those voted-in computers can do it, and they change over time based on new votes. This way, it's quicker and cheaper than other methods, and people can choose who they trust.