NAME : Anshika Singh

Roll no : 230163 (Assignment 1)

Question 1)

1.Increased Financial Transactions

More transactions will be done through the blockchain that is secure as well as fast for any financial transaction that is bank-not-related. It helps with cost-cutting and hastening peer-to-peer transaction costs.

Use:-Peer-to-peer campus organization's event funding and crowdfunding; loans can get much easier with blockchain's payment system that is free of malpractices involving any foul play.

2. Tracking products in the supply chain

Blockchain will help track goods. Logistics and manufacturing will present an entire scenario of fraud and authentication. Blockchain campus application

3. Academic records issuance and authentication.

One of the elementary examples of Blockchain implementation in schools is the release of digital certificates or transcript. The records cannot be altered and can be accessed swiftly by anyone from any part of the world. Any verifications require no protracted procedures.

For IITK: Imagine your degree or transcripts to be a safe and secure digital certificate easily verifiable by any employer or university anywhere in the world. No more waiting or fears of false claims!

4. Health Care Data Management

Blockchain usage for storing medical records such that sensitive health information can be available only to the authorized people.

Use: Campus health can use blockchain to safely manage the medical records of students in such a manner that doctors will easily have access without risks associated with data.

5. Fair and Transparent Voting

Blockchain can develop voting systems that cannot be changed. It will record every vote securely so that no alteration is made in results, making them fair.

Question 2)

1. BTC: Bitcoin is the first, most popular, and indeed the most prominent blockchain for digital currency transactions. It's basically a store of value and a medium of exchange.

Consensus Mechanism-: Proof of Work-PoW makes miners have to solve complicated puzzles to validate transactions and secure the network, though it is highly energy-intensive.

2. Ethereum: Ethereum is a blockchain developed specifically for smart contracts. This gives developers the ability to build Apps and platforms .

Consensus Mechanism-: Proof of Stake

After the update to 2.0, Ethereum went to PoS, thus also saving energy consumption. Validators are verifying blocks and use ETH as collateral instead of mining.

3. Ripple (XRP): Ripple aims at simplifying cross border payments and currency exchange, widely used by banks and the finance sector in making cross boundary transactions.

Consensus Mechanism: Ripple Protocol Consensus Alg. -: Unlike PoW or PoS, RPCA is trusted with the use of validators. This has its energy consumption faster compared to rate but very central.

4. DOT (Polkadot) : This connects a good number of blockchains together to assist in seamless sharing of information and functionality between the diverse networks.

Consensus Mechanism: Nominated Proof of Stake (NPoS) :- NPoS offers the ability to nominate validators for token holders, which in return makes parachains decentralized and secure.

5. Hyperledger Fabric : It is the newest business blockchain framework, specific to that mainly creates permissioned blockchains for supply chain management and health care, mainly finance applications.

Consensus Mechanism: PBFT :- PBFT can guarantee the atomicity of transaction approvals among the subset of nodes; thus it is very efficient for a private environment.

Question 3)

```
import hashlib

import time

def find_nonce(input_string):

    nonce = 0

    threshold = '000'  # Threshold with 3 leading zeros

    start_time = time.time()  # Record the start time

    while True:

        combined_string = input_string + str(nonce)     # Combine input string with current nonce

        hash_result = hashlib.sha256(combined_string.encode()).hexdigest()   # Calculate SHA-256 hash of combined string

        hash_result = hashlib.sha256(combined_string.encode()).hexdigest()

        if hash_result[:3] == threshold:          # Check if hash starts with '000' (threshold)

            end_time = time.time()                # Record the end time

            time_taken = end_time - start_time

            return nonce, time_taken


        nonce += 1
```

```
if __name__ == "__main__":
    user_input = input("Enter the input string: ")
    nonce, time_taken = find_nonce(user_input)
    print(f"Nonce found: {nonce}")
    print(f"Time taken to find nonce: {time_taken:.4f} seconds")
```

Question 4)

An **Unspent Transaction Output (UTXO)** refers to the portion of a cryptocurrency transaction that remains unspent after the transaction is executed. In essence, it's the "change" you receive after making a purchase. Each UTXO represents a specific amount of cryptocurrency that can be used as input in future transactions.

Question 5)

A blockchain is said to be immutable: once the data is inputted, it cannot be altered or deleted. The immutability of the blockchain comes as a result of its decentralized structure where each block contains a cryptographic hash of the previous block, hence locking in the entire chain. If any information in a block were to be changed, then so would every subsequent block in the chain.

Question 6)

In a Proof of Work blockchain, fraudulent blocks added without an attack at 51% would have the network resolve it by accepting the longest valid chain. Miners are always working on one that has gathered the highest proof of work, hence the fraudulent blocks are virtually canceled.

Question 7)

In the Proof of Stake (PoS) systems, there is the "nothing-at-stake" problem. Here, validators can vote on multiple blockchain forks without having any cost incurred, thus possibly causing network instability. Penalties such as slashing discourage dishonest behaviour in validators and make them refrain from supporting multiple forks.

Question 8)

Actually, Proof-of-Stake systems are less inclined to be attacked by risking 51% since herein an entity would need a manipulation major control that is having 51 percent of staked cryptocurrency controlling an attack by manipulating the blockchain.
It is much more hard and expensive to obtain the portion of total staked assets involved, as compared to acquiring more than 50% of the network's mining power in Proof of Work systems.

Question 9)

Digital signatures authenticate the source and integrity of transactions while simultaneously doing so in blockchains. They work with a public key for other people while using a private key unique only to him. Digital signing is where the user deploys the private key to the user's blockchain to sign for their transaction. Others can verify the signature through the public key so that the transaction will have authenticity and integrity.

Question 10)

This Oracle Problem occurs in blockchain every time there is a requirement of information by the smart contracts from the outer world, which blockchain cannot source itself. Oracles, that is, the trusted middlemen who give the real-world data to the blockchain so that it can function with smart contracts based on the outside event, solve this problem.

Question 11)

Zero-knowledge proofs (ZKPs) are cryptographic tools that allow one party to demonstrate a fact about information to another party, without actually releasing the information itself. That is, in terms of blockchain, ZKP can let the validation of transaction take place without leaking sensitive data of it. This means the validation of the transaction will only be done without breach on confidentiality and integrity in every blockchain network.