BlockBloom Assignment – 1

Aryavart Dahiya – 230223

Ques 1

5 Different Uses of Blockchain Technology Relevant to IITK Students:

1. **Payment Records for Mess and Canteen:**
   The payment transactions within messes and canteens can be securely stored on a blockchain. Similar to attendance records, blockchain provides a robust system for maintaining trustworthy transaction logs. Features like setting monthly spending caps or pre-loading a specific amount for spending can also be implemented to promote budget management among users.

2. **Voting Systems:**
   Blockchain technology offers a secure and transparent solution for storing voting details during elections. By recording votes on a blockchain, the system becomes highly resistant to cheating, ensuring that elections are held fairly. Additionally, this approach enhances transparency and reduces the manpower required for electoral processes.

3. **Healthcare Records:**
   Blockchain can be leveraged to store medical records securely and privately. When a record is generated, it can be signed by the patient and added to the blockchain. To ensure confidentiality, records can be encrypted before storage. This method safeguards sensitive patient information while maintaining data integrity.

4. **Attendance Records:**
   In our college, blockchain can be utilized to maintain a safe and secure record of student attendance. To simplify, all attendance records for a course on a particular day can be grouped together. Using biometric data ensures the authenticity of these records, thereby providing a reliable and efficient attendance system.

5. **Research Publications:**
   Blockchain technology can securely store research publications with proper timestamps, ensuring ownership and preventing plagiarism. Each publication can be recorded on the blockchain with proper timestamps, ensuring that the original author is credited and their intellectual property rights are protected.

Ques 2

Popular Blockchain Networks and Their Features:

- **Bitcoin:**
  Bitcoin is the pioneer of decentralized digital currencies. It enables secure and transparent value transfers without requiring intermediaries like banks.
  Consensus Mechanism: Proof of Work (PoW).
- **Ethereum (ETH):**
  Ethereum is a highly versatile blockchain platform that supports smart contracts and decentralized applications (dApps). It provides the foundation for countless innovations in the blockchain space.
  Consensus Mechanism: Proof of Stake (PoS).
- **Binance Smart Chain:**
  Binance Smart Chain is optimized for fast and cost-effective transactions. It is widely used in decentralized finance (DeFi), tokenized assets, and cross-chain compatibility.
  Consensus Mechanism: Proof of Staked Authority (PoSA).
- **Cardano (ADA):**
  Cardano is built for secure and efficient development of decentralized applications, identity management, and supply chain tracking. Its design emphasizes sustainability and scalability.
  Consensus Mechanism: Proof of Stake (PoS).

Ques 3

Python Code:

```
import hashlib
import time

def find_nonce(input_string, threshold):
    nonce = 0
    threshold = int(threshold, 16)
    start_time = time.time()

    while True:
        combined = f"{input_string}{nonce}".encode('utf-8')
        hash_value = hashlib.sha256(combined).hexdigest()
        if int(hash_value, 16) < threshold:
            end_time = time.time()
            return nonce, hash_value, end_time - start_time
        nonce += 1

if __name__ == "__main__":
    input_string = input("Enter the input string: ")
    threshold = "000fffff" + "f" * 56

    nonce, hash_value, time_taken = find_nonce(input_string, threshold)
```

```
print(f"Smallest Nonce: {nonce}")
print(f"Hash: {hash_value}")
print(f"Time Taken: {time_taken:.6f} seconds")
```

Ques 4

UTXO stands for **Unspent Transaction Output**. It is a model used in cryptocurrencies like Bitcoin for tracking transfers of coins. Instead of working like a bank account, this model works more like physical cash. The amount of cryptocurrency a person has is basically the total of all UTXOs they own. These UTXOs are kind of like physical coins or notes, meaning they can't be divided into smaller parts.

Ques 5

A blockchain is considered **immutable** because it uses a distributed ledger system, meaning that the data is stored across many computers or nodes in a network, making it hard to tamper with. Each block in the blockchain is linked to the previous one using a unique cryptographic hash (like SHA-256), so if someone tries to change a block, it would alter the hash, breaking the chain and making it easily detectable. Additionally, blockchain networks use consensus mechanisms like Proof of Work (PoW) or Proof of Stake (PoS), where miners must agree on the validity of the data before it's added. In PoW, for example, miners must solve complex problems to add a new block. These features make blockchain data extremely difficult to alter, ensuring that once information is recorded, it remains secure and permanent.

Ques 6

In a blockchain with a Proof of Work (PoW) consensus mechanism, if a fraudulent block is added by a criminal who does not have the ability to perform a 51% attack, the network resolves the fork using the **longest chain rule**.
Longest Chain Rule:
In this scenario, some miners start building on the fraudulent block, while others stick to the legitimate chain. Nodes don't immediately adopt a fork or block into their version of the chain. Instead, they wait for one chain to grow longer than the other. Since honest miners in the network are usually in the majority and have more computational power, the legitimate chain grows faster than the fraudulent one. An attacker would need over 50% of the network's computational power to outpace the chain, which is extremely unlikely in a typical setup.

Ques 7

The 'Nothing-at-Stake' problem is a potential issue in PoS that happens when validators in the system decide to build on every fork during a chain split.

- Validating on multiple forks in PoS doesn't cost much since it's computationally cheap. Unlike PoW, there's no significant energy or hardware expense involved. It makes financial sense for validators to validate on all forks.

To address this problem, following strategies are used:

- **Security Deposits:**
  Validators have to lock up a security deposit, which they lose if they are found to produce invalid blocks or act maliciously. This creates a strong disincentive for dishonest behavior.
- **Slasher Algorithm:**
  This method punishes validators who sign blocks on multiple conflicting forks. By making it financially harmful to support multiple chains, the algorithm ensures that validators stick to a single chain.

Ques 8

A 51% attack happens when one entity or group manages to control more than half of a blockchain network's validation power. This kind of attack is far less likely in PoS than in PoW because:

- **Cost of Acquiring Majority:** In PoW, an attacker needs to gain control of 50% of the network's computational power, which, while difficult, is not as expensive as acquiring 50% of the network's staked cryptocurrency in PoS.
- **Economic Incentive:** Any attack on a cryptocurrency usually results in a significant drop in its market value. Since the attacker owns 50% of the cryptocurrency, they would suffer massive losses due to this depreciation.

Ques 9

In the context of blockchains, digital signatures are used to verify the authenticity and integrity of transactions. When a user wants to carry on a transaction, they create a hash of the transaction data and sign it using their private key. This private key is known only to them only and thus is used to generate signature. To verify the transaction, others in the network can use the sender's public key. If the signature is valid, it proves the transaction was signed by the correct owner of the private key and that the data has not been tampered with.

Ques 10

The Oracle Problem in blockchain refers to the challenge of bringing real-world data onto the blockchain. Blockchains are closed systems and cannot access external data directly, which creates the need for reliable sources to supply that information.

- **Cryptographic Signatures and Verification:**
  Oracles use cryptographic techniques to sign and verify the data they provide. This ensures that the data sent to the blockchain is authentic and hasn't been tampered with.

- **Incentive Mechanisms:**
  Some systems use incentive mechanisms to ensure oracles provide accurate data. Oracles that submit incorrect or manipulated data can be penalized, ensuring they act in the network's best interest.