# BlockBloom Project Assignment 1

Manas Todi
Roll Number: 230627

December 21, 2024

## Answers

### 1. Five Uses of Blockchain Technology

1. **Healthcare:** Patient records can be securely stored with proper timestamps through blockchain technology. Using public and private key encryption, the patient would have control over who accesses their medical records.

2. **Health Insurance:** Similar to healthcare, blockchain ensures that medical records used for insurance claims are tamper-proof, leading to reduced insurance scams.

3. **Elections:** Blockchain enables secure and transparent voting systems by immutably recording votes with timestamps. Public and private key encryption ensures voter anonymity while allowing verification of their vote.

4. **Academic Bank of Credits (IITK):** Blockchain can secure students' academic credits, ensuring authenticity and simplifying credential verification processes for employers and institutions.

5. **Research Publications:** Blockchain can securely store research publications with timestamps, protecting intellectual property and preventing plagiarism.

### 2. Five Blockchain Networks in Use

1. **Bitcoin (BTC):** The first cryptocurrency, known for its large network and resistance to 51% attacks. It uses Proof of Work (PoW).

2. **Ethereum (ETH):** A major cryptocurrency that transitioned to Proof of Stake (PoS), improving energy efficiency and transaction speeds.

3. **Dogecoin (DOGE):** Popularized by a meme, it operates on PoW.

4. **Binance Smart Chain (BSC):** Offers fast, low-cost transactions using PoS.

5. **Litecoin (LTC):** A ”lighter” version of Bitcoin, designed for daily use. It employs PoW.

## 3. The link provided for this question is:

Google Colab Notebook.

## 4. UTXO Model

In the UTXO model, transactions are stored instead of coins. To pay someone, transactions with values equal to or greater than the required amount are selected. Any surplus after covering the transaction fee can be sent back to the sender, another recipient, or used as the fee. This model ensures traceability and efficiency in transaction processing.

## 5. Blockchain Immutability

Blockchain is immutable due to its distributed ledger system, where data is stored across multiple nodes. Each block is linked to the previous one using a unique cryptographic hash. Any tampering alters the hash, breaking the chain. Consensus mechanisms like PoW or PoS ensure that only valid data is added, making alterations computationally prohibitive.

## 6. Fraudulent Block Resolution in PoW

If a fraudulent block is added to a blockchain using PoW, the network resolves the fork by adopting the longest chain rule. Miners continue to add blocks to the valid chain, which grows faster than the fraudulent one. Eventually, the network discards the fraudulent block, ensuring consistency and security.

## 7. Nothing-at-Stake Problem in PoS

The "Nothing-at-Stake" problem arises when validators can support multiple chains without incurring a cost. Solutions include:

- **Slashing:** Penalizing validators by reducing their staked cryptocurrency for validating conflicting blocks.
- **Chain Selection Rules:** Incentivizing validation of the longest chain to discourage support for multiple forks.

## 8. 51% Attack in PoS

A 51% attack is less likely in PoS because an attacker needs to control 51% of the staked cryptocurrency, which is financially prohibitive. PoS systems also employ slashing, where dishonest validators lose their stakes, further discouraging attacks.

## 9. Role of Digital Signatures

Digital signatures ensure the authenticity and integrity of blockchain transactions. Users sign transaction data with their private keys, generating a unique signature. The sender's public key allows others to verify the signature, proving ownership and data integrity.

## 10. Oracle Problem in Blockchain

The Oracle Problem refers to the challenge of bringing real-world data onto the blockchain. Solutions include:

- **Trusted Oracles:** Third-party services that provide reliable data.
- **Decentralized Oracles:** Aggregating data from multiple sources to ensure accuracy and reliability.