BlockBloom Assignment 1 :

1. List out 5 different use cases of blockchain technology. Mention at least one use case relevant to IITK Campus Community.

- Pay without banks. First and most well-known is Cryptocurrency. With no centralized banks needed to stores you money and no central authority to keep you record but a decentralized legder where everyone has a record of all the transactions happenening. The most famous implementations of Blockchain for cryptocurrency are Bitcoin, Ethereum.
- Hardcopy documents can be tampered and lost. Recently document checking happened in the campus, almost 1.5 year after I stepped foot for the first time in IITK. Not knowing when the checking is going to occur, I always kept the document in hostel room. It did not happen but times when I stored my belongings in the common room, my bag could have been misplaced and stolen leading to loss of the original copy of my document thus not being able to verify my credibility and further harsh consequences. To tackle this, we use integrate blockchain to automate document verification. This paper doing so.
- Copyright and Royalties. Another famous implementation of blockchains is NFTs that are non fungible tokens. These have emerged as a groundbreaking innovation allowing Artists to protect claim their work and put it on the internet where anyone can buy them in exchange for any cryptocurrency thus making a new income source for them. There are famous sites where photographer have found a way to upload their works and make a living out of it.
- Using the smart contracts, we can reliably and securely automate processes in big factories and workplaces or even automate IoT devices.

2. List out 5 different blockchain networks in use. Write down what their speciality/specific use case is. What consensus mechanism do they use?

- Bitcoin (BTC)
    - The first and most widely used cryptocurrency, primarily designed for decentralized peer-to-peer transactions and a store of value.
    - Proof of Work (PoW)

- Ethereum (ETH)
    - A platform for decentralized applications (dApps) and smart contracts, enabling various use cases such as DeFi, NFTs, and tokenized assets.
    - Proof of Stake (PoS)

- Binance Smart Chain (BSC)
    - A blockchain for fast and low-cost smart contracts, optimized for decentralized finance (DeFi) and decentralized exchanges (DEXs).
    - Proof of Staked Authority (PoSA), a hybrid of PoS and Proof of Authority (PoA), allowing for quick transaction finality.
- Polkadot (DOT)
    - Focuses on interoperability by enabling multiple blockchains to communicate and share data securely.
    - Nominated Proof of Stake (NPoS), which combines staking with validator nominations to secure the network.
- Solana (SOL)
    - Known for its high throughput and low transaction costs, Solana is optimized for scalable decentralized applications (e.g., DeFi, gaming, NFTs).
    - Proof of History (PoH) combined with Proof of Stake (PoS).

4. Find out what UTXO is. Explain it in a few words.

- UTXOs are Unspent Transaction Outputs. They are the amount of cryptocurrency you have not spent.
- In simple words, they are like any currency bills.
- Rather than storing how much money a person has, we assign purses to the person and the purse is visible to everyone but it is not visible who it belongs to.
- Summing up all the bills in the purses makes up the balance of the person.
- The purse contains the bills and like conventional ruppee notes they are indivisble, you can use then to get change that is you have to consume a whole UTXO to get a new UTXO as the remaining amount but you cannot just bring out 5 ruppee note if you have only 10 ruppee note in the purse.

5. Why is a blockchain said to be immutable?

- Each block in the blockchain contains some data and the hash of previous block. Suppose we change something entry in one block, due to property of the hashing algorithm(generally SHA-256), the hash of that block changes.
- As the next block in line contained this current block's hash, we will have to update the prev-hash entry in the next block. Now this update causes changes in the hash of this block.
- Therefore we will require to recalculate all the next blocks which breaks the integrity of the chain, hence not possible.

6. When a fraudulent block is added to a blockchain with PoW consensus mechanism by a criminal who does not have the ability to perform 51% attack, how is the fork resolved ?

- Suppose a criminal adds a fraud block and transmits to you. You appnend it to your chain, whereas you also recieve an alternative block from an honest miner, this creates a fork. Now since according to proof of work, you stick to the chain in which most work has been put into, so the criminal need to keep adding the blocks in the fraud line of the fork and doing so is computationally expensive unless you have more than 50% of the resources.

7. What is 'Nothing-at-stake' problem in PoS? How is this avoided?

- Say you are a validator and fork has occured in the blockchain, so since for you there is no disincentive in adding block to the wrong chain unlike in PoW where adding block to wrong chain will be a wastage of resources that are generally expensive. Therefore you add blocks to both the all the chain in the fork and you will be rewarded for whichever is the correct chain. This is the Nothing at Stake problem that could the forks to grow simultaneously and not resolve.

8. Explain why 51% attack is less probable with PoS than with PoW.

    - In PoS 51% attack would require an entity to have 51% of total staked coins. This becomes prohibitively expensive in a cryptocurrency with high market cap.
    - PoS systems often have measures such as staking caps, slashing conditions (penalizing malicious actors), and decentralized governance, making it challenging to accumulate and exploit a majority stake whereas in PoW there is the regulation over mining practices, big players in mining can pool resources over a cumulative 51% and easily execute the 51% attack.
    - PoW attackers can sometimes temporarily rent hashing power from mining pools or markets like NiceHash to achieve a 51% attack whereas in PoS, acquiring control requires sustained ownership of tokens, which is not easily rented or borrowed.

9. What are digital signatures in the context of blockchains?

- Digital Signatures are mathematical concept that are used to authenticate whether the given message has been really sent by the right author only. They ensure that
    - The message is sent by the claimed sender i.e. Authentication.
    - The sender cannot deny having sent the message i.e. Non-repudiation.
    - The message was not altered in the transit i.e. Integrity.

- They use asymmetric cryptography, involving a pair of keys: a private key (kept secret) and a public key (shared with others).

- The sender uses their private key to sign the transaction data, creating a unique digital signature.
- The recipient or network nodes use the sender's public key to verify the signature.
- If the signature is valid, the transaction is accepted; otherwise, it is rejected.

10. What is the Oracle Problem? How is it solved?

- The Oracle Problem refers to the challenge of securely and reliably bridging blockchains (which are isolated, deterministic systems) with off-chain data from the real world. Blockchains cannot directly access external data, such as weather information, stock prices, or IoT sensor readings, because this would compromise their decentralization and security.
- Oracles act as intermediaries that feed external data to blockchains, but they introduce potential vulnerabilities:
    - Centralization: If the oracle is controlled by a single entity, it becomes a single point of failure.
    - Trust: Users must trust the oracle to provide accurate and tamper-proof data.
    - Manipulation: Malicious or faulty oracles can supply incorrect data, leading to flawed smart contract execution.
- Solutions to the Oracle Problem :
    - Use multiple oracles to aggregate and validate data from various sources.
    - Use techniques like zero-knowledge proofs or Merkle proofs to verify the accuracy and origin of the data without exposing sensitive information.
    - Introduce economic incentives and penalties for oracle participants to encourage honesty and punish malicious behavior.

11. (Bonus/Optional) What are Zero-knowledge proofs? How are they used in the context of blockchains?
    - Often times, a prover tries to convince a verifier that he/she has a piece of information. If could be done by sharing the piecce of info with verifier but this is trivial and involves the verifer becoming aware our sensitive information. To get rid of this, there are protocols through which the prover can convince the verifier to have possesion of certain piece of info without the verifier having any knowledge of it is. These protocols are called Zero Knowledges Proofs.