Assignment-1

1) Five Use Cases of Blockchain Technology

1. **Supply Chain Management**: Blockchain enables end-to-end visibility and traceability of goods, ensuring product authenticity and reducing fraud. It provides a tamper-proof record of transactions at each step of the supply chain.
2. **Digital Identity Verification**: Blockchain can create self-sovereign digital identities, allowing individuals to control their data and share it securely. This reduces identity theft and fraud.
3. **Healthcare**: Blockchain secures and streamlines the storage and sharing of medical records. Patients can grant access to their data only to authorized parties, ensuring privacy and security.
4. **Voting Systems**: Blockchain provides a transparent, tamper-proof, and decentralized voting mechanism. It ensures that every vote is counted correctly while maintaining voter anonymity.
5. **Credential Verification:**Blockchain can be used to securely store and verify student degrees, grades, and certificates. This eliminates the need for manual verification processes and ensures authenticity, especially during placements or higher studies applications.(use case relevant to IITK Campus Community)

2) Five Blockchain Networks and Their Specialties

1. **Bitcoin**
   - **Specialty**: Bitcoin is the first and most widely used cryptocurrency. It is optimized for secure and decentralized peer-to-peer financial transactions.
   - **Consensus Mechanism**: **Proof of Work (PoW)** – requires miners to solve cryptographic puzzles to validate transactions.
2. **Ethereum**
   - **Specialty:** Ethereum supports smart contracts and decentralized applications (dApps), enabling programmable transactions and DeFi platforms.
   - **Consensus Mechanism**: Initially **Proof of Work (PoW)**, now **Proof of Stake (PoS)** after Ethereum 2.0.
3. **Cardano**
   - **Specialty**: Cardano is designed for scalability, interoperability, and sustainability in blockchain networks, often used in academic research and enterprise applications.
   - **Consensus Mechanism**: **Ouroboros Proof of Stake (PoS)** – a research-driven PoS protocol.
4. **Hyperledger Fabric**
   - **Specialty**: Hyperledger Fabric is a permissioned blockchain framework optimized for enterprise use cases such as supply chain management and financial services.
   - **Consensus Mechanism**: Modular (supports **PBFT**, **RAFT**, and others).
5. **Polkadot**
   - **Specialty**: Polkadot enables interoperability between multiple blockchains, allowing them to share information and assets securely.
   - **Consensus Mechanism**: **Nominated Proof of Stake (NPoS)** – validators and nominators collaborate to secure the network.

3) Code in Python :

4) UTXO :

UTXO (Unspent Transaction Output) refers to the outputs of previous transactions that have not been spent yet. In a blockchain, when a transaction is made, the inputs are unspent outputs from previous transactions. These unspent outputs are then used as inputs in new transactions. UTXOs provide a way to track ownership of funds in a transparent and secure manner, ensuring that each unit of currency is accounted for.

5) Is blockchain immutable?

Yes, blockchain is immutable because it cannot be easily altered or deleted. This is due to the use of cryptographic hashes and consensus mechanisms. Each block in the blockchain contains a hash of the previous block, forming a linked chain. Changing any block would require recalculating the hashes for all subsequent blocks, which is computationally infeasible. This structure ensures that the data on the blockchain remains secure and unaltered over time, providing a tamper-proof record.

6)

When a fraudulent block is added to a blockchain with a Proof of Work (PoW) consensus mechanism by an attacker who cannot perform a 51% attack, the fork is typically resolved based on the rule that the longest chain with the most accumulated work is considered the valid one. Honest miners will continue to build on the valid chain, ignoring the fraudulent one. The chain with the most computational effort (the longest chain) prevails, and the fraudulent block is abandoned. This process ensures the integrity of the blockchain by maintaining a consistent and tamper-proof record.

7) Nothing-at-Stake :

The **Nothing-at-Stake** problem in Proof of Stake (PoS) occurs when validators can vote on multiple competing blocks without risk, since their "stake" is not directly put at risk. This allows them to benefit from multiple possible outcomes without any downside.

To avoid the **Nothing-at-Stake** problem, mechanisms like penalties or slashing are used. In these systems, if a validator is found to have voted on multiple competing chains, they are penalized, losing a portion of their stake. This discourages validators from attempting to game the system and aligns their incentives with maintaining the integrity of the blockchain.

8)

A 51% attack is less probable with Proof of Stake (PoS) than with Proof of Work (PoW) because in PoS, the attacker needs to control a majority of the total staked tokens, which is significantly harder and more costly than controlling a majority of the mining hash power in PoW. In PoW, attackers only need to control more than 50% of the computational power, which is often easier and less expensive to aggregate. In contrast, in PoS, the attacker must accumulate a majority of tokens across multiple validators, which requires a substantial financial investment and incentivizes honest participation. This economic requirement makes PoS networks more resistant to 51% attacks.

9) Digital signatures :

Digital signatures in the context of blockchains are cryptographic mechanisms used to authenticate the sender of a transaction or message. They involve a private key creating a unique signature for each transaction, which can be verified using the corresponding public key. This ensures the integrity and authenticity of the transaction, confirming that the sender has control over the private key and thus owns the funds or data associated with the transaction. Digital signatures prevent tampering and ensure that data on a blockchain remains secure and trustworthy.

10) Oracle Problem :

The **Oracle Problem** in blockchains refers to the challenge of securely integrating external, off-chain data into the blockchain environment. Since blockchains operate in isolation without direct access to real-world data, the Oracle Problem arises when they need to reference or use information from outside sources. To solve this, oracles act as intermediaries that collect, verify, and transmit this data to the blockchain. They can be centralized or decentralized; decentralized oracles, such as those provided by platforms like Chainlink, are designed to enhance security and reliability by aggregating data from multiple sources.

11) Zero-knowledge proofs :

Zero-knowledge proofs are a cryptographic method that allows one party to prove to another party that they possess certain information (like knowledge of a private key or specific data) without actually revealing the information itself. This is done by demonstrating that the knowledge exists without disclosing the content. In the context of blockchains, zero-knowledge proofs are used to enhance privacy by enabling transactions or data verification without exposing sensitive details. They allow users to prove ownership or validity of data without revealing the underlying information, which is particularly useful for preserving privacy in public blockchain systems like Zcash and Ethereum.

- Hrushikesh Roop Avvari
230249