BlockBloom

Assignment – 1

Aarav Oswal – 230012

1. The different use cases for blockchain technology are:
   1. Attendance Record of Students:

In the campus community, Blockchain technology can be used to keep a record of the attendance of students in lectures. A block can be used to record a collection of messages like “ ‘A’ attended ‘course’ on ‘date’ ”. For convinience, we can also group all messages of a course on a particular day together. The biometric (fingerprint) of students can be used as the digital signature which authenticates that a particular message is true. This structure will help in keeping a safe and untamperable record of student attendance.

* 1. Payment Records of Mess and Canteen:

The Payment Records of Mess and Canteen can be stored using Blockchain as well. We can use a similar structure to the one above. In this way, we can have a trustable and robust record of all transactions. To prevent overspending, we can also put a cap on the maximum amount spendable in a month, or alternatively, use a system where each person is allowed to spend money only which he/she has ‘bought’ earlier.

* 1. Product Tracking in the Food Industry:

Blockchain Technology can be used for tracking the route of food product from its origin. This is particularly useful in case of a disease outbreak as the source of the outbreak can be quickly found out and the outbreak controlled.

* 1. Healthcare:

Blockchain Technology can be used to store the medical record of patients securely. When a medical record is genetrated, it can signed by the patient and put into the blockchain. Records can also be encrypted before storing, thus providing for privacy.

* 1. Voting:

Blockchain technology can be used to store voting details during elections. Storing voting details in blockchain would make it near impossible to tamper with. Blockchain also provides transparency in the electoral process, reducing the man-power required.

1. The different blockchain networks currently in use are:
   1. Bitcoin (BTC):

Bitcoin is a decentralized digital currency used for secure and transparent value transfer without intermediateries.

Consensus Mechanism: Proof of Work (PoW)

* 1. Ethereum (ETH):

Ethereum is a programmable blockchain platform enabling smart contracts and decentralized applications (dApps).

Consensus Mechanism: Proof of Stake (PoS)

* 1. Binance Smart Chain (BSC):

BSC is used for fast and low-cost transactions. It is optimized for DeFi(Decentralized Finance), tokenized assests and cross-chain compatibility.

Consensus Mechanism: Proof of Staked Authority (PoSA)

* 1. Cardano (ADA):

Cardano is designed for secure and efficient dApp development, identity management, and supply chain tracking.

Consensus Mechanism: Proof of Stake(PoS)

* 1. Polkadot (DOT):

Polkadot facilitates interoperability between blockchains, allowing multiple specialized blockchains (parachains) to operate together.

1. The program is written in Python:

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

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")

1. UTXO stands for Unspent Transaction Output. The UTXO model is a book-keeping model used in cryptocurrencies like bitcoin to track the ownership and transfer of cryptocurrencies. The UTXO model works like physical cash rather than a bank account. The way it works is that the amount of cryptocurrency a user has is the sum total of the UTXOs owned by him. These UTXOs are like physical cash, i.e, they cannot be divide into smaller denominations. Each transaction in the UTXO model creates new UTXOs which are basically the leftover change that is reassigned back to the sender at the end of each transaction. A transaction in the UTXO model works by transferring ownership of the particular UTXO to the reciever in the transaction. The database in a UTXO model is populated with records of ownership changes. This model allows users to track ownership of all portions of that crytocurrency rigth back to the time it was given as block record.
2. A blockchain is said to be immutable because once data is recorded in it’s ledger it is nearly impossible to alter or delete it. This immutability is because of a number of key features of blockchain technology:
3. Cryptographic Hashing:

Each block in the blockchain contains a cryptographic hash of its data (using strong crytographic functions like the SHA-256). The data used as input to the crytographic hash functions includes the block’s index no, transaction details as well as the previous block’s hash. This makes changing the data of a particular block very difficult as it would completely change the hash of of the current block, invalidating it as well as invalidating all the blocks that follow.

1. Decentralized Network:

Blockchains are maintained by a decentralized network of nodes (computers) that work together to validate and store the data. All the nodes in a network store copies of the blockchain. When there is a clash between two copies, the network accpets the one which has a majority. Thus to change data, one has to convince the majority of the nodes to accept it, which is infeasible in a proper network.

1. Consensus Mechanism:

Blockchains use Consensus Mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) to agree on the validity of the new block. Altering a block would require re-mining or re-validating that block and all subsequant blocks, which is computationally expensive and impractical.

1. Economic Incentives:

In blockchains like Bitcoin, participants are incentivized to act honestly due to the costs associated with mining and staking. Altering data is disincentived becauuse the cost of rewriting history offen exceeds the potential rewards.

1. When a fradulent block is added to a blockchain with PoW consensus mechanism, by criminal who doesn’t have the ability to perform a 51% attack, the blockchain resolves the situation in the following manner:
2. Verification of Block:

Each node in the network independently verifies the validity of a block before adding it to their copy of the blockchain. A fraudelent block will fail validitation due to inconsistencies like invalid transactions, incorrect PoW, mismatch with previous block references.

1. Longest Chain Rule

In case a broadcasted fraudulent block is accepted by some miners, it results in the creation of a fork, where some miners build on the fraudulent block and others build on the legitimate chain. Now the way a fork is resolved is through the longest chain rule. When a fork is created, nodes don’t directly accept a fork/block into their copy. Rather they wait some time for either of the fork to become bigger. Now in a typical network, there are more honest miners as compared to fraudulent ones. And the computational power of honest miners is much greater than the attacker (the attacker will require the computational power of more than 50% of the network to successfully carry out the attack). Therefore the legitimate chain fast outpaces the fraudulent chain. Thus the legitimate chain is accpeted into the network according to the longest chain rule and the fork is resolved.

1. The ‘Nothing-at-Stake’ problem is a theoretical problem in PoS, that occurs when every validator in the systrem build on every fork when a fork takes place. There are two proimary reasons why validators are expected to do so. First the fact that in PoS, it costs validators nothing to validate on multiple forks. It is computationally inexpensive. Secondly, because it is in the validator’s financial self-interest to do so. If a validator mines on both forks, then they will collect transaction fees on whichever fork ends up winning.

There are several strategies to prevent the ‘Nothing-at-stake’ problem:

1. Security Deposits: Validators are required to place a security deposit, which is forfeited if they produce invalid blocks or behave maliciously.
2. Slasher Algorithm: This algorithm penalizes validators for signing multiple conflicting blocks, making it economically unviable for them to support multiple forks.
3. A 51% attack occurs when a single entity or group gains control of more than 50% of the blockchain network's validation power, enabling them to manipulate the blockchain. Such an attack is much less probable in PoS than in PoW for the following reasons:
4. The Cost of Acquiring: The cost of acquiring the majority stake in PoW is much less than PoS. In PoW, the attacker needs control of 50% of the computational power whereas in PoS, the attacker needs control of 50% of the network’s staked cryptocurrency. The 50% of cryptocurrency is very costly to acquire.
5. Economic Incentive: In PoS, the attacker has a very strong economic disincentive. This is because in case of attack on a cryptocurrency, it’s market value will largely depreciate. This will be harm the attacker as he owns 50% of the crytocurrency, and he/she will incur a huge loss.
6. In blockchains, digital signatures ensure the authenticity and integrity of transactions. When a user initiates a transaction, they generate a hash of the transaction data and sign it using their private key, which is known only to them. This process creates a unique signature for the transaction. To verify the transaction, other network participants use the sender's public key. A valid signature confirms that the transaction was signed by the rightful owner of the private key and that the transaction data remains unaltered.
7. The Oracle Problem in blockchain refers to the difficulty of integrating real-world data (such as stock prices, weather conditions, or sports outcomes) into the blockchain. Since blockchains are isolated systems that cannot directly access external data, they rely on external providers, known as oracles, to supply this information.

Solutions:

1. Trusted Oracles: These are third-party services that collect, verify, and deliver real-world data to the blockchain. While effective, they introduce a dependency on trust and the risk of manipulation, making the oracle's reliability crucial.
2. Decentralized Oracles: To mitigate the risks associated with a single trusted entity, decentralized oracles aggregate data from multiple independent sources. This approach enhances accuracy and reliability by reducing the reliance on any one source.