PRACTICAL: 1

AIM:

In a peer-to-peer (P2P) fund transfer system, transactions between users must be stored securely, verified, and immutable to ensure trust and transparency. Blockchain technology can be leveraged to achieve this goal. Each block in the blockchain will represent a set of fund transfer transactions, ensuring that the data remains secure, validated through cryptographic puzzles, and immutable unless explicitly modified for testing or auditing purposes.

Perform following tasks:

I. Create a Blockchain with 5 Blocks

- Build a blockchain structure where the first block is the genesis block.
- Each block stores a set of fund transfer transactions between users.
- Each block will include:
    - Block Version
    - Timestamp
    - Transaction Data
    - Hash of the Previous Block

II. Implement Mining Logic to Validate Blocks

- Develop a mining process that uses **cryptographic mathematical puzzles** (like Proof of Work).
- Miners must solve these puzzles to add new blocks to the blockchain.

III. Set Difficulty for Blocks

- Define and set a difficulty level for mining each block, ensuring the system's security by controlling block creation time.

IV. Define Block Parameters

- Each block will include the following parameters:
    - Block Version: Indicates the block structure version
    - **Timestamp:** Exact time when the block was created.
    - **Transaction Data:** Financial transactions (e.g., Alice sends 10 BTC to Bob).
    - **Previous Hash:** Hash of the previous block in the chain.

V. Verify the Blocks

- Implement logic to validate each block by:
    - Checking its hash and previous hash linkage.
    - Ensuring the cryptographic puzzle is solved correctly.

VI. Access All Financial Transactions

- Implement functionality to retrieve and display all stored financial transactions across the blockchain.

VII. Modify Block Data from Ledger (For Testing)

- Allow authorized modifications of transaction data within the blockchain to simulate real-world audit or debugging processes.

Implement following functionality using using NodeJS.

- Include functions to:
- Add transactions to blocks.
- Perform mining and validate blocks.
- Access and retrieve transaction history.
- Modify and verify block data for testing purposes.

THEORY:

Blockchain is a decentralized digital ledger technology that securely records transactions across multiple computers in such a way that the registered transactions cannot be altered retroactively. It operates on the principle of transparency, security, and decentralization.

Features of Blockchain

1. **Decentralization:** In centralized transaction systems, each transaction must be validated in the central trusted agency (e.g., the central bank), naturally resulting in cost and performance jams at the central servers. In contrast to the centralized mode, a third party is not needed in the blockchain. Consensus algorithms in blockchain maintain data stability in a decentralized network.

2. **Persistency:** Transactions can be validated quickly and invalid transactions would not be admitted by persons or miners who mining the crypto. It is not possible to delete or roll back transactions once they are included in the blockchain network. Invalid transactions do not carry forward further.

3. **Anonymity:** Each user can interact with the blockchain with a generated address, which does not disclose the real identity of the miner. Note that blockchain cannot guarantee perfect privacy preservation due to the permanent thing.

4. **Auditability:** Blockchain stores data of users based on the Unspent Transaction Output (UTXO) model.
   Every transaction has to refer to some previous unspent transactions. Once the current transaction is recorded into the blockchain, the position of those referred unspent transactions switches from unspent to spent. Due to this process, the transactions can be easily tracked and not harmed between transactions.

5. **Transparency:** The transparency of blockchain is like cryptocurrency, in Bitcoin for tracking every transaction is done by the address. For security, it hides the person's identity between and after the transaction. All the transactions are made by the owner of the block associated with the

address, this process is transparent and there is no loss for anyone who is involved in this transaction.

6. **Cryptography:** The blockchain concept is fully based on security and for that, all the blocks on the blockchain network want to be secure. For security, it implements cryptography and secures the data using the cipher text and ciphers.

Core Components of Blockchain

1. **Node:** Nodes are network participants and their devices permit them to keep track of the distributed ledger and serve as communication hubs in various network tasks. A block broadcasts all the network nodes when a miner looks to add a new block in transactions to the blockchain.

2. **Transactions:** A transaction refers to a contract or agreement and transfers of assets between parties. The asset is typically cash or property. The network of computers in blockchain stores the transactional data as a copy with the storage typically referred to as a digital ledger.

3. **Block:** A block in a blockchain network is similar to a link in a chain. In the field of cryptocurrency, blocks are like records that store transactions like a record book, and those are encrypted into a hash tree. There are a huge number of transactions occurring every day in the world. The users need to keep track of those transactions, and they do it with the help of a block structure. The block structure of the blockchain is mentioned in the very first diagram in this article.

4. **Chain:** Chain is the concept where all the blocks are connected with the help of a chain in the whole blockchain structure in the world. And those blocks are connected with the help of the previous block hash and it indicates a chaining structure.

5. **Miners:** Blockchain mining is a process that validates every step in the transactions while operating all cryptocurrencies. People involved in this mining they called miners. Blockchain mining is a process to validate each step in the transactions while operating cryptocurrencies.

6. **Consensus:** A consensus is a fault-tolerant mechanism that is used in computer and blockchain systems to achieve the necessary agreement on a single state of the network among distributed processes or multi-agent systems, such as with cryptocurrencies. It is useful in record keeping and other things.

Data Storage and Management

1. **Header:** It is used to identify the particular block in the entire blockchain. It handles all blocks in the blockchain. A block header is hashed periodically by miners by changing the nonce value as part of normal mining activity, also Three sets of block metadata are contained in the block header.

2. **Previous Block Address/ Hash:** It is used to connect the i+1th block to the ith block using the hash. In short, it is a reference to the hash of the previous (parent) block in the chain.

3. **Timestamp:** It is a system that verifies the data into the block and assigns a time or date of creation for digital documents. The timestamp is a string of characters that uniquely identifies the document or event and indicates when it was created.

4. **Nonce:** A nonce number which used only once. It is a central part of the proof of work in the block. It is compared to the live target if it is smaller or equal to the current target. People who mine, test, and eliminate many Nonce per second until they find that Valuable Nonce is valid.

5. **Merkel Root:** It is a type of data structure frame of different blocks of data. A Merkle Tree stores all the transactions in a block by producing a digital fingerprint of the entire transaction. It allows the users to verify whether a transaction can be included in a block or not.

CODE:

N/A

OUTPUT:

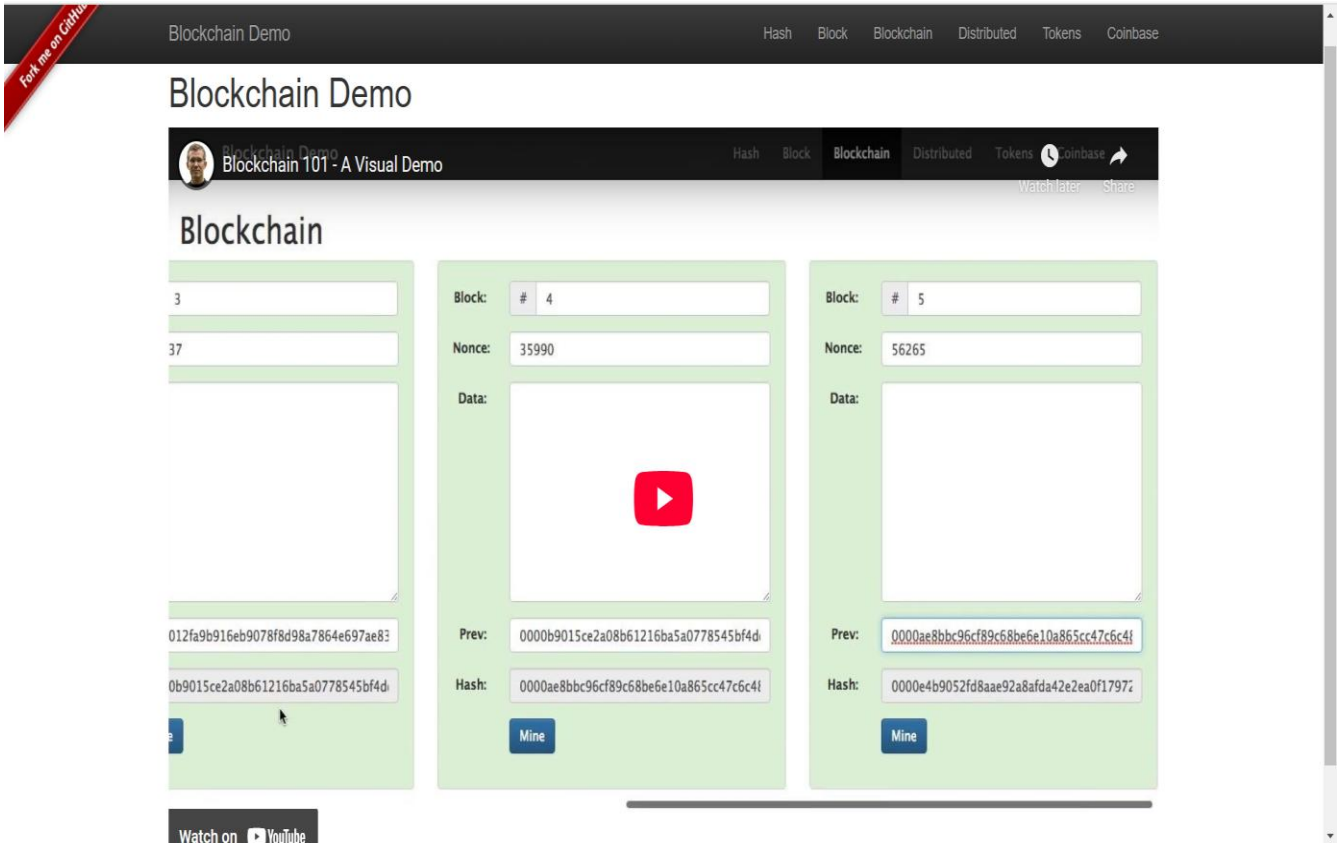

Figure 1:This is homepage of Blockchain demo and YouTube video link

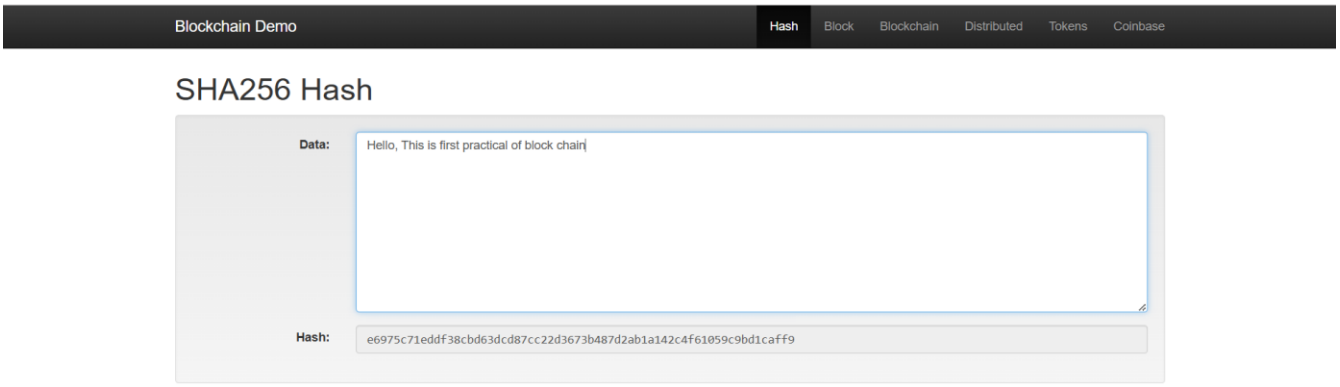

Figure 2:Calculate SHA256 hash value for our data

Figure 3:Create a block

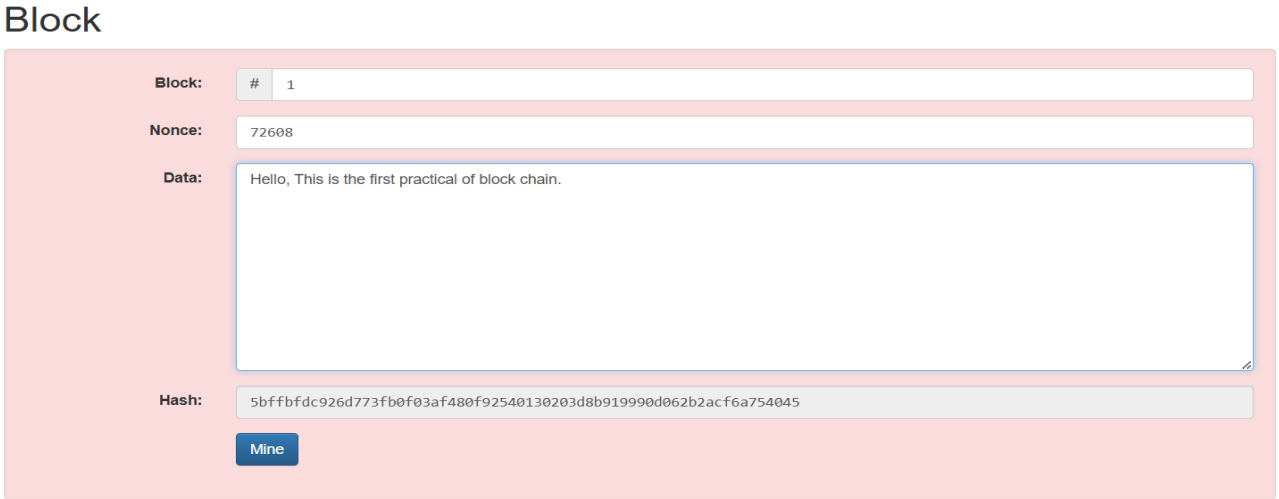

Figure 4:Add data to block and observe the change in hash value

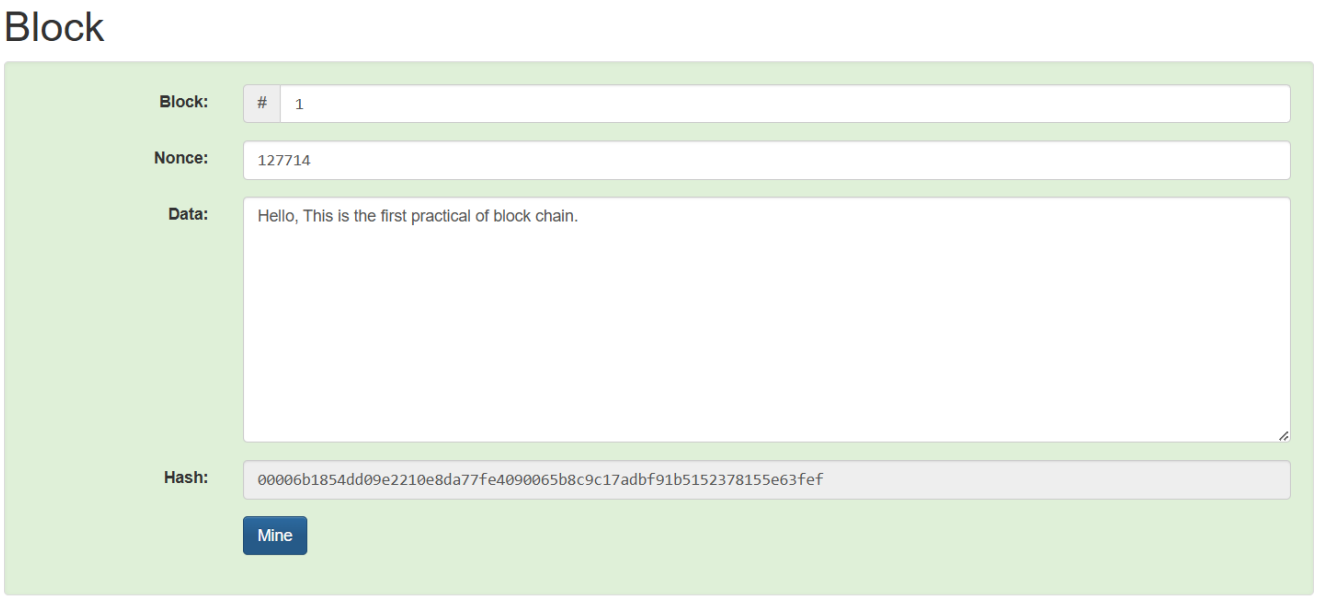

Figure 5:Change the Nonce and validate the transaction

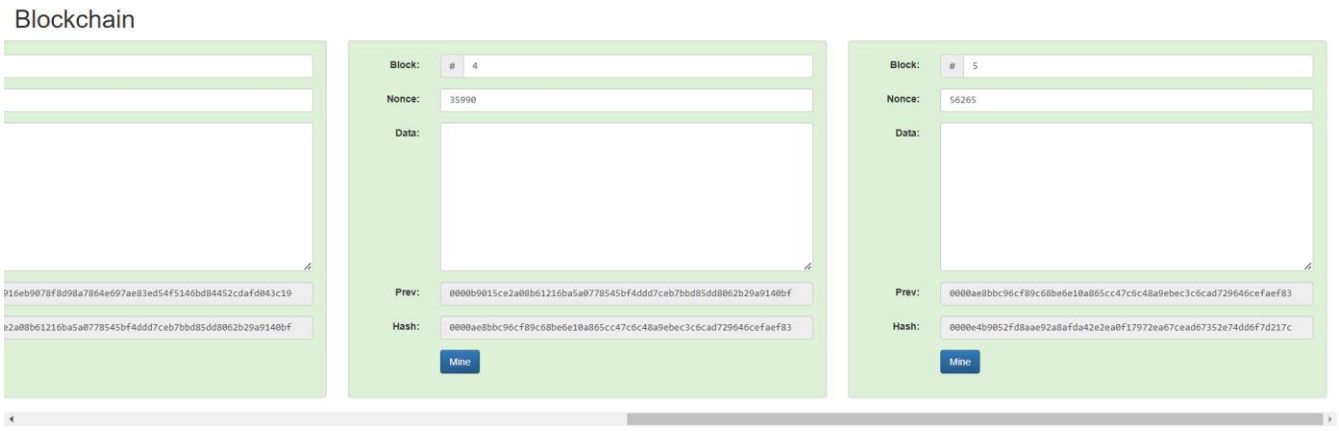

Figure 6:This is chain of blocks and hash value is depends on previous block

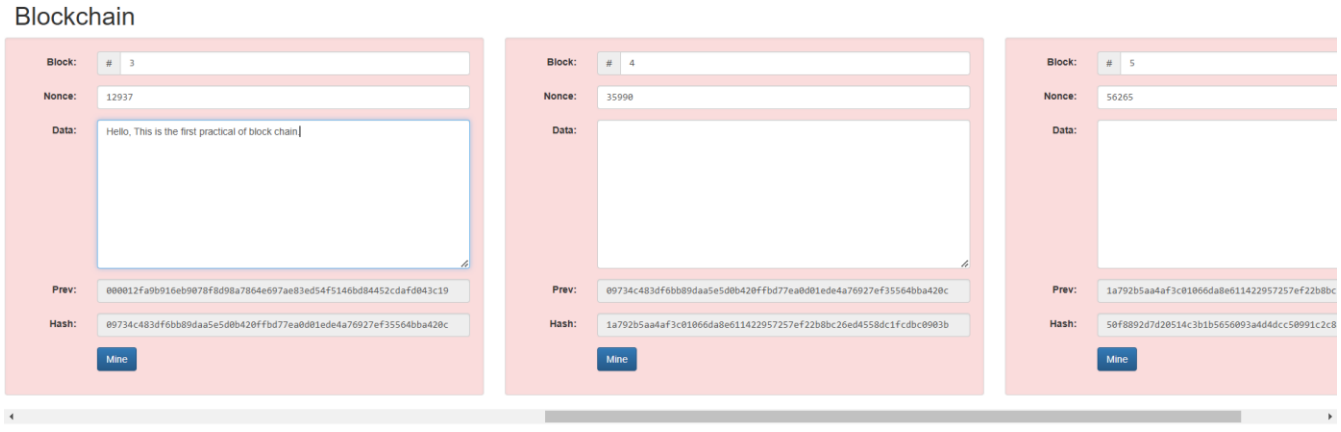

Figure 7:Change the data in block no 3 and observe the block number 4 and 5

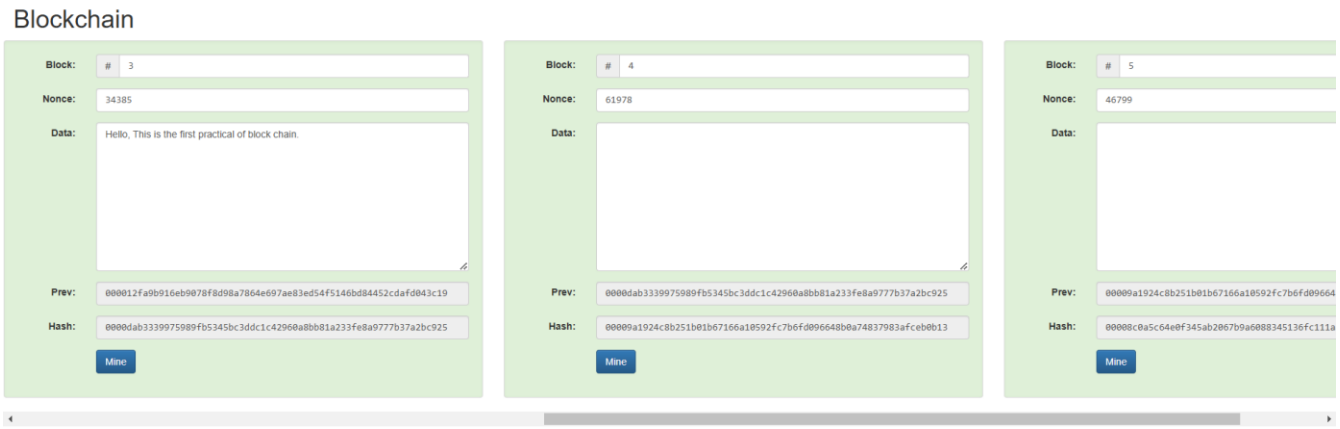

Figure 8: After mining we validate the block

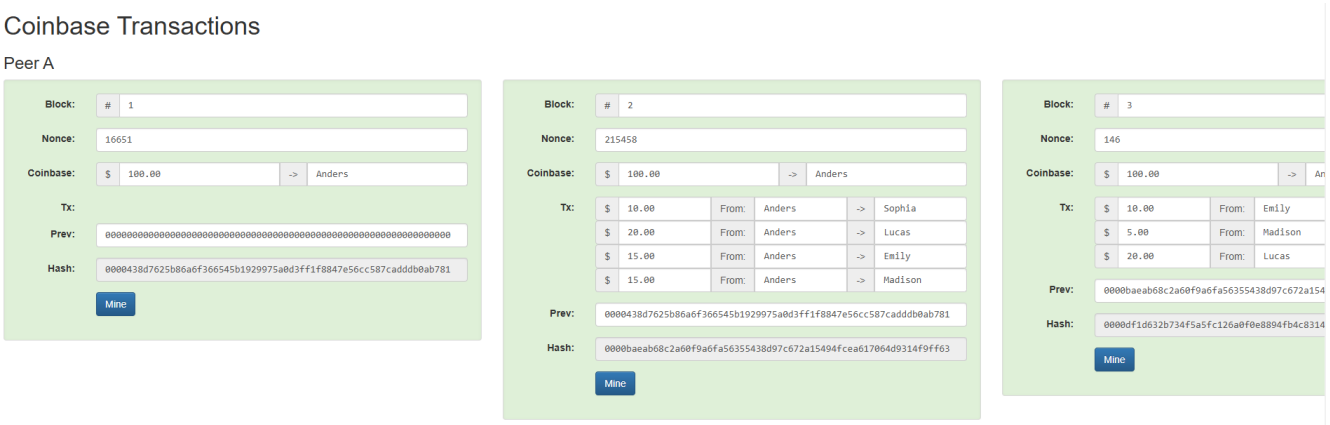

Figure 9:This is Coinbase transactions

LATEST APPLICATIONS:

- Cryptocurrency and Decentralized Finance(e.g., Aave, Uniswap)
- Supply Chain Management (e.g., IBM Food Trust, VeChain)
- NFTs (Non-Fungible Tokens) (e.g., Bored Ape Yacht Club, OpenSea)
- Blockchain for Healthcare (e.g., BurstIQ, Solve.Care)
- Digital Identity Verification (e.g., uPort, Sovrin)

LEARNING OUTCOME:

In this practical, I learned the fundamentals of blockchain, including its structure, mining process, and smart contracts.

REFERENCES:

1. Blockchain demo : https://github.com/anders94/blockchain-demo
2. ChatGPT : https://chatgpt.com/
3. GeeksforGeeks : https://www.geeksforgeeks.org/blockchain-structure/