

NAME- DEVANSHU SURANA

ELECTIVE ROLL NO-BT1-18

PANEL ROLL NO- PC-23

PRN-1032210755

PANEL-C

Assignment 1

Basic demonstration of blockchain technology

1). Aim : Provide a foundational understanding and basic demonstration of blockchain technology.

2). Objectives :

- Introduce core principles of blockchain.
- Demonstrate basic blockchain structure and functionality.
- Guide hands-on creation and interaction with a simple blockchain.
- Provide a practical understanding of blockchain's decentralized and immutable characteristics.

3). Theory :

1). Blockchain Technology :

- Blockchain technology is a decentralized and distributed ledger system designed to secure and authenticate digital transactions. It consists of a chain of blocks, each containing a cryptographic hash of the previous block, creating an immutable record. Utilizing consensus algorithms like Proof of Work or Proof of Stake, participants validate transactions, enhancing security. Smart contracts, self-executing coded contracts stored on the blockchain, automate processes. Cryptographic techniques ensure data integrity and confidentiality. This transparent, tamper-resistant system finds applications in finance, supply chain, and beyond, fostering trust by eliminating the need for intermediaries and providing a secure, transparent, and efficient framework for digital interactions.

2). Decentralisation :

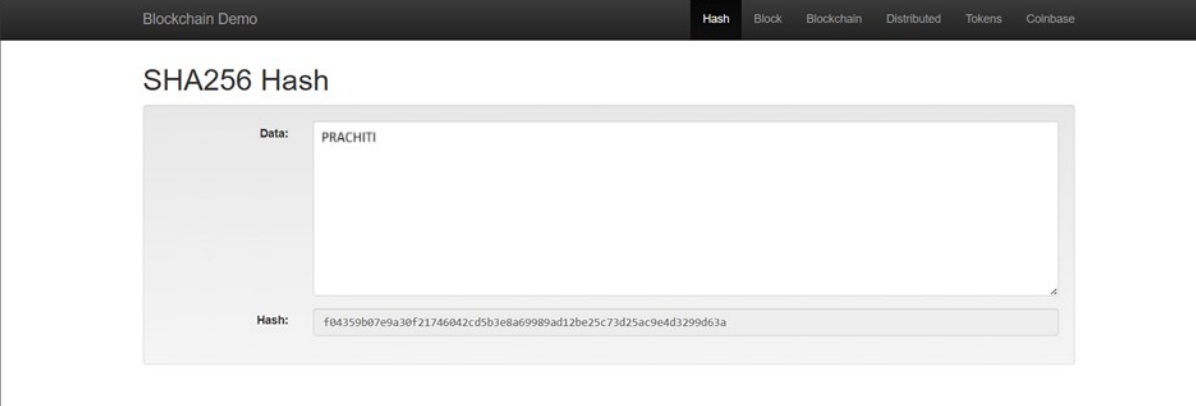
- Decentralization is a fundamental principle in various technological systems, including blockchain. In a decentralized framework, control and decision-making are distributed across

a network, removing the need for a central authority. In the context of blockchain, this entails a distributed ledger where each participant holds a copy. This architecture enhances security by eliminating a single point of failure and reducing vulnerability to malicious attacks. Decentralization also promotes transparency, as information is accessible to all participants, fostering trust. This approach is integral to blockchain's resilience, ensuring a more democratic and resilient structure for various applications, from finance to governance and beyond.

3). Tokens and Coinbases :

- In the realm of blockchain technology, coins and tokens play pivotal roles. Coins typically refer to native cryptocurrencies, such as Bitcoin or Ethereum, serving as a medium of exchange within their respective blockchain networks. These coins operate on their own blockchain and facilitate various transactions and operations. On the other hand, tokens are assets created on existing blockchain platforms, like Ethereum's ERC-20 tokens. They represent ownership of specific assets, access to services, or even voting rights. Smart contracts underpin tokens, enabling programmable functionalities. Both coins and tokens contribute to the diverse applications of blockchain, from decentralized finance to creating digital assets and fostering innovative ecosystems.

4). Implementation:



The screenshot shows a web application titled "Blockchain Demo" with a navigation bar containing links for "Hash", "Block", "Blockchain", "Distributed", "Tokens", and "Coinbase". The main content area is titled "SHA256 Hash" and features a form with two input fields. The first field, labeled "Data:", contains the text "PRACHITI". The second field, labeled "Hash:", displays the resulting SHA256 hash: "f04359b07e9a30f21746042cd5b3e8a69989ad12be25c73d25ac9e4d3299d63a".

1.1). SHA-256 example

Block

| | |
|-----------------------|--|
| Block: | # 1 |
| Nonce: | 16972 |
| Data: | Transaction 1 |
| Hash: | 0000ebaf53012c1072673649b57b87df1880639aa3c0f14c635415cbc7f145 |
| <button>Mine</button> | |

1.2). Demonstration of a sample block

Block

| | |
|-----------------------|--|
| Block: | # 1 |
| Nonce: | 88600 |
| Data: | Confirmed Transaction |
| Hash: | 00002b138b25a4575e36be5ad82c052fc9e1f575a5912b588f2018c3abdac95b |
| <button>Mine</button> | |

1.3). Demonstration of a sample block with different data

Blockchain Demo

HashBlockBlockchainDistributedTokensCoinbase

Blockchain

Block: # 1

Nonce: 22823

Data: One

Prev: 00

Hash: 00002352c160056e0a004b746ba20f56f8aa38dbfcd9a4bb4

Mine

Block: # 2

Nonce: 35230

Data:

Prev: 00002352c160056e0a004b746ba20f56f8aa38dbfcd9a4bb4

Hash: 440ab049d52e908c7a6ade11e16223fefcd178f930a34ddb6

Mine

Block: # 3

Nonce: 12937

Data:

Prev: 440ab049d52e908c7a6ade11e16223fefcd178f930a34ddb6

Hash: 1192cf6a675930ea942bf7c7808

Mine

1.4). Demonstration of a sample blockchain with changed data, showcasing immutability

Blockchain Demo

HashBlockBlockchainDistributedTokensCoinbase

Blockchain

Block: # 1

Nonce: 22823

Data: One

Prev: 00

Hash: 00002352c160056e0a004b746ba20f56f8aa38dbfcd9a4bb4

Mine

Block: # 2

Nonce: 80491

Data: Two

Prev: 00002352c160056e0a004b746ba20f56f8aa38dbfcd9a4bb4

Hash: 00009406adddf1ecbf672d2aef6b29ddf5730745b3ac7767

Mine

Block: # 3

Nonce: 130470

Data:

Prev: 00009406adddf1ecbf672d2aef6b29ddf5730745b3ac7767

Hash: 000000d720473922fb9ebd14484

Mine

1.5). Demonstration of a simple blockchain with sample data

5). FAQs:

1). What is SHA256?

Definition: SHA-256, or Secure Hash Algorithm 256-bit, is a cryptographic hash function belonging to the SHA-2 family. It produces a fixed-size 256-bit (32-byte) hash value, typically represented as a hexadecimal number.

Key Points:

Cryptographic Hash Function: SHA-256 is designed to be a one-way function, meaning it is computationally infeasible to reverse the process and obtain the original input from its hash value.

Uniqueness: Different inputs should produce different hash values, and even a small change in the input should result in a significantly different hash.

Used in Blockchain: In blockchain technology, SHA-256 is widely used to create a unique digital fingerprint (hash) for each block, ensuring the integrity of the block's content.

2). What is a block? What are its components?

Definition: A block is a fundamental component of blockchain technology, representing a set of transactions grouped together and added to the blockchain in a sequential and immutable manner.

Components:

Block Header:

Version: A version number to track the evolution of the blockchain protocol.

Previous Block Hash: The hash of the preceding block, creating a chain of blocks.

Merkle Root: A hash of all transactions in the block, ensuring integrity and organization.

Timestamp: The time when the block is added to the blockchain.

Nonce: A number used in the mining process to find a suitable hash.

Transactions:

A block contains a set of transactions, each detailing the transfer of assets or information. These transactions are bundled together and validated.

Block Hash:

The block header, including the Merkle Root and other details, is hashed using a cryptographic hash function like SHA-256 to create a unique identifier for the block. This hash is crucial for linking blocks in the chain.

Proof of Work (PoW):

In many blockchain systems, a proof-of-work mechanism requires miners to find a nonce that, when combined with the block header, produces a hash meeting certain criteria. This process ensures the security and immutability of the blockchain.

Size and Limitations:

Blocks have a maximum size to optimize network performance and scalability. Transactions are prioritized and selected based on factors like fees and data size.

Reward and Fees:

In proof-of-work blockchains, miners are rewarded with newly minted cryptocurrency and transaction fees for successfully adding a block to the blockchain.

3). List 5-10 features of blockchain technology

1. Decentralization: Blockchain operates on a decentralized network, eliminating the need for a central authority.
2. Immutability: Once data is added to the blockchain, it cannot be altered or deleted, ensuring a tamper-resistant record.
3. Transparency: All participants in a blockchain network have access to the same information, promoting transparency and trust.
4. Security: Blockchain uses cryptographic techniques to secure transactions, ensuring the integrity and confidentiality of data.
5. Smart Contracts: Self-executing smart contracts automate and enforce predefined contractual agreements when specified conditions are met.
6. Consensus Mechanisms: Various consensus algorithms, like Proof of Work (PoW) or Proof of Stake (PoS), ensure agreement among network participants.
7. Interoperability: Blockchain can be integrated with existing systems and technologies, enhancing compatibility.
8. Anonymity: While transactions are transparent, participants can maintain a degree of privacy through cryptographic methods.
9. Distributed Ledger: The ledger is distributed across all participants, ensuring a synchronized and shared record of transactions.
10. Tokenization: Blockchain facilitates the creation and transfer of digital tokens, representing assets or utility within a network.

4). List 5-10 uses of blockchain technology

1. Cryptocurrencies: The most well-known application, blockchain underpins cryptocurrencies like Bitcoin and Ethereum.
2. Supply Chain Management: Blockchain enhances transparency and traceability in supply chains, reducing fraud and ensuring product authenticity.
3. Smart Contracts in Legal Processes: Automate and enforce legal agreements, reducing the need for intermediaries.
4. Cross-Border Payments: Facilitate faster and cost-effective international transactions by bypassing traditional banking systems.
5. Identity Verification: Improve security in identity verification processes, reducing identity theft and fraud.
6. Healthcare Data Management: Ensure secure and interoperable management of healthcare records and patient data.
7. Voting Systems: Enhance the integrity of voting systems by providing secure and transparent platforms.
8. Real Estate Transactions: Simplify and streamline real estate transactions by reducing paperwork and minimizing fraud.

9. Intellectual Property Protection: Use blockchain to timestamp and protect intellectual property rights.
 10. Energy Trading: Enable peer-to-peer energy trading among users within a decentralized grid, promoting efficient energy distribution.
-

5). How are private and public keys used in blockchain technology?

- **Key Pair Generation:**
Users generate a private key (kept secret) and a corresponding public key (shared openly).
- **Public Key Cryptography:**
Public key creates a user address, visible on the blockchain.
- **Transaction Signing:**
Private key signs transactions, creating a digital signature.
- **Verification:**
Anyone can verify the signature using the public key, ensuring transaction authenticity.
- **Secure Transactions:**
Private key ownership is crucial for secure and valid transactions.
- **Wallets:**
Wallets manage private keys, simplifying user interactions.
- **Address Reuse:**
While possible, generating new addresses per transaction enhances security.
- **Key Rotation:**
Periodic private key changes can enhance security.
- **Multi-Signature Transactions:**
Involving multiple private keys adds security layers, common in corporate settings.

6). Conclusion: Went through a foundational exploration of blockchain technology, got introduced to its core principles and practical applications. Through hands-on exercises, gained insights into the creation and interaction with a basic blockchain, witnessing firsthand its decentralized, transparent, and immutable characteristics.