SOCIETE GENERALE

AI ML HACKATHON – BLOCKCHAIN BASED E-VAULT SYSTEM

College: PSG College Of Technology

Members: Devadharshini K (21L207), Visrutha M (21L262)

Branch: Electronics and Communication Engineering

Date: 13.07.2024

BLOCKCHAIN:

Blockchain is a distributed ledger technology that records transactions across many computers so that the record cannot be altered retroactively. Each block in the chain contains a list of transactions and is linked to the previous block through cryptographic hashes, ensuring data integrity and chronological order.

Key Characteristics:

- Decentralization: No single entity controls the entire blockchain; it is maintained by a network of nodes.
- Transparency: Transactions are visible to all participants on the network.
- Immutability: Once data is written to a block, it cannot be altered or deleted.
- Security: Data is secured using cryptographic techniques, making it resistant to tampering and fraud.

e-VAULT SYSTEM:

An e-Vault system is a digital storage service that provides secure, encrypted, and reliable storage for electronic documents. A blockchain-based e-Vault system enhances traditional e-Vault systems by utilizing blockchain's security and immutability features.

Key Characteristics:

- Smart Contracts: Self-executing contracts with the terms of the agreement directly written into code. They automate the management and retrieval of documents.
- Decentralized Storage: Documents are stored on a decentralized network, ensuring data redundancy and availability.
- Access Control: Fine-grained access control mechanisms to ensure only authorized users can access or modify documents.
- Auditability: Every interaction with the e-Vault is recorded on the blockchain, providing a tamper-proof audit trail.

WORKFLOW OF BLOCKCHAIN BASED EVAULT SYSTEM:

1. User Authentication:

- Users authenticate themselves using cryptographic keys or digital signatures.
- Each user has a unique address on the blockchain.

2. Document Upload:

- Users upload documents to the e-Vault.
- Documents are hashed to create a unique identifier.
- The document hash, metadata, and ownership information are recorded on the blockchain via a smart contract.

3. Document Storage:

- The actual document can be stored in a decentralized storage network (e.g., IPFS, Storj) to reduce the burden on the blockchain.
- Only the hash of the document is stored on the blockchain, ensuring the integrity and authenticity of the document without storing the actual content.

4. Document Retrieval:

- Users can retrieve documents by querying the blockchain with the document hash.
- The smart contract verifies the user's permissions and, if authorized, retrieves the document from decentralized storage.

5. Access Control and Permissions:

- Smart contracts manage access control, allowing only authorized users to view or modify documents.
- Permissions can be dynamically updated by the document owner.

6. Audit and Compliance:

- Every action, such as document upload, access, or modification, is logged on the blockchain.
- This provides an immutable audit trail, ensuring compliance with regulations and enabling transparent audits.

4. Benefits of Blockchain-Based e-Vault Systems

- Security: Enhanced security through cryptographic techniques and decentralized architecture, reducing the risk of data breaches and unauthorized access.
- Immutability: Ensures that once data is stored, it cannot be altered, providing a reliable and trustworthy record of all transactions.
- Transparency: All transactions are recorded on a public ledger, providing transparency and auditability.
- Redundancy: Decentralized storage ensures that data is replicated across multiple nodes, enhancing data availability and fault tolerance.
- Automation: Smart contracts automate processes, reducing the need for intermediaries and increasing efficiency.

5. Use Cases of Blockchain-Based e-Vault Systems

- Legal Documents: Secure storage and immutable records of legal documents such as contracts, wills, and deeds.
- Financial Records: Tamper-proof storage of financial documents and transaction records.
- Medical Records: Secure and privacy-preserving storage of patient medical records, ensuring only authorized access.

- Intellectual Property: Proof of ownership and secure storage of intellectual property like patents, trademarks, and copyrights.
- Supply Chain: Immutable records of supply chain documents and transactions, ensuring traceability and authenticity.

E-VAULT.SOL

```
// SPDX-License-Identifier: MIT

pragma solidity ^0.8.0;

/// @title EVault Contract

/// @notice This contract allows users to upload and retrieve documents.

contract EVault {

    struct Document {

        uint id;

        address owner;

        string hash;

        string name;

        uint timestamp;

    }

    uint public documentCount = 0;

    mapping(uint => Document) public documents;

    event DocumentUploaded(

        uint id,

        address owner,

        string hash,

        string name,

        uint timestamp

    );

    function uploadDocument(string memory _hash, string memory _name) public {

        require(bytes(_hash).length > 0, "Hash is required");

        require(bytes(_name).length > 0, "Name is required");

        documentCount++;

        documents[documentCount] = Document(documentCount, msg.sender, _hash, _name,
            block.timestamp);

        emit DocumentUploaded(documentCount, msg.sender, _hash, _name, block.timestamp);

    }
```

```
    function getDocument(uint _id) public view returns (Document memory) {
        return documents[_id];
    } }
```

INDEX.JS

```
const express = require('express');
const Web3 = require('web3');
require('dotenv').config();
const app = express();
const port = 3000;
const web3 = new Web3(new
        Web3.providers.HttpProvider(`https://mainnet.infura.io/v3/${process.env.INFURA_PROJECT
        _ID}`));
const contractABI = [ /* ABI from the compiled smart contract */ ];
const contractAddress = process.env.CONTRACT_ADDRESS;
const contract = new web3.eth.Contract(contractABI, contractAddress);
app.use(express.json());
app.post('/upload', async (req, res) => {
    const { hash, name } = req.body;
    const account = web3.eth.accounts.privateKeyToAccount(process.env.PRIVATE_KEY);
    const tx = contract.methods.uploadDocument(hash, name);
    const gas = await tx.estimateGas({ from: account.address });
    const data = tx.encodeABI();
    const nonce = await web3.eth.getTransactionCount(account.address);
    const signedTx = await account.signTransaction({
        to: contractAddress,
        data,
        gas,
        nonce,
        chainId: 1 // Mainnet
    });
    web3.eth.sendSignedTransaction(signedTx.rawTransaction)
        .on('receipt', receipt => {
            res.send(receipt);
```

```
    })
    .on('error', error => {
      res.status(500).send(error.toString());
    });
});
app.get('/document/:id', async (req, res) => {
  const documentId = req.params.id;
  try {
    const document = await contract.methods.getDocument(documentId).call();
    res.send(document);
  } catch (error) {
    res.status(500).send(error.toString());
  }
});
app.listen(port, () => {
  console.log(`eVault backend running at http://localhost:${port}`);
});
```

CONCLUSION:

A blockchain-based e-Vault system offers a robust and secure solution for storing and managing sensitive digital documents. By leveraging the principles of blockchain technology, such systems provide enhanced security, transparency, and immutability, making them suitable for a wide range of applications where data integrity and trust are paramount.