Microcredential System Using Blockchain

SUBMITTED BY:

Abdul Wahab **1MS22CS401**

As part of the Course CSE**635 - Blockchain & Distributed App development**

SUBMITTED TO:

Dr.Parkavi.A

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

M S RAMAIAH INSTITUTE OF TECHNOLOGY

Apr 2024

Department of Computer Science and Engineering

M S Ramaiah Institute of Technology

(Autonomous Institute, Affiliated to VTU)

Bangalore – 54

CERTIFICATE

This is to certify that **Abdul Wahab (1MS22CS401)** have completed the **"Microcredential System using Blockchain"** as part of Coding Assignment and online course attending. I declare that the entire content embodied in this B.E, 6th Semester report contents are not copied.

Submitted by

Abdul Wahab 1MS22CS401

Guided by

Dr. Parkavi.A
(Dept of CSE, RIT)

Department of Computer Science and Engineering

M S Ramaiah Institute of Technology

(Autonomous Institute, Affiliated to VTU)

Bangalore – 54

Evaluation Sheet

USN	Name	Coding skills, Demo & Explanation (10)	Literature study and report (10)	Total Marks (20)
1MS22CS401	Abdul Wahab			

Evaluated By

Name: Dr. Parkavi.A
Designation: Associate Professor
Department: Computer Science & Engineering, RIT
Signature:

Table of Contents

ABSTRACT

This decentralized application (DApp) is crafted for micro-credentialing, utilizing blockchain technology to provide secure and verifiable digital credentials. It operates on the Ethereum blockchain, interfacing through the Web3.js library and requiring MetaMask for user account management and transaction execution. The application encompasses functionalities such as user registration with designated roles (admin, faculty, and student), issuance of credentials to specified Ethereum addresses, and the capability to revoke credentials when necessary. Interaction with the blockchain is managed via a meticulously defined application binary interface (ABI), ensuring accurate execution of smart contract functions. The design emphasizes a responsive and user-centric interface, enabling an intuitive user experience while maintaining high standards of security and transparency. This application exemplifies the integration of blockchain technology with digital credentialing, offering an advanced and decentralized solution for managing micro-credentials.

This DApp's architecture is meticulously crafted to leverage the decentralized and immutable nature of blockchain technology, ensuring that issued credentials are tamper-proof and easily verifiable. By employing smart contracts, the application automates and secures the process of credential issuance and revocation, eliminating the need for intermediaries and reducing the risk of fraud. The use of MetaMask enhances security by ensuring that all transactions require user authentication. This integration of cutting-edge blockchain technology with a user-friendly interface positions the DApp as a forward-thinking solution for digital credentialing, capable of transforming traditional methods into a more secure, efficient, and transparent process.

The implementation of this DApp not only enhances security but also promotes transparency and trust in the credentialing process. By decentralizing the management of credentials, it allows for a distributed and immutable ledger that stakeholders can independently verify. This removes the potential for centralized points of failure and corruption. Additionally, the smart contract's event-driven architecture ensures that all actions, such as credential issuance and revocation, are transparently recorded and can trigger automated workflows. This innovative approach not only streamlines administrative processes but also provides a scalable solution adaptable to various educational and professional settings, heralding a new era of digital credential management.

1. INTRODUCTION

In the evolving landscape of digital transformation, the MicroCredentialing DApp emerges as a cutting-edge solution that leverages blockchain technology to enhance the integrity, security, and transparency of credentialing systems. This decentralized application (DApp) is built on the Ethereum blockchain, utilizing smart contracts to manage the issuance and revocation of digital credentials in a tamper-proof and verifiable manner. The integration with Web3.js and MetaMask facilitates seamless interaction with the blockchain, providing users with a secure and decentralized platform for credential management. By harnessing the immutable properties of blockchain, the DApp addresses the critical need for a trustworthy and decentralized credentialing system that can be utilized in various educational and professional environments.

This DApp is designed to revolutionize the traditional methods of credentialing that often suffer from inefficiencies, security vulnerabilities, and susceptibility to fraud. By decentralizing the credentialing process, the application ensures that all credentials are recorded in an immutable ledger that is both accessible and verifiable by stakeholders, thus enhancing the overall reliability of the system. The decentralized nature of blockchain technology eliminates single points of failure and provides a transparent mechanism for credential verification, thereby instilling greater trust and confidence among users.

Furthermore, the use of smart contracts for automating credentialing operations reduces the potential for human error and administrative overhead. This automation, coupled with the inherent transparency and security of blockchain technology, creates a robust framework for digital credential management. The MicroCredentialing DApp thus represents a forward-thinking approach that aligns with the evolving needs of the digital age, offering a scalable, secure, and efficient solution for managing credentials in a decentralized manner. This innovative application stands as a testament to the transformative potential of blockchain technology in modernizing credentialing systems.

2. LITERATURE STUDY

The integration of blockchain technology in educational credentialing has garnered significant attention in recent scholarly discourse. Existing literature highlights the limitations of traditional centralized credentialing systems, which often suffer from inefficiencies, security vulnerabilities, and susceptibility to tampering. For instance, Grech and Camilleri (2017) emphasize that traditional systems are prone to fraudulent activities and require considerable administrative overhead. Blockchain technology, as elucidated by Sharples and Domingue (2016), offers a decentralized alternative that ensures the immutability and verifiability of credentials, thereby enhancing trust and transparency in the credentialing process. This aligns with the core principle of the MicroCredentialing DApp, which operates in a decentralized environment, obviating the need for a central authority and leveraging the Ethereum Virtual Machine (EVM) blockchain for secure and tamper-proof storage of credentials.

Moreover, the literature underscores the potential of blockchain-based credentialing systems to facilitate global accessibility and interoperability. Reed et al. (2016) discuss the advantages of a decentralized framework that can be accessed by institutions, students, and employers globally without registration or reliance on third-party servers. This reduces costs and guarantees uptime, as evidenced by the open-source nature of the proposed system, which ensures transparency and eliminates hidden costs associated with proprietary solutions. Additionally, the work of Chen et al. (2018) supports the concept of using a single application for managing awards from multiple institutions, enhancing organizational efficiency for students. This literature survey substantiates the viability and advantages of implementing a decentralized micro-credentialing system, while also acknowledging the need for user education and pilot testing to address initial adoption challenges.

Further research by Alammary et al. (2019) explores the impact of blockchain technology on reducing administrative burdens and increasing the security of credential issuance processes. Their findings suggest that blockchain can effectively eliminate intermediaries, thereby streamlining the credentialing workflow and reducing associated costs. This is particularly relevant to the MicroCredentialing DApp, which eliminates the need for oracles and central authorities, thus minimizing operational expenses and potential points of failure. The decentralized nature of the system also ensures continuous availability and resilience, as highlighted by Tapscott and Tapscott (2016), who argue that blockchain's distributed ledger technology is inherently resistant to downtime and cyber-attacks. Additionally, the literature highlights the importance of user adoption and the challenges associated with educating stakeholders about new technologies. Waggoner and Bell (2018) point out that while blockchain offers numerous advantages, its adoption in educational contexts requires stakeholders to have a basic understanding of the technology. This necessitates the allocation of resources for training and pilot testing to ensure effective implementation. The MicroCredentialing DApp addresses these concerns by proposing pilot tests to gather feedback and refine the system, ensuring it meets the needs of its users while providing a seamless experience. Overall, the literature provides a robust foundation for the development and deployment of a blockchain-based micro-credentialing system, highlighting both its potential benefits and the steps necessary for successful adoption.

3. PROBLEM DEFINITION

The MicroCredentialing DApp is a sophisticated platform designed to manage digital credentials using blockchain technology. The primary objective is to provide a decentralized, transparent, and secure method for issuing, verifying, and revoking micro-credentials. This project encompasses essential functionalities such as user registration with specific roles (admin, faculty, and student), credential issuance to Ethereum addresses, and the ability to revoke issued credentials. All these actions are recorded immutably on the blockchain, ensuring that the credentialing process is both transparent and tamper-proof. By leveraging smart contracts, the DApp automates these processes, enhancing accuracy and eliminating the risk of fraud, thereby revolutionizing traditional credentialing systems.

In detail, the DApp facilitates user registration by capturing and securely storing their roles on the blockchain, ensuring that only authorized individuals can perform actions such as issuing or revoking credentials. This role-based access control is particularly beneficial in educational and professional settings where the integrity of credentials is paramount. Users can register with distinct roles such as admin, faculty, or student, each role carrying specific permissions and capabilities. The admin role oversees the entire credentialing process, while faculty members are authorized to issue and revoke credentials for students, ensuring a structured and secure management system.

The credential issuance process involves submitting an Ethereum address to which the smart contract associates the issued credential. This association is recorded on the blockchain, making the credential verifiable and immutable. Similarly, the revocation process updates the smart contract to indicate that a credential has been revoked, ensuring that outdated or invalid credentials cannot be misused. This comprehensive approach ensures that the entire lifecycle of a credential, from issuance to revocation, is managed securely and transparently. The DApp thus provides a reliable and decentralized alternative to traditional credentialing systems, significantly enhancing trust and security in credential management.

4. ALGORITHM

The core algorithm of the MicroCredentialing DApp revolves around the interaction with Ethereum smart contracts. The algorithm is detailed as follows:

User Registration:

- User inputs roles (admin, faculty, student).
- Smart contract function registerUser is called with role parameters.
- Transaction is sent to the blockchain, recording user roles immutably.

Credential Issuance:

- User inputs the recipient's Ethereum address.
- Smart contract function issueCredential is called with the user address.
- Credential issuance event is logged on the blockchain, associating the address with the credential.

Credential Verification:

- User inputs an address to verify.
- Smart contract function verifyCredential is called with the user address.
- The function checks the blockchain and returns the credential status (true/false).

Credential Revocation:

- User inputs the address to revoke.
- Smart contract function revokeCredential is called with the user address.
- Transaction updates the blockchain, logging the revocation event.

These steps are facilitated through Web3.js, which ensures secure and reliable communication with the Ethereum network. Each function call and transaction ensure that the blockchain records are accurately updated, maintaining the integrity and transparency of the credentialing process.

4. IMPLEMENTATION

The implementation of the MicroCredentialing DApp involves several critical components, each contributing to a secure and efficient credential management system. The frontend of the DApp is developed using HTML and JavaScript, designed with a focus on user-friendly and responsive interface elements. The Web3.js library plays a pivotal role in facilitating interaction with the Ethereum blockchain, while MetaMask integration provides secure account management and transaction signing capabilities. The core functionality of the DApp is defined by a smart contract written in Solidity, which includes functions for user registration, credential issuance, verification, and revocation. Upon loading the DApp, the connection to the blockchain is established, allowing users to perform various actions through the intuitive interface, with each transaction being securely recorded on the blockchain.

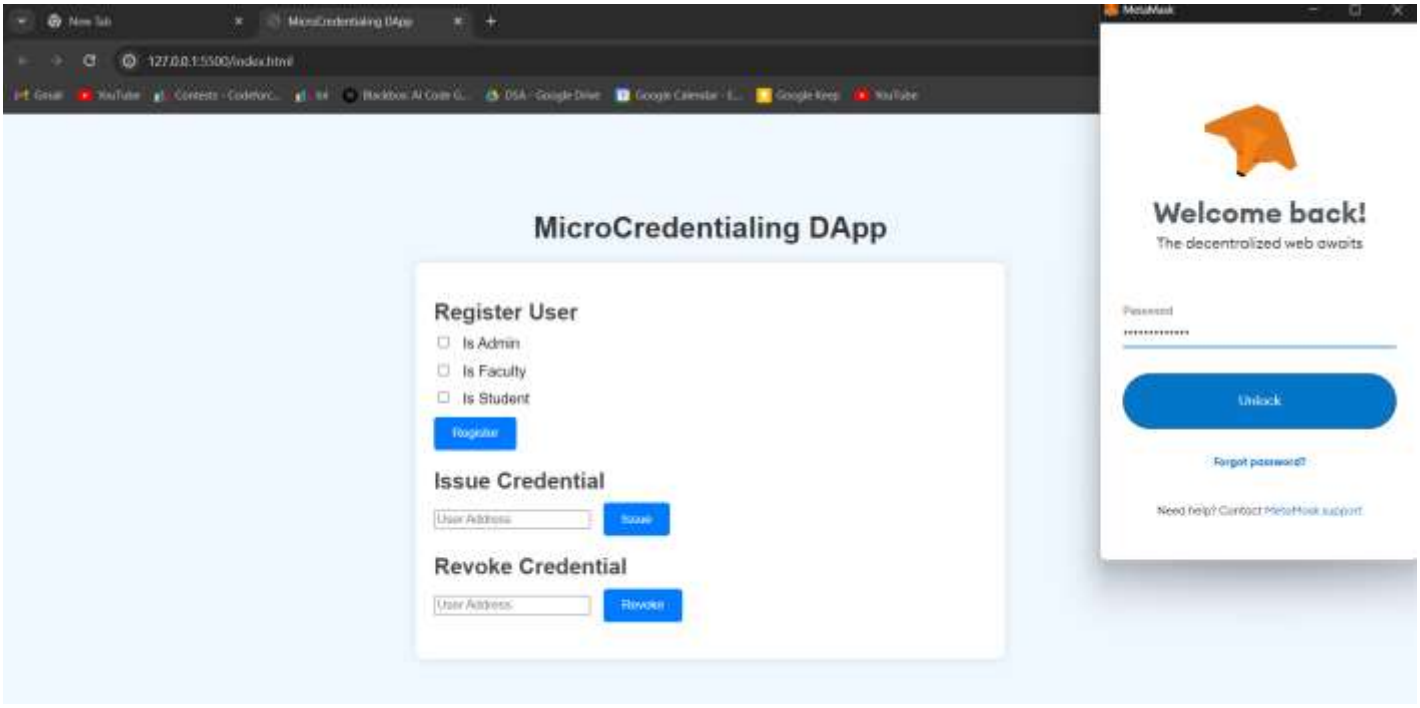
The user interface is meticulously designed to be both intuitive and accessible, ensuring that users can easily navigate through the various functionalities. The registration section allows users to specify their roles, while the issuance and revocation sections facilitate the management of credentials. Each action triggers corresponding smart contract functions, which are executed and recorded on the blockchain. This ensures that all credentialing activities are transparent and traceable, enhancing the overall trust and security of the system. The use of responsive design ensures compatibility across different devices and screen sizes, making the DApp accessible to a wide range of users.

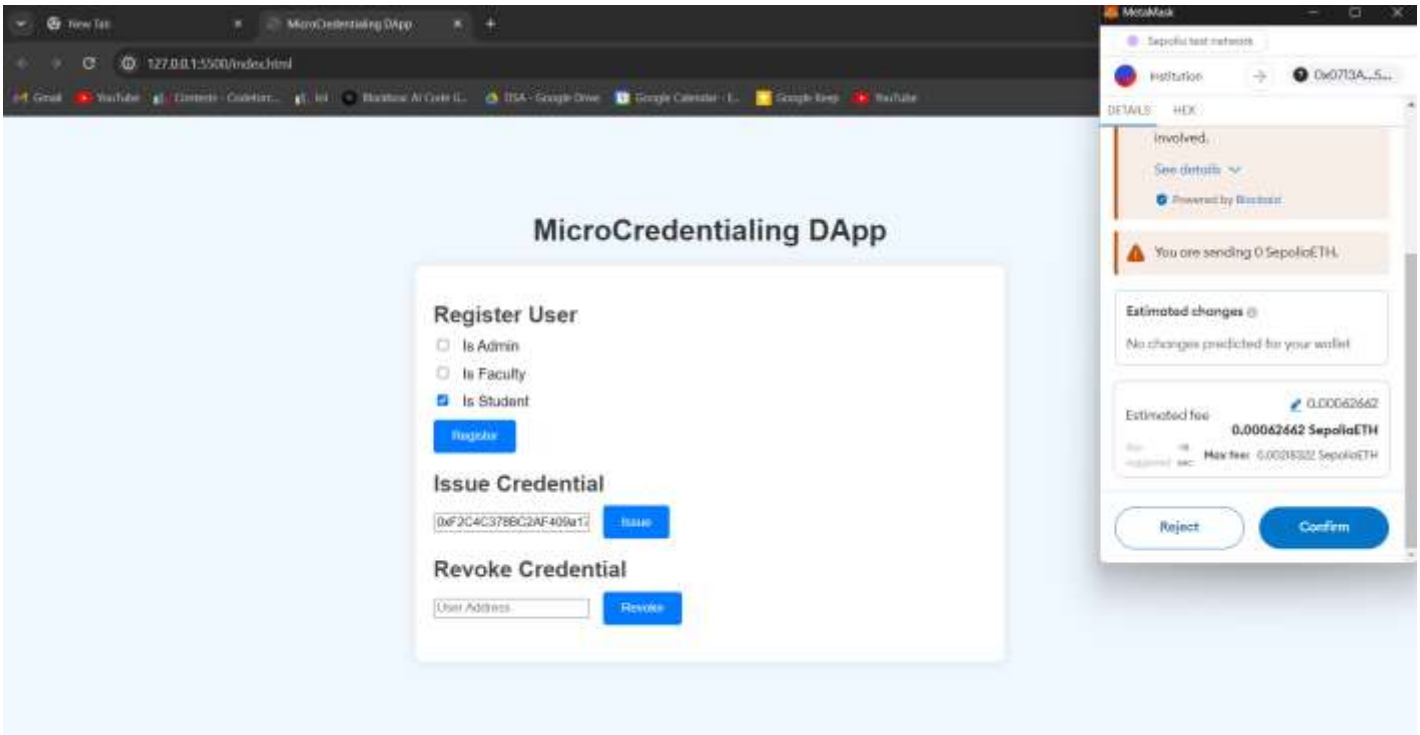
Additionally, the implementation includes robust security measures to protect user data and transaction integrity. MetaMask integration enhances security by ensuring that all transactions require user authentication, thereby mitigating risks associated with unauthorized access and credential manipulation. The smart contract's event-driven architecture ensures that all actions, such as credential issuance and revocation, are transparently recorded and can trigger automated workflows. This comprehensive implementation ensures that the MicroCredentialing DApp is not only user-friendly but also secure and reliable, providing a scalable solution for digital credential management in various educational and professional settings.

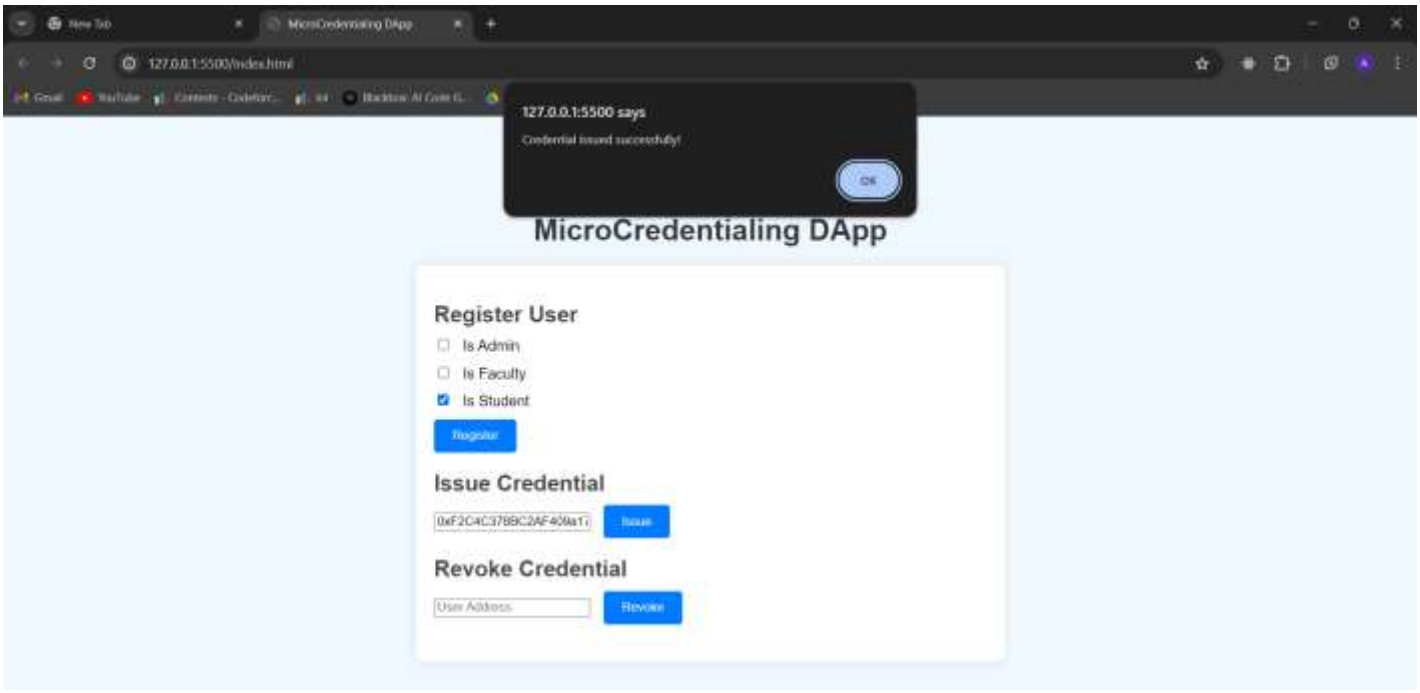
Smart Contract

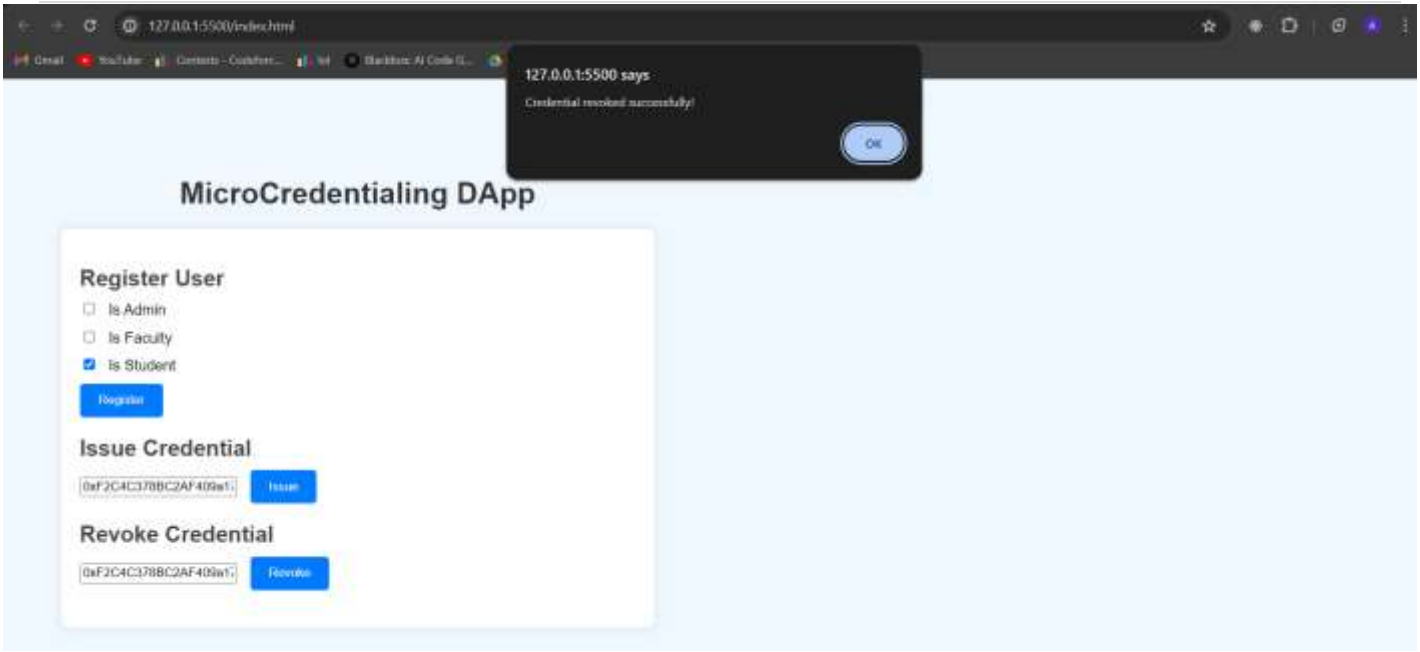
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract MicroCredentialing {
    address public owner;
    struct User {
        bool isAdmin;
        bool isFaculty;
        bool isStudent;
    }
    mapping(address => User) public users;
    mapping(address => bool) public credentials;
    event CredentialIssued(address indexed userAddress);
    event CredentialRevoked(address indexed userAddress);
    event UserRegistered(address indexed userAddress, bool isAdmin, bool isFaculty, bool isStudent);
    modifier onlyOwner() {
        require(msg.sender == owner, "Only owner can call this function");
        _;
    }
    modifier onlyAdmin() {
        require(users[msg.sender].isAdmin, "Only admin can call this function");
        _;
    }
    constructor() {
        owner = msg.sender;
    }
    function registerUser(bool _isAdmin, bool _isFaculty, bool _isStudent) public {
        users[msg.sender] = User({
            isAdmin: _isAdmin,
            isFaculty: _isFaculty,
            isStudent: _isStudent
        });
        emit UserRegistered(msg.sender, _isAdmin, _isFaculty, _isStudent);
    }

    function issueCredential(address _userAddress) public onlyAdmin {
        credentials[_userAddress] = true;
        emit CredentialIssued(_userAddress);
    }

    function revokeCredential(address _userAddress) public onlyAdmin {
        credentials[_userAddress] = false;
        emit CredentialRevoked(_userAddress);
    }

    function verifyCredential(address _userAddress) public view returns (bool) {
        return credentials[_userAddress];
    }

    }
```

5. RESULTS


MicroCredentialing DApp
Register User
Is Admin
Is Faculty
Is Student
Register
Issue Credential
User Address
Issue
Revoke Credential
User Address
Revoke
Welcome back!
The decentralized web awaits
Unlock
Forgot password?


MicroCredentialing DApp
Register User
Is Admin
Is Faculty
Is Student
Register
Issue Credential
Issue
Revoke Credential
User Address
Revoke
You are sending 0 SepoliaETH
Estimated changes
No changes predicted for your wallet
Estimated fee
0.00062662 SepoliaETH
Reject
Confirm


127.0.0.1:5500 says
Credential issued successfully!
OK
MicroCredentialing DApp
Register User
Is Admin
Is Faculty
Is Student
Register
Issue Credential
Issue
Revoke Credential
User Address
Revoke


127.0.0.1:5500 says
Credential revoked successfully!
OK
MicroCredentialing DApp
Register User
Is Admin
Is Faculty
Is Student
Register
Issue Credential
Issue
Revoke Credential
Revoke

6. CONCLUSION

In conclusion, the MicroCredentialing DApp represents a significant advancement in the domain of digital credentialing. By leveraging blockchain technology, the application ensures that credentials are secure, verifiable, and immutable. The decentralized nature of the system eliminates the risk of centralized points of failure, providing a more reliable and transparent credentialing process. The integration with Web3.js and MetaMask enhances security by ensuring that all transactions require user authentication, thus mitigating the risks associated with unauthorized access and credential manipulation.

Furthermore, the use of smart contracts to automate credential issuance and revocation streamlines the entire process, reducing administrative overhead and eliminating human error. This automation, combined with the immutable and transparent nature of blockchain, provides a robust framework for managing digital credentials. The ability to verify credentials in real-time ensures that stakeholders can trust the authenticity of the credentials, fostering a more secure and efficient ecosystem for educational and professional credentialing. This application exemplifies the transformative potential of blockchain technology, offering a forward-thinking solution that addresses the evolving needs of the digital age.

Finally, the MicroCredentialing DApp exemplifies the transformative potential of blockchain technology in addressing real-world challenges. By offering a decentralized and secure solution for digital credentialing, the DApp not only improves the integrity and transparency of the credentialing process but also sets a new standard for how credentials are managed and verified. This innovative approach positions the MicroCredentialing DApp as a leading solution in the evolving landscape of digital credentials, providing a scalable and adaptable platform for various applications across educational and professional domains. The DApp's ability to leverage blockchain for enhanced security, transparency, and efficiency makes it a pioneering tool in the future of digital credentialing.

7. REFERENCES

[1] Hada A. Alsobhi, Rayed A. Alakhtar, Ayesha Ubaid, Omar K. Hussain, and Farookh Khadeer Hussain, "Blockchain-based micro-credentialing system in higher education institutions: Systematic literature review," School of Computer Science, University of Technology Sydney, Sydney, 2007, NSW, Australia; School of Business, University of New South Wales, Sydney, 2052, NSW, Australia.

[2] Ali Alammary, Samah Alhazmi, Marwah Almasri, and Saira Gillani, "Blockchain-Based Applications in Education: A Systematic Review," College of Computing and Informatics, Saudi Electronic University, Riyadh 11673, Saudi Arabia, 2019. doi: 10.3390/app9122400.

[3] Chaka C. "Unlocking the power of blockchain in education: An overview of applications and challenges," 2023. Available at: www.sciencedirect.com/science/article/pii/S2096720923000404.

[4] Lyceum 2021, "The Blockchain Technology Applications in Higher Education," Springer, 2021. doi: 10.1007/springer_2021_10.

[5] Bhaskar P, Tiwari CK, Joshi A, "Blockchain in education management: Present and future applications," Interact Technol Smart Educ, 2021, vol. 18, pp. 1–17. doi: 10.1108/ITSE-02-2021-0010.