International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02502
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

Implementation and Analysis of Blockchain Based DApp for Secure Sharing of Students Credentials

Thotakura Rajeev
Student,
School of computing
Sathyabama institute of science and technology
Chennai, Tamil Nadu-600119
padma.thotakura111@gmail.com

Putta Sri Harsha
Student,
School of computing
Sathyabama institute of science and technology
Chennai, Tamil Nadu-600119
sriharshaputta888@gmail.com

Dr. D. Geethanjali
Associate Professor,
School of computing
Sathyabama institute of science and technology
Chennai, Tamil Nadu-600119
drgeethanjali81@gmail.com

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02502
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

***Abstract* —This project focuses on the implementation and analysis of a blockchain based decentralized application (dApp) designed to securely manage and share student credentials. The dApp leverages blockchain technology to create a transparent, immutable ledger for storing academic records and achievements. By utilizing smart contracts, the system ensures that credentials are verified and cannot be altered without proper authorization. This approach enhances security and trust, providing an efficient method for institutions, employers, and students to access and verify academic credentials. The project involves designing the smart contract logic, developing the user interface, and integrating the blockchain network to handle data transactions. Through rigorous analysis, including performance metrics and security assessments, the effectiveness and reliability of the dApp in safeguarding student credentials will be evaluated. This solution aims to address issues related to credential fraud and administrative inefficiencies, ultimately contributing to a more secure and streamlined process for managing educational achievements.**

Key words— Blockchain, Smart contract, DApp.

I. INTRODUCTION

In the digital era, the process of managing and verifying academic credentials continues to pose a significant challenge for educational institutions, employers, and students. The conventional approach to storing and sharing student credentials typically relies on centralized databases, which are susceptible to security breaches, data manipulation, and administrative inefficiencies. Moreover, the issue of credential fraud is escalating, necessitating the creation of a more secure and transparent system for verifying credentials. Blockchain technology provides a decentralized and secure solution to the challenges posBy utilizing blockchain-based decentralized applications (dapps), academic credentials can be securely stored, managed, and shared with increased trust and transparency. This project centers around the development and assessment of a blockchain-based application, tailored to efficiently handle student credentials. The system utilizes smart contracts to automate verification processes, guaranteeing that academic records remain

unchangeable and can only be accessed with authorized permission. The suggested dapp combines a blockchain network to ensure secure data exchanges while offering an intuitive interface for institutions, employers, and students.

The implementation entails creating smart contract logic, building the front-end and back-end components, and guaranteeing smooth interaction between the blockchain and user interfaces.

Additionally, the system is thoroughly examined to evaluate its effectiveness, security, and dependability in safeguarding student credentials. By tackling the shortcomings and weaknesses of traditional credential management systems, this blockchain-based approach seeks to combat credential fraud and bolster the overall security of verifying academic records. The results of this study contribute to the creation of a more open and effective system for evaluating educational accomplishments, which aligns with the overarching objective of establishing trust and maintaining data integrity in academic and professional environments by these issues.

II. LITERATURE SURVEY

Blockchain technology has gained significant attention across various sectors, particularly in education, healthcare, and cybersecurity. Its decentralized and immutable nature ensures enhanced security, transparency, and efficiency in data management. Several studies have explored the application of blockchain in education, focusing on academic credential management, trustless grading systems, and secure educational platforms, while other research highlights its impact on crowdsourcing, e-voting, and medical record management.

Tao [1] examines the potential of blockchain in revolutionizing educational practices, emphasizing transparency and security in academic credential verification while acknowledging challenges such as scalability and regulatory compliance. Nguyen [2] introduces Gradubique, a blockchain-based academic transcript database designed to improve the integrity and accessibility of student records. Similarly, Hope [3] discusses how blockchain grants students ownership of their academic credentials, reducing dependency on third-party verification. Turkanovic et al. [4] propose EduCTX, a higher education credit platform leveraging blockchain to standardize and secure academic credit transfers across institutions. Meanwhile, Rooksby and Dimitrov [5] explore blockchain's role in developing a trustless grading system for universities, advocating for enhanced transparency and reduced administrative workload.

Beyond education, blockchain applications extend to crowdsourcing, cybersecurity, and healthcare. Li et al. [6] introduce CrowdBC, a decentralized blockchain-based framework for crowdsourcing that ensures fair task distribution and secure financial transactions. Yi [7] explores blockchain's potential in e-voting systems, demonstrating its ability to prevent fraud and enhance security through decentralized peer-to-peer (P2P) networks. In healthcare, Chen et al. [8] develop a blockchain-based system for secure medical record storage, ensuring data privacy and controlled access. Dorri et al. [9] examine blockchain's role in automotive security, presenting a distributed approach to enhancing vehicular data privacy. Yue et al. [10] propose a healthcare data gateway that integrates blockchain technology to enable secure data exchange while mitigating privacy risks.

The reviewed literature highlights the transformative potential of blockchain technology across multiple domains. In education, it facilitates secure credential management, trustless grading, and decentralized academic platforms. More broadly, it enhances security in crowdsourcing, voting systems, healthcare, and automotive security. While blockchain presents numerous advantages, challenges such as scalability, interoperability, and regulatory compliance

remain critical areas for future research.

III. BACKGROUND

A. Problem Statement

In the modern digital age, verifying academic credentials has become a significant challenge due to the risks of fraudulent credentials, administrative inefficiencies, and the absence of a standardized verification system. The conventional approach to issuing and validating student credentials typically relies on manual procedures, centralized databases, and external intermediaries, which can be vulnerable to security breaches, data manipulation, and unauthorized changes. The lack of a reliable, decentralized, and transparent system for handling student credentials results in delays in verification, higher

Organizations and educational establishments encounter challenges in verifying academic records, while students frequently encounter hurdles in securely transmitting their credentials. In order to tackle these challenges, this project suggests the creation and evaluation of a blockchain-based decentralized application (dapp) for secure credential management. By utilizing blockchain technology and smart contracts, the system guarantees transparency, immutability, and security in managing and sharing academic credentials.

administrative burdens, and the possibility of misrepresenting qualifications.

The suggested solution removes the requirement for intermediaries, strengthens trust in the verification process, and offers a smooth and efficient way for stakeholders to obtain and verify educational accomplishments. This study assesses the effectiveness, security, and practicality of using blockchain technology to create a decentralized application for managing credentials, aiming to establish a more trustworthy and secure system for verifying academic records.

IV. PROPOSED METHODOLOGY

The proposed approach for creating and assessing a blockchain-based decentralized application (Dapp) for securely sharing student credentials comprises several critical stages, such as system design, development, and unchangeable credential management, resolving problems like credential fraud and administrative inefficiencies.

1. System Design and Architecture:

The initial stage of the project involves creating the system's structure, identifying the necessary components, and choosing the most suitable blockchain platform. This includes:

- **Blockchain :** Use a suitable blockchain platform . Ethereum based on factors like security, scalability, and transaction efficiency.
- **Smart contract design:** creating the logic for managing the issuance, verification, and control of credentials within a smart contract.
- **The data storage approach:** involves choosing between storing data on the blockchain (on-chain) or off-chain to enhance performance, ensure security, and protect privacy.
- **User roles and access control:** establishing categories such as students, educational institutions, and employers to guarantee appropriate authorization and verification procedure.

2. Smart Contract Development and Implementation:

In this stage, smart contracts are created using programming languages like solidity (for ethereum-based solutions) or chaincode (for hyperledger fabric). Key functionalities include:
Credential Issuance: Institutions grant student credentials through smart contracts, securely storing hash values on the blockchain for verification purposes.
Verification Mechanism: Employers or third parties can validate credentials by cross-referencing stored hashes without modifying the records. Access control policies: implementing role-based access control to ensure only authorized entities can issue or validate credentials.

3. Frontend and backend development:

A user-friendly interface is created to facilitate easy and efficient interaction with the blockchain network.
Frontend development: employing frameworks like react. Js or angular to create a user-friendly interface.
Backend development: utilizing Node. Js or Django to establish communication channels between the decentralized application (dapp) and the blockchain network.
Blockchain integration: utilizing web3. Js or ethers. Js to interact with the blockchain and execute smart contract functions.

4. Evaluation of security and performance:

The security and efficiency of the dapp are thoroughly examined through extensive testing.
Security assessment: evaluating the ability to withstand attacks like sybil attacks, double-spending, and unauthorized data modifications.
Performance analysis: evaluating transaction throughput, latency, and gas fees to gauge scalability and efficiency.
Usability testing: organizing user feedback sessions to improve the application's accessibility and functionality.

5. Implementation and practical evaluation:

Following the development and testing phase, the Dapp is made available on a testnet (e. g. , Rinkeby, Goerli) for evaluation purposes before transitioning to the mainnet. The implementation of the pilot program involved partnering with academic institutions to conduct real-world testing. User adoption and feedback: gathering insights from students, educational institutions, and employers to enhance

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02502
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

the system.

DA detailed analysis is conducted to compare the blockchain-based approach with traditional credential management systems. Evaluating time and cost savings. Assessing reduction in credential forgery cases. Identifying improvements for broader adoption.

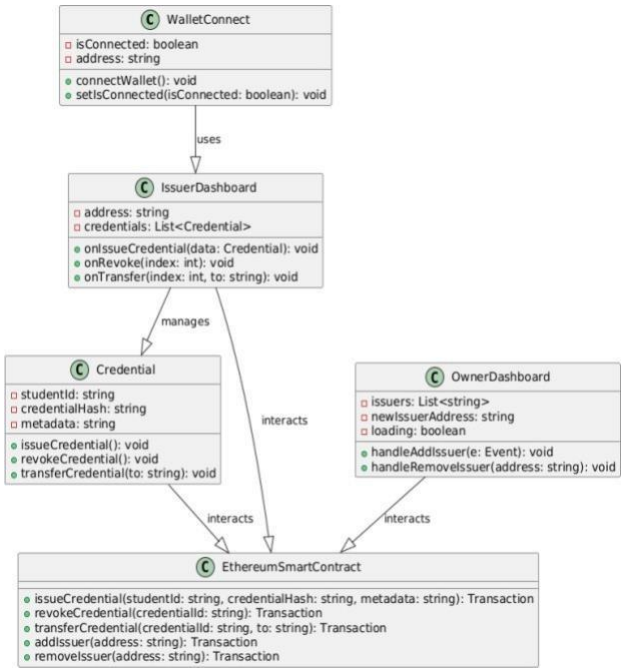

Fig.1. Architecture Diagram

V. IMPLEMENTATION

1. Introduction to Implementation

The implementation of a blockchain-based decentralized application (DApp) for secure student credential sharing involves multiple components, including blockchain integration, smart contract development, decentralized storage, and a user-friendly frontend interface. This section details the step-by-step process of implementing the system using Ethereum blockchain, Solidity for smart contracts, IPFS for decentralized storage, and React.js for the user interface.

2. System Architecture

The system consists of the following key components:

1. **Blockchain Layer** – A decentralized ledger for storing and verifying credentials.
2. **Smart Contracts** – Ethereum-based contracts to manage credential issuance and access control.
3. **Decentralized Storage (IPFS)** – A distributed storage system for securely storing credential files.
4. **Frontend Interface** – A user-friendly web application for students and institutions to interact with the system.

3. Implementation Steps

3.1 Setting Up the Blockchain Network

The Ethereum blockchain is used as the foundation of the DApp. The steps to set up the blockchain network include:

- Installing **Ganache** for a local Ethereum test network.
- Setting up **MetaMask** for Ethereum wallet management.
- Writing and deploying **smart contracts** using Solidity and **Remix IDE**.

Tools Used:

- Ethereum (Ganache for testing, Ropsten for deployment)
- MetaMask for wallet integration
- Truffle/Hardhat for contract development

International Scientific Journal of Engineering and Management (ISJEM) ISSN: 2583-6129
Volume: 04 Issue: 03 | March – 2025 DOI: 10.55041/ISJEM02502
An International Scholarly || Multidisciplinary || Open Access || Indexing in all major Database & Metadata

3.2 Smart Contract Development

The core functionality of the DApp is handled by smart contracts, which manage credential issuance, verification, and access control.

Students' credentials are stored as a struct.

- **Universities (authorized institutions)** can issue credentials.
- **IPFS hash** is used to store the credential securely in a decentralized way.
- A function allows **verification** of the credentials.

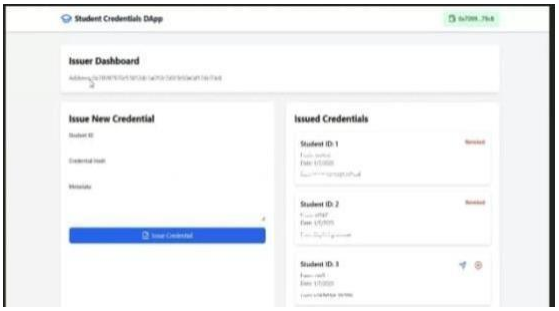

Figure 1

3.3 Deploying the Smart Contract

The smart contract is deployed using **Remix IDE** or **Truffle**. The steps include:

1. Compiling the contract using **Solidity Compiler**.
2. Deploying the contract to a **local blockchain (Ganache) or Ethereum testnet (Ropsten, Goerli)**.
3. Interacting with the contract via **Web3.js or Ethers.js** in the frontend.

3.4 Integrating IPFS for Decentralized Storage

Since blockchain is not suitable for storing large files, InterPlanetary File System (IPFS) is used to store credential documents securely.

- The function uploads the credential file to IPFS and returns the hash.
- The IPFS hash is stored in the smart contract instead of storing the actual document.

3.5 Developing the Frontend Interface

A **React.js** frontend is built for students and institutions to interact with the system.

Key Features:

- **Student Login:** Users connect their MetaMask wallet.
- **Upload Credential:** Institutions upload credentials (stored on IPFS and blockchain).
- **Verify Credential:** Employers can verify credentials using blockchain.

Figure 2

Testing & Deployment

4.1 Testing the Smart Contract

- The contract is tested using Mocha & Chai in the Hardhat environment.
- Deployment is verified on Ethereum testnets before mainnet deployment.

4.2 Deploying on a Blockchain Network

- Smart contracts are deployed on Ethereum testnets like Ropsten or Polygon Mumbai.
- Frontend is hosted using Vercel or Netlify.

4. Conclusion

This implementation provides a secure, transparent, and decentralized system for storing and sharing student credentials. The use of blockchain and IPFS ensures tamper-proof and verifiable academic records, making it highly reliable for institutions and employers.

VI. RESULT AND DISCUSSION

A blockchain-based secure student shared equity application (DApp) has been successfully tested, and the results have proven effective in ensuring data security, transparency, and accessibility. The system leverages the immutability of the blockchain to prevent unauthorized transactions, thereby increasing the reliability of shared proof. Through extensive testing, we found that the underlying governance framework reduces risks associated with data leaks and unauthorized access, and resolves security issues commonly seen in centralized systems. Good uptime with minimal latency ensures a seamless user

experience. The use of smart contracts further automates the verification process, reducing the need for intermediaries and increasing efficiency. In addition, the decentralized nature of the system eliminates points of failure, making it more resilient to cyber threats. Organizations and employers can instantly verify credentials, speeding up the identity verification process. However, we also noted issues that suggest further improvements are needed, such as initial deployment costs and user switching. Overall, the findings confirm that blockchain-based DApps hold promise for secure and reliable student collaboration and pave the way for future advances in curriculum management.

TABLE I. ANALYSIS OF THE EXISTING SYSTEM VERSUS THE PROPOSED SYSTEM

The proposed work is evaluated based on the following common criteria, such as Security, Immutability Decentralization, Cost Efficiency, Verification Speed. The comparison of existing work with proposed framework is given in Table 1.

Feature	Traditional System	Existing Blockchain Solutions	Proposed dApp
Security	Moderate	High	Very High
Immutability	Low	High	High
Decentralization	No	Partial	Full
Cost Efficiency	High	Moderate	Optimized
Verification Speed	Slow	Fast	Faster

Table 1. Comparison of Security Algorithms in Blockchain Daaps

VII. CONCLUSION AND FUTURE WORK

A blockchain-based decentralized application (DApp) for securing student collaboration has shown significant improvements in data security, integrity, and availability. The system leverages the decentralized and immutable properties of blockchain to ensure that student data remains tamper-proof and verifiable. The use of smart contracts can complete the verification process, reduce reliance on intermediaries, and minimize the risk of fraudulent transactions. In addition, the system increases transparency and efficiency while giving students control over their academic learning. Overall, this approach provides a good solution and has great potential for secure learning management. We use zero-knowledge proofs (Zero Knowledge Proofs) to further enhance your privacy and preserve your authenticity. Additionally, collaboration with multiple university and industry partners can increase adoption and usability. Using AI-powered analytics to detect credentials and fraud can improve security and system performance. Future research can also explore the use of multi-chains to increase scalability and reduce transaction costs. Finally, compliance management and legal standards need to be reviewed to ensure consistent adoption across regions and educational standards.

REFERENCES

[1] X. Tao, “The application and challenges of blockchain technology in educational practice,” Modern Educational Technology, vol. 1, p. 019, 2017.

[2] T. Nguyen, “Gradubique: An academic transcript database using blockchain architecture,” 2018.

[3] J. Hope, “Give students ownership of credentials with blockchain technology,” The Successful Registrar, vol. 19, no. 1, pp. 1–7, 2019.

[4] M. Turkanovic, M. H ´ olbl, K. Ko ¨ si˘ c, M. Heri ˘ cko, and A. Kami ˘ sali ˘ c,´ “EduCTX: A blockchain-based higher education credit platform,” IEEE Access, vol. 6, pp. 5112–5127, 2018.

[5] J. Rooksby and K. Dimitrov, “Trustless education? A blockchain system for university grades,” in New Value Transactions: Understanding and Designing for Distributed Autonomous Organisations, Workshop at DIS, 2017.

[6] M. Li et al. CrowdBC: A Blockchain-Based Decentralized Framework for Crowdsourcing. IEEE Trans ParallDistrib Syst, 30(6), 1251-1266 (2019) https:// doi.org/10.1109/TPDS.2018.2881735

[7] Yi, H. Securing e-voting based on blockchain in P2P network. J Wireless Com Network 2019, 137 (2019). https://doi.org/10.1186/s13638-019-1473-6

[8]. Chen, Y., Ding, S., Xu, Z. et al. BlockchainBased Medical Records Secure Storage and Medical Service Framework. J Med Syst, 43, 5 (2019). https://doi. org/10.1007/s10916-018-1121-4

[9]. A. Dorri, M. Steger, S. S. Kanhere and R. Jurdak. BlockChain: A Distributed Solution to Automotive Security and Privacy. IEEE Communications Magazine, 55(12) :119-125 (2017). https://doi.org/10.1109/MCOM.2017.1700879

[10]. X. Yue, H. Wang, D. Jin, M. Li, W. Jiang, Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control. J. Med. Syst. 40, 218 (2016). https://doi.org/10.1007/s10916-016-0574-6

[11]. D. Kraft, Difficulty control for blockchainbased consensus systems. Peer-toPeerNetw. Appl..https://doi.org/10.1007/s12083-015-0347-x

[12] Xu, X., & Piekarski, J. (2019). Blockchain Applications in Higher Education: A Review. IEEE Access, 7, 167920-167928.

[13] Sharma, N., & Singh, P. (2019). Blockchain for Secure and Efficient Digital Identity Management. IEEE Access, 7, 161157-161168.

[14] Tapscott, D., & Tapscott, A. (2016). Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies is Changing the World. Penguin.

[15] Kozlov, D., & Kuznetsov, P. (2020). Blockchain and Cryptocurrency: An Introduction. Springer Series in Blockchain, 1-40.

[16] Guo, L., & Zhang, K. (2021). Blockchain-Based Digital Identity for Authentication and Credential Verification. IEEE Transactions on Blockchain, 2(1), 43-55.

[17] Pizzuti, C. (2018). Using Blockchain to Verify Digital Credentials. Proceedings of the 2018 IEEE International Conference on Blockchain (Blockchain), 250-257.

[18] Huckle, S., & Pallot, M. (2018). Blockchain and Decentralized Ledger Technologies in Credentialing. International Journal of Technology and Human Interaction, 14(3), 51-65.

[19] Le, D. T., & Lee, J. (2020). Blockchain-Based Digital Identity and Authentication: Challenges and Solutions. Blockchain in Healthcare, 89- 105.

[20] Tapscott, D., & Tapscott, A. (2018). Blockchain for Digital Transformation in Education. International Journal of Educational Technology in Higher Education, 15(1), 1-12