International Journal of Scientific Research in Computer Science, Engineering and Information Technology

ISSN : 2456-3307

OPEN ACCESS

Available Online at : www.ijsrcseit.com

doi : https://doi.org/10.32628/CSEIT2410266

SuperCert - An Anti-Fraud Identity Intelligence Blockchain Solution for Educational Certificates

Akanksha Gairola[1], Amira Shaikh[1], Shriya Salian[1], Shankar Malve[1],Mr. Pravin Jangid[2]

[1]Student, Computer Engineering Department, Shree LR Tiwari College of Engineering, Mira Road, Mumbai, Maharashtra, India

[2]Assistant Professor, Computer Engineering Department, Shree LR Tiwari College of Engineering, Mira Road, Mumbai, Maharashtra, India

ARTICLEINFO

Article History:

Accepted: 10 April 2024

Published: 18 April 2024

Publication Issue

Volume 10, Issue 2

March-April-2024

Page Number

541-550

ABSTRACT

In recent years, the proliferation of fraudulent educational certificates has posed significant challenges to academic institutions, employers, and individuals alike. Such certificates not only undermine the credibility of educational achievements but also jeopardize the integrity of various industries. To combat this issue, this research introduces SuperCert, an innovative anti-fraud identity intelligence blockchain solution tailored for educational certificates. SuperCert leverages blockchain technology to establish a decentralized, immutable ledger that securely stores educational credentials. The system incorporates smart contract functionality to automate verification processes, thereby reducing administrative overhead and enhancing efficiency.

Keywords : Transcript, Verification, Authentication, Confidentiality, Blockchain, Smart Contract, IPFS, Ethereum, Metamask, University.

I. INTRODUCTION

In today's increasingly digital and interconnected world, the validity and authenticity of educational certificates have become paramount. Traditional methods of certificate verification, relying on manual processes and centralized databases, have proven inadequate in addressing the growing sophistication of fraudsters. Falsified documents, altered credentials, and identity theft continue to plague educational institutions, employers, and individuals, leading to widespread distrust and inefficiencies in the verification process. To combat this pervasive issue, this research introduces SuperCert, an innovative anti-fraud identity intelligence blockchain solution specifically designed for educational certificates. SuperCert harnesses the power of blockchain technology, which offers a decentralized, immutable ledger capable of securely recording and verifying transactions. SuperCert incorporates smart contract functionality, enabling automated verification processes and reducing the administrative burden on educational institutions and employers. SuperCert incorporates smart contract functionality, enabling automated verification processes and reducing the administrative burden on educational institutions and employers. Ultimately, this research contributes to the ongoing discourse on blockchain-based solutions for

identity management and underscores the transformative potential of SuperCert in ensuring the integrity of educational certificates in the digital age.

II. BACKGROUND

Hard copies of student transcripts were traditionally kept in secure locations, such as a school's academic department or registrar's office. The problem occurs when students pursue further education and the institution needs to verify the transcript they have been given. The difficulty with the certificate for validation is its size; occasionally, the data can get lost or changed. The validator finds it challenging to validate every certificate. With the development of technology, forging fake certifications is simpler. Differentiating between real and fake credentials takes a lot of effort and time. Because of centralization and digitization, the problem of fake credentials has become a nuisance for organizations and recruitment firms alike. Because of centralization and digitization, the problem of fake credentials has become a nuisance for organizations and recruitment firms alike. Innocent people could lose their lives as a result of fake medical care provided by counterfeit doctors and fraudulent structures created by fraudulent engineers.Even the institute engages in time-consuming collaboration with colleges and universities.

III. PROBLEM STATEMENT

The development of a blockchain application that enables educational institutions to preserve immutable transcript records for their students necessitates the creation of an accessible user interface for administrators and students alike. After courses are finished or academic milestones are reached, administrators enter relevant data into the application, which generates digital transcripts that are time-stamped and cryptographically signed. Together with their cryptographic signatures, these transcripts are securely stored on a blockchain network, ensuring transparency and immutability. Afterwards, by obtaining access to the blockchain and confirming the veracity of transcripts, corporations can view comprehensive academic records with cryptographic proof of integrity. Data security and privacy are given top priority by the program through the use of robust encryption and access controls.Scalability and interoperability are important considerations since they can handle various data volumes and interact with existing academic systems with ease. Ongoing technical support and maintenance ensure smooth operation, maximizing adoption and usefulness. All things considered, this blockchain application assists students and companies who verify educational qualifications by enhancing the security, transparency, and dependability of academic information. The current methods are functional, but since the process often takes several weeks, efficiency and security need to be increased. This is costly and environmentally damaging, in addition to being inconvenient and time-consuming.

The solution to this problem is to recognize fake certificates, store certificates, and streamline the internal verification process of an organization's certificates without using a third party.

IV. RELATED WORK

The possibilities of blockchain technology outside of cryptocurrency have attracted a lot of interest lately, especially in the field of education. A number of topics have been studied by academics, such as secure data sharing frameworks, smart contracts for record verification, and decentralized credentialing systems. Initiatives like the Blockchain-based Educational Record Repository (BcER2) [1], which build upon this fundamental research, provide workable options for securely organizing and disseminating educational records. BcER2 promises to transform educational record management by enabling the easy transfer, sharing, and distribution of e-diplomas and e-certificates among professionals in academia and

business. This is achieved by utilizing blockchain's intrinsic qualities of authenticity and immutability.

The principles and uses of blockchain technology in a variety of fields, especially education,. Blockchain is still underutilized in supply chain management, banking, insurance, healthcare, and electronic voting, despite its global recognition. It highlights how blockchain has the ability to revolutionize traditional credentialing procedures by highlighting its decentralized structure and unmatched security. The study creates a blockchain certificate system by utilizing Ethereum's platform and the Ethereum Virtual Machine (EVM). [2] This ensures tamper-proof verification through the creation of blocks and distinct hash codes. To maximize blockchain functionality, several consensus methods are used, including Proof of Work (PoW), Proof of Stake (PoS), and Proof of Capacity (PoC). To guarantee the integrity of digital diplomas, the suggested authentication technique makes use of blockchain APIs for transaction validation and verification as well as issuance applications. In general, the research highlights blockchain's role in revolutionizing transparency, expediting verification processes, and fostering trust in the educational ecosystem.

A thorough analysis of blockchain-based digital degree certificate verification. It highlights how important it is to have a decentralized application to effectively handle counterfeit issues, especially considering how many students in India graduate each year. The suggested system seeks to offer verifiable digital certificates with anti-counterfeit safeguards by utilizing blockchain's immutable feature. The procedure involves creating a paper certificate with a unique code attached to it and then uploading it to a public blockchain for safe verification. With less time and money spent on manual verification techniques, this novel approach aims to expedite certificate verification procedures and provide users with more control over their data. [3] It describes the system's architecture and design.

The security of educational certificate verification processes is enhanced through the use of Hyperledger Fabric to construct a blockchain-based architecture. The suggested system provides advantages such as permissioned access, distinctly recognizable digital certificates, transparent network communication, and effective grievance redressal methods by utilizing Hyperledger's permissioned network capabilities. In general, the study enhances the dependability and security of document verification in the academic field, with consequences for ownership, authorization, privacy, and secrecy. [4]

A system that transforms centralized storage into distributed storage records transactions via a decentralized system rather than a centralized one and allows each node to verify the transaction. For this reason, it can be used to store fingerprints from transcripts and official diploma documents that are made public. In order for contracts like diplomas and transcripts uploaded on the Ethereum blockchain to distribute and produce diploma validation and the authenticity of transcripts with transaction hash, consensus, and compliance with ERC-721 token standardization, [5] smart contracts are required for making contract transactions to Ethereum with programming code.The findings demonstrated that it is simple to verify the authenticity of a sample of five electronic documents in PDF format that were published and secured using Ethereum blockchain technology. Our proposed and developed system accounts for invalid and failure cases by providing the user with the appropriate feedback.

The management, preservation, authentication, and potential for tampering of traditional paper and electronic certificates present issues. Certificates are frequently faked, and the fakes are frequently identical to the real ones. As such, the process of certification and verification needs to be improved immediately. We suggest a project that uses blockchain technology for certificate verification in order to safeguard the problems. The college certificate will be uploaded, and the university will enter the student's roll number first.

It will then be saved on the Interplanetary File System (IPFS) [6] and assigned a distinct hash value. Then, with the roll number and distinct hash value, anybody—student, recruiter, or administrator—can obtain and validate the college certificate. In the event that the produced hash value is lost, certificate validation can also be carried out by supplying the certificate and the student's roll number. This method promises speedier verification of educational diplomas, lower expenses, and increased security.

IPFS is a modular set of data organizing and transfer protocols founded on content addressing and peer-to-peer networking. [8] [9] Because IPFS is open-source, it has a wide range of implementation options. While IPFS has various uses, its primary purpose is to publish data (files, directories, webpages, etc.) in a decentralized manner. The use of IPFS facilitates data storage and sharing on distributed networks.

The study explores the development of a distributed file system (DFS) using Solidity [11], a programming language designed for smart contracts on Ethereum. Its aim is to create a user-friendly application for sharing and managing files using blockchain technology. The methodology includes several components, including the design of a smart contract that defines the rules and functions of file management. Tools like Pinata and MetaMask allow users to effectively interact with the system. Uploaded files are assigned a unique ID and are stored in the InterPlanetary File System (IPFS) and Pinata file hosting. MetaMask emphasizes user participation, but smart contract rules govern the storage and retrieval of final files. The DFS architecture consists of several layers: an intelligent application layer, a network layer that ensures proper distribution of files, a storage layer that uses IPFS storage, and a security layer that uses blockchain technology.

The security themes needed for the blockchain-based verification of educational certificates were found and examined in this study. [20] Furthermore, a blockchain-based framework based on the Hyperledger Fabric Framework is suggested for the verification of educational certificates, with an emphasis on certain issues. The blockchain's security themes of ownership, privacy, confidentiality, authorization, and authentication are necessary for the verification of educational diplomas. Employers will be able to see through authentication that the student is reliable and capable of substantiating their statements about their education. Through authorization, the student will be able to complete duties for which they are legally allowed and with the required permits. Confidentiality and privacy will demonstrate that the information and identity contained in the certificate are safeguarded. The suggested framework will be used and applied to a few chosen educational institutions for subsequent work.

V. PROPOSED SOLUTION

To address the difficulty of storing and authenticating transcripts without a central authority while also providing an immutable record using IPFS and the Ethereum Public Blockchain, this solution allows higher education institutions to use this website to check students' transcripts directly through the website. This contributes to the elimination of third parties/centralized authorities, such as universities and colleges, by leveraging blockchain's immutability to prevent tampering or alteration of educational records once they are recorded on the ledger, as many colleges and universities use their own private servers, resulting in centralization.

Using IPFS, the system may deliver high performance and low latency, making it an ideal solution for file storage and sharing. IPFS generates CIDs (content identifiers, which are labels used to point to stuff in IPFS) that can be used as proof of work for transcripts. SuperCert enables educational institutions to register on SuperCert and securely issue digital certificates upon program completion. A real-time verification system that allows instant validation of certificates by educational institutions, or any third-party verifier which enables decentralized verification

by providing direct access to blockchain records, ensuring trustworthiness and transparency.

SuperCert offers a comprehensive solution to combat fraud in educational certificates by leveraging blockchain technology, robust verification mechanisms, anti-fraud measures, and a user-centric approach. Through continuous improvement, SuperCert aims to establish itself as the go-to platform for secure and trustworthy verification of educational credentials.

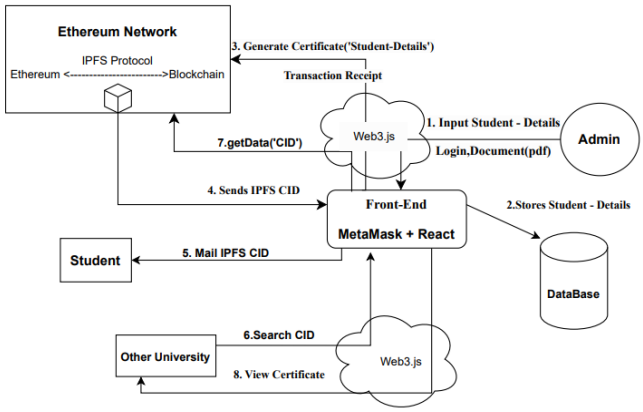

Fig. 1. Data Flow diagram of the Proposed System

Pseudo code: For Admin:

```
// Admin enters credentials
credentialsForm = displayForm() // Display a form for the admin to enter credentials
pdfFile = credentialsForm.uploadPDF() // Admin uploads a PDF file of minimum 10MB
studentEmail = credentialsForm.getEmail() // Admin enters student email
studentName = credentialsForm.getName() // Admin enters student name

// Payment process through Metamask
paymentStatus = metamaskPayment() // Initiate payment process through Metamask
if paymentStatus == approved:
  // Generate CID and store in IPFS
  cid = generateCID(pdfFile) // Generate CID for the uploaded PDF file
  ipfsStore(cid, pdfFile) // Store PDF file in IPFS with generated CID

  // Send CID through email
sendEmail(studentEmail, "Your CID", cid) // Send generated CID to student's email
```

Pseudo code: For verifier:

```
// Verifier verifies CID
function verifyCID(cid, studentName, verifierName, organizationName):
  if cidExistsInIPFS(cid):
    // Open document
    document = openDocument(cid) // Retrieve document associated with CID from IPFS
    displayDocument(document) // Display the document to the verifier
    logVerification(cid, studentName, verifierName, organizationName, "Verified") // Log verification status
    return "Document opened"
  else:
    return "Credentials not found"
```

To understand the proposed solution more clearly, here is the architecture of the system:

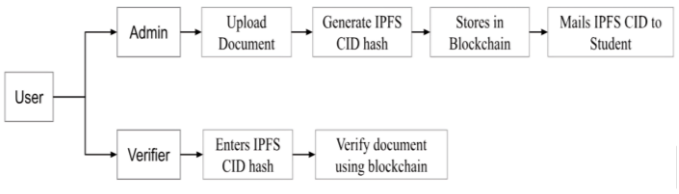

Fig. 2. Architecture of the Proposed System

We have two modules: Admin and Verifier. In this case, the administrator is in charge of uploading students'

transcripts and storing them on the blockchain, whilst the verifiers are higher education institutions.

To ensure effective file management, the system utilizes Pinata, an easy-to-use IPFS service. Users create Pinata accounts and generate API keys, allowing their smart contracts to seamlessly connect to Pinata's services. Solidity contracts are compiled into bytecode and then deployed on a suitable blockchain network, such as Ethereum.

Easy to use, typically found in web applications, promotes user participation. Users can begin transactions and perform file operations using the user interface (UI) of the decentralized application (dApp) by connecting their wallets, usually through Metamask. An essential tool in this procedure is the widely used Ethereum wallet plugin, Metamask. Installing Metamask, setting it up to connect to the file system API, and granting the required rights are the steps that users take to ensure safe and verified interactions.

The system is thoroughly tested and makes use of test tokens.

VI. METHODOLOGY

Planning and Design: Developing a decentralized file system with Blockchain, Pinata, IPFS, Solidity programming for smart contracts, and Metamask involves several distinct steps that result in a seamlessly integrated system. The process begins with careful planning and design, in which the project's objectives and requirements are defined. This phase also entails defining the structure of the smart contracts and their interactions with IPFS and Pinata, as well as determine user roles in the system.

Development of Solidity Smart Contracts: The core logic for file operations and interactions with IPFS is encapsulated within Solidity Smart Contracts. Key functions are defined to handle file uploading, retrieval, and management while ensuring data integrity and security.

Setting up an IPFS Node: An IPFS node is established to host and retrieve files in a distributed manner. Understanding Content Identifiers (CIDs) is crucial for locating and retrieving files on the IPFS network.

Integration of Pinata: Pinata, a user-friendly IPFS service, is integrated into the system for robust file management. Users sign up for Pinata accounts and generate API keys to enable interactions with Pinata's services.

Smart Contract Deployment: Solidity contracts are compiled into bytecode and deployed onto a suitable blockchain network, such as Ethereum. Funding the contract with cryptocurrency facilitates interactions within the decentralized ecosystem.

User Interface (UI) Development: A user-friendly UI, typically a web application, is developed to enable user interaction. Users connect their wallets, often through Metamask, to the dApp, allowing them to initiate transactions and perform file operations.

File Upload and Retrieval: Users initiate file upload and retrieval through the UI, triggering interactions with smart contracts. Smart contracts interact with IPFS and Pinata to store files and metadata for uploading and retrieving files for users.

Testing and Optimization: Rigorous testing and optimization are conducted to ensure functionality, security, and efficiency. Smart contracts and UI interactions are fine-tuned to minimize gas fees and enhance the user experience.

VII. RESULTS AND DISCUSSION

The result of implementing the suggested system demonstrates its usefulness in enabling decentralized file management using blockchain technology. Users may securely upload and retrieve documents by

combining services like Pinata and IPFS with smart contracts, ensuring access and data integrity over time. The deployment of smart contracts on blockchain networks like Ethereum enables seamless interactions within the decentralized ecosystem, which is powered by cryptocurrency transactions.

Frontend Development:

Develop front-end user interfaces using web technologies (HTML, CSS, JavaScript, and React). Integrating it with Metamask for transaction authentication and signing. Create forms and interfaces for uploading, managing, and sharing files.

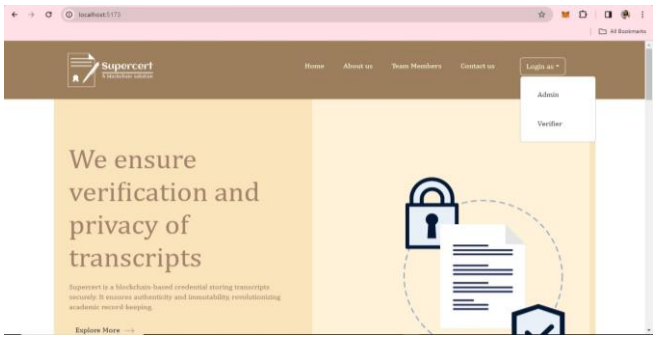

Fig. 3. Dashboard of SuperCert

Solidity Smart Contract Development:

Develop smart contracts to store IPFS CID tokens and payments. Create contracts covering storage credentials, access rights, and file metadata management. Defines how files can be loaded, updated, and deleted.

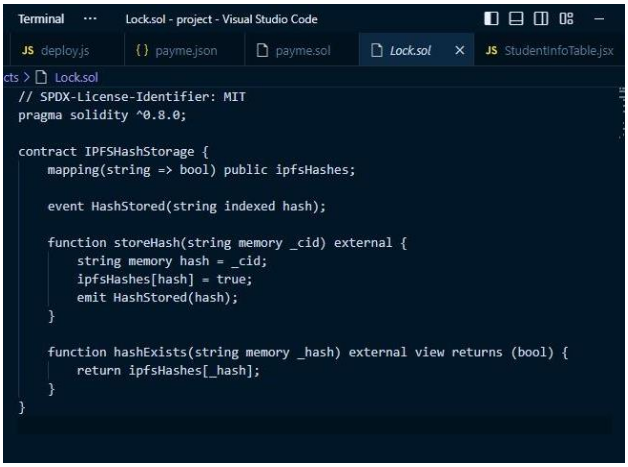

Fig. 4. Smart Contract For IPFS Hash Storage

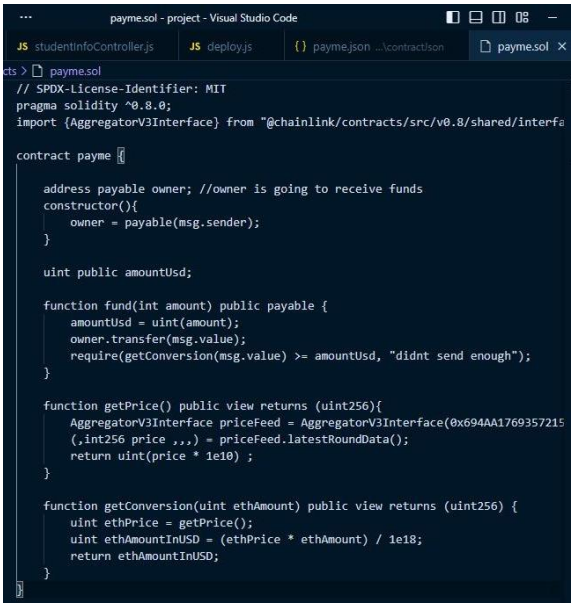

Fig. 5. Smart Contract For Payment

Backend Development:

Developing a backend server that communicates with IPFS and the Ethereum blockchain. Which manage file uploads and retrievals, respond to user requests, and communicate with smart contracts. Implement user administration features like verification details and transaction information.

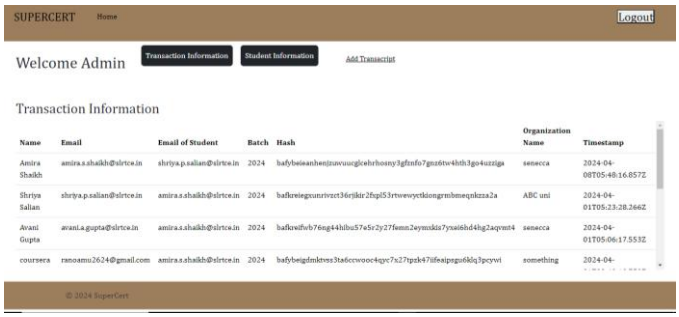

Fig. 6. Admin dashboard.

IPFS Integration:

Interacting with IPFS for file storage through Pinata's API. Keeping file contents on IPFS, and for reference, log the resulting IPFS CID hashes in smart contracts and store them in blockchain.

Testing:

Testing the system is secure and operating as intended by thoroughly testing it. Conducting smart contract unit tests. Checking the frontend's compatibility with

Metamask and ease of use. Test Pinata and IPFS file uploads and downloads.

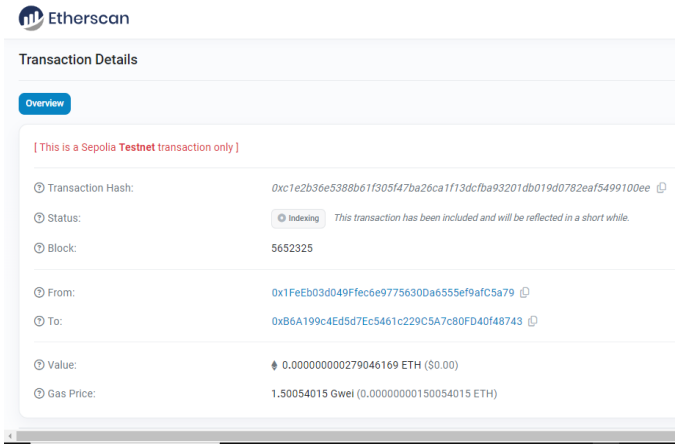

Fig. 7. Transaction details using Sepolia

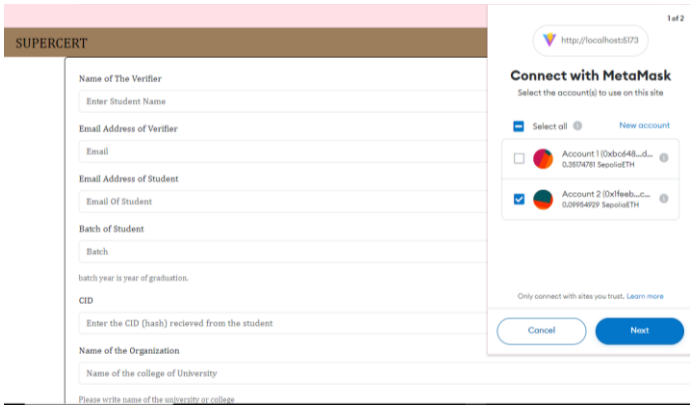

Fig. 8. Testing payment with Metamask.

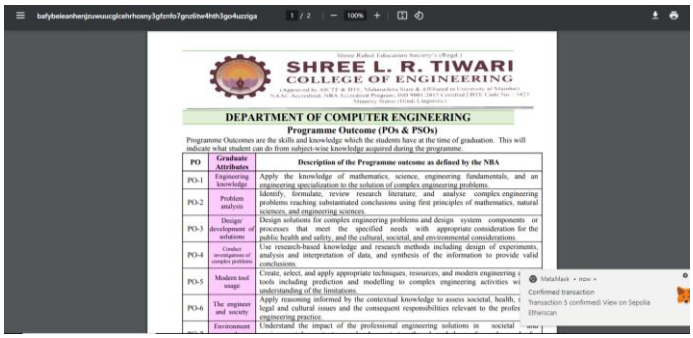

Fig. 9. Testing the after-payment output.

Updating and maintenance:

Monitoring and maintaining your system continuously. implementing improvements and modifications in response to customer feedback and evolving technologies.

The cost of utilizing the system was assessed, including blockchain transaction fees, storage prices, and other costs. The results showed that the pricing was reasonable and competitive, making it an acceptable value for users according to the service provided.

VIII. CONCLUSION

In conclusion, SuperCert represents an advanced and innovative solution for addressing the challenges associated with educational certificates, such as fraud, verification, and data security. Certificates recorded on the blockchain become tamper-proof and can be easily verified by educational institutions and employers. The system incorporates robust identity verification processes to validate the identity of applicants, making it difficult for fraudulent individuals to exploit the system. Data security is a top priority, and SuperCert employs encryption and secure storage mechanisms to protect sensitive user information and certificates. The use of blockchain technology enhances transparency in the certification process, fostering trust among educational institutions. By automating the certificate verification process and reducing the administrative burden on educational institutions, SuperCert improves efficiency in the educational certification ecosystem.

IX. FUTURE SCOPE

The future scopes include working with universities and educational institutions to establish blockchain-based credential verification systems on a larger scale. This might include standardizing the process across numerous colleges and leveraging blockchain technology into current student databases. In addition to educational credentials, blockchain technology can be used to verify professional qualifications, licenses, and legal documents. Exploring the expansion of blockchain verification to these domains could boost trust and transparency across sectors. Constantly upgrading security procedures inside blockchain

systems would be required to protect against cyber threats and preserve the integrity of stored certificates. This may include investigating advanced encryption techniques, multi-factor authentication, and biometric verification methods. Promoting widespread use of blockchain-based certificate verification systems on a worldwide scale. This could include raising awareness, offering training and support, and addressing regulatory issues to make implementation easier across multiple countries and jurisdictions. Interoperability, refers to the development of standards and protocols that enable different blockchain networks and systems to communicate with each other. This will enable the easy interchange and verification of certificates across several systems, increasing efficiency and usefulness.

X. REFERENCES

[1] Bessa, Emanuel E., and Joberto SB Martins. "A blockchain-based educational record repository." arXiv preprint arXiv:1904.00315 (2019).

[2] Pathak, Shivani, et al. "Blockchain-based academic certificate verification system—a review." Advanced Computing and Intelligent Technologies: Proceedings of ICACIT 2022 (2022): 527-539.

[3] Bele, Roshani S., and Jayant P. Mehare. "A review on digital degree certificate using blockchain technology." IJCRT 9.2 (2021): 2320-2882.

[4] Saleh, Omar S., Osman Ghazali, and Muhammad Ehsan Rana. "Blockchain based framework for educational certificates verification." Journal of critical reviews (2020).

[5] Chaniago, Nero, Parman Sukarno, and Aulia Arif Wardana. "Electronic document authenticity verification of diploma and transcript using smart contract on Ethereum blockchain." Register 7.2 (2021): 149-163.

[6] Raghavender, K. V., et al. "Decentralized Smart Contract Certificate System Using Ethereum Blockchain Technology." Second International Conference on Emerging Trends in Engineering (ICETE 2023). Atlantis Press, 2023.

[7] Doan, Trinh Viet, et al. "Toward decentralized cloud storage with IPFS: opportunities, challenges, and future considerations." IEEE Internet Computing 26.6 (2022): 7-15.

[8] Trautwein, Dennis, et al. "Design and evaluation of IPFS: a storage layer for the decentralized web." Proceedings of the ACM SIGCOMM 2022 Conference. 2022.

[9] Alizadeh, Morteza, Karl Andersson, and Olov Schelén. "Efficient decentralized data storage based on public blockchain and IPFS." 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE). IEEE, 2020.

[10] Singh, Akanksha, Harsh Vardhan Gupta, and Vaishnavi Gupta. "Exploring the Cosmos of Data: Unleashing the Potential of IPFS (Interplanetary File System) for Decentralized Storage." Vidhyayana-An International Multidisciplinary Peer-Reviewed E-Journal-ISSN 2454-8596 8.6 (2023).

[11] Hujare, Ankush R., et al. "DECENTRALIZED FILE SYSTEM USING BLOCKCHAIN."

[12] Enwerem, Udochukwu C. "BLOCKCHAIN RESULT AND TRANSCRIPT MANAGEMENT SYSTEM: A CASE STUDY OF FEDERAL UNIVERSITY OF TECHNOLOGY OWERRI." International Conference on Communication and E-Systems For Economic Stability| CeSES. 2023.

[13] Mohanty, Debasis, et al. "Blockchain interoperability: Towards a sustainable payment system." Sustainability 14.2 (2022): 913.

[14] Kuonen, David. "The process of creating, testing, and deploying smart contracts on the Ethereum blockchain using Solidity." (2023).

[15] Soares, Pamella, et al. "Extending the Docstone to Enable a Blockchain-based Service for Customizable Assets and Blockchain Types."

Journal of Software Engineering Research and Development 11.1 (2023): 15-1.

[16] Das, Moumita, et al. "A blockchain-based integrated document management framework for construction applications." Automation in Construction 133 (2022): 104001.

[17] Imam, Iftekher Toufique, et al. "DOC-BLOCK: A blockchain based authentication system for digital documents." 2021 Third International Conference on Intelligent Communication Technologies and Virtual Mobile Networks (ICICV). IEEE, 2021.

[18] ONWUASOANYA, NC, and BE EZE. "MYTRANSCRIPT: AN ACADEMIC TRANSCRIPT DECENTRALISED WEB APPLICATION SYSTEM BASED ON THE ETHEREUM BLOCKCHAIN." (2022).

[19] Shakan, Yassynzhan, et al. "Verification of university student and graduate data using blockchain technology." International Journal of Computers Communications & Control 16.5 (2021).

[20] Meirobie, Isyak, et al. "Framework Authentication e-document using Blockchain Technology on the Government system." International Journal of Artificial Intelligence Research 6.2 (2022).