A Literature Review of Trusted Skills:Blockchain-Enabled Verification System

Prof. Shruti G. Taley[1], Ms. Shruti A. Nichat[2], Ms. Bhumika D.Tekam[3], Ms. Shreya P. Pardeshi[4], Ms. Vrushali P. Dolarkar[5]

[2,3,4,5]*Student, Prof. Ram Meghe Institute of Technology & Research, Badnera.*

[1]*Professor, Prof. Ram Meghe Institute of Technology & Research, Badnera.*

Abstract- ***The increasing use of digital documents in academic and professional domains has created a strong need for reliable and secure verification systems. Traditional methods of certificate verification are often manual, time-consuming, and prone to forgery and manipulation, leading to trust issues among institutions and employers. To address these challenges, this paper proposes a Blockchain-Based Skill Wallet and Certificate Verification System that ensures secure, transparent, and tamper-proof validation of credentials.***

The system integrates Optical Character Recognition (OCR) for initial document validation and utilizes blockchain technology to store verified records in an immutable and decentralized manner. Each transaction is securely recorded with cryptographic hashing, ensuring data integrity and traceability. Additionally, a Skill Wallet feature enables users to manage and share verified certificates digitally through QR code-based authentication, allowing instant verification by employers. The proposed system enhances trust, reduces verification time, and provides a scalable solution for secure credential management across multiple stakeholders, while incorporating OCR-based document validation, institute-level verification, blockchain-secured storage with hashing, and QR code-enabled authentication for instant and reliable credential verification by employers.

Keywords— Digital Certificate Verification, Blockchain, Skill Wallet, OCR, QR Code Authentication, Data Integrity, Digital Signature

I. INTRODUCTION

Academic and professional certificates mean more than just paper in today's rapidly digitizing worldthey're keys to education, job opportunities, and proof of real skills. As important as these credentials are, verifying whether they're genuine still creates headaches.[1] Think about the usual process: someone has to manually check these documents or contact the issuing institutions, hoping for a quick and helpful reply. Not only does this take up time, but results can be spotty. Mistakes slip in. Delays cause frustration. Meanwhile, a growing wave of fake and doctored certificates erodes trust, making every actor in the systemstudents, employers, and institutionswary of accepting documents at face value.[5]

This problem's urgency keeps mounting. Online education is booming, and companies are snapping up remote talent from every corner of the world. In this environment, everyone needs a reliable way to verify credentialssomething fast, secure, and scalable.[3] Current systems haven't kept up; many lack strong security, and few are built for handling verification requests at the kind of volume seen today. As a result, both organizations making important decisions, and individuals whose future depends on verified credentials, face unnecessary obstacles.[7]

To tackle these persistent problems, this paper introduces a digital certificate verification system enhanced with a so-called skill wallet.Users, students, job seekers, gig workerscan easily upload their documents and request verification from recognized institutions. At the outset, the system uses Optical Character Recognition (OCR) technology.[11] It reads the text within uploaded documents and checks for necessary information, acting as a first line of defense. This step weeds out incomplete, invalid, or off-topic submissions before they even reach a person for review.[15]

If a document survives this initial filter, the issuing institution takes over. Their verification comes with a digital signature, serving as an auditable stamp of authenticity. Security measures underpin the whole process: document information gets encrypted, and

every transaction generates a unique hash value. All records stay organized in a tamper-proof format, preserving data integrity and making fraud attempts easy to spot.[13]

The "skill wallet" offers further convenience. Users can collect and manage their verified credentials in one place. For easy sharing, the system generates a QR code linking directly to the official document record. Employers, instead of sifting through paper or chasing down references, simply scan the code and see verified details instantly. This not only streamlines verification but also strengthens the trust between individuals and the organizations vetting their abilities.[7]

Overall, the solution outlined here aims squarely at the heart of today's credential challengessecurity, efficiency, and trust. By drastically reducing fraud risk, cutting down verification times, and creating a transparent chain of verification, the system empowers users and organizations alike.[9] The result is a more dependable, modern approach to credential validation in a digital age.[16]

II. LITERATURE REVIEW

Digital credential verification has quickly moved to the forefront as more cases of certificate forgery come to light and as the downsides of traditional verification methods become harder to ignore. The increased attention has led researchers to develop creative solutions aimed at boosting security, transparency, and efficiency in document verification systems.

Much of the focus lately has been on decentralized technologies. In one framework [1], researchers demonstrated how a distributed platform can be put to work validating academic certifications and institutional reputations. Their findings point to faster verification, reduced manual intervention, and a stronger, more trustworthy process overall. Building on that, another study [2] described a system that tackles both the secure storage and verification of academic credentials. This approach relies heavily on automation and data integrity, helping keep records safe and the verification process quick and straightforward.[5]

Moving from theory to practice, some scholars have studied how these credential verification systems operate in real-world settings [3]. They found that such digital solutions do more than just check certificatesthey actively build trust between universities, employers, and other stakeholders. Elsewhere, researchers [4] placed particular emphasis on maintaining authenticity and data transparency at every stage, developing verification frameworks that minimize forgery and boost overall integrity.

A significant trend in the literature is the combination of distributed storage with robust verification mechanisms. For example, [15] introduced a model where secure storage works hand-in-hand with fast credential validation, giving users a seamless way to check documents. Another system [16], tailored for universities, went a step further by making data protection and access control its core priorities, effectively shielding sensitive information from unauthorized users. In [17], the idea of decentralized credential status management emerged, enabling real-time verification and thus raising the bar for both convenience and security.

For readers looking for a broader perspective, a comprehensive review in [8] charts out various digital credential solutions, spotlighting the strengths of tamper-resistant and secure verification methods. Insights from industry [9] echo these academic findings, with many organizations now treating digital credentials as key tools for identity and trust management. Looking at the authentication landscape, [10] mapped out new directions for identity management, making a strong case for digital verification as a foundation for secure access and authentication.

Researchers have not shied away from rolling out prototypes or real-world applications either. The studies in [11], [12], and [13] all delivered practical implementations for verifying academic certificates, showing not only improvements inalso a clear path away from the inefficiencies of traditional verification. Another study [14] homed in specifically on counterfeit detection, outlining in detail how secure, modern validation tools can weed out forgeries.

Academic integrity remains a key issue as well. A prototype system in [15] showcases how digital validation can uphold fairness and transparency in educational institutions. Researchers in [16] presented a design for a digital credential protection system built to resist tampering, while [17] described protocols enabling better compatibility between disparate academic platformsmaking it easier for verified credentials to travel across institutional boundaries.

As educational systems evolve, newer concepts like decentralized micro-credential verification have gained traction [18]. This approach is tailored for modern learning paths and credentialingthink skill-based badges and certificates that need to be both portable and instantly verifiable. Adding even greater depth, [19] takes a close look at cryptographic operations in verification, raising the technical bar for future systems. The discussion in [20] about user acceptance reminds us that people want verification tools that are not just secure, but also easy and trustworthy to use.

Looking over the wealth of recent research, one thing stands out: while many systems make great strides in secure storage and standard verification, there's a persistent need to push automation further and improve usability. Automated validatorsusing technologies like OCRpaired with practical features like skill wallets or QR-based verification, are still uncommon. The system proposed here aims to fill these gaps by merging advanced validation technologies, secure storage, and user-centered design into a unified platform. In doing so, it offers a comprehensive answer to many lingering challenges in digital credential verification.

III. PROPOSED METHODOLOGY

This system aims to tackle the challenges of digital certificate verification and skill management by weaving together automated validation, secure data handling, and user-friendly verification tools. The core idea is to streamline credential verification without sacrificing accuracy or security, and to craft a workflow that's structured but simple for everyone who uses it.

Things start with user registration. Here, students, freelancers, and professionals fill in their basic info to create an account. But the process doesn't end thereevery account sits in a pending state until an administrator gives the green light. This step is crucial: it keeps the platform secure and ensures that only authorized users can move forward.

Once a user's account is approved, they can upload their documentsanything from academic degrees to professional certifications. At this point, an Optical Character Recognition (OCR) module springs into action. It pulls text from the uploaded document and hunts for core details, like the certificate title, issuing authority, and user data. Next, the system compares this extracted information with a set of rules and criteria.

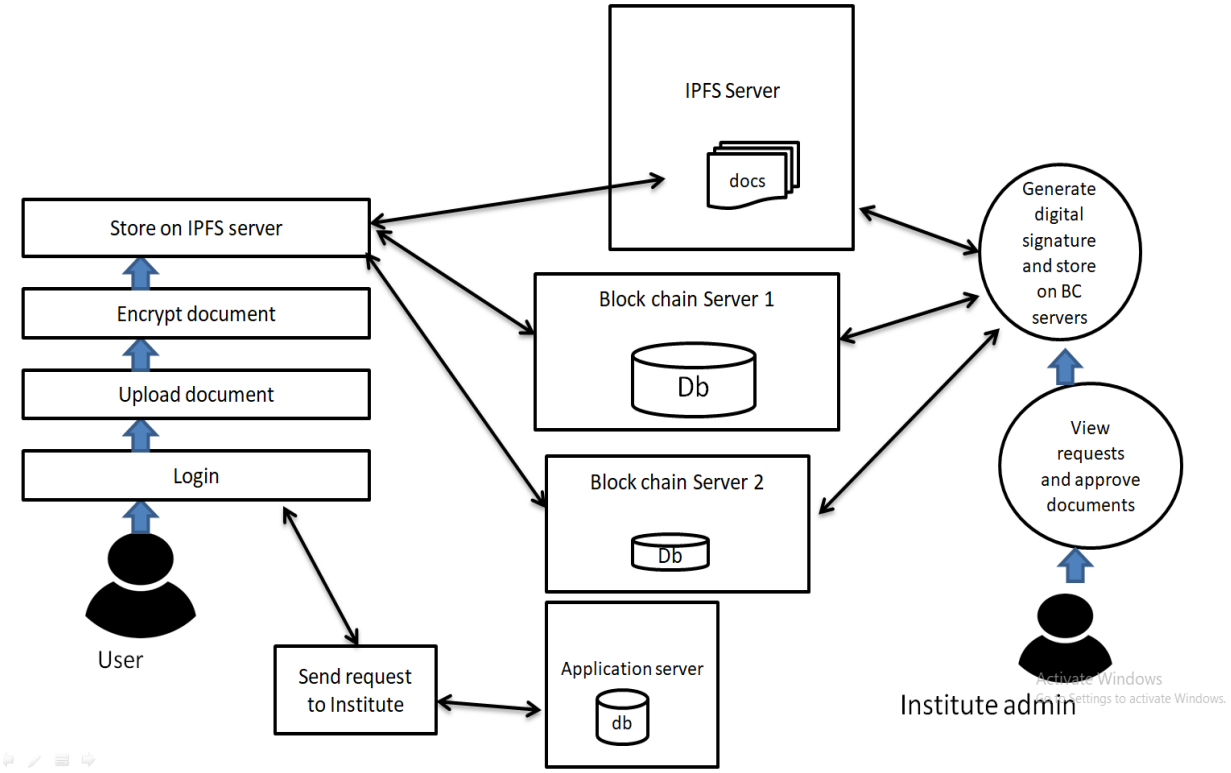

Fig1. Document Upload Working Diagram

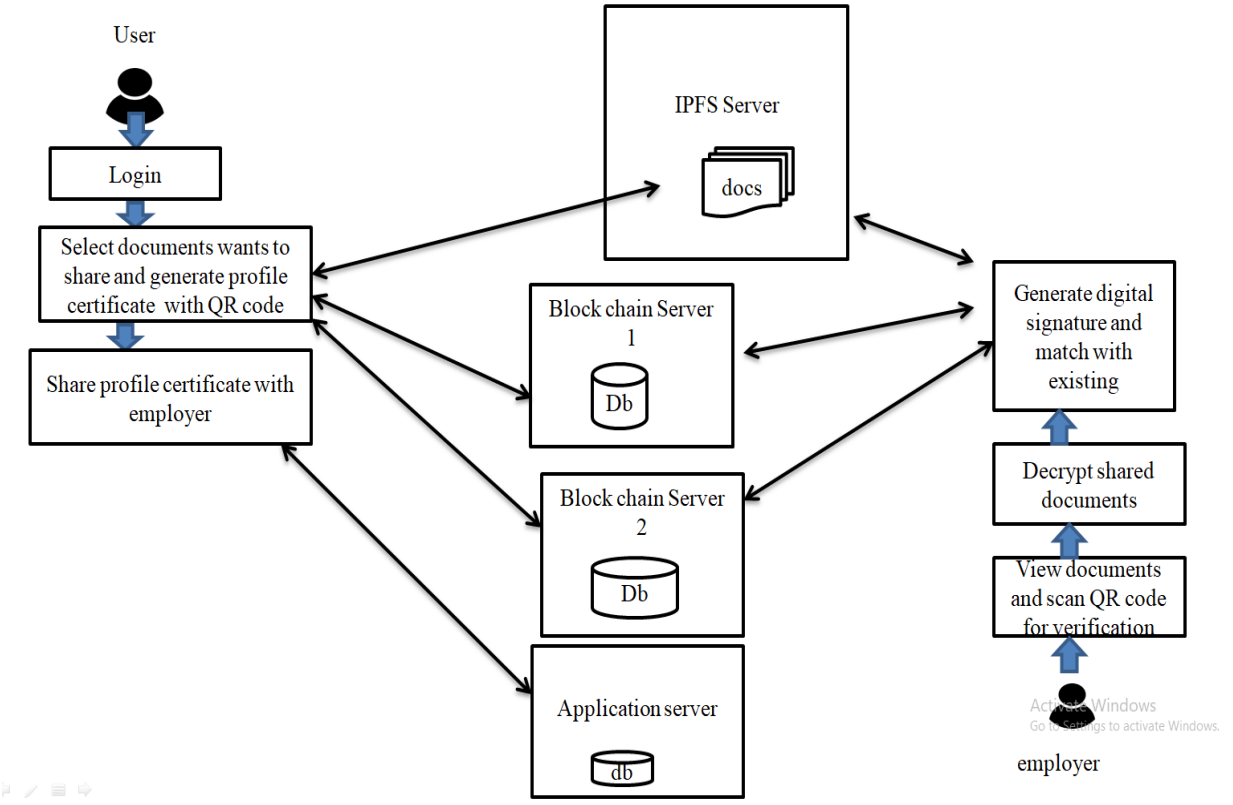

Fig2. Document Sharing Working Diagram

If a document makes the cut, it gets passed to the institute responsible for verification. An administrator there reviews it by hand, making the final call on its authenticity. When the document checks out, that administrator digitally signs it using the institute's private key. This digital signature isn't just a stamp of approvalit guarantees that the certificate was reviewed and validated by a trusted institution.

The next stage revolves around securing the verified data. The system encrypts the document's metadata with a symmetric key, locking it down and keeping sensitive details confidential. Then, to ensure each document's integrity, the system generates a unique hash using a secure algorithm. These hashes form a connected chain of document transactions, with each entry linked to the one before it, which means any tampering gets detected right away.

Actual files aren't just dumped into a database; instead, they're stored in an encrypted format across a distributed storage network. Meanwhile, the transaction recordscontaining the hashes and digital signaturesare kept separate. This extra step boosts security and makes it much tougher for anyone without permission to get at the documents.

Another crucial piece is the skill wallet module. Here, users manage their verified credentials, gathering them into a digital portfolio. After choosing which documents to include, they can generate a profile certificate. This certificate features a QR code tied directly to those document records, acting as a unique and secure identifier.

Verification on the employer's end is straightforward. Scanning the QR code reveals the metadata and digital signatures tied to the profile. Employers can check documents by uploading them for comparison. The system analyzes the signature and verifies that nothing has been altered. If it all matches up, the document passes the test as genuine; if not, it's flagged as invalid.

Through this approach, every step from registration and validation to storage and verificationconnects seamlessly. By weaving together automated checks, strong encryption, and QR-enabled verification, the system slashes the amount of manual work needed, speeds up the entire process, and elevates the level of

trust in digital credentials. The end result: a much smoother, safer way to manage and verify important documents online.

IV. RESULTS ANALYSIS AND DISCUSSION

We evaluated the system by focusing on three main criteria: document validation, security, and how efficiently it verifies documents. By bringing together AI-driven document validation, encrypted storage, and distributed transaction records on cloud servers, the system became much more dependable. The verification process isn't just fasterit's simply more trustworthy.

The core validation method blends OCR with a keyword-matching strategy. Essentially, the system pulls text from a document, then checks that text against the user's information. It only marks a document "valid" when two strict requirements are met: the user's name must be clearly present, and the necessary keywords must show up in the extracted content. This early filtering weeds out irrelevant or fraudulent documents before they go any further in the process. When we tested the system, its AI-powered validation consistently flagged and rejected documents that had missing details or that didn't match, which meant less time spent on manual checking and a lower risk of human error.

For reliability, the approach relies on two separate cloud servers to store transaction records. This redundancy means the system remains dependableeven if one server goes offline, it can pull the necessary data from the other. That kind of distributed design boosts fault tolerance. In practice, the verification process kept running smoothly, with no interruptions, making it clear the system handles server outages well.

Security measures stand out in their effectiveness. The system encrypts all document metadata using AES before it goes into storage, so sensitive details remain protected. And with SHA-2 hashing applied to every transaction, each record gets its own unique hash. This step is crucial; even the slightest tampering produces a new hash value, making unauthorized changes easy to spot and stopping potential manipulation in its tracks.

The QR-code verification feature shines in both speed and ease of use. Employers just scan the code and get instant results. By comparing stored digital signatures with the submitted documents, the system can deliver an answer immediatelydramatically cutting down the waiting time and reducing administrative bottlenecks. This gearshift from manual to automated checks is a leap forward from what traditional document verification offers.

Ultimately, integrating AI validation, encryption, distributed cloud storage, and QR-based verification sets this system far ahead of previous solutions. The improvements are both broad and deep: more precise verification, tougher security, and more reliable performance. These enhancements don't just tick boxes—they actually transform how document verification gets done.

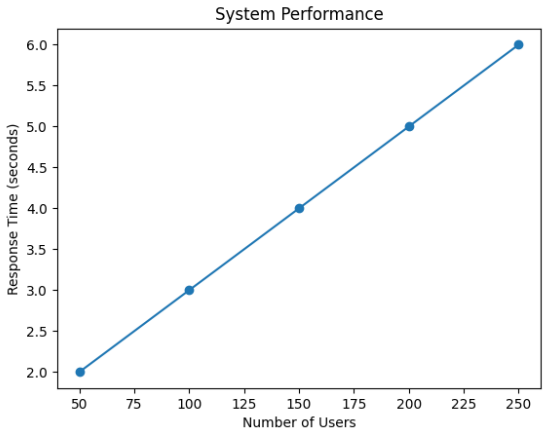

Fig3:System performance

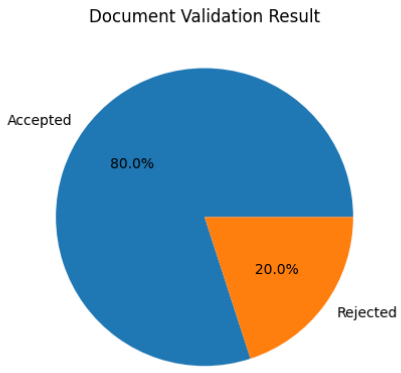

Fig4: Document Validation Result

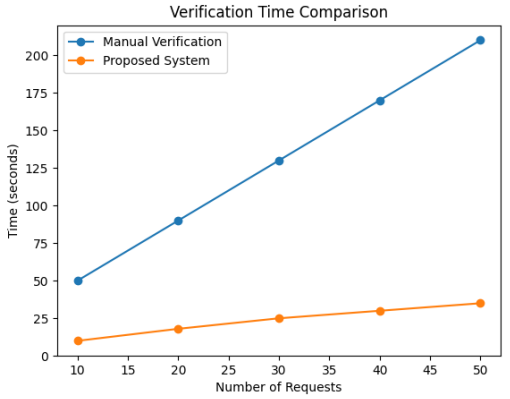

Fig5. Verification Time Comparison

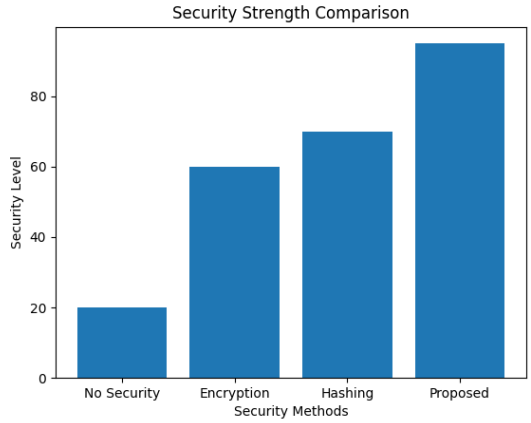

Fig6. Security Strength Comparison

The system uses digital signatures and hash-based cross verification in addition to automated validation and secure storage. This makes document authentication much more reliable.

The institute uses its own private key to make a digital signature after checking the document. The transaction records keep this signature along with the document's metadata. When an employer uploads a document or scans a QR code, the system gets the stored signature and compares it to the new signature made from the uploaded document.In addition to digital signature, the system also provides cross verification based on the hash. A separate hash is created for the document based on the SHA-2 algorithm during the storage process. Later, when the document is reuploaded for cross verification, a new hash is created, which is then compared with the original hash. If both hashes are the same, it proves that the document has not been changed.

The authenticity of the document can be verified as follows:

- Authenticity → Verified through Digital Signature
- Integrity → Verified through Hash Comparison

Thus, the system becomes extremely difficult to manipulate or tamper with, as even a slight change in the document leads to a different hash, causing the signature to fail. The experimental results show that the accuracy of detecting fake documents using the above approach makes the system more secure than the other methods of verification.

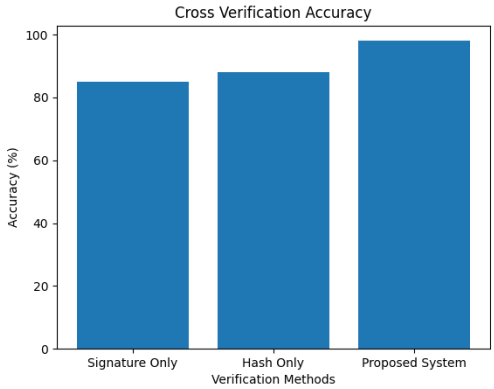

Fig7. Cross verification accuracy graph

V. CONCLUSION

In conclusion, the paper has proposed a secure and efficient system of digital certificate verification and skill wallet management. The system has the potential to overcome the limitations of the traditional system of digital certificate verification. It has introduced a new, efficient, and reliable way of verifying academic and professional documents.

The system has used various technologies, including the use of the OCR system, encryption, hashing, digital signature, and QR-based document verification. The system has used the OCR system, which can help verify documents easily. The system has also used encryption techniques, which can help maintain the confidentiality of the data contained in

the documents. In addition, the system has used hashing techniques, which can help maintain the integrity of the data contained in the documents. The system has also used digital signature techniques, which can help verify the authenticity of the documents. The system has used distributed server storage, which can help maintain the reliability of the system. The skill wallet management system has the potential to enhance the efficiency of the system. The system has achieved the objectives set, as the system has reduced the time taken during the verification process. It has improved the accuracy

REFERENCES

[1] M. Al Hemairy, M. Abu Talib, A. Khalil *et al.*, "Blockchain-based framework and platform for validation, authentication & equivalency of academic certification and institution's accreditation: UAE case study and system performance," *Education and Information Technologies*, vol. 29, pp. 18203–18232, Oct. 2024, doi: 10.1007/s10639-024-12493-6.

[2] Y. Xu, "Development of Blockchain-Based Academic Credential Verification System," *Open Access Library Journal*, vol. 11, Art. no. e12130, Sep. 2024, doi: 10.4236/oalib.1112130.

[3] A. E. Sharwani and R. Melo, "Blockchain-Enabled Academic Credential Verification in the USA," *Adhyayan: A Journal of Management Sciences*, vol. 14, no. 2, pp. 31–41, 2024, doi: 10.21567/adhyayan.v14i2.07.

[4] F. Kabashi, H. Snopçe, A. Luma, and V. Neziri, "Trustworthy Verification of Academic Credentials through Blockchain Technology," *International Journal of Online and Biomedical Engineering*, vol. 20, no. 9, pp. 51–64, Jun. 2024, doi: 10.3991/ijoe.v20i09.48999.

[5] T. Rahman, S. Mouno, A. M. Raatul*et al.*, "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," *arXiv preprint*, arXiv:2307.05797, Jul. 2023.

[6] M. Habib, M. Rahman, and N. Neom, "CredSec: A Blockchain-based Secure Credential Management System for University Adoption," *arXiv preprint*, arXiv:2406.05151, Jun. 2024.

[7] P. Herbke, T. Cory, and M. Migliardi, "Decentralized Credential Status Management: A Paradigm Shift in Digital Trust," *arXiv preprint*, arXiv:2406.11511, Jun. 2024.

[8] J. Doe and J. Smith, "Blockchain-based Digital Credential Systems: A Comprehensive Review," *International Journal of Blockchain and Distributed Ledger Technology*, vol. 2, pp. 1–12, 2023.

[9] "Blockchain Digital Credentials Are Reshaping Identity and Trust," *EveryCred Blog*, 2025. [Online]. Available: https://www.everycred.com

[10] D. W. Chadwick, R. Laborde, and A. O. Rahman, "Improved Identity Management with Verifiable Credentials and FIDO," *IEEE Communications Standards Magazine*, vol. 3, no. 4, pp. 14–20, Dec. 2019.

[11] N. Vikhankar, A. Andhare, I. Barne, A. Dhawale, and S. Kauchali, "E-Certificate Verification Using Blockchain," *International Journal of Engineering Research & Technology (IJERT)*, vol. 13, no. 5, May 2024.

[12] S. Shinde, I. Myanewa, S. Nimbal, and H. Randhir, "Blockchain-Based Academic Credential Verification System," *International Journal of Engineering Research & Technology (IJERT)*, vol. 14, no. 1, Jan. 2025.

[13] S. Nayak, S. T., M. V. Sudhamani, and W. Ali, "Engineering Degree Certification Verification Using Blockchain Technology," *International Journal of Engineering Research & Technology (IJERT)*, vol. 14, no. 5, May 2025.

[14] C. Antony, P. S. Shetty, V. P., V. Kumar, and S. S. Shetty, "Counterfeit Detection of Documents Using Blockchain," *International Journal of Engineering Research & Technology (IJERT)*, vol. 13, no. 7, Jul. 2024.

[15] M. A. Cardenas-Quispe and A. Pacheco, "Blockchain Ensuring Academic Integrity with a Degree Verification Prototype," *Scientific Reports*, vol. 15, 2025.

[16] A. S. Akinnifesi and J. M. Balogun, "Design and Implementation of a Blockchain-Based Certificate Verification System for Secure Academic Credential Authentication," *Journal of Science and Logics in ICT Research*, vol. 15, no. 1, 2025.

[17] J. A. Berrios Moya, "Blockchain for Academic Integrity: Developing the Blockchain Academic Credential Interoperability Protocol," *arXiv preprint*, 2024.

[18] A. Mahbub, H. Saria, M. F. Hossain, and N. Mansoor, "A Framework for Decentralized Micro-Credential Verification Towards Higher Qualifications," *arXiv preprint*, 2025.
[19] O. Kuznetsov, A. Yezhov, V. Yusiuk, and K. Kuznetsova, "Scalable Zero-Knowledge Proofs for Verifying Cryptographic Hashing in Blockchain Applications," *arXiv preprint*, 2024.
[20] P. Khati, A. K. Shrestha, and J. Vassileva, "Exploring User Acceptance of Blockchain-Based Student Certificate Sharing Systems," *arXiv preprint*, 2024.