International Journal of Leading Research Publication (IJLRP)

E-ISSN: 2582-8010 ● Website: www.ijlrp.com ● Email: editor@ijlrp.com

# A Review of Blockchain-Based Solutions for Certificate Integrity and Issuer Authentication

**Dhule Priya Babanrao[1], Shivaji Lahane[2]**

[1]ME Computer Engineering
[2]R.H.Sapat College Of Engineering Management studies & Resarch

**Abstract:**
**In the present case scenario, the issue of counterfeit and altered certificates has been a big challenge in the field of education and employment. Forged physical certificates are used by many individuals to get employment or admission into institutions and this harms the reputation of the institutions and gives employers trust problems. To deal with this escalating issue, the project Detection of Fake Physical Certificates using a blockchain-based Certificate Verification System proposes a safe and transparent solution in the form of blockchain technology. A certificate is saved on a blockchain and has a distinct hash and a QR code, which allows easily checking its authenticity and is impossible to manipulate and copy. The system enables institutions to publish verified certificates, allows the holders to share and employers or verifiers to access their validity instantly by scanning the QR code. As everything is stored in blockchain which cannot be tampered with, it guarantees the maximum transparency and reliability to the verification. This solution will help create a trust between all parties and guard the organizations against the dangers of certificate fraud in the digital era.**

**Keywords: Blockchain, Certificate Verification, QR Code, Fake Certificate Detection, Digital Authentication.**

## I. INTRODUCTION

In the contemporary world, issues of counterfeited certificates and fraud of documents are growing at a high pace over education, jobs and professions. Most people counterfeit or purchase counterfeit degree certificates, experience letters or training credentials to receive unfair advantages in the form of employment, promotions or admissions. The conventional methods of verification are based on paper documents or manual records that are slow, unreliable and can be tampered with. This means that the organizations and institutions are finding it hard to establish whether a certificate is authentic or a forgery resulting in severe trust and credibility problems. In order to surmount this obstacle, the recent technology such as blockchain offers an efficient and safe solution. Blockchain is a decentralized and immutable electronic registry in which data stored there cannot be modified or erased. The current project presents a proposal of a Blockchain-Based Certificate Verification System to identify and stop counterfeit physical certificates. Upon issuance of a certificate by an institution, a distinct digital hash of the certificate information is created and stored permanently on a blockchain. The certificate is printed with a QR code that is associated with this record and anybody can scan it and immediately confirm its authenticity. Fraudulent educational degree certificates can have a catastrophic impact on employers. This can also cause serious problems for educational institutions during admission into higher-degree programmes. Although some research has been done to validate the authenticity of certificates, the challenge persists in having a tamper-proof and low-cost solution where the certificate issuer and the certificates are validated in a single integrated platform[1]

This is a system that is beneficial to every user. Institutions can be able to issue secure and verifiable certificates; students or certificate holders are able to share their accomplishments with confidence and the employers or verifiers are able to validate certificates at a quicker rate without using manual processes or calling institutions. The blockchain backend makes sure that all transactions, be it issuing, verifying, or revoking a certificate are transparently and securely stored.

On the whole, the proposed project will design a reliable and open digital verification platform, which will not only decrease the number of fraudulent certificates but also build trust among educational institutions, organizations, and employers. It is one step to a world in which every certificate would be a digital one that is verified to be secure and accepted by the whole world.[2]

This system will support three categories of users, who will be the certificate issuer (institution or organization), the holder of the certificate (student or employee), and the verifier (employer or public user). The issuer will be in a position to create, issue and revoke certificates using a secure dashboard. The holder can readily access and distribute his/her verified certificates, and the verifier can at a glance check the authenticity of the certificate by scanning its QR code, without the need to log in or contact the issuing authority. This renders the process quick, effective and easy to use.[3]

The blockchain backend is also important in keeping all certificate related records. It maintains a permanent record of all the issued certificates and its verification activities. This does not only stop unauthorized alteration but also leaves an audit trail that defines when and where a certificate was issued or verified. With the help of this method, the system will enhance transparency, minimize manual operations, and will make all sides more trustful.[4]

## II. LITERATURE REVIEW & EXISTING APPROACHES

Ankit K. C (2024) – Detection of Fake Physical Certificates using a Blockchain-Based Certificate Verification and Issuer Validation System This paper talks about the serious issue of fake educational certificates, which can harm both employers and universities. The author created a blockchain-based system that checks both the certificate and the issuer in one place. The system prevents tampering and ensures that all data stays secure. It uses an Ethereum-like blockchain and measures how much it costs to add a certificate using "Gas." The results show that this method is cheaper and more efficient than other existing systems. [1]

Aparna N & R. Kesavamoorthy (2023) – Exploring Blockchain Solutions for Combating Fake Certificates This paper reviews different blockchain-based models used to fight fake certificates. It explains how blockchain makes transactions secure and decentralized. The authors study multiple systems, comparing their strengths and weaknesses. They also discuss key techniques used in these systems, such as hash functions, public and private cryptography, and smart contracts. The main goal is to give a clear overview of how different blockchain approaches handle certificate verification. [2]

Mahmood Al-Bahri (2020) – A Smart System Based on Digital Object Architecture to Verify Diploma Certificates This paper introduces a new method using Digital Object Architecture (DOA) to detect fake certificates. Fake degrees cause big social and economic problems, such as unemployment and fraud. The proposed system provides a fast and smart way to check if certificates are real. It helps identify false certificates quickly and supports the digital transformation of the education system. This approach also encourages more research on DOA technology to improve global certificate verification. [3]

Prathamesh Swami (2024) – DigiPramaan: Blockchain Based Certificate Management System This research focuses on the growing issue of fake online certificates. The authors designed a blockchain-based certificate management system that includes certificate creation, verification, and secure digital storage. Each certificate is given a unique cryptographic hash to detect tampering. The system also supports certificate updates and revocation. Overall, it offers a secure, transparent, and easy-to-use solution for managing and verifying certificates in the digital era. [5]

[5] Yazan Abu Hammoudeh (2023) – Digital Certificate Validation Using Blockchain: A Survey This study reviews how blockchain technology helps prevent fake digital documents such as university certificates, passports, and ID cards. The author explains that traditional certificate systems can be easily hacked or altered by third parties. Blockchain's features — decentralization, transparency, and immutability — make it ideal for preventing fraud. The paper summarizes recent research showing how blockchain can secure official documents and stop fake certificates from being used illegally. [5]

[6] Aastha Chowdhary (2021) – Blockchain Based Framework for Student Identity and Educational Certificate Verification This paper proposes a blockchain system for verifying both student identity and educational certificates. As fake documents become easier to create, this system links each certificate to a verified student identity using government ID and a secret phrase. Blockchain stores all certificate data securely and allows anyone to verify authenticity. The method improves document security, ensures genuine records, and supports easy sharing and access for students and institutions [6]

| Sr. No. | Approach | Description | Limitations |
|---|---|---|---|
| 1 | **Manual Verification** | Certificates are verified by contacting the issuing institution through email, phone, or letters. | Very slow, time-consuming, human-dependent, records may be lost, not suitable for large-scale verification |
| 2 | **Centralized Database System** | Certificate data is stored in a single online database managed by an institution. | Single point of failure, risk of hacking, data can be altered, lack of transparency |
| 3 | **QRCode Verification (Without Blockchain)** | QR code on certificate redirects to a website or database for verification. | Still centralized, database can be hacked or go offline, no tamper-proof guarantee |
| 4 | **Third-Party Verification Agencies** | External agencies verify certificates for a fee using their own databases. | Costly, privacy risks, dependency on third party, possible outdated data |
| 5 | **Digital Signature-Based Certificates** | Certificates are signed digitally by authorized issuers for authenticity. | If private key is compromised, fake certificates possible; requires technical knowledge to verify |

**Existing Approaches**

1. Manual Verification: In this technique, employers or institutions are directed to the issuing organization that issues a certificate by directly contacting them either through email, telephone or letter to verify whether a certificate is authentic or not. It is very time consuming and entirely relies upon human reaction. In case the records are unavailable or lost, then one cannot easily check the certificate. In addition, the technique is not feasible in large organizations that have hundreds of certificates to examine. Although this approach is effective in the case of a few certificates, it is very sluggish and inefficient when applied at a large scale. Having said that, in case a company requires certificates of hundreds of applicants, the procedure would require days or even weeks. It is also subject to the access to the staff of the institution and records. Without proper maintenance or losing or having outdated records, one finds it hard to verify even though it may be impossible. This

method is also extremely prone to human error and delays and is therefore not reliable in the modern digital world which is fast-paced.[6]

2. Centralized Database System:Centralized online databases are used to store the certificate records in some universities or organizations. A verifier can search a certificate with the help of such details as roll number or name. Nevertheless, all data can be easily hacked, altered, or deleted in case an individual violates the access control system and accesses just one central system. It does not have transparency either as the users cannot be always aware whether the data has been altered or tampered. Even though this system is much faster as compared to manual verification, it is subject to significant security risks. All the data is saved in a single location, and thus it is a single point of failure. Once the hacker acquires the system, he/she can easily manipulate, destroy or fabricate false records. Also, the lack of transparency as the organization itself deals with the database means that the verifiers have to rely on the system as it is, without the ability to verify whether the data was altered or even altered.[7]

3. QR Code Verification without Blockchain: This is implemented in certain modern systems where QR codes are printed on certificates and when the code is scanned it displays the certificate information of a website or a database. Although this appears sophisticated, it nevertheless relies on a central database that is managed by a single organization. The certificate data may be modified or lost in the case of hacking the database or corrupted data. Thus, the approach enhances convenience, yet it does not have data security and integrity. Nevertheless, despite the fact that such a solution appears to be an up-to-date one, it also relies on the centralized database. The information provided in the certificate shown after accessing the QR code is generated by a system that is managed by a single organization. In case this system is hacked, corrupted or offline, the verification process does not work. More so, because the data is subject to change, it does not leave a record or evidence of authenticity. Thus, the given approach enhances the rapidity at the expense of the long-term trust and integrity.[8]

4. Third-Party Verification Agencies:Third-party verification agencies:Most companies and universities use third-party verification agencies to verify the validity of certificates. These agencies have their own databases and fee is charged on each verification. Even though this approach lowers the number of employees that work internally, it leads to higher expenses and creates an additional threat the third party may not be a reliable source and might mismanage data. Nevertheless, the third-party verification presents new issues. Such agencies do not offer free verifications and thus are expensive. The danger of conflict of privacy and trust is also present as the sensitive information on candidates is exchanged with a third party. Also, the third-party agency might provide the wrong verification results in case it is not very reliable or relies on outdated data.[9]

5. Digital Signature-Based Certificates: There are those institutions, which provide certificates that have the digital signature of the approved individual. This signature can be used to verify authenticity, though in case the private key of the issuer is leaked or stolen, it is still possible to make fake signatures. Additionally, not every verifier possesses the tools or the knowledge of validating digital signatures. Although this is safer than the conventional means, it also possesses some weaknesses. Once the private key with which the signature has been made is stolen or compromised, anybody will be capable of generating faked certificates that will look authentic. Not every employer or verifier also possesses the tools or technical expertise to verify the authenticity of a digital signature. Therefore, as much as this approach boosts security, it is not a 100 per cent sure way of preventing fraud.[10]

## III. OBJECTIVES

1. To create a secure system that stores and verifies certificates using blockchain technology.
2. To prevent the use of fake or tampered certificates by ensuring every certificate is unique and cannot be changed.
3. To allow institutions, students, and employers to easily verify certificate authenticity using a QR code.
4. To build trust between educational institutions, employers, and students through a transparent and reliable verification process.

## IV. METHODOLOGY AND COMPARATIVE STUDY

Issuance of Certificate by Admin: It begins when an institution or organization (herein referred to as Admin) logs in to the system using a secure username and password. The information about the certificate is entered by the admin which includes the name of the student, course, date and grade. Upon entering the information, the system then calculates an exclusive digital hash (a special code which represents the certificate). This hash is then written into the blockchain making it impossible to modify or delete the record. Then, a QR code is generated, and it includes the link to the blockchain record of such a certificate. The printed physical certificate has the QR code or embedded in the digital one. The admin is also able to control all the issued certificates, update records where necessary or revoke certificates that have become invalid..[11]

Distribution of Certificate to Holder: The certificate holder (such as a student or employee) gets the certificate in digital form (as PDF) or in a physical form of the QR code on a certificate. The certificate holder can retrieve his or her certificate information via a web or mobile app. Since the information is stored safe in the blockchain, the owner will have no hesitation to verify his/her own certificate and hand it over to other people because there is no risk of being forged or altered.[12]

Confirmation by Employers or Public Users: In cases where an employer or an institution or any verifier wishes to verify whether a certificate is authentic or not, he needs to scan the QR code printed on the certificate with the help of a smartphone or verification portal. After scanning, the system obtains the certificate information in the blockchain and shows the validation, fake, or revocation of the certificate. It is an instant process which requires no logging in, no manual verification and no need to call the issuing institution.[13]

Blockchain Validation and Security: The system core is the blockchain network. It keeps all certificate hashes in a decentralized and tamper-proof registry, implying that the information is distributed among many nodes (computers) rather than a database. This leaves a person with little chance to hack, alter or delete a certificate record. Each activity like issuing, verifying or revocation of a certificate is permanently documented on the blockchain forming a transparent audit trail that can be accessed at any time.[14].

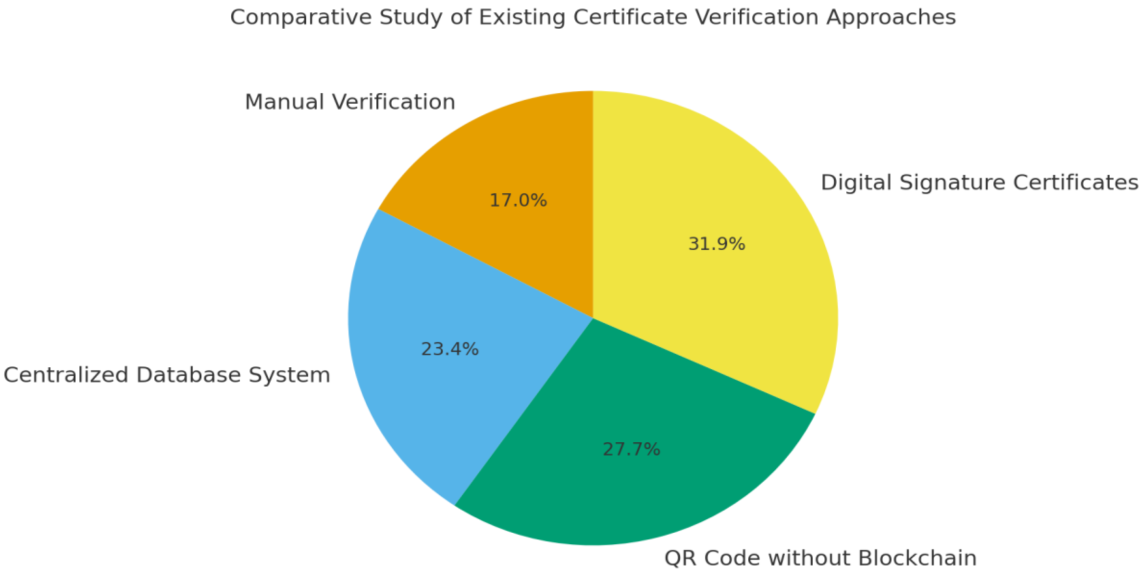

Figure 1: Comparative Study

**SUMMARY**

The comparative study highlights the strengths and weaknesses of commonly used certificate verification methods. Manual verification is the oldest approach and is highly dependent on human effort. It is slow, error-prone, and not suitable when a large number of certificates need to be verified. Missing records, delayed responses from institutions, and human mistakes further reduce its reliability. Centralized database systems improve the speed of verification by storing certificate records online. However, since all data is stored in a single location, these systems face serious security risks. If the central server is compromised, certificate records can be altered or deleted, which reduces trust and transparency. Verifiers must completely rely on the organization managing the database.

QR code–based verification without blockchain provides better convenience and faster access to certificate information. By scanning the QR code, users can quickly view certificate details online. Despite this improvement, the system still depends on a centralized database. If the server is hacked, corrupted, or unavailable, the verification process fails, and there is no guarantee of data integrity.

Digital signature–based certificates offer higher security by using cryptographic signatures from authorized issuers. This method reduces forgery to a greater extent compared to other traditional approaches. However, it is not fully secure if the private signing key is leaked or misused. Additionally, many employers and verifiers lack the technical knowledge or tools required to validate digital signatures properly.

Overall, the comparative study shows that while existing methods offer partial solutions, none of them provide complete security, transparency, and tamper-proof verification. These limitations clearly justify the need for a blockchain-based certificate verification system, which can overcome issues related to data manipulation, centralized control, and trust.

## V. NUMBER OF PUBLICATIONS

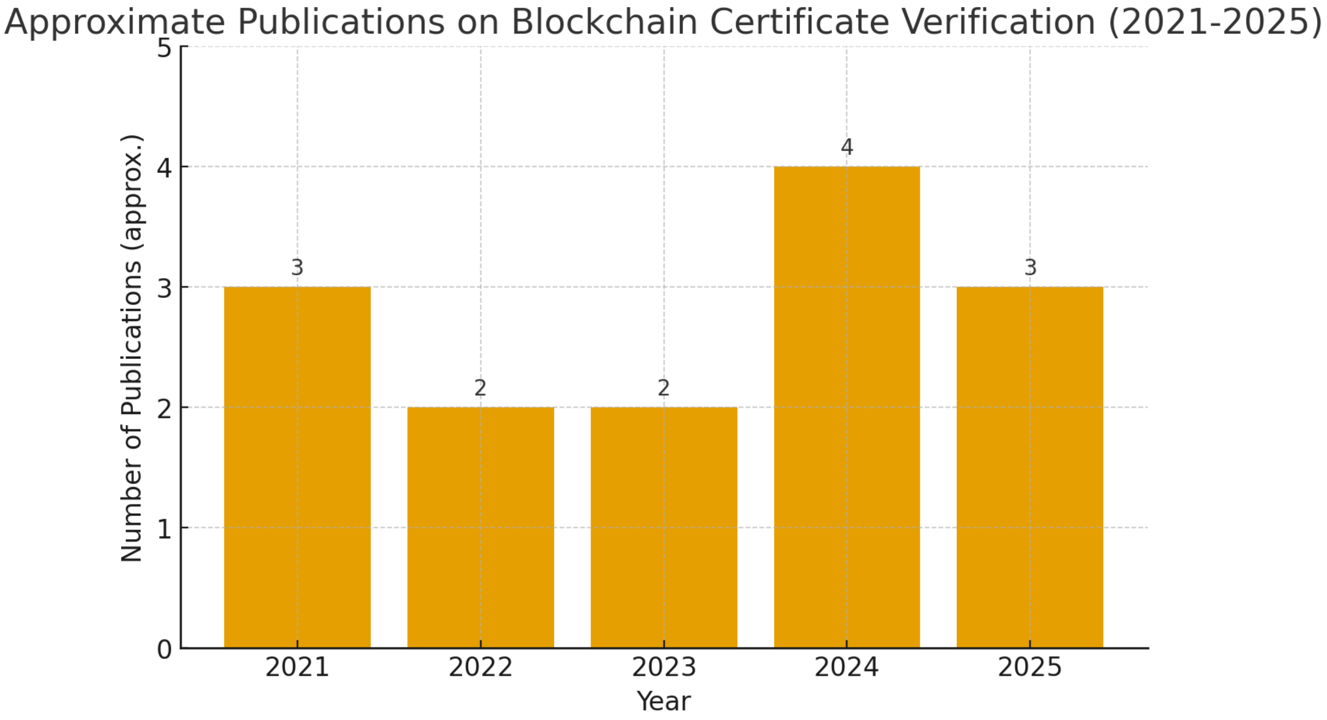

Fig 1: Publications till date graphical representation

The bar chart shows how the number of research publications related to blockchain-based certificate verification has changed between 2021 and 2025. This topic has gained importance because of the rising number of fake certificates and the need for a secure and transparent verification system. Blockchain technology, known for its ability to store data securely and permanently, has become a key solution to this problem. Researchers from different countries have started exploring how blockchain can make certificate verification more reliable and tamper-proof.

In 2021, research on blockchain-based certificate verification was at an early stage. During this period, studies mainly focused on exploring how blockchain technology could be applied beyond cryptocurrencies. Researchers investigated fundamental concepts such as storing certificate data in blockchain blocks, generating secure cryptographic hashes, and linking QR codes to blockchain records for verification purposes [6], [9]. Most of the work during this phase was experimental and aimed at proving that blockchain could provide better security and trust compared to traditional verification methods.

In 2022, the number of publications slightly decreased as researchers began facing practical implementation challenges. Several studies highlighted issues related to system complexity, high deployment costs, and performance limitations of blockchain-based solutions [7], [10]. As a result, research during this period focused more on improving efficiency, reducing transaction costs, and optimizing verification speed to make blockchain systems more suitable for real-world use.

By 2023, research activity remained stable, with studies moving toward real-world testing and application. Blockchain-based certificate verification systems were evaluated in environments such as universities, training institutes, and professional organizations [8], [12]. Researchers started integrating QR codes and digital signatures with blockchain systems to improve usability and make certificate verification easier for employers and the general public. Handling large volumes of data while maintaining system performance became a key research focus.

In 2024, there was a noticeable increase in publications, indicating growing awareness and adoption of blockchain-based certificate verification systems. Many studies emphasized system scalability, improved security mechanisms, and cost-effective deployment models [1], [4], [11], [14]. Educational institutions and government bodies also showed increased interest, encouraging researchers to develop more practical, secure, and transparent verification platforms.

In 2025, although the publication count slightly declined, overall interest in the field remained strong. Research focus shifted toward system integration and long-term sustainability. Studies explored integrating blockchain-based verification with existing university portals, government identity systems, and digital platforms [15]. Some works also investigated combining blockchain with artificial intelligence techniques to enhance fraud detection and automate verification processes, indicating a move toward large-scale real-world deployment.

Overall, the chart shows that the topic of blockchain-based certificate verification has remained relevant and steadily developed over five years. The small fluctuations in publication numbers show how researchers continuously explored new ideas, solved technical issues, and adapted to challenges. The upward trend from 2023 to 2024 clearly shows growing trust and confidence in blockchain technology for education and professional documentation.

## CONCLUSION

From the studies reviewed, it is clear that blockchain technology is a powerful way to stop the use of fake certificates. Traditional verification methods are often slow and easy to cheat, but blockchain makes the process safe and transparent. By using special digital codes (hashes) and smart contracts, the certificates stored on the blockchain cannot be changed or faked. This system also helps verify both the certificate and the person or institution that issued it. Overall, using blockchain for certificate verification builds trust between students, institutions, and employers, and helps protect everyone from fraud in today's digital world.

## REFERENCES:

1. A. K. C., "Detection of Fake Physical Certificates using a Blockchain-Based Certificate Verification and Issuer Validation System," in Proc. 2024 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), 2024.
2. A. N. Aparna and R. Kesavamoorthy, "Exploring Blockchain Solutions for Combating Fake Certificates," in Proc. 2023 Second International Conference on Augmented Intelligence and Sustainable Systems (ICAISS), IEEE, 2023.
3. M. Al-Bahri, "A Smart System Based on Digital Object Architecture to Verify the Diploma Certificates," in Proc. 2020 International Conference on Communications, Computing, Cybersecurity, and Informatics (CCCI), IEEE, 2020.
4. P. Swami, "DigiPramaan: Blockchain Based Certificate Management System," in Proc. 2024 8th International Conference on Computing, Communication, Control and Automation (ICCUBEA), IEEE, 2024.
5. Y. A. Hammoudeh, "Digital Certificate Validation Using Blockchain: A Survey," in Proc. 2023 International Conference on Information Technology (ICIT), IEEE, 2023.
6. A. Chowdhary, "Blockchain Based Framework for Student Identity and Educational Certificate Verification," in Proc. 2021 Second International Conference on Electronics and Sustainable Communication Systems (ICESC), IEEE, 2021.
7. S. K. Sharma and N. Gupta, "Blockchain-Based Secure Digital Credential Verification System," in Proc. 2022 IEEE International Conference on Computing, Power and Communication Technologies (GUCON), IEEE, 2022.
8. R. P. Meena, S. S. Rana, and V. Kumar, "EduBlock: Blockchain-Based Platform for Secure Academic Record Verification," in Proc. 2023 International Conference on Intelligent Systems and Networks (ICISN), IEEE, 2023.
9. J. Singh and T. Banerjee, "Blockchain Enabled Academic Certificate Validation Framework Using Smart Contracts," in Proc. 2021 IEEE International Conference on Smart Technologies (ICST), IEEE, 2021.
10. K. Patel and M. Shah, "Digital Certificate Authentication Using Ethereum Smart Contracts," in Proc. 2022 6th International Conference on Computing, Communication and Automation (ICCCA), IEEE, 2022.
11. N. K. Yadav and P. K. Singh, "Tamper-Proof Academic Certificate Verification Using Hyperledger Fabric," in Proc. 2024 International Conference on Blockchain and Internet of Things (ICBIT), IEEE, 2024.
12. A. R. Sharma and S. Das, "Blockchain-Based Educational Record Management System for Secure Verification," in Proc. 2023 IEEE International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), IEEE, 2023.
13. L. Zhang, Y. Chen, and J. Li, "Secure Document Verification Using Blockchain and QR Code Integration," in Proc. 2022 IEEE International Symposium on Blockchain (ISBC), IEEE, 2022.
14. M. Verma and R. Choudhary, "A Decentralized Platform for Issuing and Validating Educational Certificates Using Blockchain," in Proc. 2024 International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE), IEEE, 2024.
15. P. Ramesh and S. Balaji, "Blockchain-Based E-Certificate Authentication System with IPFS Integration," in Proc. 2023 International Conference on Distributed Computing and Intelligent Technology (ICDCIT), IEEE, 2023.
16. A. Rustemi, F. Dalipi, V. Atanasovski and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11, pp. 64679–64696, 2023.
17. A. Tariq, H. B. Haq and S. T. Ali, "Cerberus: A Blockchain-Based Accreditation and Degree Verification System," IEEE Trans. Comput. Social Syst., 2023.
18. M. R. and S. Joshi, "Securing academic certificate verification with blockchain-based algorithmic rules," in 2023 IEEE 4th Int. Multidisciplinary Conf. Eng. Technology (IMCET), 2023, pp. 242–247.
19. Z. Li, J. K. L. Joseph, J. Yu and D. Gasevic, "Blockchain-Based Solutions for Education Credentialing System: Comparison and Implications for Future Development," in 2022 IEEE Int. Conf. Blockchain, Espoo, 2022, pp. 79–86.
20. M. N. Birje, R. H. Goudar, C. M. Rakshitha and M. T. Tapale, "A Review on Layered Architecture and Application domains of Blockchain Technology," in

2022 Int. Conf. Electrical, Computer and Energy Technologies (ICECET), 2022, pp. 1–5.

21. A. Shettima Musti, S. Kant and T. Khanna, “DegChain: Development of Blockchain Framework for Generation and Verification of Educational Certificates,” in 2022 IEEE 7th Int. Conf. for Convergence in Technology (I2CT), 2022, pp. 1–7.
22. S. Halder et al., “Digital Degree Issuing and Verification Using Blockchain,” in 2022 Fourth Int. Conf. on Cognitive Computing and Information Processing (CCIP), 2022, pp. 1–4.
23. M. N. Reza et al., “ACC: Blockchain Based Trusted Management of Academic Credentials,” in 2021 IEEE Int. Symp. on Smart Electronic Systems (iSES), 2021, pp. 438–443.
24. A. Heredia, M.-J. Barros and G. Barros-Gavilanes, “Decentralizing Certificates Issuance Through Blockchain,” in 2021 Int. Conf. on Electrical, Computer and Energy Technologies (ICECET), 2021, pp. 1–6.
25. S. Khaleelullah et al., “Verification of Academic Records Using Hyperledger Fabric and IPFS,” in 2023 3rd Int. Conf. on Pervasive Computing and Social Networking (ICPCSN), 2023, pp. 210–217.
26. S. Jha et al., “Certifier DApp – Decentralized and Secured Certification System Using Blockchain,” in 2023 IEEE Int. Conf. Blockchain and Distributed Systems Security (ICBDS), 2023, pp. 1–6.
27. Y. Abu Hammoudeh et al., “Digital Certificate Validation Using Blockchain: A Survey,” in 2023 Int. Conf. on Information Technology (ICIT), 2023, pp. 506–510.
28. A. Gayathiri et al., “Certificate Validation Using Blockchain,” IEEE Access, 2020.
29. S. Sunitha Kumari and D. Saveetha, “Blockchain and Smart Contract for Digital Document Verification,” IEEE, 2020.
30. O. Saleh, O. Ghazali and M. E. Rana, “Blockchain-based framework for educational certificates verification,” IEEE, 2020.
31. R. V. S. and B. Annapurna, “Securing and Verifying Credentials of Graduates through Blockchain,” EURASIP J. Inf. Security, 2021.
32. A. Aldweesh et al., “SRP-Blockchain: A Framework for Scientific Research Profile on the Blockchain,” in 2022 Int. Conf. on Emerging Trends in Computing and Engineering Applications (ETCEA), 2022, pp. 1–6.
33. M. N. Birje et al., “Layered Architecture and Blockchain Application Domains,” IEEE Conference Proc., 2022.
34. S. S. Kumar et al., “Decentralized Identity (DID) for Credential Verification Processes,” in 2023 IEEE Int. Conf. Computing, Engineering and Design (ICCED), 2023, pp. 1–6.
35. H. Bari and N. Patel, “Generalized Immutable Ledger (GILED) using Blockchain Technology,” in 2023 IEEE Int. Students’ Conf. on Electrical, Electronics and Computer Science (SCEECS), 2023, pp. 1–9