ISSN: 2582-7219

International Journal of Multidisciplinary Research in Science, Engineering and Technology

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Impact Factor: 8.206

Volume 8, Issue 4, April 2025

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804380

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Study on Blockchain-Based Certificate Verification and Validation

Ms. Sobhika. S[1] , Dr. M. Rathi [2]

Student, Department of Computer Technology, Dr. N. G. P. Arts and Science College, Coimbatore, India[1]

Professor & HOD, Department of Computer Technology, Dr. N. G. P. Arts and Science College, Coimbatore, India[2]

ABSTRACT: This review critically examines the developing state of blockchain technology as an evolutionary measure to improve the security, transparency and efficiency of certificate authentication and verification processes. Conventional approaches are usually susceptible to forgery, time-consuming manual actions and lacking inherent trust. The core features of immutability, decentralization, cryptographic hashing and verifiable chain of transaction provided by Blockchain create a profitable paradigm shift to create tamper-proof and easily verifiable digital certificates. This paper gives an up-to-date and comprehensive review of the literature, sets the background context necessary for understanding the challenges of legacy systems, critically surveys the various methodologies being sought and employed, emphasizes new and emergent applications in an extensive range of industries and concludes by briefly discussing open issues and promising areas for future research and development in this emerging field.

KEYWORDS: Blockchain, Certificate Verification, Cryptographic Security, Secure Authentication, Digital Identity.

I. INTRODUCTION

The core features of immutability, decentralization, cryptographic hashing and verifiable chain of transaction provided by Blockchain create a profitable paradigm shift to create tamper-proof and easily verifiable digital certificates [1]. The accurate and proper verification and validation of numerous different types of certificates, from academic credentials and professional certifications all the way through to electronic licenses and authenticity seals, are building-block processes in a wide variety of industries, governments and organizational regimes [2]. Traditional paper-based systems are vulnerable to fraudulent abuse by their very nature and will most likely necessitate costly and time-consuming labor-intensive manual verification processes, thereby creating widespread inefficiencies and risk of human error [3]. The growing digitization of certificates, as it presents certain advantages in the areas of access and dissemination, has at the same time introduced new challenges to do with preserving the long-term integrity of electronic documents, setting up strong mechanisms for authentication and enabling smooth and consistent validation procedures in distributed settings [4]. Blockchain technology, such advanced distributed ledger technology with decentralized architecture and cryptographic security, is a most promising and revolutionary solution for overcoming these age-old limitations effectively by offering an open, secure and auditable platform for the total management and frictionless verification of digital certificates [5]. This book review aims to present an up-to-date synthesis of research and development circumstances in the usage of blockchain technology on the compelling fronts of certification validation and verification, presenting progressive insights into the varied methodologies that are being examined, the extended range of nascent and nascent applications on divergent industry fronts and ultimately the future orientation of this paradigmatic technology of transformation.

II. LITERATURE REVIEW

The increasing interest in using blockchain technology for managing certificates has seen a significant number of academic papers investigating different aspects of such usage. One of the primary methods is to pin cryptographic hashes of certificate information to the blockchain in a way that authenticity can be verified independently without exposing sensitive personal data in the certificate [6]. It has thoroughly studied the application and deployment of various blockchain platforms, such as public permissionless blockchains such as Ethereum, permissioned enterprise blockchains such as Hyperledger and R3 Corda and hybrid versions customized according to the requirement of a specific use case, for the construction of decentralized and reliable certificate verification systems [7]. Herein, in addition to other novel digital advancements, huge research works have also been aimed at the deployment and

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804380

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

planning of advanced smart contracts – enforceable contracts whose terms are computer coded directly – with the objective of enabling full-proof automated functioning of relevant processes like secure issue of certificates, clean revocation techniques whenever necessary and instant on-request confirmation procedures all for enabling greater openness, permanence of the records and reduced dependence on the intermediary agents [8]. Moreover, active working on integration of blockchain technology with next-generation decentralized identity (DID) protocols and verifiable credentials (VC) standards is aimed at developing more user-centric, privacy-enhancing and interoperable certificate authentication solutions that give people better control of their digital credentials and enable frictionless cross-organizational verification [9]. The overall findings from this new literature strongly suggest the substantial potential of blockchain technology to greatly reduce certificate fraud activity risk, improve efficiency and speed in verification procedures and enable higher levels of trust and transparency in various fields of applications.

III. BACKGROUND

Traditional certificate validation and verification processes tend to depend on centralized entities, like educational institutions, professional organizations or government agencies, for issuing and maintaining credential records [2]. Centralized approach has a number of inherent security flaws and shortcomings [2]. Figure 1 shows a comparative diagram at the high level of traditional centralized certificate verification and a generic blockchain-based certificate verification system. This picture would show in a clear way the differences in data storage, verification process and trust models [12].First, it produces single points of failure, under which the breach of the central database can cause large-scale data compromise and the potential for malicious certificate issuance or modification [3]. Second, the verification process of paper certificates or even certain digital certificates is labor-intensive, time-consuming and subject to human error [3]. Confirmation of a graduate's degree, for example, might take days or weeks in contacting the university that issued the degree [3]. Thirdly, the lack of transparency in the verification process undermines trust, as there is limited visibility for relying parties on the integrity and authenticity of the provenance of the certificate [4]. With the advent of sophisticated forgery technologies, these issues are exacerbated even further, which makes it increasingly hard to separate legitimate certificates from fakes [3]. There is an urgent demand for a secure, efficient and transparent mechanism for the authentication and verification of certificates that has become even more critical in the present age of globalization and digitization [4], making it possible to experiment and integrate new-age technologies such as blockchain [5].

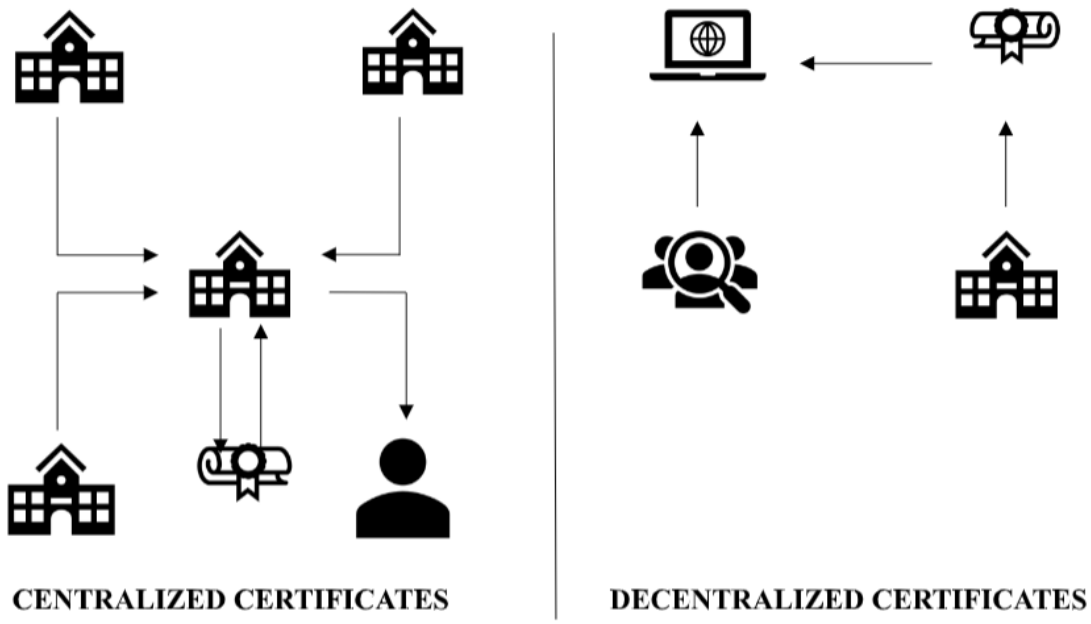

Figure 1

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804380

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

IV. METHODOLOGY

This review article follows a systematic and serious approach in synthesizing and critically reviewing the most recent and most appropriate studies entailing the use of blockchain technology to the verification and validation of certificates. A thorough and recent search was done painstakingly in top-tier academic databases, pre-prints repositories, prominent industry journals and related technical reports, using a properly curated and iteratively improved list of keywords and search terms such as "blockchain certificate verification," "decentralized credential validation," "immutable digital credentials," "verifiable credentials blockchain," and so forth [10]. The established and applicable research outputs, i.e., white papers and technical reports, peer-reviewed articles and conference articles, were categorically grouped based on their inherent contributions, such as the significant factors like the envisioned system architectures, the utilized actual blockchain platform types, the consensus mechanisms utilized to guarantee data integrity, the incorporation with other future technologies (e.g., VCs, DIDs), the actual domains applied and the utilized security and privacy features [11]. Then a critical comparative review of the wide-ranging methodologies and methods described in the literature was performed to look for common styles in architecture, technology implementation discrepancies, salient technology trade-offs and a worthwhile discussion of the advances that have been reported, likely limitations and described research gaps for each method. Figure 2 describes the typical process flow of a blockchain certificate issuance and validation process. This can illustrate the issuer, blockchain, certificate holder, verifier roles, and also the most important steps involved (issuance request, blockchain transaction, verify query, blockchain lookup, and verification result). This systematic and ordered review process aims to provide an integrated, mature and forward-looking understanding of the state of present research and of the sophisticated and changing methodologies currently being researched and actively pursued within the fast-growing discipline.

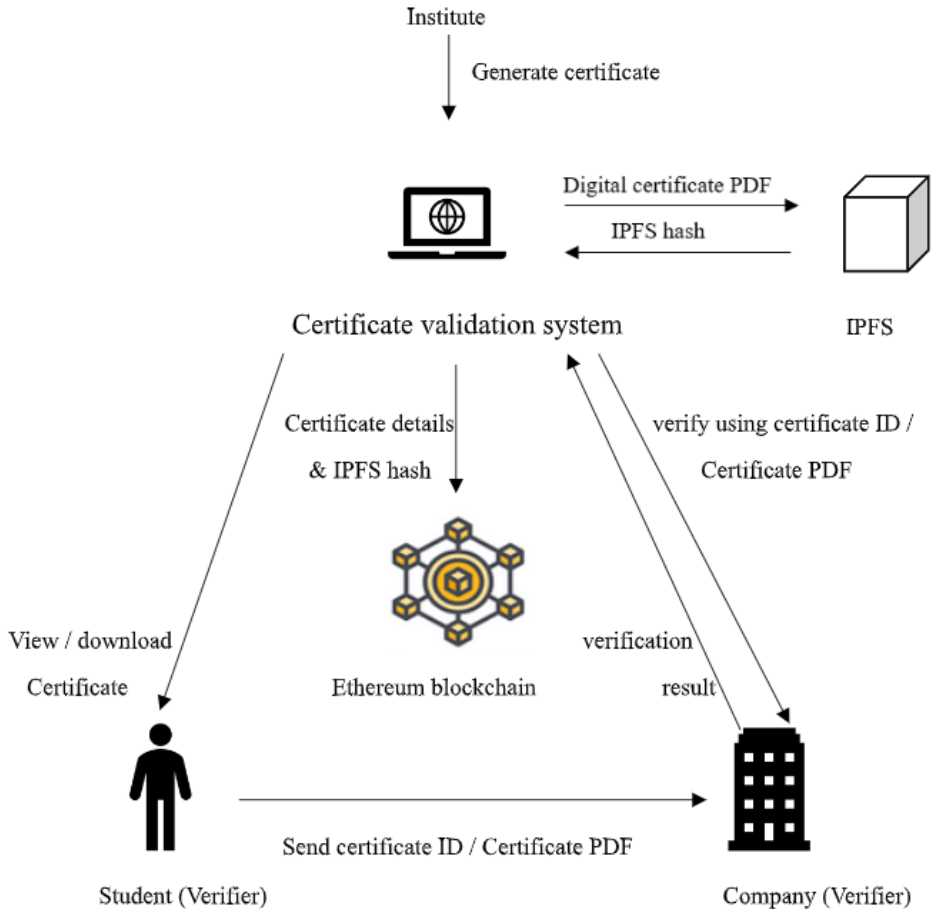

Figure 2

© 2025 IJMRSET | Volume 8, Issue 4, April 2025| DOI:10.15680/IJMRSET.2025.0804380

ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 8.206| ESTD Year: 2018|

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

(A Monthly, Peer Reviewed, Refereed, Scholarly Indexed, Open Access Journal)

Workflow process:

1. Certificate Generation: The Institute creates a digital version of the certificate, typically in PDF format. This is the initial step where the official record of achievement or qualification is produced. This digital form allows for easier storage and transmission.
2. Data Storage on IPFS: The generated digital certificate (PDF) is stored on the InterPlanetary File System (IPFS). IPFS is a decentralized storage network, unlike traditional centralized servers. This storage method enhances data resilience and reduces the risk of single points of failure.
3. Hash Storage on Blockchain: The unique cryptographic hash of the stored certificate on IPFS is recorded on the Ethereum Blockchain. This hash acts as a digital fingerprint of the certificate, ensuring its integrity. Any alteration to the certificate will result in a different hash.
4. Certificate Sharing: The Institute shares the certificate or its identifying details (including the IPFS Hash) with the Certificate Validation System. The Student can also access and download their certificate and share it with potential verifiers. This facilitates easy access and transfer of credential information.
5. Verification Request: A Verifier (like a Company) initiates the verification process by sending a request to the Certificate Validation System. This request includes the certificate details and the IPFS Hash, which are crucial for the system to perform the check.
6. Verification Process: The Certificate Validation System receives the request and uses the provided certificate details and IPFS Hash to query the Ethereum Blockchain. The system retrieves the IPFS Hash that was originally stored on the blockchain.
7. Certificate Retrieval and Verification: The System then uses the retrieved IPFS Hash to fetch the actual digital certificate (PDF) from the IPFS network. It verifies the certificate's authenticity by comparing the retrieved hash with a newly generated hash of the fetched certificate.
8. Verification Result: Finally, the Certificate Validation System sends the result of the verification process back to the requesting Verifier (Company). This result confirms whether the certificate is valid and authentic.

V. APPLICATIONS

The scope of applications in blockchain certificate validation and verification is growing fast and plays a gigantic role in helping to reshape trust and efficiency for wide ranges of industries. In the educational sector, blockchain provides a secure and transparent foundation for awarding and validating degrees, diplomas, micro-credentials, and transcripts and thus combats the disadvantages of degree mills and streamlines the normally-labored process of degree verification for employers and other schools [13]. In professional certification and licensing, blockchain can offer easily verifiable and tamper-evident professional licenses, continuing education units, and credentials, increasing professional competence confidence and regulatory compliance. Blockchain can be applied in the healthcare industry to securely share and manage verifiable medical certifications of healthcare professionals to improve patient safety and minimize administrative costs. Additionally, blockchain can be used to strengthen the supply chain by supplying authenticatable certificates of origin, compliance, and authenticity of products and counterfeiting prevention and product integrity. In digital identity, verifiable credentials based on blockchain can enable individuals to have self-sovereign ownership of their digital identity and the ability to selectively reveal verified attributes, like certificates, in an authenticatable yet privacy-preserving way. There are some of the new uses verifiable ownership of digital artwork, secure handling of intellectual property rights, and tamper-evident voting schemes where voters' qualification and integrity of the ballot can be verifiable cryptographically. Figure 2 would also be helpful with a diagram to describe the typical process flow of a blockchain certificate issuance and validation process. This can illustrate the issuer, blockchain, certificate holder, verifier roles, and also the most important steps involved (issuance request, blockchain transaction, verify query, blockchain lookup, and verification result).Blockchain technology offers a transformative and potentially earthquake-inducing change in the issuance, management, verification and validation of certificates. Its own attributes of immutability, decentralization, transparency and cryptographic protection offer a solution that tackles directly long-standing constraints and weaknesses of traditional, often centralized, certificate management systems to offer a safer, more efficient and reliable way for establishing the authenticity and integrity of electronic credentials across a broad variety of applications [14]

VI. CONCLUSION

This review has given an up-to-date, broad overview of the research world as it's changing, illustrating the various approaches being sought after, the increasingly diverse set of possible applications and the essential backdrop that

establishes necessity for these types of solutions. Although the blockchain certificate management industry remains in a comparatively early phase, with scalability, interoperability, standardization and regimes of regulation concerns still ongoing, the giant leaps and the sheer quantity of possible uses quite easily demonstrate its potential to make an impact. Future research has to consider resolving these issues of the time, examining how blockchain interacts with other newer technologies like decentralized identity systems and zero-knowledge proofs and creating strong governance and standardization frameworks to attain global use and allow full potential of blockchain to set in for creating a more secure and credible space for validation and verification of certificates.

REFERENCES

[1] Nakamoto, S., & Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin, 4*(2), 15.
[2] Mirzamany, E., & Hani, M. (2018). Blockchain: An Enabler of Efficiency Choice and Agility in Education. *JISC*..
[3] Graham, R. S., Humer, S. G., Lee, C. S., & Nagy, V. (Eds.). (2025). *The Routledge international handbook of online deviance*. Routledge, Taylor & Francis Group.
[4] Allen, J. P., & Seaman, J. (2017). Digital credentials in higher education: *Landscape and trends*. WCET and Tyton Partners.
[5] Crosby, M., Poursanidis, D., Pratap, V., & Vadgama, B. (2016). BlockChain Technology. *Applied Innovation*, *2*(6), 6-19.
[6] Zhang, Y., & Chen, J. (2017). Digital certificate management based on blockchain. *Security and Communication Networks*, *2017*.
[7] Casino, F., Dasaklis, T., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: current status, classification and open issues. *Telematics and Informatics*, *36*, 55-81.
[8] Christidis, K., & Vasiliadis, G. (2016). Blockchains and smart contracts for the internet of things. *IEEE Internet of Things Journal*, *4*(5), 1222-1232.
[9] Genise, N., & David, B. (2021). Cryptography Review of W3C Verifiable Credentials Data Model (VCDM) and Decentralized Identifiers (DIDs) Standards and Cryptography Implementation Recommendations.
[10] Muniraju Hullurappa, Mohanarajesh Kommineni, "Integrating Blue-Green Infrastructure Into Urban Development: A Data-Driven Approach Using AI-Enhanced ETL Systems," in Integrating Blue-Green Infrastructure Into Urban Development, IGI Global, USA, pp. 373-396, 2025.
[11] Petticrew, M., & Roberts, H. (2006). *Systematic reviews in the social sciences: A practical guide*. Blackwell Publishing.
[12] Kitchenham, B. A. (2004). Procedures for performing systematic reviews. *Keele University, Technical Report TR/SE-0401*.
[13] Swan, M. (2015). *Blockchain: Blueprint for a new economy*. " O'Reilly Media, Inc.".
[14] Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE access*, *6*, 5112-5127.
[15] Underwood, S. (2016). Blockchain beyond bitcoin. *Communications of the ACM*, *59*(11), 15-17.

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH

IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com