JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

# A Blockchain-based System for Digital Certificate Verification

**[1]Dheeraj Shukla, [2]Pranjal Rajput, [3]Priti Jadhav, [4]Neha Jadhav, [5]Jayshri Thakur**

[1]Assistant Professor, [2]Student, [3]Student, [4]Student, [5]Student,
[1]Department of Computer Engineering,
[1]P.S.G.V.P. Mandal's D.N. Patel College of Engineering, Shahada, Maharashtra, India

***Abstract :*** A student acquires many certificates during his/her entire duration of studies. For recruitment students need to produce these certificates in different institutions or companies. For the recruiters, verifying the authenticity of such certificates has been a job that uses resources and time. In cases where there is no anti-forge system in place, it may lead to recruitment with forged certificates. In addition, from the student perspective the certificate data should be secured and digitized so it will be available whenever needed. This paper proposes a solution for verification of digital certificates using a Blockchain-based system. The system makes use of Ethereum decentralized platform to create a Blockchain where the certificates issued to a student from an institute will be stored. These certificates have unique Certificate Block Id and can be verified by recruiter companies as per their requirements. The system provides features like confidentiality, security, immutability to ensure data safety and implementation of anti-forge mechanism.

***Index Terms*** **- Blockchain Technology, Digital Certificates Verification, Ethereum, Confidentiality, Security.**

## I. INTRODUCTION

Blockchain technology has gained significant attention in recent years due to its ability to revolutionize various industries, including education and certification [1]. One promising application is in the verification of digital certificates, where blockchain can offer transparency, security, and immutability [2].

Blockchain is a method of storing information in a way that is impossible or very difficult for anyone to change, hack, or manipulate it. A blockchain is a distributed ledger that duplicates and distributes transactions across the network of computers participating in the blockchain [3].

Blockchain Technology works on a structure called "Digital Ledger" where the transactional records are stored in "Block". These blocks are "Chained" together to form a public database distributed in a peer-to-peer network [3].

To authorize a transaction in the ledger the system uses the owner's digital signature. The digital signature of the owner authenticates the transaction and make the block data tamper proof. This mechanism ensures the information stored in the ledger is highly secured [3].

In existing systems, the problem of fake certificates is a big one. Companies that hire thousands of freshers spend a lot of money verifying applicants' educational credentials and qualifications. To address this issue, we are implementing a digital certificate verification system for validating educational certificates using blockchain technology.

The objective of the proposed system is to create a digital immutable and easily verifiable academic certificate of students who obtain academic qualifications from the University.

## II. RELATED WORKS

Blockcerts is an open standard for creating, issuing, and verifying blockchain-based digital certificates. Developed by MIT Media Lab and Learning Machine, Blockcerts utilizes the Bitcoin blockchain to anchor certificate data, ensuring immutability and tamper resistance. It provides a decentralized approach to certificate verification, allowing individuals to independently verify their credentials without relying on centralized authorities [4].

Open Badges is an open standard for digital badges developed by the Mozilla Foundation. While not exclusively blockchain-based, Open Badges can leverage blockchain technology for secure and verifiable credentialing. Organizations such as Credly have implemented blockchain integration with Open Badges to enhance the security and trustworthiness of digital credentials [5].

The Sovrin Identity Network is a decentralized identity platform built on blockchain technology. It aims to provide individuals with control over their digital identities and credentials while ensuring privacy and security. Sovrin's decentralized architecture enables verifiable credential exchange without relying on intermediaries, making it suitable for digital certificate verification use cases [6].

Learning Machine, in collaboration with MIT Media Lab, has developed a blockchain-based platform for issuing and verifying digital diplomas and certificates. The platform, built on the Blockcerts standard, enables educational institutions to issue tamper-evident digital credentials that can be independently verified by employers, universities, and other parties [7].

IBM offers a blockchain-based credentialing solution that leverages Hyperledger Fabric to create, issue, and verify digital certificates. The platform provides a secure and transparent way for organizations to manage credentials, ensuring integrity and authenticity throughout the verification process. IBM's solution targets various industries, including education, healthcare, and supply chain management [8].

Accredible is a commercial platform for issuing and managing digital certificates and badges. While not strictly blockchain-based, Accredible offers blockchain integration as an optional feature to enhance the security and trustworthiness of digital credentials. By anchoring certificate data to the blockchain, Accredible provides a verifiable record of achievement for individuals and organizations [9].

Entrust Certificate Services is a web-based certificate lifecycle management platform that helps you manage all your digital certificates, from Entrust and other Certification Authorities. The system is a collection of tools that help users to generate detailed report which improves system uptime and prevent security issues. Benefit from 24x7 web-based access to technical insights, status updates, and website scanning for end-to-end lifecycle management of all your digital certificates [10].

Employer's Graduates Verification is a system by the University of Nairobi used to verify graduate academic certificates by employers. The approach used by the system is like the verification process adopted by many other higher learning institutions which are also the issuer of academic documents. First, it requires registration forms for the verifier, and it requires one to submit a certificate of incorporation. Once the required documents are submitted, they get approved, and they may get verified documents manually by the institution. This process involved additional cost for each document that needs verification. This complex and expensive process leads to employers avoiding the process and considering only the face value of the document which is not sufficient to detect fraud [11].

The EUniCert: Ethereum Based Digital Certificate Verification System proposes a solution for issuing and verifying digital certificates. The system integrates a new consensus algorithm used in Ethereum platform in the Unicoin network. The Unicoin network is used to verify, and store issued digital certificate information. Compared to previous solutions, the system has improved performance based on latency to validate transactions and the number of verified blocks in the blockchain network. This is a simple blockchain system to illustrate the management operation of the digital certificates on the Ethereum platform [12].

A Gayatri et al. developed a software package to avoid counterfeiting certificates. Thanks to the dearth of associate in nursing anti-forge mechanism, the graduation certificate is to be solid. So, the decentralized application was designed to support Ethereum blockchain technology. First, generate the digital certificate for the paper certificate then hash worth created for the certificate is kept within the blockchain system. Even if it wants to verify the credibility of the certificate it needed another scanning app to scan the certificate. The system saves on paper, stops document forgery. However, the QR Code should be scanned with a smartphone and an online association is needed [13].

## III. PROPOSED FRAMEWORK

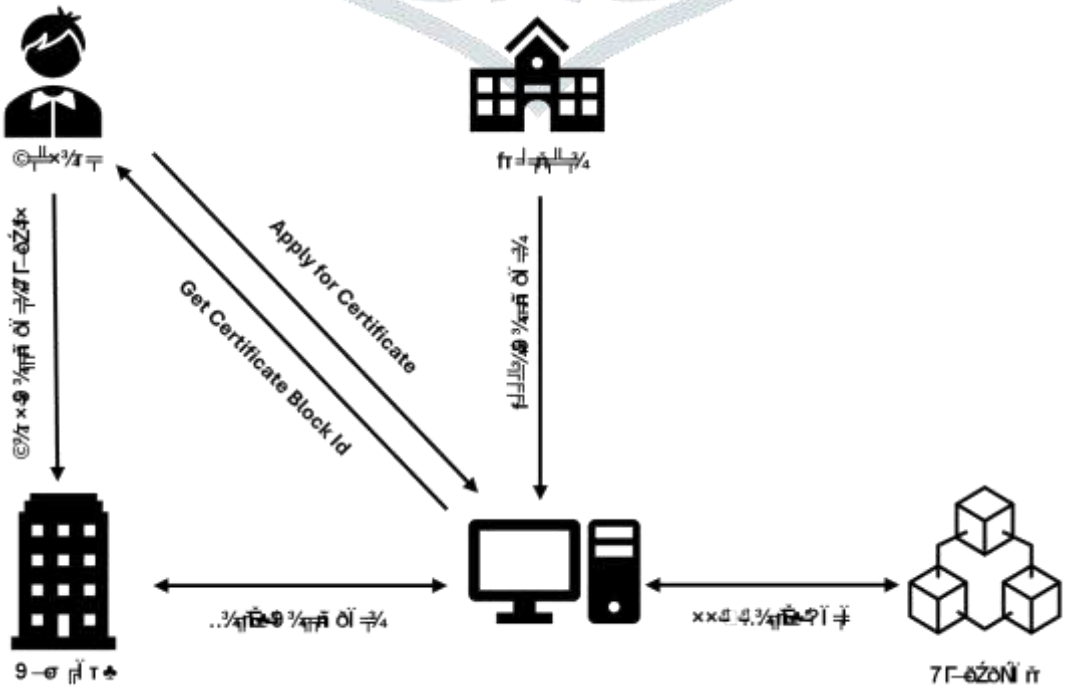


Figure 1. Proposed Framework for Digital Certificate Verification

The proposed framework shown in Figure 1 illustrates the working of the system. The process begins with a student who applies for a digital certificate. The issuer institute, after verifying the details of the student, issues the certificate. The system generates a block on Blockchain corresponding to the certificate and adds it to the Blockchain. The student then receives the Block Id for corresponding certificate. The company who wishes to verify the certificate gets the Certificate Block Id from the student and verifies it from the Blockchain using the system.

## IV. Technical Details

The proposed system will be developed on the Ethereum decentralized platform. The smart contracts are deployed on the Ethereum blockchain to manage certificate issuance, storage, and verification. Digital certificates are tokenized as non-fungible tokens (NFTs) on the Ethereum blockchain. The decentralized identity solutions Ethereum Name Service (ENS) enable individuals to create and manage their digital identities on the blockchain. The system uses IPFS decentralized storage network to store certificate metadata and associated files. The verification process involves querying smart contracts or off-chain databases to retrieve certificate information based on a unique certificate ID.

## V. Applicability

- Student: The student faces less risk of losing or damaging a certificate and the validation of certificate can also be done quite easily.
- College: It is very hard to keep track and validate huge amounts of records. The certificate verification system using blockchain is useful for colleges.
- Recruiter: Organization can easily detect fraud certificates of any employee using certificate verification system.
- Government: It will be easy to detect fake certificates using the certificate verification system.

## VI. Conclusion

The proposed systems offer a convincing solution to enhance the security, transparency, and decentralization of credentialing processes. By leveraging Ethereum's blockchain infrastructure, smart contract functionality, and decentralized identity solutions, these systems provide a robust framework for issuing, storing, and verifying digital certificates. The use of smart contracts enables the automation of certificate issuance and verification processes, ensuring that certificates are issued according to predefined rules and can be independently verified without reliance on centralized authorities. Tokenization of certificates as non-fungible tokens (NFTs) on the Ethereum blockchain ensures secure storage and transferability.

## References


**[1]** A. Nigmatov, A. Pradeep and N. Musulmonova, "Blockchain Technology in Improving Transparency and Efficiency in Government Operations," 2023 15th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Bucharest, Romania, 2023, pp. 01-06, https://doi.org/10.1109/ECAI58194.2023.10194154.

**[2]** Gautami Tripathi, Mohd Abdul Ahad, Gabriella Casalino, A comprehensive review of blockchain technology: Underlying principles and historical background with future challenges, Decision Analytics Journal, Volume 9, 2023, 100344, ISSN 2772-6622, https://doi.org/10.1016/j.dajour.2023.100344.

**[3]** "Blockchain", https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology.

**[4]** "Blockcerts", https://www.blockcerts.org/about.html.

**[5]** "Open Badges", https://www.1edtech.org/clr/faq.

**[6]** N. Naik and P. Jenkins, "Sovrin Network for Decentralized Digital Identity: Analysing a Self-Sovereign Identity System Based on Distributed Ledger Technology," 2021 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 2021, pp. 1-7, https://doi.org/10.1109/ISSE51541.2021.9582551.

**[7]** "Learning Machine", https://www.media.mit.edu/projects/story-learning-machine/overview/.

**[8]** "IBM Digital Identity", https://www.ibm.com/blockchain-identity.

**[9]** "Accredible", https://www.accredible.com/solutions/digital-credentials.

**[10]** "Entrust", https://www.entrust.com/products/digital-certificates/tls-ssl/entrust-certificate-services.

**[11]** "Employer's Graduates Verification System", https://www.academia.edu/36242135/UNIVERSITY_OF_NAIROBI_AN_ACADEMIC_CERTIFICATION_VERIFICATION_SYTEM_BASED_ON_CLOUD_COMPUTING_ENVIRONMENT.

**[12]** Huynh, Trong Thua and Pham, Dang-Khoa, Eunicert: Ethereum Based Digital Certificate Verification System (2019). International Journal of Network Security & Its Applications (IJNSA) Vol. 11, No.5, September 2019, Available at SSRN: https://ssrn.com/abstract=3870897.

**[13]** A. Gayathiri, J. Jayachitra and S. Matilda, "Certificate validation using blockchain," 2020 7th International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 2020, pp. 1-4, http://doi.org/10.1109/ICSSS49621.2020.9201988.