


Verifiable Authentication and Issuance of Academic Certificates Using Permissioned Blockchain Network

Erukala Suresh Babu, National Institute of Technology, Warangal, India*

B. K. N. Srinivasarao, National Institute of Technology, Warangal, India

Ilaiah Kavati, National Institute of Technology, Warangal, India

Mekala Srinivasa Rao, Lakireddy Bali Reddy College of Engineering, Mylavaram, India

 <https://orcid.org/0000-0001-7706-8028>

ABSTRACT

Fake certificates pose a severe problem in today's world; they vouch for an individual's false skillset and put an organization's reputation at risk. Moreover, the existing verification process is performed in a centralized manner, often too cumbersome and time-consuming to the end-user, lacking transparency in the educational institutions' Issuance of certificates. Of-late, blockchain is a promising technology that provides transparent, secure, and reliable features, which offers solutions to the education sector. This paper provides the solution to the educational certification problem by employing the blockchain network. We proposed a permissioned blockchain network that identifies, authenticates the Issuer, adequate verification, securely shares academic records to the recipients, and stores the certificate credentials in the blockchain in a distributed manner.

KEYWORDS

Academic Certificates, Blockchain Network, Hyperledger Fabric, Immutability, Transparency

1. INTRODUCTION

Certificates are documents that serve as proof of a specific education received by a person or a series of tests that (s) he has qualified. They are signals of achievements or memberships and are proof of a person's skill sets. Usually vouched by a trustworthy organization in the respective field, they mark excellence in education fields (Bessa, E. E., & Martins, J. S. (2019) ; Yumna, H., Khan, M. M., Ikram, M., & Ilyas, S. (2019, April). Degrees issued by universities vouch for the professional skill sets of an individual in numerous various areas. The current system for the Issuance of certificates is predominantly analog, making it slow and introduces innumerable complications, which essentially renders it unreliable. For any certificate provided by a candidate applying for a job, the verification process has to be tunneled to the respective institute that issued the certificate in the first place. The problem aggravates when it needs to be verified where the institute is not fraudulent and whether it issued that certificate to that applicant. The only way out in general is to check the institute's validity by the government authority to which it is affiliated; after that, request the institute to verify the applicant's credentials. Intuitively, we can observe the complications that arise with such a system. One of the solutions prevalent is to issue online certificates secured using cryptographic methods, but that

DOI: 10.4018/ijisp.2022010107

predominantly makes sending and receiving the certificates easier. Still, the problems of credibility of the Issuer and the validity of the certificates remain a problem. Fraudulent online certificates are also a threat to this system. Certification is plagued by the threat of fake certificates, which affects such an essential and vital document's trust value. The essence of certification is fundamental in everyday life. There are many advantages to creating a digital infrastructure for certificates. Still, it involves a trusted third party, incurs the additional cost, and for each attempt to verify a certificate's credentials, the third-party entity needs to be contacted. Another bottleneck that surfaces are the case where a certificate needs to be revoked due to some discrepancies. The issuing authority can forward the request to the trusted third party. Still, even after cancellation, the recipient has a copy of the original one, which can be misused, i.e., a dynamic mechanism for certificate validation is absent, which can add a temporal dimension to each validation attempt to any copy of the certificate that ever existed. This paper provides the solution to the educational certification problem by employing the blockchain network. This network work as a trusted system for securing, transparent, sharing, and verifying academic achievements that can be applied to the non-formal and formal education sector to safeguard their brands and reputations. Specifically, this network manages the academic credentials in distributed nature, recorded and immutable; new entries are initiated and validated without any third-party intermediaries as the keeper of trust. Further, the participants of the blockchain network (BN) can certify the integrity of the whole. To achieve this, first, we will create a blockchain network for issuing certificates. Second, establishing the cryptographic identity management system for different participants. Third, ensuring the integrity, transparent Issuance, and more effortless verification procedure for all participants by eliminating a trusted third party requirement. Hence, we provide a scalable, efficient, and durable network for educational institutions, which ensures transparency, immutability, trust, and ease of use to all participants.

This section also presents the literature survey, which provides the basis for the proposed work. Initially, we presented some of the limitations of current digital certificates based on a web of trust. First, to ensure the integrity of any digital data or transaction, digital signatures make use of a third-party certificate for controlling any aspect of the certification and verification process, which can be disingenuous. Second, Current digital signatures do not have a universally used open standard. Third, Due to its centralized nature, a single point of failure can easily destroy the electronic records or be prone to large-scale data-leaks due to digital certificates' registries. Based on these issues, Existing literature proposed various mechanisms to provide the solutions. In (MIT Media Lab, 2018), Blockcerts provides a solution that has been explored partially to issue digital certificates to groups of individuals using blockchain, called Blockcerts. MIT Media Lab implements this Blockcert. The Blockcerts provides the solutions to issue, view, and verify certificates using blockchain and provides the facility to revoke a certificate. In (World's first blockchain career verification platform, 2018), Gary McKay et al. proposed the APPII platform that provides recruitment, career management, and online verification. This APPII is a blockchain-based framework that verifies individuals' assertions, where the employer can easily find the top talent of individuals and increase productivity. However, this method is very costly and time-consuming. In (Instantly Verify Qualifications", Gradbase, 2018) The Gradbase is a London startup-based company. They provided the solutions to rules out the fraudsters at the beginning of the recruiting process. They use the Bitcoin Blockchain technology that verifies the individual data instantaneously of their true qualifications and guarantees the degree claim's authentication. But it is a third-party company that assures the recruiters and Issuers (educational institutions) who upload the student records on gradbase Bitcoin Blockchain. EKO (<https://www.echolink.info>, 2018) is a public blockchain-based system for Distributed Applications (DApps) that verifies education certificates. Specifically, it provides trusted information to the job providers on the candidate's education, skill, and work experience. However, a public blockchain is not suitable for the certification system because it has privacy, scalability, and storage issues.

In (Li, H., & Han, D. (2019)) proposed the EduRSS scheme to store and share educational records using a blockchain network. Their work is based on an off-chain storage mechanism that stores the

22 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage: www.igi-global.com/article/verifiable-authentication-and-issuance-of-academic-certificates-using-permissioned-blockchain-network/284052

Related Content

Information Ethics from an Islamic Perspective

Salam Abdallah (2007). *Encyclopedia of Information Ethics and Security* (pp. 355-361).

www.irma-international.org/chapter/information-ethics-islamic-perspective/13496

E-Mail Worm Detection Using Data Mining

Mohammad M. Masud, Latifur Khan and Bhavani Thuraisingham (2007). *International Journal of Information Security and Privacy* (pp. 47-61).

www.irma-international.org/article/mail-worm-detection-using-data/2470

Several Oblivious Transfer Variants in Cut-and-Choose Scenario

Chuan Zhao, Han Jiang, Qiuliang Xu, Xiaochao Wei and Hao Wang (2015). *International Journal of Information Security and Privacy* (pp. 1-12).

www.irma-international.org/article/several-oblivious-transfer-variants-in-cut-and-choose-scenario/148063

Managing End-of-Life Information in Palliative Care: Between Discord and Conceptual Blends

Alexandre Cotovio Martins (2019). *Emerging Trends and Innovations in Privacy and Health Information Management* (pp. 169-187).

www.irma-international.org/chapter/managing-end-of-life-information-in-palliative-care/228344

Authentication Through Elliptic Curve Cryptography (ECC) Technique in WMN

Geetanjali Rathee and Hemraj Saini (2018). *International Journal of Information Security and Privacy* (pp. 42-52).

www.irma-international.org/article/authentication-through-elliptic-curve-cryptography-ecc-technique-in-wmn/190855