Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

Blockchain Based Academic Credential Verification System

Dr.Sandhya Shinde
Dr.D.Y Patil International University,Pune

Isha Myanewa r
DYPIEMR
ishamyanewa

Surdatt Nimbal
DYPIEMR

Harsh Randhir
DYPIEMR

Abstract
In an more and more virtual international, the need for steady, transparent, and tamper-proof systems to verify academic certificate is critical. Traditional strategies of certificate issuance and verification are liable to fraud, loss, and time delays. Blockchain generation offers a promising strategy to those demanding situations by using offering a decentralized, immutable, and secure platform for storing and validating pupil certificates. This paper presents a blockchain-based totally gadget for student certificates validation, wherein academic institutions difficulty digital certificates at once onto a blockchain community. The machine ensures that certificate are cryptographically signed and time stamped, preventing unauthorized adjustments or forgeries. Students can securely share their certificate with ability employers or educational establishments, who can instantly confirm the authenticity through a decentralized community, without counting on intermediaries. By making use of smart contracts, the machine automates certificates validation strategies, reducing administrative overhead and expenses. Additionally, the decentralized nature of blockchain ensures transparency and enhances believe in the educational certification process. This method not simplest secures instructional credentials however additionally streamlines the verification process for institutions and employers globally.

Keywords: **Blockchain Technology, Digital Certificate, Certificate Validation,Smart Contracts, Data Integrity**

I. INTRODUCTION

The rise of blockchain technology has affected many sectors, with education also absorbing this trend. One of the global issues faced by educational institutions, employers, and learner's, in general, is assessment of academic certificates presented to them. Most of the time, the traditional way of employee's credential verification may also involve a lot of time since the issuing institution may have to carry out a manual verification of it or a third party may be hired such as a credential verification agency which can even take days or weeks or place it in the archives. Various methods of assessment are also prone to artificial errors, deception, ineffectiveness therefore providing credible assurance for a document such as a certificate or a degree is a nightmare. Given that academic and professional qualifications have taken center stage in this global marketplace we all exist in today, there has been increased claimer for a system that can be safely, confirmed, and quickly used in that order to verify the qualifications. This is where the power of Blockchain technology comes into play.

A blockchain refers to a distributed and immutable database where records are managed by a consensus. In simple terms, it is a way of keeping or archiving and retrieving information without the risk of tampering or going through intermediaries. In relation to this form of technology, the educational sector can use it, especially in the issuance and verification of certificates. Whenever a student is awarded a degree or diploma by any educational institution, that particular credential can be uploaded into a blockchain..

II. LITERATURE REVIEW

Certificate Verification and Validation on the Blockchain As per the statistics of the Ministry of Education in India, the area of document verification is a multifaceted area which includes a lot of processes which are extremely cumbersome in a bid to authenticate various degrees. The incidents of a graduating class's diploma issuance without the graduate is very common, primarily due to the absence of an efficient means of counter-appropriation. To address the challenge of counterfeiting diplomas, the introduction of the certificate system build on the distributed ledger technology known as the blockchain is suggested. To students, academic credentials are perhaps the most significant papers, which is issued to them by their respective institutions only. But since the process of issuing them is not that simple and accountable, there is an easy way to produce fraudulent copies of certificates.

Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

SURVEY	AUTHOR	YEAR	EXPLANATION
SURVEY 1: Blockchain and smart contract for digital certificate	Jiin-chiou etal.,,	2018	▪ generate the electronic file and calculate hash value for it. ▪ system creates a QR-code Pros : certificate granting are open and transparent in the system. Cons : QR-code must be scanned with smartphone and internet connection is required.
SURVEY 2: Blockchain based certificate transparency and revocation	Zewang Jingqiang Lin etal.,,	2019	CAs signed certificates and their revocation status information of an SSL/TLS web server are published by the subject and append it to the global certificate blockchain . ▪ Blockchain act as public logs to monitor CAs certificate signing and revocation operations Pros: Avoids the certificate fraudulent Cons: : Certificate validation delay and false sense of security
Survey 3: Certificate transparency using blockchain	Dsv madala etal.,,,	2018	Hyperledger fabric is used. CTB smart contract. Pros : logs-consistency Cons: low scalability and less transaction

SURVEY	AUTHOR	YEAR	EXPLANATION
SURVEY :4 Decentralized Digital Certificate Revocation system based on blockchain	DSV madala Etal.,,	2018	The consortium blockchain technology is collaborative management of digital certificate revocation lists by multiple CAs and introduces secret sharing scheme OSCP(online certificate status protocol is used Pros: Trusted and reliable CRL. Cons : False sense of security.
SURVEY 5: Certificate validation through public ledgers and blockchain	Macro baldil etal.,,	2017	▪CRLs are distributed through the use of a private blockchain, shared among CA(certificate authority). ▪CAs, are responsible for issuing certificates to requestors who meet the requirements and maintain CRLs. ▪users just need to read certificates Pros : Provide reliability Cons: CA ecosystem is fragile and prone to compromises

Fig 1 Comparison to previous system

III. OBJECTIVES OF THE PROPOSED SYSTEM

Everything has become digitized in the present scenario. Similar is the case with the SSLC, HSC, and even academic certificates which are all available in the educational institution and offered to students upon request. Majority of the students find it hard to keep their degree certificates. To both organization and institution, the checking and the verification of certificates turn out to be difficult and laborious. Our project will assist in storing the certificate into the block chain system and shelve it efficiently. To start with all the relevant paper certificates, there is a need to transform them into an electronic format. The attack of chaotic search is used to design the hashing code value for the certificate. The next step involves the incorporation of the certifications into the blockchain. And these certificates are verified with the help of a mobile application.

Expanding compartments usable by the proper blocking can interfere the traditional system from making such changes less secure. To the dismiss of the entities exercising the digital certificate authority, The Let us consider the problem of forgery of registers and how it can be adjusted for resolving the particular issue, The cause of counterfeiting certificates would be addressed by proposing a solution that involves the use of digital certificates embedded with blockchain technology.

IV. PROPOSED SYSTEM

A. Methodology

An elaborate approach to the validation of student certificates includes a series of steps aimed at ensuring the authenticity and correctness of the documents in question. To begin with, the stakeholders in the process should provide a centralized database or an electronic platform on which all the certificates will be kept for easy inspection. This system should bear unique identifiers such as QR codes or serial numbers on the documents, for quick authentication purposes. Thereafter, such records should also be reconciled with the particular student's records, such as units completed, grades, and the dates of release of such records. To add on the level of protection, an option of placing the information on the blockchain may be added resulting in the creation of secure and unalterable records. In instances where the scrutiny has to be manual, clearly outlined procedures must be in place that will allow those wishing to validate certificates, to contact the relevant issuing authority. Non hand-written signatures can also be used as forms of deterring such practices. The reinforcement of the validation systems should be encapsulated with the scheduling of checks and reviews of the procedures in order to sustain the usefulness of the system

B. Creation of Digital Certificates

The process of designing and generating a digital certificate on a blockchain follows a systematic approach. To begin with, the requisite detailed information about the certificate is prepared, for instance, the name of the student, the programme completed, proffered date, and the specific certificate ID. institution-specific information such as the name of the institution and the digital signature may be incorporated to improve the credibility of the data. Then, it is the turn to select a blockchain platform based on aspects such as the type of network, the costs encompassed, and scalability. Among these options are public blockchains such as Ethereum and closed networks such as Hyperledger which provide different levels of limitations in regard to security and accessibility. On those haof platforms that allow the use of smart contracts a specific smart contract was designed to deal with the task of management of the certificates. This contract contains procedures on how to create new certificates, check the status of existing certificates and how to delete, if need be, profiled certificates. After such a smart contract has been designed, it is then uploaded to the blockchain which allows for the certificates to be issued in a secure manner by institutions and all those credentialing purposes by the certificates, can be carried out 'online' by the verifying agencies.

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

C. Hash Code Generation

When creating hash values for digital certificates, in the first place a secure hash algorithm is chosen. For example, SHA-512 is mostly used in blockchain applications and therefore preferred also for certification. Then, collect all the details of the certificate secured for hashing: a name of… the student, a name of the program, an organization that issued the certificate, dates, and the internal code of the certificate. That data is prepared and fed into the algorithm of SHA 512 to produce a string of characters of set length referred to as a hash code which is specific to the certificate information. This hash code is specific to the data of the certificate, which means that if any data changes (even one letter) the hash would vary completely thus making falsification easy. This hash may then be incorporated in the blockchain so that everyone who has the certificate data can recalculate the hash and check it with what is kept in the blockchain relating to the document.

D. Digital certificate validation

Digital One of the aspects of using the blockchain for the validation of digital certificates is the connection of the certificate particulars with the corresponding hash available on the blockchain, and confirming that the certificate as well as its contents are genuine. For example, for an employer or an educational institution wishing to verify a certain certificate, first they need to get such particulars as the name of the certificate holder, the name of the course taken, the dates, and the registration number. These particulars are then merged together and fed into the same hashing set as the one that was used in the creation of the certificate i.e. SHA-
512. Finally, the resulting hash code is checked against the hash which has already been incorporated into the blockchain. If the two hash codes correspond, it gives a guarantee that such a certificate has been tenable and no alterations made to it after its issuance by the institution. Such a system allows for the safe and easy means of credential verifications as it guarantees that the document has no forgery or alterations purely thanks to decentralization. Furthermore, added functionality is provided by some blockchain solutions that can include also revoke capabilities and thus if certificate is no longer in force it is possible to find out this information on the blockchain as well increasing the security during the verification process.

E. Working of Application

A digital certificate validation application based on blockchain technology works by securely controlling the generation, management, and verification of all certificates. Whenever a school, college, university, and any other educational institution issues a certificate, a number of details are fed into the application including, the name of the student, course undertaken, date of issuance of the certificate, and registration number. This information undergoes further processing in a secure hashing algorithm (most likely SHA-512),which produces a characteristic representation of the information of the specific certificate by way of a hash. After that, this hash and other necessary information including metadata, is embedded using a smart contract in the blockchain making the certificate protected from any alteration and permanently retained. A digital copy of the certificate is then provided to the student in their digital wallet. In instances when the certificate is needed for verification, the employers or organization can access the details of the certificate, obtain the same and rehash it using the same algorithm, and compare the hash generated with the hash on the blockchain. In such a situation when both of the hashes are the same, then it is assumed that the certificate is genuine. The system can also allow mobile and web applications enabling institutions to mark certificates as revoked whenever that is necessary to prevent fraud or abuse, with the blockchain reflecting these updates in real time. The system is a secure and user-friendly system for the authenticity check of academic qualifications – trust is built and the chances of trust abuse are minimal.

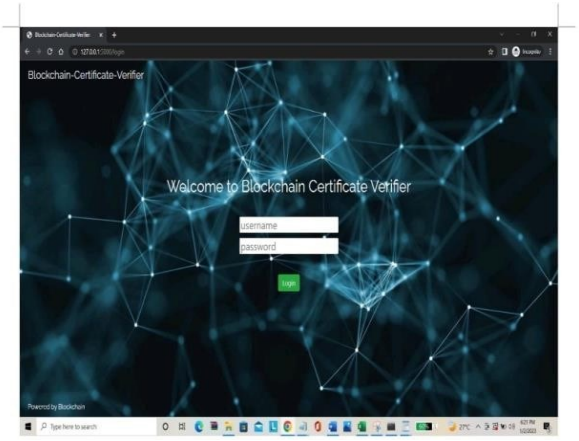

Fig 2: Blockchain Certificate Verifier

Fig 3.Certificate Successfully Verified

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 14 Issue 01, January-2025

V. CONCLUSION

Finally, needless to say, the design and implementation of a blockchain-enabled system for the validation of academic credentials is the way of the future. With the help of blockchain, which is by nature immutable as well as transparent, it will enable the issuance of secure, verification ready, fraud resilient and low weight academic credentials thus reducing the level of fraud and administrative burden significantly. The entire cycle of issuing, keeping and checking of such documents becomes much smoother and cheaper for educational establishments and employers. Besides, more flexibility is exercised for students as they venturing out to access the job market can show their qualifications with less hassle as those can be packaged and made accessible to the world. This is notably a more efficient and trusted solution of managing one's educational accomplishments. Certainly there are issues in implementing this technology especially regarding its initial cost and complexity but the benefits, especially in the long run, make this technology suitable for innovation in the status quo of the credentialing practice in Education and Professional attainment verification.

VI. REFERENCES

[1] Jiin-Chiou Cheng; Narn-Yih Lee; Chien Chi; Yi-Hua Chen, "Blockchain and Smart Contract for Digital Certificate" IEEE International Conference on Applied System Invention (ICASI),2018.

[2] Wang Z., Lin J., Cai Q., Wang Q., Jing J., Zha D. (2019) Blockchain-Based Certificate Transparency and Revocation Transparency. In: Zohar A. et al. (eds) Financial Cryptography and Data Security. FC 2018. Lecture Notes in Computer Science, vol 10958. Springer, Berlin, Heidelberg.

[3] D. S. V. Madala, M. P. Jhanwar, and A. Chattopadhyay, "Certificate Transparency Using Blockchain," 2018 IEEE International Conference on Data Mining Workshops (ICDMW), Singapore, Singapore, 2018, pp. 71-80, doi: 10.1109/ICDMW.2018.00018.

[4] Aisong Zhang and Xinxin Ma, "Decentralized Digital Certificate Revocation System Based on Blockchain", Journal of Physics: Conference Series, Volume 1069, 3rd Annual International Conference on Information System and Artificial Intelligence (ISAI2018) 22–24 June 2018, Suzhou.

[5] Marco Baldi, Franco Chiaraluce, Emanuele Frontoni, Giuseppe Gottardi, Daniele Sciarroni, and Luca Spalazzi "Certificate Validation through Public Ledgers and Blockchains In Proceedings of the First Italian Conference on Cybersecurity.

[6] Nitin Kumavat, Swapnil Mengade, Dishant Desai, JesalVarolia, " Certificate Verification System using Blockchain" Computer Engineering Department, Mumbai University.

[7] S.Sunitha kumari, D.Saveetha "Blockchain and Smart Contract for Digital Document Verification" Department of Information Technology- SRM Institute of Science and Technology.

[8] Omars Saleh, osman ghazali, muhammad ehsan rana, "Blockchain based framework for educational certificates verification" Studies, Planning and Follow-up Directorate, Ministry of Higher Education and Scientific Research, Baghdad, Iraq. School of Computing, University Utara Malaysia, Kedah, Malaysia.

[9] Trong Thua Huynh, Trung Tru Huynh, Dang Khoa Pham, Anh Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain" https://dx.doi.org/10.1109/ATC.2018.8587428.

[10] Maharshi Shah, Priyanka Kumar, "Tamper Proof Birth Certificate Using Blockchain Technology" International Journal of Recent Technology and Engineering (IJRTE).