INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH IN ENGINEERING AND MANAGEMENT (IJSREM)
VOLUME: 08 ISSUE: 03 | MARCH - 2024 SJIF RATING: 8.448 ISSN: 2582-3930

Academic Credentials Issuance and Validation System Using Blockchain

BHAVANI K
Information Technology
Sri Manakula Vinayagar Engineering College
Puducherry, India
bhavaniit@smvec.ac.in

SUMAN K
Information Technology
Sri Manakula Vinayagar Engineering College
Puducherry, India
sumanit@smvec.ac.in

KIRAN YADAV S
Information Technology
Sri Manakula Vinayagar Engineering College
Puducherry, India
kiranyadavit@smvec.ac.in

GADIRAJU RAJESH VARMA
Information Technology
Sri Manakula Vinayagar Engineering College
Puducherry, India
rajeshvarmait@smvec.ac.in

Abstract: Certificate generation and validation have long been essential processes in various domains, from education and professional certifications to document authentication. However, traditional methods of issuing and verifying certificates often suffer from issues like fraud, tampering, and inefficient record-keeping. Digital certificates with distinctive cryptographic hashes are produced using blockchain technology and safely stored there. This increases trust and lowers the danger of certificate counterfeiting by making certificates easily available and tamper-proof. Blockchain facilitates seamless validation. By instantaneously verifying certificates against the blockchain, anyone with access permissions can streamline the verification process by doing away with middlemen. It could make certificates easily available across institutions and borders, offering to revolutionize the way we validate credentials in the sectors of education, healthcare, and other professions. It provides a clear and effective method of managing and validating certificates, ushering in a time of efficiency and confidence in the digital era. With the help of blockchain technology, certificates are now not only safe but also simple to access from different institutions and geographical locations. It offers a clear and effective method for managing and validating certificates, and it is expected to transform the way we check credentials and identities across a range of sectors, including supply chain management, healthcare, and education. Blockchain-powered certificate production and validation provide a bright future of trust and efficiency in a society that is becoming more and more dependent on digital records.

I. INTRODUCTION

Blockchain was introduced in the year 2008 by Satoshi Nakamoto. Blockchain is one of the online ledgers which provide decentralized and transparent data sharing. In this project, we design an android application used to provide secure verification of our certificates. In nowadays, all Graduation certificates and transcripts hold information that is easily tampered illegally by individuals and should not be easily accessible to outside entities. Therefore, there is a great need for an effective system that can ensure that the data in these certificates is authentic, indicating that the document came from a trustworthy source and authorized source and is not forged.

Various systems have been designed to secure e certificates for education institutions and to store them securely in cloud-based systems. Blockchain is the main tool to felicitate this need and when combined with different hashing techniques, this becomes a powerful method for protecting the data. It also aids in doing away with the requirement for ongoing certificate verification. By improving the security, validity, and confidentiality of graduation certificates, blockchain technology helps lower the frequency of certificate forgeries.

Technologies that exist in security domains include digital signatures, which are used in digital documents to provide authentication, integrity, and non-repudiation. Also with blockchain in play, the storage of certificates are more secure. With these technologies, an application created that facilitates the secure validation of digital certificates.

1.1 Blockchain

The core technology that powers new cryptocurrencies like Bitcoin is called blockchain. Decentralization is widely regarded as the primary benefit of blockchain technology. It can facilitate the establishment of disintermediary peer-to-peer (P2P) transactions, coordination, and cooperation in distributed systems that lack mutual trust and centralized control among individual nodes. These systems can be based on time-stamping, data encryption, distributed consensus algorithms, and economic incentive mechanisms. Because of this, blockchain technology may present a fresh approach to the well-known issues of high operating costs, poor efficiency, and possible security hazards associated with data storage in conventional centralized systems. Blockchain, which is regarded as the next evolution of cloud computing, is anticipated to fundamentally alter how people and organizations behave, facilitating the shift from the Internet

A distributed database called blockchain is frequently used to keep track of unique transactions. A block that already contains records of multiple transactions is added to once a consensus is reached among various nodes. The hash value of each block's previous counterpart for the connection is contained in it. A blockchain is created when all the linked blocks come together. Data are dispersed among multiple nodes, resulting in decentralized data storage. As a result, the nodes collaborate to maintain the database. A block in a blockchain is only considered validated when it has been confirmed by several parties. Moreover, it is impossible to change the data in blocks in an arbitrary way. For instance, a blockchain-based smart contract eliminates uncertainty regarding the accuracy of information, resulting in a dependable system.

1.2 Smart Contract for Digital Certificate

The various certificates, transcripts of grades, diplomas, and other evidence of the students' outstanding performance earned during their studies will be a valuable resource for new employers or institutions of higher learning. Just the names of the schools and the students are entered when schools create different awards or diplomas. Events that lead to the forging of the graduation certificate are frequently noticed because there is no reliable antiforge mechanism in place. The blockchain-based digital certificate system would be suggested as a solution to the issue of certificate forgeries. A digital certificate that is both verifiable and anti-counterfeit could be created thanks to the blockchain's immutable feature. In this system, the process for issuing a digital certificate is as follows. Create an electronic file of a paper certificate and add any relevant information to the database first. In the meantime, determine the hash value of the electronic file. Lastly, in the chain system, store the hash value in the block. To attach to the paper certificate, the system will generate an inquiry string code and corresponding QR-code. This paper certificate through mobile phone scanning or website inquiries. The system electronically lowers the risk of various types of certificates being lost, while simultaneously enhancing the credibility of various paper based certificates thanks to the immutable characteristics of the blockchain.

1.3 Ethereum

Ethereum is a decentralized, open platform that supports a range of derivative applications and has Turing completeness. Ethereum is used to create the majority of smart contracts and decentralized autonomous organizations. Ethereum would be the global computing system if the blockchains supporting Bitcoin were thought of as a global payment network. In addition, Ethereum is an open-source platform that resembles Google's Android. It offers the infrastructure needed for developers to produce apps. Ethereum and those developers both work on and maintain the infrastructure.

The following are some of Ethereum's primary features:

1) **Incorruptible:** third-parties are not able to modify any data.
2) **Secure:** errors derived from personnel factors are avoided because the decentralized applications are maintained by entities rather than individuals;
3) **Permanent:** blockchain does not cease to operate even if an individual computer or server crashes. The Ethereum Virtual Machine (EVM) is a blockchain that can be programmed. In contrast to Bitcoin, which offers a predetermined set of commands, developers can run any program in any way they choose on the EVM. Developers use a high-level language called Solidity to tell the EVM how to run applications.

II. LITERATURE REVIEW

Jin-chiou et al [1] created software to prevent the falsification of certificates. Due to the lack of an anti-forge mechanism, the graduation certificate is to be forged. so, the decentralized application was designed based on etherum blockchain technology. First, generate the digital certificate for the paper certificate then hash value created for the certificate is stored in the blockchain system. Even it used to verify the authenticity of the certificate it required another scanning app to scan the certificate. The system saves on paper, prevent document forgery. But the QR-Code must be scanned with a smartphone and an internet connection is required.

Ze Wang et al [2] designed a blockchain-based certificate transparency and revocation transparency system. In this system, the certificate authority (CA) signed the certificate and the revocation status information of the respected certificates are published by the subject (Certificate Authority). Public logs are used to monitor the CAs

operation. This system was implemented with firefox and nogix. This system provided the trust but Certificate validation is delayed and a false sense of security.

Madala et al [3] used the Hyper ledger Fabric blockchain platform. Under this system, the Certificate Transparency (CT) technique, developed by Google, allows CAs to only issue certificates after receiving approval from the domain owner. The aim to prevent SSL/TLS CA from issuing certificates for a domain without visible to the owner of the domain. However, there were fewer transactions and poor scalability.

Aisong Zhang et al [4] designed a system based on consortium blockchain technology. They used a secret sharing scheme. It can validate the digital certificate to protect the user's information and also the property of the user. The digital certificate revocation lists have collaborated among the CAs. The trust and reliable CRL(Certificate Revocation List)are more compared with the traditional system. The user only needs to use the public key to decrypt the signature in order to validate the certificate. Additionally, the outcome will be contrasted with the message's original hash algorithm. Should the outcome remain constant, it would demonstrate that the digital certificate was unaltered. But there is a false sense of security.

Macro Baldi et al [5] designed a system named certificate validation through public ledgers and blockchain. In this system, CRLs(Certificate Revocation List) were distributed through the use of a private blockchain, and it shared among CA(certificate authority).CAs are responsible for issuing certificates to requestors who meet the requirements and maintain CRLs. The certificate revocation list was available and authentication was provided at any time for a certificate. The certificate revocation list for a set of the certificate was maintained by the same certification authority who issued the certificates. CA ecosystem is fragile and prone to compromise.

III. BACKGROUND WORK

Credential Fraud has existed for a long time, and there is substantial evidence that degrees were widely sold in German universities in the 18th century. However, due to two major drivers in the twentieth century, this phenomenon gained rapid traction: first, as Johnson stated,

As the author convincingly argues, rising global competition in job markets has resulted in a widespread culture of credentialism, with employers 'overly relying on degrees as proof of job competency', even for low-to-moderate skill positions. This practice almost certainly contributes significantly to the black market for forged credentials.

Second, the twentieth century saw the rise of the "for-profit" education model in schools and universities, with academic excellence and integrity increasingly competing with economic and business interests. This situation was complicated further by the rapid expansion of higher education institutions through distance learning programs, flexible and distributed learning modes, branch campuses, franchising, and credit transfer schemes. The distributed and transnational nature of these schemes makes enforcing independent quality and integrity checks much more difficult.

As a result, there is a widespread and thriving culture of credential fraud, as well as a billion-dollar industry. Although concrete figures on credential fraud are not available, some investigations reveal an alarming extent of this trend. For example, in the United States, which has the most diploma mills in the world, Ezell et al. report that the number of fake PhD degrees purchased each year exceeds 50,000, far outnumbering the 40,000-45,000 legitimate PhDs awarded by universities. One diploma mill, run by Americans with offices in Europe and the Middle East, has sold over 450,000 degrees and earned more than $450,000 in revenue.

The United Kingdom is thought to have the most diploma mills in Europe. The University of Wales, the second-largest university in the country with a 120-year history, was a prominent example, with 70,000 students enrolled in 130 colleges around the world. Following the discovery of numerous scams and administrative failures, the registrar resigned and the university shut down its highly profitable degree validation program, which accounted for nearly two-thirds of institutional revenue.

Fraud is also common in developing countries. According to one estimate, half of all high school transcripts in Chinese students' overseas university admissions applications are falsified. This issue is also very prevalent in India, and the trafficking of fake certificates has been described as a 'pan-India' crime. According to a 2015 study, one out of every nine politicians in Russia's lower house had a plagiarized or fake degree. The government of Indonesia established a task force in to be established.

Here we broadly classify various categories of credential fraud:

a) **Document Fraud:** typically entails illegal forgeries, deceptive alteration of legitimate credentials (modification of

name, signatures, degree, details, etc.), or complete fabrications (using forged logos, seals, and serial numbers). This category also includes doctored or misleading translations and credential evaluations.

A recent example is the case of degree shops that have recently sprung up on the Syrian-Turkish border, where merchants exploit desperate Syrian migrants and refugees on their way to Europe by selling them forged documents. A high school diploma is said to cost USD $600, while a university degree can cost up to USD $2,500.

b) **Institutional Fraud:** refers to the situation in which institutional staff is compromised. Such fraud may involve the university registrar or other officials creating an illegitimate credential that is retroactively appended to the university's official record. This method is more reliable than document fraud because the credential is genuine and can usually withstand cursory scrutiny because it is supported by university records.

Busoga University in Uganda was investigated in 2016 for issuing over 1,000 "premium-tuition" degrees to South Sudanese students, the majority of whom were military officers seeking easy degrees to secure government positions.

c) **Diploma Mills:** sell forged credentials from fictitious universities and are the market leader in credential fraud. These organizations operate in a highly structured and sophisticated manner, with a corporate culture that includes dedicated marketing and sales teams, and offer customized "products" to buyers. These mills frequently maintain flawless websites for fictitious universities.

Axact, a Pakistan-based company that operated a web of more than 370 diploma mills that collectively earned millions of dollars in revenue by selling fake degrees and certificates from hundreds of fictitious universities to clients worldwide, is a recent example of an international scandal. Axact has also been accused of extorting money from customers after making sales to them by threatening to reveal their credentials.

d) **Accreditation Fraud:** refers to the situation in which the accreditation body that validates a credential as authentic may be compromised or fictitious. Diploma mills frequently use sham accreditation mills to legitimize the credentials they sell.

The Federal Investigation Agency in Pakistan has investigated several cases in which regulatory bodies verified fake degrees of powerful officials without due diligence. Recently, a company that was investigating the credentials of Chinese student applicants on behalf of prominent US universities was forced to withdraw from the project due to allegations that it was corrupt engaged in widespread application fraud itself. In order to validate his fake degrees, a man from Connecticut ran a phony accreditation agency in parallel called the National Distance Learning Accreditation Council. Employers face very difficult challenges as a result of these practices

VII. CONCLUSION

Various technologies has been discussed to reduce the incidence of certificate forgeries and ensure that the security, validity and confidentiality of graduation certificates, even though there are many limitations regarding the security and privacy of data. A fresh system built on blockchain lowers the rate of certificate fraud. The system allows for open and transparent automated certificate granting. Thus, businesses or organizations can ask the system for details about any certificate. In addition to reducing paper usage and management expenses, the system guards against document forgeries and offers trustworthy and accurate data on digital certificates.

ACKNOWLEDGMENT

We sincerely thank each and every member of our Institution for their steadfast commitment to the blockchain theme and support. Our work's success and completion are largely due to our team's effort

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 Systems

[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] Sifat Nur Billah , Farjana Hossain , Rehana Pollobe , Nahid Murad Abir, Afsana Zaman Zarin , Dr. M.F. Mridha. Blockchain Based Architecture for Certificate Authentication. Bangladesh University of Business and Technology, Dhaka-1216, Bangladesh.

[7] A.Gayathiri , J.Jayachitra , Dr.S.Matilda. Certificate validation using blockchain. In this proposed system the academic, sports certificates are converted into digital certificates using sampling and quantization.

[8] Neethu Gopal, Vani V Prakash. Survey on Blockchain Based Digital Certificate System. This system saves on paper, cuts management costs, prevents document forgery, and provides accurate and reliable information on digital certificates.

[9] Aamna Tariq, Hina Binte Haq and Syed Taha Ali. Cerberus: A blockchain-based accreditation and degree verification system.

[10] Tuti Nurhaeni, Indri Handayani, Frizca Budiarty and Desy Apriani.Blockchain revolution in higher education.

[11] Saha Reno, Mamun Ahmed, Saima Ahmed Jui, Shamma Dilshad. Securing Certificate Management System Using Hyperledger Based Blockchain

[12] P.Sheela Rani, S.Baghavathi Priya Trustworthy Blockchain Based Certificate Distribution for the Education System.

[13] Sara Nikolic, Sasa Matic, Darko Capko, Srdan Vukmirovic, Nemanja Nedic. Development for blockchain based application for digital certificates in education.

[14] Antonio J, Cabrera-Gutierrez, Luis Parrilla, Diego P.Morales, Encarnacion Castillo. Blockchain-based implementation of Tradable Green Certificates.

[15] Kum Che , Muhamad Ehsan Rana Recommendations for implementing a Blockchain based educational certificate distribution system.

[16] Mark Staples, Adnene Guabtni, Qinghua Lu. Software Architecture for Bloackchain based Trade Certificate Systems.

[17] Manjula, Prem Gumathanavar, Kavya Maremmagol. Blockchain and IPFS-Based Performance Analysis of E-Certificate Generation and Verification

[18] Ze Wang, Jingqiang Lin, Quanwei Cai, Qiongxiao Wang, Daren Zha, Jiwu Jing. Transparency of Revocation and Certificates Based on Blockchain.

[19] Shahriar Karim Shawon, Hosnian Ahammad, Shumrose Zaman Shetu, Mahfujur Rahaman, Syed Akhter