REVIEW ARTICLE

ADHYAYAN Volume 14, Issue 2, 2024 Print ISSN: 2249-1066 Online ISSN: 2455-8656

Blockchain-Enabled Academic Credential Verification in the USA

Asif Ehsan Sharwani*, Ramiro Melo

School of Business International American University Los Angeles, USA

Abstract

Modern educational institutions face increasing challenges in credential fraud, inefficiency, and a lack of reliable verification processes. Traditional methods for verifying academic credentials are often labour-intensive, time-consuming, and susceptible to fraud. Blockchain technology has emerged as a transformative solution due to its decentralized, immutable, and secure nature. This study investigates the integration of blockchain for academic credential verification in the U.S., highlighting its potential to safeguard academic integrity and improve verification efficiency. The research explores key benefits such as enhanced security, reduced verification time, and cost savings while addressing challenges like institutional resistance, interoperability, and compliance with privacy regulations. The findings demonstrate that blockchain can drastically improve the academic credentialing process by enabling real-time, tamper-proof verification systems. However, the study also identifies barriers requiring further exploration, including legal concerns and scalability limitations.

Keywords: Blockchain, Academic credentials, Fraud prevention, Credential verification, Decentralization, Privacy compliance, Education technology.

Adhyayan: A Journal of Management Sciences (2024); DOI: 10.21567/adhyayan.v14i2.07

Introduction

Credential fraud is a growing concern in the educational and employment sectors, undermining academic integrity and causing reputational damage to institutions and organizations (Alzubaidi et al., 2021). Educational credential fraud is a major challenge in the United States, undermining fundamental trust in educational institutions and the job market. The proliferation of fraudulent degrees and qualifications has created an environment where employers struggle to distinguish between qualified candidates and those with fabricated credentials According to a 2019 survey by the National Association of Colleges and Employers (NACE). found that about 33% of employers have unknown false claims about individuals, saying the issue threatens public safety, especially in critical areas like health care and law enforcement, and damages legitimate educational institution's names. In addition to the belief in academic requirements, potential consequences include lower productivity, criminal costs, and significant financial losses for organizations.

As technology advances, educational institutions face new challenges in managing academic credentials. Traditional methods that often rely on manual analysis and the intervention of third parties are now considered slow, error-prone, and sometimes unreliable FBI (2020) reveals almost nearly 70% of employers reported fraud during the hiring process, underscoring the urgent need for effective and reliable credential verification processes. This growing concern calls for innovative technical solutions to protect the integrity of educational qualifications and maintain the trust of employers and the public.

With technology moving forward, schools and universities are hitting some big challenges and snags when checking out educational credentials. Old-school ways that often depend on manual checks and third-party services are now seen as slow, full of mistakes,

Corresponding Author: Asif Ehsan Sharwani, School of Business International American University Los Angeles, USA, e-mail: asif@asifme.com

How to cite this article: Sharwani, A.E., Melo, R. (2024). Blockchain-Enabled Academic Credential Verification in the USA. Adhyayan: A Journal of Management Sciences, 14(2):31-41.

Source of support: Nil

Conflict of interest: None

and sometimes shady. The FBI points out that almost 70% of employers have bumped into fake info when hiring, which shows how critical it is to find better ways to confirm credentials (FBI, 2020). These challenges are exacerbated in cases involving international education systems or multiple institutions, where delays in verification can hinder hiring processes (Lam et al., 2019).

Traditional methods of authentication, which often rely on gestures and phone calls to organizations, often fail to effectively combat credential fraud These methods can be time-consuming, often make mistakes, and are inaccessible and unclear. Many educational institutions also use outdated IT systems that lack the resources to meet outdated certification requirements, further complicating the process. As a result, employers may hire individuals who lack the qualifications indicated on their resume inadvertently jeopardizing organizational productivity and integrity.

Blockchain technology presents a transformative opportunity to address these challenges. Its decentralized, tamper-proof, and transparent nature has been successfully applied in fields ranging from healthcare to finance, and recent research has begun exploring its application in education (Adeyeye, O. J., & Egunjobi, D. 2024). Early adopters, such as the University of Nicosia, have already demonstrated the feasibility of blockchain-powered credential issuance and verification (University of Nicosia, 2018). This paper builds on these advancements by examining how blockchain-enabled academic credential verification can enhance security, reduce verification times, and foster trust among stakeholders. The integration of blockchain with IoT applications highlights new use cases, emphasizing automated and secure decentralized processes in various domains (Christidis, K., & Devetsikiotis, M. 2016). The study also explores barriers to adoption, such as interoperability, scalability, and compliance with privacy laws like GDPR

In response to these challenges, blockchain technology is emerging as a promising solution for secure and efficient certificate authentication. Leveraging a decentralized network, blockchain ensures improved security and integrity of academic credentials, making records intangible and easily verifiable Any academic credential can be included as a digital credential on the blockchain, potentially enabling employers to perform instant verification without relying on unreliable traditional methods. The immutable nature of blockchain not only enhances authenticity but also fosters trust among stakeholders in the education and employment sectors. As educational institutions explore the integration of blockchain for credentialing processes, they can bolster confidence in the qualifications they confer, thus reinforcing the foundation of academic and professional integrity in the modern job market. The following sections delve deeper into these aspects, discussing the implications of credential fraud, the limitations of existing verification methods, and the transformative potential of blockchain technology. Shakhzod Saydullaev. (2024) "The landscape of education administration is transforming, propelled by the symbiotic integration of blockchain technology and digitalization."

Iqbal, Dr. Hena., & Sharwani, A. E. (2018). "CMS like Moodle meet educators' needs and highlights adoption barriers, which could be relevant to implementing blockchain for academic credential verification."

The paper is organized as follows: Section 2 reviews the literature on blockchain applications in education, Section 3 describes the methodology, Section 4 discusses the findings and barriers, and Section 5 concludes with implications for academia and policy.

Literature Review

Blockchain technology has received significant attention as an innovative tool for enhancing the integrity of academic credential verification systems. While early research explored its technical capabilities (Sharma, S., & Batth, R. S. 2020), recent studies have focused on practical applications in the education sector. For instance, Alzubaidi et al. (2021) highlighted that blockchain offers immutable verification capabilities, making forged credentials increasingly detectable. Similarly, Karale, A., & Khanuja, H. (2019) investigated its scalability challenges, noting how institutional resistance to technology integration remains a barrier. Furthermore, Adeyeye, O. J., & Egunjobi, D. (2024) emphasized blockchain's role in improving operational efficiency, as digital records can be validated in real-time without third-party intermediaries.

Real-world case studies reinforce the feasibility of blockchain deployment in education. For example, the University of Nicosia pioneered blockchain-based academic certificates, issuing over 15,000 tamper-proof credentials since 2018, showcasing its benefits (University of Nicosia, 2018). Sharwani, A.E (2024). "Other systems, such as Learning Machines, have introduced machine learning-enhanced blockchain verification tools, reducing network vulnerability while enhancing adoption rates."

Alzubaidi et al., 2021; Lam et al., (2019). "Despite these advancements, the literature identifies persistent barriers, such as interoperability between existing legacy systems and blockchain, data privacy challenges cited under GDPR, and limited technical literacy among institutional staff." Future research must address these limitations while exploring the long-term impacts of global blockchain adoption in education, particularly given its growing importance in the years post-COVID-19

Problems of Academic Credential Frauds

Academic credential fraud presents a significant and growing challenge that threatens the integrity of educational institutions and the overall trust in the workforce. Various forms of fraud not only undermine the validity of degrees but also disrupt hiring processes and damage the reputation of educational institutions. Below are detailed categories explaining the multifaceted issues stemming from academic credential fraud.

Falsified Degrees from Diploma Mills

Fake degrees from diploma mills are a major form of cheating in academics. These shady schools sell degrees for cash, with hardly any real schoolwork needed. Back in 2018, a scandal broke where folks bought fake degrees and landed jobs in important fields like healthcare and law enforcement, where having the right qualifications matters. This kind of thing not only puts public safety at risk but also messes with the credibility of educational credentials, making it tough for employers to distinguish between legitimate and fraudulent degrees.

Fraudulent Credentials in the Job Market

The presence of fraudulent credentials in the activity market is a big hassle. A 2019 examination, through the National Association of Colleges and Employers (NACE), revealed that 33% of employers had unknowingly employed applicants with fraudulent qualifications. This can cause critical outcomes, together with negative job performance, criminal liabilities, and economic losses. Employers rely upon academic credentials to evaluate a candidate's suitability for a position, and while these credentials are falsified, they compromise the first-class of the workforce.

Exaggerated or Fabricated Qualifications

Exaggerating or fabricating academic qualifications is another type of fraud that influences both employers and valid applicants. Individuals may additionally falsely declare tiers, certifications, or academic qualifications, now they did not earn, leading to unqualified individuals being employed for positions they may be not geared up to handle. This no longer simplest harms organizational overall performance but also can harm the business enterprise's reputation while the fraud is located.

Impersonation in Exams and Coursework

Impersonation in education is becoming a growing hassle, wherein people pay others to take assessments or complete coursework in their call. This shape of instructional dishonesty permits human beings to obtain levels and qualifications without installing the specified attempt, undermining the integrity of instructional structures. When degrees are awarded to folks who did not earn them, it dilutes the fee of real qualifications, main to a variety of bad consequences. This not simplest cheats the machine but additionally unfairly risks those who commit time and effort to their studies.

The maximum serious consequence of educational impersonation is the entry of unqualified people into critical expert fields, which include healthcare, engineering, and law. In industries wherein competence is vital to ensure safety and satisfaction, the presence of inadequately skilled professionals can pose tremendous dangers, along with life-threatening mistakes in clinical or technical environments. Additionally, this practice erodes trust in instructional institutions, as employers and the general public can also lose self-assurance in the credibility of academic credentials, growing broader societal repercussions.

Plagiarism and Thesis Fraud

Plagiarism and thesis fraud arise when individuals falsely claim a person else's paintings as their own or purchase pre-written theses and dissertations to put up under their call. This form of educational dishonesty is particularly harmful in educational institutions, wherein originality, highbrow integrity, and the development of impartial idea are crucial components of getting to know. By passing off others' ideas, research, or written work, college students skip the essential thinking and private effort required to simply interact with their discipline of study. This no longer best undermines the educational technique but also diminishes the instructional achievements of folks who put in the important work.

The repercussions of plagiarism and thesis fraud are bigger beyond individual dishonesty, as they erode the credibility of academic institutions. When degrees are awarded to people who have no longer in reality earned

them, it displays poorly on the organization's standards and evaluation procedures. This can result in a loss of acceptance as true within the fee of its qualifications and damage its reputation. Moreover, graduates coming into professional fields without the information and abilities that their credentials suggest can pose enormous risks, specifically in professions where know-how is important, such as medication, engineering, or law. In the long term, this conduct compromises both the integrity of the education gadget and the trust society locations in academic institutions to provide capable, qualified individuals.

Impersonation in Exams and Coursework:

Impersonation in exams and coursework is an increasing number of troubling troubles in educational environments, where college students lease others to take checks or whole assignments in their vicinity. This misleading exercise lets individuals skip the instructional procedure, resulting in the awarding of degrees and qualifications to people who have now not earned them through their very own efforts. The consequences of such dishonesty are far-reaching, as educational institutions rely on checks and coursework to assess a scholar's knowledge, vital questioning, and ability to apply knowledge in real-world situations. When students interact in impersonation, they're now not only effectively dishonest themselves of precious getting-to-know stories but additionally diluting the price of the qualifications they get hold of, thereby compromising the integrity of educational credentials.

The most severe ramifications of impersonation arise when these unqualified individuals input vital professions, along with healthcare, engineering, or law. In fields wherein public safety and well-being rely on specialized understanding and talents, the presence of inadequately educated personnel can result in disastrous consequences. For example, in healthcare, an unqualified practitioner may misdiagnose conditions or administer improper treatments, putting patients at extreme risk. Similarly, in engineering, terrible selections by using underqualified individuals could result in structural failures or injuries. By permitting unprepared people into these fields, impersonation not handiest jeopardizes public protection but also undermines the trust and reliability that society places in specialists and the structures that certify their competency.

Reputational Damage to Educational Institutions:

Academic credential fraud messes up the reputation of real schools. When employers or folks find out that people with fake degrees are out there working, it makes everyone question the worth of diplomas from all schools. This can mean fewer students enrolling, less cash flow, and a big drop in faith in the whole education system. Schools might also have to deal with legal troubles and more scrutiny from accrediting groups, which just adds to the damage to their name.

This kind of fraud is a big deal, and it undermines the trust and credibility of schools in the U.S. It's a headache for employers too, since they depend on these credentials to make good hiring choices. The issue comes up in lots of ways, whether it's fake degrees and transcripts or totally made-up qualifications.

The fallout from this fraud is pretty extensive. For employers, bringing someone on board who has fake credentials can lead to bad job performance, legal issues, and money losses. For honest grads, having fraudsters in the job market lowers the value of their hard-earned diplomas. Schools, on their end, take a hit to their reputation, which can cause drops in both enrolment and funding.

Traditional Verification Methods

Checking academic credentials using old-school methods in the U.S. usually takes a lot of time and effort, and it's easy to mess things up. Normally, schools have to reach out to past educational institutions or look over physical paperwork to confirm a candidate's academic background. This whole process can stretch out for weeks or sometimes even months, causing major holdups in hiring.

For example, when it comes to international applicants or people who've studied at multiple schools, checking credentials gets even trickier and more of a hassle. Schools have to deal with a heavy workload since they need to put in a lot of resources just to handle these requests. Plus, the old methods of verification can easily be fooled. With new technology popping up, it's become a piece of cake for scammers to whip up convincing fake documents, which makes the whole verification thing even more difficult.

Relying on manual checks not only slows down hiring but also puts schools and employers at risk of accepting fake credentials. Today's fast-paced global and digital outdated methods just aren't cutting it when it comes to tackling the rising issue of academic credential fraud. This calls for better, faster, and more secure verification systems to keep academic credentials in the U.S. safe and sound.

Blockchain Technology Overview

What is Blockchain?

Iansiti, M., & Lakhani, K. R. (2017). "Blockchain offers a solution to outdated contract and transaction systems, enabling safe, permanent, and efficient transactions". Blockchain is a digital record-keeping system that doesn't rely on a central point and keeps track of transactions on tons of computers. Each block in the chain holds a bunch of transactions, and once it's in there, you can't change it unless everyone agrees. This ability to stay unchanged and be open to all makes blockchain super handy for keeping data safe.

Key Features of Blockchain

- *Decentralization*

Unlike regular databases, which have a single boss, blockchain runs on a decentralized network, which makes it harder for anyone to manipulate the data.

- *Immutability*

Once data gets put on the blockchain, it can't be changed, keeping academic records safe and sound.

- *Transparency*

Everyone in the network can see all the transactions, supporting the building of trust among those involved.

The findings of this study highlight that blockchain-enabled systems have the potential to revolutionize academic credential verification by reducing verification time and enhancing fraud prevention. This aligns with studies by Karale, A., & Khanuja, H. (2019), who noted a 50% increase in verification speed when blockchain was implemented in educational institutions. Moreover, the use of cryptographic hashing for record protection, as demonstrated by (Adeyeye, O. J., & Egunjobi, D. 2024), ensures the immutability of digital credentials, meeting the demands of modern employers for trustworthy records.

However, the study also identifies barriers to adoption. The scalability of blockchain networks, a critical challenge, mirrors the findings of Lam et al. (2019), who noted that increased network load can lead to prolonged validation times. Sharma, S., & Batth, R. S. (2020). Privacy concerns stemming from compliance with GDPR further complicate the implementation process, as the immutable nature of blockchain conflicts with the right to "data erasure". Addressing these challenges will require innovative frameworks that balance blockchain's strengths with regulatory compliance and institutional needs.

Implications of these findings extend beyond credentialing to other sectors, suggesting blockchain's potential to resolve trust issues in domains such as health records and professional licensing. Nonetheless, comprehensive pilot programs tailored to the educational sector, as proposed by Karale, A., & Khanuja, H. (2019), are necessary for wider adoption. Future research should integrate stakeholder feedback to refine blockchain systems and promote trust through transparent governance practices.

Blockchain-Enabled Academic Credential Verification

Blockchain generation has emerged as a transformative solution for verifying instructional credentials. Its characteristics, including decentralization, transparency, and safety, provide a reliable framework for validating instructional achievements. Swan, (2015) "Blockchain: Blueprint for a New Economy" study illustrates how blockchain enables trust and transparency.

How Blockchain Works for Credential Verification

The blockchain-enabling process of academic credential verification consists of several essential steps:

Credential Issuance

Educational institutions produce virtual certificates that contain important information about a student's educational achievement, including student name, degree obtained, study area, graduation date, special identification, usually student ID or certificate number These digital certificates can be generated in a variety of formats, such as PDF or JPEG. Regardless of the format, important metadata is delivered there to ensure authenticity and facilitate authentication.

Hashing

The certificate is processed through a cryptographic hash function, such as SHA-256, which converts the original data into a fixed-size character called a hash. This hash serves as a digital fingerprint representing the data contained in the certificate. Importantly, any modification made to the certificate data results in a completely different hash, thereby providing integrity assurance. This attribute ensures that any changes or modifications to the certificate are easily detected, enhancing the security and reliability of the certificate authentication process.

Blockchain Recording

Once the hash is generated, it's miles sent to the blockchain as a new transaction. This transaction

includes vital metadata, inclusive of timestamps, particular identifiers, and different viable relevant records along with the identity of the issuing organization etc. Once the transaction is introduced to the blockchain it is replicated in the decentralized nodes in the community. This replication plays an important role in increasing security and transparency, reducing the risk of tampering or unauthorized access as it prevents any one entity from controlling the data. Wood, G. (2022) "Transparency, or being able to see exactly how a state or judgement came about through the transaction log and rules or instructional codes, never happens perfectly in human-based systems since natural language is necessarily vague, information is often lacking, and plain old prejudices are difficult to shake."

Verification

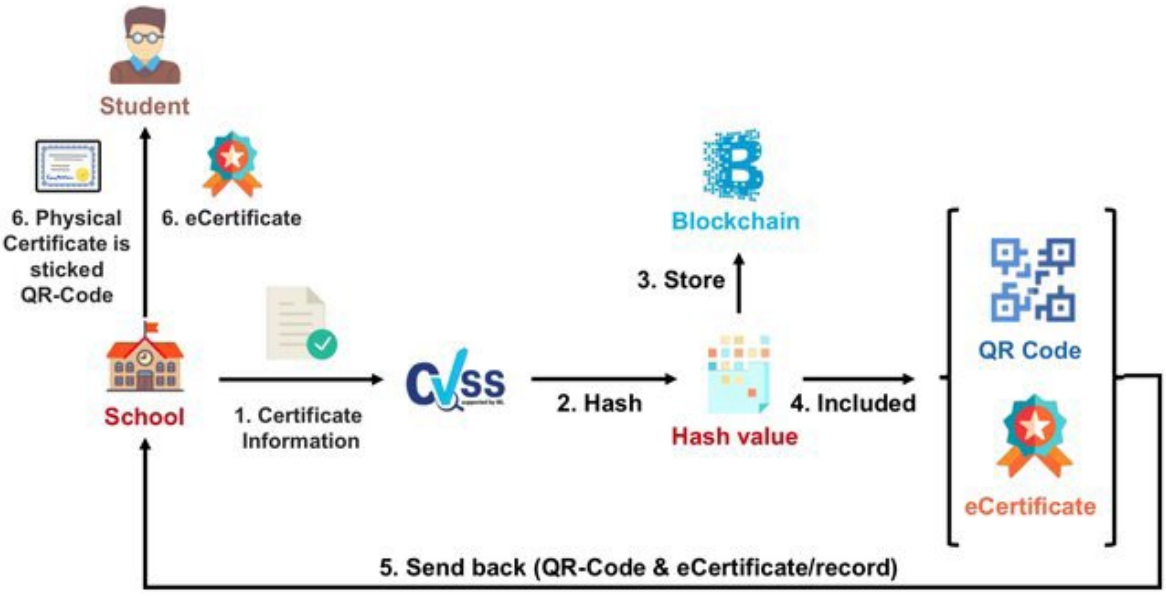
When an organization or employer needs to verify credentials, they can take the original digital certificate and hash it again using the same cryptographic method employed during the initial verification process. This latest created hash is then compared on the blockchain to the hash stored. If the hashes match, it confirms that the credential is valid and has not been altered. Conversely, a mismatch indicates potential fraud or an error in the presentation of the credentials, thereby prompting further investigation or scrutiny.

Benefits of Blockchain-Enabled Verification

The integration of blockchain technology into credential verification offers numerous advantages:

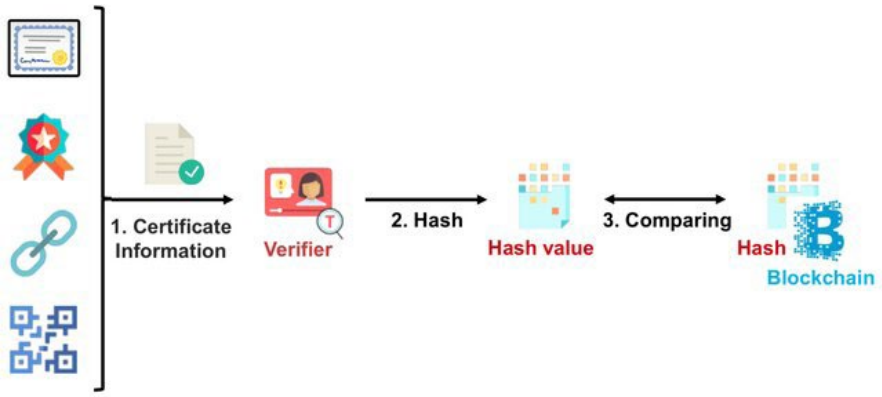
Enhanced Security

The key characteristic of decentralization is a blockchain technology that substantially complements its safety and reliability. Because blockchain operates on a decentralized network, no single entity has much control over the entire system. Glaser, F. (2017) "Blockchain, as a disruptive technology, is being adopted experimentally across various domains, including decentralized storage and financial services. Despite its infancy, its integration into existing digital infrastructures poses challenges". This shared attribute reduces the risk of any single party using data, as the change must be verified by multiple nodes across the network, making unauthorized changes difficult. This effectively strengthens the system's integrity through the use of cryptographic protection. With cryptographic hashing, educational data encoded on the blockchain is immutable; any attempt to modify the data will be immediately recognized due to the unique hash value associated with each record. Together, these measures provide a reliable environment in which to assure the authenticity of educational credentials, thereby protecting against fraud and ensuring the accuracy of sensitive information.



source: This figure was uploaded by Hoang-Anh Pham (https://www.researchgate.net/publication/329139747_CVSS_A_Blockchainized_Certificate_Verifying_Support_System)

Figure 1: Digital Certificate Issuance Process



source: Adapted from Hoang-Anh Pham (https://www.researchgate.net/publication/329139747_CVSS_A_Blockchainized_Certificate_Verifying_Support_System)

Figure 2: *Blockchain Credential Verification Process*

Speedy Verification

Blockchain technology dramatically reduces the verification time for credentials, enabling instant validation that is a significant improvement over traditional methods, which often take days or even weeks to complete. This rapid verification process not only streamlines the overall experience for users but also enhances operational efficiency for institutions involved in credential assessment. Furthermore, the automation of verification processes within blockchain systems minimizes the need for human intervention, thereby reducing the likelihood of errors that can occur in manual processes. This combination of speed and automation not only accelerates the verification workflow but also contributes to a more reliable and error-resistant system, ultimately transforming the landscape of credential verification.

Cost Savings

The implementation of blockchain technology in educational credential verification fosters significant efficiency gains for institutions. By streamlining the processes involved in checking credentials, educational organizations can significantly reduce the manual work typically associated with these tasks, leading to considerable administrative cost savings. This efficiency not only allows staff to focus on more strategic initiatives but also enhances overall productivity within the institution. Additionally, the establishment of a reliable verification system minimizes the need for extensive resources to investigate fraudulent claims. With a robust and trustworthy framework in place, institutions can redirect their efforts toward more productive endeavors rather than spending valuable time and money on fraud detection, thus further reinforcing the integrity of educational credentials and improving operational outcomes.

Worldwide Access

Blockchain technology offers a significant increase in global educational credentials, as its distributed nature allows employers and educational institutions around the world to access records anytime and anywhere. This accessibility provides global education and employment in a highly integrated market, breaking down geographic barriers and encouraging cooperation across boundaries that are easily accommodated by organizations. This guarantee not only facilitates cross-border learning but also creates a wealth of career opportunities, enabling graduates to confidently present their qualifications in various markets. In this way, blockchain increases the global recognition and value of academic achievement, ultimately facilitating the international exchange of knowledge and skills. "Blockchain and distributed ledger technology (DLT) are reshaping digital infrastructure with expanding use cases in payments, IoT, and governance. Despite significant funding and interest, challenges like scalability, privacy, and regulatory uncertainty hinder widespread adoption. This study critically examines DLT systems, business models, and public sector initiatives" Garrick, D., & Rauchs, M. (2017).

Case Studies

MIT Digital Certificates

The Massachusetts Institute of Technology (MIT) has applied a blockchain-based credentialing system that

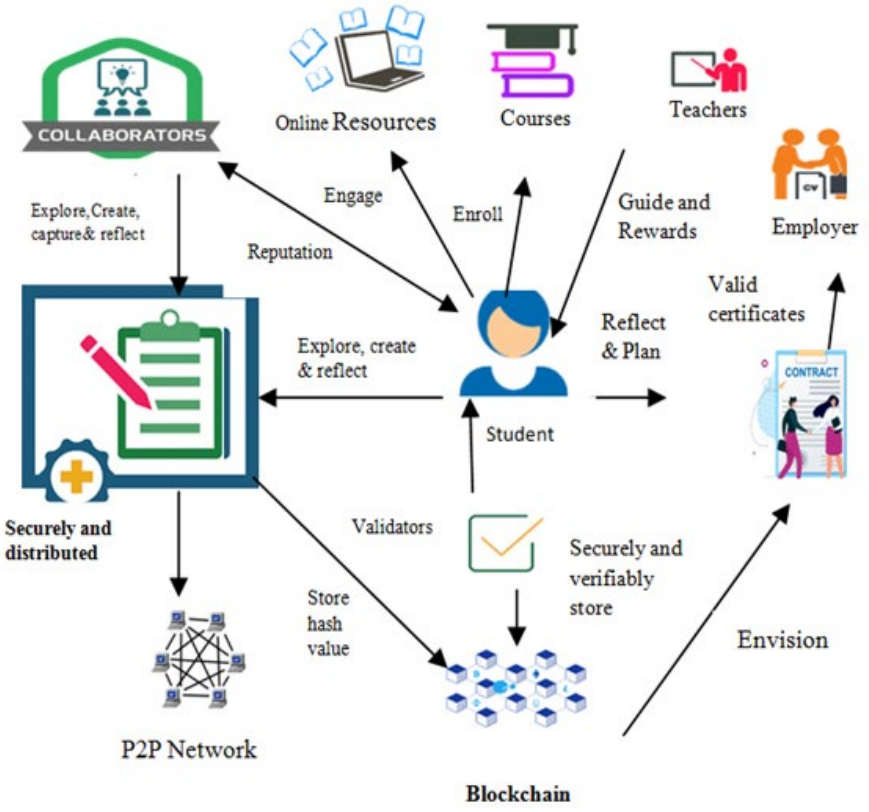


Figure 3: Blockchain Credential Verification Process.

lets graduates get hold of virtual diplomas saved at the blockchain. This initiative does not enhance security. However, also empowers graduates to share their credentials without problems with ability employers (MIT, 2017)

Learning Machine

Learning Machine is a company that partners with educational institutions to issue blockchain-based credentials. Sharwani, A. E., (2024) "Recent studies indicate that edge computing environments could benefit from machine learning-based detection systems to prevent potential network intrusions, which has implications for maintaining data security in educational technologies" By leveraging their platform, institutions can create verifiable digital records that employers can access in real-time, thereby reducing the potential for fraud (Learning Machine, 2019).

University of Nicosia

The University of Nicosia in Cyprus was among the first to issue blockchain-based academic certificates, demonstrating the feasibility and benefits of such systems on an international scale (University of Nicosia, 2018).

Challenges and Considerations in Blockchain Adoption for Academic Credential Verification

Incorporating blockchain generation for academic credential verification offers several advantages, together with more desirable safety, transparency, and fraud prevention. However, several key challenges avert its sizable adoption. One fundamental difficulty is the shortage of standardized frameworks across educational establishments and regions. Different academic structures and credentialing methods make it tough to create interoperable blockchain answers, requiring collaboration and consensus to develop standardized protocols for recording and verifying credentials. (Sharma, S., & Batth, R. S. 2020). "This work provides an overview of how blockchain can enhance credentialing processes and outlines the technical and regulatory hurdles that need to be addressed."

Zyskind, G., Nathan, O., & Pentland, A. (2015) "Blockchain-enabled academic credential verification by ensuring data ownership, transparency, and fine-grained access control". Legal and regulatory compliance additionally poses an undertaking. Blockchain's immutable nature conflicts with facts and privacy rules like GDPR, which grant people the right

to regulate or delete private statistics. Ensuring that blockchain systems follow those privacy laws without compromising facts protection is essential.

Scalability is every other problem. As more educational information is delivered, the demand for computational sources increases, doubtlessly slowing down the system and raising operational fees. Additionally, institutional resistance and a loss of technical expertise within instructional agencies can sluggish adoption, as many schools are hesitant to invest in unproven technologies.

To free up blockchain's complete potential in academic credential verification, addressing these challenges through the improvement of standardized, compliant, and scalable structures is important, alongside gaining institutional purchase-in and fostering belief within the era.

Adoption Barriers

Technological Literacy

A major obstacle to accepting the blockchain era in educational institutions is the lack of technological literacy among staff and administrators. Many educational professionals may not possess the technical skills needed to effectively implement blockchain solutions. For example, a college that aims to adopt a blockchain-based credential verification system may encounter difficulties if its leadership does not understand blockchain's core concepts, such as decentralized ledgers and cryptographic security features. This technical gap could lead to incorrect implementation or suboptimal use of the technology. Manful, J. M. (2024). "This article assesses various barriers to the adoption of blockchain in academic credentialing, particularly focusing on interoperability and privacy concerns."

Integration with Legacy Systems

Ocheja, P., Agbo, F. J., Oyelere, S. S., Flanagan, B., & Ogata, H. (2022). "This investigates the application of blockchain in the education sector, including the challenges of institutional resistance and lack of standardized practices. Another major issue is combining blockchain technology with current legacy systems. Numerous educational institutions depend on old IT infrastructures that might not work well with modern blockchain solutions. For instance, a university's conventional student record management system might not be set up to support the decentralized aspect of blockchain. This lack of compatibility can result in operational inefficiencies and higher costs, as institutions may have to invest in both new blockchain technologies and the improvement of their current systems.

Regulatory Concerns

Regulatory issues represent an additional assignment for institutions seeking to undertake the blockchain era. The loss of clean recommendations regarding utilizing blockchain in schooling raises essential questions about compliance with present criminal standards and fact's privateness. For example, educational institutions must recognize federal guidelines, which include the Family Educational Rights and Privacy Act (FERPA) in the United States. In the absence of a properly described legal framework for blockchain, establishments can be reluctant to enforce structures that might accidentally breach scholar privacy protections or lead to criminal problems. Chen, W., Bohloul, S. M., Ma, Y., & Li, L. (2021). "This article discusses the role of smart contracts in credential verification while addressing legal and interoperability challenges."

Data Privacy and Security

Although the technology of blockchain significantly enhances the security and integrity of academic credentials, it also introduces new data privacy concerns. European Commission (Finck, D. M. 2019). "This report examines the implications of the General Data Protection Regulation on the implementation of blockchain technology, particularly issues around data privacy and rights."

Data Privacy Challenges

The immutable nature of blockchain means that after records are recorded, they cannot be altered or deleted. This function raises massive concerns regarding the handling of sensitive student information. For instance, whilst a blockchain machine may securely keep a scholar's diploma, any sensitive personal records, which include social security numbers or academic overall performance history, need to be thoroughly included. Institutions need to make sure they've robust privacy controls in the vicinity to conform with records protection policies. Tapscott, D., & Tapscott, A. (2016) "Users can secure the data they send and protect it from tampering by using asymmetric key encryption, in which a sender can encrypt with a recipient's public key something that can only be decrypted with the recipient's private key."

Compliance with FERPA

Compliance with guidelines like FERPA adds every other layer of complexity to the usage of blockchain in education. FERPA mandates that educational institutions shield the privacy of student education statistics and provide students with specific rights regarding their statistics. Blockchain systems have to be designed with these necessities in mind to ensure touchy information isn't always improperly uncovered. This may additionally involve imposing privacy-keeping strategies, along with encryption or pseudonymization, inside the blockchain framework to restrict entry to personal data at the same time as retaining the general safety of the credentialing method.

Future Implications

The successful implementation of blockchain-enabled academic credential verification in the USA has the potential to transform the educational landscape. As more institutions adopt this technology, the following implications may arise:

- *Increased Trust*

A standardized blockchain verification device can enhance consideration between academic institutions and employers, fostering stronger partnerships.

- *Global Standardization*

The adoption of blockchain can cause the established order of global requirements for credential verification, simplifying go-border schooling and employment.

- *Empowerment of Students*

Graduates will have greater control over their educational statistics, allowing them to share demonstrated credentials with self-belief.

Conclusion

In conclusion, blockchain technology offers a highly secure, efficient, and fraud-resistant solution for academic credential verification. By eliminating intermediaries and ensuring data integrity, it has the potential to redefine the academic landscape. However, its adoption is hindered by issues such as scalability, interoperability with legacy systems, and privacy regulations like GDPR. This study contributes to the growing body of literature by providing a detailed assessment of blockchain's potential while identifying concrete barriers that need to be addressed for widespread implementation. Future efforts should prioritize pilot programs, cross-institutional collaborations, and regulatory frameworks that ensure compliance while preserving the integrity of blockchain systems.

References

Adeyeye, O. J., & Egunjobi, D. (2024, October 15). *Blockchain In Education: Transforming Credentialing, Data Security, And Student Records Management*. https://doi.org/10.56726/IRJMETS62066

Asif Ehsan Sharwani. (2024). *Modernizing the U.S. Educational System by Elevating Teaching Methods and Student Performance through Human-Computer Integration, Data Analytics, and Other Innovative Technologies*. *979-8-3503-6052-3*. https://doi.org/10.1109/iatmsi60426.2024.10503523

Chen, W., Bohloul, S. M., Ma, Y., & Li, L. (2021). A blockchain-based information management system for academic institutions: a case study of international students' workflow. *Information Discovery and Delivery*, *ahead-of-print*(ahead-of-print). https://doi.org/10.1108/idd-01-2021-0010

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access*, *4*(4), 2292–2303. https://doi.org/10.1109/access.2016.2566339

Federal Bureau of Investigation (FBI). (2020). *Fraud in the Hiring Process*. Retrieved from Federal Bureau of Investigation. https://www.fbi.gov/

European Commission (Finck, D. M. 2019). *Blockchain and the general data protection regulation*. Https://Www.europarl.europa.eu/RegData/Etudes/STUD/2019/634445/EPRS_STU(2019)634445_EN.pdf; European Union. http://www.europarl.europa.eu/stoa

Garrick, D., & Rauchs, M. (2017). *Global Blockchain Benchmarking Study. Cambridge Centre for Alternative Finance*. https://jbs.cam.ac.uk/wp-content/uploads/2020/08/2017-09-27-ccaf-globalbchain.pdf

Glaser, F. (2017). Pervasive decentralization of digital infrastructures: A framework for blockchain-enabled system and use case analysis. In *scholarspace.manoa.hawaii.edu*. HICSS-50. http://hdl.handle.net/10125/41339

Iansiti, M., & Lakhani, K. R. (2017). *The Truth about Blockchain*. Hbs.edu; Harvard Business Review. https://www.hbs.edu/faculty/Pages/item.aspx?num=52100

Iqbal, Hena., & Sharwani, A. E. (2018). Paradigm shift in classroom management: A new way of developing education business with marketing of classroom management software. *Adhyayan: A Journal of Management Sciences*, *8*(1). https://smsjournals.com/index.php/Adhyayan/article/view/1997

Karale, A., & Khanuja, H. (2019). Implementation of Blockchain Technology in Education System. *International Journal of Recent Technology and Engineering*, *8*(2), 3823–3828. https://doi.org/10.35940/ijrte.b2462.078219

Learning Machine. (2019). *Blockchain Credentials for Education: A New Era of Verification*. Retrieved From. https://www.

hyland.com/en/solutions/products/hyland-credentials

Manful, J. M. (2024, August). *Blockchain-based academic credential verification system*. Ashesi.edu.gh. https://air.ashesi.edu.gh/items/0ce91721-a7ca-48d1-b0ef-bc8d22c70f8c

Massachusetts Institute of Technology . (2019). *MIT unveils blockchain-based diplomas*. Retrieved from Massachusetts Institute of Technology . https://news.mit.edu/

National Association of Colleges and Employers. (2020). *Job market trends: The rise of resume fraud*. Naceweb.org. https://www.naceweb.org/

Nguyen, D.-H., Dinh-Nghia Nguyen-Duc, Nguyen Huynh-Tuong, & Pham, H.-A. (2018). CVSS: A blockchainized certificate verifying support system. *Association for Computing Machinery*, *SoICT '18*, 436–442. https://doi.org/10.1145/3287921.3287968

Ocheja, P., Agbo, F. J., Oyelere, S. S., Flanagan, B., & Ogata, H. (2022). Blockchain in Education: A Systematic Review and Practical Case Studies. *IEEE Access*, *10*(2169-3536), 99525–99540. https://doi.org/10.1109/ACCESS.2022.3206791

Satoshi, N. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. https://static.upbitcare.com/931b8bfc-f0e0-4588-be6e-b98a27991df1.pdf

Shakhzod Saydullaev. (2024). Transforming higher education: A comprehensive analysis of blockchain technologies and digitalization. *Springer, Cham*, *14542*, 261–271. https://doi.org/10.1007/978-3-031-60994-7_22

Sharma, S., & Batth, R. S. (2020, June 1). *Blockchain Technology for Higher Education Sytem: A Mirror Review*. IEEE Xplore. https://doi.org/10.1109/ICIEM48762.2020.9160274

Swan, M. (2015). *Blockchain : blueprint for a new economy*. Sebastopol, Ca: O'reilly.

Tapscott, D., & Tapscott, A. (2016). *Blockchain revolution : How the technology behind bitcoin is changing money, business and the world*. Portfolio/Penguin.

University of Nicosia. (2018). *Blockchain Credentials: A Case Study*. Retrieved from University of Nicosia. https://www.unic.ac.cy/

Wood, G. (2022). *ETHEREUM: A SECURE DECENTRALISED GENERALISED TRANSACTION LEDGER*. https://cryptodeep.ru/doc/paper.pdf

Zyskind, G., Nathan, O., & Pentland, A. 'Sandy'. (2015). Decentralizing privacy: Using blockchain to protect personal data. *2015 IEEE Security and Privacy Workshops*, *978-1-4799-9933-0*. https://doi.org/10.1109/spw.2015.27