FUDMA Journal of Engineering and Technology
ISSN: 3092-9385
https://fjet.fudutsinma.edu.ng/index.php/fjet/
Volume 2, Issue 1, 2026, 124-135

Determinants of Blockchain Adoption for Academic Certificate Verification: Insights from Verification Officers for Sustainable Education in Nigerian Higher Education Institutions

Usman A. ALI[1*], Munir A. ADEWOYE[2], Adamu U. ABDULLAHI[3]
[1*,2,3]Department of Computer Science Education, Federal College of Education (Technical), Gombe, Nigeria

[1*]usmanali@fcetgombe.edu.ng, [2]ademunir@fcetgombe.edu.ng, [3]abdullahiadamu@fcetgombe.edu.ng

Abstract
Academic credential fraud and slow, unreliable verification practices remain major challenges for higher education institutions around the world. Blockchain technology has long been proposed as a viable answer because of its decentralized, transparent, and tamper-proof nature. Yet, despite its clear strengths, the rate at which institutions are actually embracing blockchain for sustainable education is still very low. In Nigeria, especially, there is limited understanding of how prepared certificate verification units are to adopt such technology. This survey explored the views of 14 verification officers drawn from 10 tertiary institutions in Gombe State, Nigeria. Data were gathered using a validated 20 items questionnaire that assessed current verification practices, existing challenges, awareness of blockchain, and key factors influencing adoption. The instrument demonstrated good reliability, with a Cronbach's alpha of 0.813. Findings revealed that most institutions still rely on manual verification methods (M = 3.64), which are slow and vulnerable to fraud. Although respondents showed strong awareness of blockchain technology (M = 3.68) and acknowledged its advantages, they also pointed to notable obstacles. The most pressing barriers were the high cost of implementation (M = 3.93) and the urgent need for staff training (M = 4.50). Overall, the study offers valuable empirical insights into institutional readiness and highlights specific adoption challenges from the perspective of verification officers. The result indicates that government involvement will be crucial, particularly through supportive policies, dedicated fundings, and structured capacity building programs. These findings contribute to ongoing conversations on digital transformation within higher education settings in developing regions.

Keywords: *Blockchain technology, certificate verification, higher education, technology adoption, academic credentials.*

1.0 Introduction

Universities across the globe are increasingly confronted with a growing crisis of trust in academic credentials which is affecting the sustainability of education. The sophistication of credential fraud continues to rise, while long standing verification systems have struggled to keep pace with these developments [1]; Silaghi and Popescu [2] asserted that, many institutions still rely on manual, paper based, and communication dependent verification procedures that introduce significant delays and inefficiencies. Such approaches often result in prolonged transcript processing times for students, reduced confidence among employers, and substantial administrative burdens for verification officers.

Although blockchain technology originated from the 2008 Bitcoin whitepaper, it has since evolved far beyond its initial association with cryptocurrencies. At its foundation, blockchain is a decentralized ledger in which entries are chronologically recorded, cryptographically secured, and effectively resistant to tampering [2]. These characteristics make it particularly suitable for academic credential management because they eliminate dependency on a single centralized database. Traditional institutional record systems which are susceptible to hacking, unauthorized manipulation, and service disruptions do not provide the same level of distributed trust and integrity.

The implications of these challenges extend beyond administrative inconvenience. Deliberate credential falsification undermines public confidence in the credibility of higher education systems [3]. Additionally, even authentic institutions may experience record keeping errors that inadvertently affect students' academic or professional trajectories. With the expansion of Massive Open Online Course (MOOCs), international online programs, and increased cross border student mobility, academic credentials now circulate across broader geographical and institutional boundaries. Consequently, secure, efficient, and reliable verification processes have become essential rather than optional [4].

Given these dynamics, a critical question emerges: despite the clear potential of blockchain technology to enhance certificate verification, why have higher education institutions been slow to adopt it? This study addresses this gap by examining the constraints faced by those directly responsible for verification activities. Rather than reiterating the theoretical benefits of blockchain, it focuses on identifying the practical barriers perceived by

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

registrars, admissions personnel, and verification officers, whose day-to-day responsibilities provide valuable insights into the institutional realities of blockchain adoption.

1.1 Problem Statement

Existing certificate verification systems face three core limitations: inefficiency, susceptibility to fraud, and poor scalability within today's increasingly digital and globally connected education environment [5], [6]. Manual verification procedures introduce delays that negatively affect both students and employers, while centralized institutional databases create single points of vulnerability that can be exploited or manipulated. Furthermore, when institutions must validate credentials originating from distant or international sources, the verification process frequently becomes slow, cumbersome, or effectively stalled [7].

According to Vikhankar el. Al., [8], traditional verification mechanisms lack the level of transparency and trust required for contemporary academic credentialing. The rapid expansion of online and remote learning has intensified these shortcomings, producing situations in which verification is inconsistent, inadequate, or entirely absent. At the same time, credential forgery techniques have grown increasingly sophisticated, making conventional document-based checks insufficient for ensuring education authenticity and sustainability [9].

Although multiple institutions and researchers have proposed blockchain-based solutions to address these issues in [10], [11], [12]. These proposals have not translated into widespread institutional adoption. A considerable gap remains between what the technology can achieve and what institutions are currently willing or able to implement.

1.2 Research Gap

Although numerous studies have proposed blockchain based architectures for certificate verification, however, none of such researches have investigated adoption from the viewpoint of institutional verification authorities, the individuals who would ultimately manage the deployment and day-to-day operation of these systems. Existing research tends to emphasize technical design features or the potential advantages for students, yet verification officers encounter distinct operational, financial, and administrative constraints that play a critical role in shaping adoption decisions.

Additionally, there is limited empirical evidence from the Nigerian higher education context. Nigeria, like many developing countries, continues to struggle with pervasive credential fraud and insufficient digital infrastructure. Despite these challenges, little is known about how verification authorities within Nigerian institutions understand blockchain technology or what specific obstacles they perceive in the process of adopting it.

1.3 Research Questions

This study addresses four key questions:

1. What are the current methods and practices for certificate verification in higher institutions in Gombe State?
2. What challenges do verification authorities face in the existing certificate verification process?
3. What is the level of awareness and understanding of blockchain technology among verification authorities?
4. What factors influence the potential adoption of blockchain-based certificate verification systems?

2.0 Literature Review and Theoretical Framework

2.1 Blockchain Applications in Certificate Verification

Since 2020, research on blockchain enabled certificate verification has expanded considerably, with researchers proposing a range of technical architectures and implementation models. Harika et. al. [5], for example, developed a system that integrates QR codes with blockchain based storage, resulting in substantial improvements in verification speed, ease of access, and fraud prevention. Their work addressed a long-standing challenge in credentials, ensuring that employers and other verifiers can validate blockchain secured credentials through a simple and efficient interface.

Quispe and Pacheco [13] advanced this line of inquiry by combining Python and Docker to build a scalable verification framework tested across multiple institutional environments. Their findings demonstrated that the block structure they employed could be adapted for different types of credentials, not only academic certificates but also transcripts, attendance records, and micro credentials. This adaptability is significant because institutions typically issue a diverse range of documents, and a system capable of supporting multiple credential types is more likely to achieve broader adoption.

From a technical implementation standpoint, Vikhankar et. al. [8], developed an Ethereum-based model using Ganache for local deployment and MetaMask for identity and wallet management. Their smart contract design supported the full lifecycle of credential management, including institutional onboarding, certificate issuance,

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

verification processes, and revocation capabilities. Importantly, their user interface separated verification functions from issuance functions, aligning the system with the actual workflow structures commonly found in university verification offices.

Kumar and Kumar [14] emphasized cryptographic robustness, employing double SHA-256 hashing to secure certificate data before storing the resulting hash on the blockchain. They complemented this approach with QR codes on physical certificates, allowing verification officers and employers to seamlessly connect printed documents to their blockchain stored records an important bridge for institutions transitioning from paper-based systems.

More recent contributions push the field further by combining blockchain with additional emerging technologies. Rustemi et.al. [15] integrated blockchain with artificial intelligence, using IPFS for decentralized document storage while Ethereum smart contracts governed the verification logic. Their AI layer supported biometric authentication and anomaly detection, enhancing the system's ability to identify sophisticated forms of credential fraud. Similarly, Farabi et. al. [16] introduced ShikkhaChain, a layered, role-based architecture that clearly distinguishes permissions and responsibilities across government authorities, educational institutions, and end users, ensuring secure and appropriate access to credential data.

2.3 Technology Organization Environment (TOE)Theoretical Framework

To guide the analysis of adoption factors, this study applies the Technology Organization Environment (TOE) framework introduced by Tomatzky and Fleischer [17] as in Figure 1. The TOE model has been widely recognized as a robust analytical tool for examining technology adoption within organizations, particularly in cases involving complex and transformative innovations such as blockchain. The framework is structured around three key dimensions:

Technological Context refers to the characteristics of the technology under consideration. For blockchain, this includes its complexity, its compatibility with existing verification systems, its relative advantage over current processes, and the perceived security and reliability of its features.

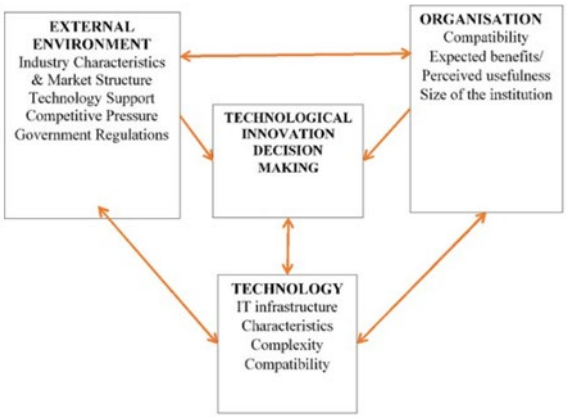

Figure 1: Technology Organization Environment (TOE) framework

Organizational Context captures internal attributes of the adopting institution, such as organizational size, availability of financial, technical, and human resources, administrative structure, and the presence of technology champions or individuals who drive innovation.

Environmental Context encompasses external influences, including regulatory policies, industry norms, competitive forces, and the broader technological and infrastructural environment.

The TOE framework aligns logically with the objectives of this study. Current verification practices and their associated challenges correspond to the technological context, helping to illuminate why existing systems fall short. Levels of blockchain awareness reflect the organizational context, indicating institutional capacity to comprehend and assess the technology. Finally, the adoption factors identified by verification officers span all three dimensions, encompassing integration requirements, cost considerations, external regulatory support, and infrastructural readiness.

This study addresses these gaps as shown in Table 1 by assessing adoption readiness from the perspective of verification authorities within the Nigerian higher education context. It employs a validated quantitative instrument, providing an approach that can be reliably replicated in other developing country settings.

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

Table 1: Summary of Reviewed Studies and Identified Gaps

Study	Focus	Method	Key Gap Addressed by Current Study
[5]	System design with QR codes	Technical implementation	Lacks institutional adoption perspective
[6]	Adoption barriers in EU/Canada	Qualitative interviews	Limited developing nation context
[18]	Tanzania certification ecosystem	Mixed methods, n=137	Didn't focus on verification authorities specifically
[8]	Ethereum-based system	Technical development	No empirical adoption assessment
[15]	AI-blockchain integration	Conceptual modeling	Missing implementation readiness data

3. Methodology

3.1 Research Design

This study adopted a survey research design appropriate for its quantitative orientation. Survey methods are particularly effective for capturing attitudes, perceptions, and opinions across a defined population and for identifying statistically meaningful patterns [19]. This design was well suited to the study's objective of assessing adoption readiness across multiple institutions and identifying shared factors that influence decisions regarding blockchain based verification systems.

3.2 Population and Sampling

Target Population: The target population comprised administrative personnel responsible for certificate verification in tertiary institutions within Gombe State, Nigeria. This group consist of 2 people from each Institution, it includes admissions officer, and verification coordinator who manage routine verification requests submitted by employers, partner institutions, and regulatory agencies. The 10 institutions consist of 20 personals in charge of verification.

Sampling Strategy: Purposive sampling was employed to ensure representation across various categories of tertiary institutions, including universities, polytechnics, colleges of education, and specialized technical colleges. This diversity was essential, as verification practices, challenges, and resource capacities can differ substantially across institutional types. Within each institution, participants were selected based on their direct involvement in verification activities and a minimum of one year of experience in their role, ensuring that respondents had practical and informed perspectives on existing verification processes.

Sample Size: The final sample consisted of 14 verification officers drawn from 10 tertiary institutions across Gombe State. Although the numerical sample may appear modest, it reflects a specialized respondent group in which verification responsibilities are assigned to a limited number of staff. Within this specialized population, the sample provided adequate coverage across institutional categories and levels of professional experience.

3.3 Data Collection Instrument

A structured questionnaire was developed for data collection, organized into five sections:

- **Section A: Demographics** captured information on respondents' institutional affiliation and years of service.
- **Section B: Current Methods of Certificate Verification (CMCV)** assessed existing verification practices through five items, examining the use of manual versus digital methods, internal communication processes, perceptions of accuracy, and time efficiency.
- **Section C: Challenges in Certificate Verification (CICV)** explored verification difficulties using five items addressing remote verification issues, cost constraints, susceptibility to fraud, response delays, and adequacy of available resources.
- **Section D: Awareness of Blockchain Technology (AOBT)** measured knowledge and understanding through five items evaluating familiarity with blockchain, perceptions of security, transparency potential, institutional exploration of the technology, and availability of relevant information.
- **Section E: Factors Influencing Adoption of Blockchain (FIAB)** examined determinants of adoption through five items focused on implementation costs, user friendliness, regulatory influence, system integration requirements, and the importance of training.

All items employed a five-point Likert scale: Strongly Agree (5), Agree (4), Neutral (3), Disagree (2), and Strongly Disagree (1). A benchmark mean of 3.00 was set, with scores above indicating agreement and scores below indicating disagreement.

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

3.4 Instrument Validation and Reliability

- **Content Validity:** The questionnaire was reviewed by an expert from the Department of Computer Education at the Federal College of Education (Technical), Gombe, to ensure clarity, relevance, and alignment with the research objectives. Feedback was used to refine wording and ensure that items effectively addressed each research question.
- **Reliability Testing:** Internal consistency was evaluated using Cronbach's alpha, yielding a coefficient of $\alpha = 0.813$. This exceeds the conventional 0.70 threshold for social science research, indicating that the instrument reliably measures the intended constructs across its sections as shown in Table 2.
-

Table 2: Reliability Analysis

Measure	Value
Cronbach's Alpha	0.813
Number of Items	14
Interpretation	Good internal consistency

- **Correlation Analysis:** Table 3 shows Inter scale correlations which were examined to confirm that the sections measured related yet distinct constructs. A significant correlation was observed between challenges (CICV) and adoption factors (FIAB) ($r = 0.558$, $p < 0.05$), suggesting that respondents who perceived greater verification challenges also identified more factors influencing the adoption of blockchain.

Table 3: Inter-Scale Correlations

Scale	CMCV	CICV	AOBT	FIAB
CMCV	1.000	–0.091	0.274	0.036
CICV	–0.091	1.000	0.063	0.558*
AOBT	0.274	0.063	1.000	0.455
FIAB	0.036	0.558*	0.455	1.000

3.5 Data Collection Procedure

The questionnaire was converted into a digital format using Google Forms, which offered several practical benefits, including streamlined distribution, automatic data collation, and flexibility for respondents to complete the survey at their convenience. The survey link was disseminated via email to verification officers across the selected institutions, and follow-up reminders were issued to enhance participation and improve response rates.

3.6 Ethical Considerations

Participation in the study was entirely voluntary, and respondents provided informed consent before beginning the questionnaire. Confidentiality was strictly maintained, ensuring that no individual participant could be identified from the data. Institutional names are reported only in aggregated form to illustrate the diversity of participating organizations without linking specific responses to any institution.

3.7 Data Analysis

Descriptive statistics including frequencies, percentages, means, and standard deviations were employed as the primary analytical techniques. Mean scores were computed for each Likert scale item to determine the level of agreement. Items with mean values of 3.00 or higher were interpreted as indicating agreement, whereas items with means below 3.00 reflected disagreement. Additionally, grand means were calculated for each scale (CMCV, CICV, AOBT, and FIAB) to identify broader trends across constructs. Correlation analyses were further conducted to examine the relationships among the scales, providing insights into how the underlying factors interact within the study context.

4. Results and Analysis

4.1 Demography

Participating Institutions A total of ten institutions participated in the survey, reflecting the diversity of the higher education sector in Gombe State. These included Federal University Kashere, Gombe State University, Federal Polytechnic Kaltungo, Gombe State Polytechnic Bajoga, Federal College of Education (Technical) Gombe, College of Education Billiri, College of Education and Legal Studies Nafada, College of Nursing Sciences Gombe, College of Health Technology Kaltungo, and the Federal College of Horticulture Dadin Kowa.

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

This group represents a broad spectrum of institution types, comprehensive universities, polytechnics, colleges of education, and specialized institutions in nursing, health technology, and agriculture. Such diversity is important, as each category of institution encounters unique verification challenges and possesses distinct levels of technological readiness.

Years of Service Respondents' years of professional experience ranged from newly recruited staff to long serving officers. The highest proportions were within the 0–5 years (n = 5) and 6–10 years (n = 4) categories, indicating that many verification officers are in the early to mid-stages of their careers. Experienced personnel were also represented, including those with 11–15 years (n = 3) and 16–20 years (n = 2) of service as shown in Figure 2. This distribution is advantageous for the study. Early career staff often demonstrate greater openness to digital tools and new technological systems, while more experienced officers contribute institutional memory, familiarity with evolving verification practices, and deeper insight into persistent operational challenges. Together, these perspectives enhance the robustness and credibility of the findings.

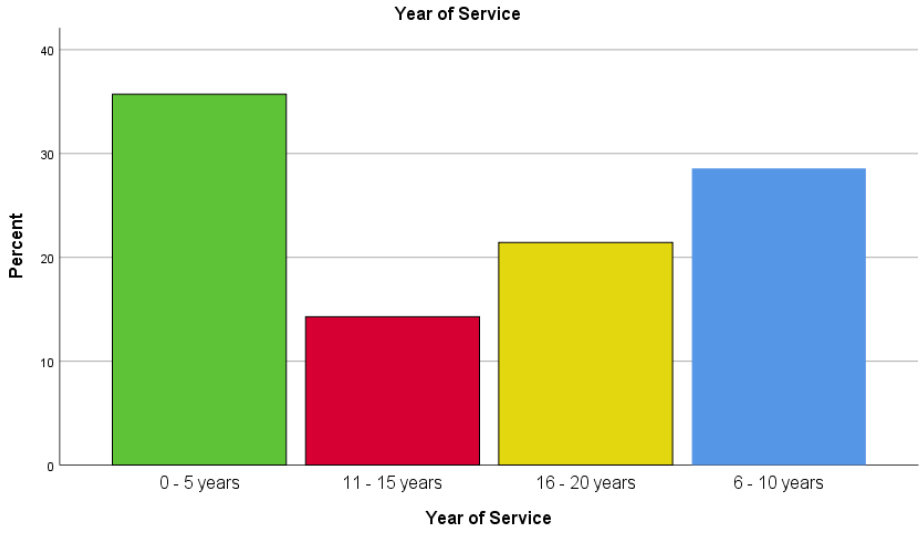

Figure 2: Year of Service of the Participants

4.2 Current Methods of Certificate Verification (CMCV)

What are the current methods and practices for certificate verification in higher institutions in Gombe State?

The descriptive results present in Table 4 is a clear pattern. Verification practices across institutions remain predominantly manual, with a high mean score for physical document checks (M = 3.64). This suggests that routine verification still involves actions such as retrieving physical files, making phone calls, and sending formal letters. In contrast, the relatively low mean for the use of digital databases (M = 2.57) indicates that digital automation has not yet been widely integrated into verification operations.

Table 4: Descriptive Statistics for CMCV Items

Item	Statement	N	Mean	SD
CMCV1	Manual methods (physical document checks) are used	14	3.64	1.393
CMCV2	Digital databases/platforms are used	14	2.57	1.284
CMCV3	Verification involves direct communication with issuing institutions	14	3.57	1.222
CMCV4	Current methods ensure low accuracy in detecting fraudulent certificates	14	3.43	1.284
CMCV5	Verification processes are time-consuming	14	3.50	1.401
	Grand Mean		**3.34**	

The strong agreement on reliance on direct communication with issuing institutions (M = 3.57) reinforces this interpretation. Verification officers often must contact the originating institution sometimes waiting days or weeks for confirmation highlighting inefficiencies in the current system.

A notable concern emerges with the item on accuracy, respondents agreed that existing methods provide limited reliability in detecting fraudulent certificates (M = 3.43). This implies that officers who work with these systems daily are aware of their vulnerabilities. Manual processes are inherently prone to errors, vulnerable to forgery, and susceptible to manipulation.

Furthermore, respondents consistently agreed that the verification process is time consuming (M = 3.50). When considered together, these findings show that current methods are slow, insufficiently accurate, and largely

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

manual, even as of 2025. The grand mean of 3.34 indicates that these challenges are not isolated but are shared across diverse higher education institutions in Gombe State.

4.3 Challenges in Certificate Verification (CICV)

What challenges do verification authorities face in the existing certificate verification process?

The results for the CICV scale in Table 5, reveal even stronger agreement than those for the current verification methods, with a grand mean of 3.69. Verification challenges related to remote institutions (M = 3.71) emerged as one of the most prominent concerns. When certificates must be verified from institutions located far away sometimes in other states or even internationally. Officers depend heavily on external communication systems and institutional responsiveness, making the process slow and unpredictable.

Table 5: Descriptive Statistics for CICV Items

Item	Statement	N	Mean	SD
CICV1	Challenges exist with verifying certificates from remote institutions	14	3.71	0.994
CICV2	Cost of verification is a significant concern	14	3.64	1.008
CICV3	Current methods are vulnerable to fraud/tampering	14	3.43	1.222
CICV4	Delays occur in receiving responses from authorities	14	3.79	0.975
CICV5	Institution lacks adequate resources to improve verification	14	3.86	0.864
	Grand Mean		**3.69**	

Cost also remains a meaningful challenge (M = 3.64). Verification demands financial resources, whether for calls, courier services, or administrative labor. For institutions operating under constrained budgets, these expenses accumulate quickly, especially when handling large volumes of verification requests. Concerns about fraud vulnerability (M = 3.43) align with earlier findings. Respondents recognize that the current processes are susceptible to tampering, including forged stamps, altered documents, and counterfeit confirmation letters issues that undermine trust in manual verification systems.

Delays in receiving responses (M = 3.79) were rated particularly high. Verification officers often submit requests and then face prolonged waiting periods, which may be due to staff shortages, institutional bottlenecks, or communication gaps at the receiving end. These delays create a ripple effect, affecting students awaiting admission decisions and employers seeking timely recruitment confirmations.

The highest rated challenge was inadequate institutional resources (M = 3.86). Many institutions lack sufficient personnel, modern digital tools, updated verification systems, or training opportunities. This underscores a critical implication: while institutions are fully aware of existing verification problems, they often lack the financial and technical capacity to implement meaningful improvements independently.

4.4 Awareness of Blockchain Technology (AOBT)

What is the level of awareness and understanding of blockchain technology among verification authorities?

The findings for the AOBT scale present a notably positive outlook in Table 6. Overall awareness of blockchain technology among verification officers is relatively high, with a grand mean of 3.68. Respondents reported moderate familiarity with blockchain and its general applications (M = 3.57), likely influenced in part by the widespread public discourse surrounding cryptocurrencies such as Bitcoin and Ethereum, which has increased general exposure to the underlying technology.

Table 6: Descriptive Statistics for AOBT Items

Item	Statement	N	Mean	SD
AOBT1	I am familiar with blockchain technology and its applications	14	3.57	1.016
AOBT2	Blockchain is secure and tamper-proof for managing digital records	14	4.07	0.616
AOBT3	Blockchain can enhance transparency in certificate verification	14	4.21	0.579
AOBT4	Institution has explored/discussed blockchain for administrative use	14	3.00	0.784
AOBT5	Sufficient information is available about blockchain	14	3.57	1.158
	Grand Mean		**3.68**	

Beyond basic familiarity, respondents expressed strong agreement regarding blockchain's security and tamper resistant nature (M = 4.07). This indicates an understanding of one of blockchain's most critical attributes, once

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

data is recorded on the ledger, altering it becomes exceptionally difficult. Such awareness shows that officers not only know about blockchain but also grasp its core strengths relevant to certificate verification.

The highest rated item in this section and one of the highest across the entire dataset was the perceived ability of blockchain to enhance transparency in certificate verification (M = 4.21). Participants clearly recognize how blockchain could streamline verification by providing instant, verifiable, and transparent records, reducing dependence on traditional communication channels that can be slow or unreliable. Institutional exploration of blockchain (M = 3.00) scored right at the threshold for agreement. This suggests that while some institutions have begun considering blockchain based administrative solutions, widespread organizational engagement has yet to occur.

Respondents also reported having adequate access to information about blockchain (M = 3.57), which may reflect the increasing availability of online materials, media discussions, and academic publications. Taken together, the grand mean of 3.68 higher than the score for current verification methods (3.34) and nearly equal to the challenges score (3.69) suggests a favorable foundation for adoption. Verification officers are aware of the shortcomings of the existing system and possess a meaningful understanding of blockchain as a viable, potentially transformative solution.

4.6 Factors Influencing Adoption of Blockchain (FIAB)

What factors influence the potential adoption of blockchain-based certificate verification systems?

The FIAB scale produced the highest grand mean in the entire dataset (4.13), underscoring how strongly verification officers value the practical conditions that would shape successful blockchain adoption as shown in Table 7. These factors are not theoretical considerations, they represent the real-world requirements institutions must meet before they can meaningfully transition to blockchain based verification.

Table 7: Descriptive Statistics for FIAB Items

Item	Statement	N	Mean	SD
FIAB1	Cost of implementing blockchain is a significant adoption factor	14	3.93	0.829
FIAB2	Blockchain systems need to be user-friendly	14	4.07	0.730
FIAB3	Government policies/regulations will play a key role	14	3.86	0.864
FIAB4	Blockchain must integrate seamlessly with existing systems	14	4.29	0.469
FIAB5	Awareness and training are crucial for adoption	14	4.50	0.650
	Grand Mean		**4.13**	

Implementation cost (M = 3.93) emerged as a major concern. Given that institutions already struggle with resource shortages as shown earlier in CICV5 (M = 3.86) the financial demands of acquiring new hardware, software, and training present a significant barrier. For many institutions, cost is not merely an influence; it may be the determinant of whether adoption is feasible. User friendliness (M = 4.07) also scored highly. Verification officers rely on administrative systems daily and understand that the success of any new technology cents on usability. Regardless of blockchain's technical sophistication, if the system is complicated or disrupts existing workflows, adoption will falter. Officers are signaling the need for intuitive interfaces and logically structured processes that align with how verification is conducted in practice.

Government policies and regulatory support (M = 3.86) were also viewed as essential. In the Nigerian context, centralized guidance from bodies such as the Ministry of Education, NITDA, NUC, or NBTE could provide the standardization, coordination, and resource pooling necessary to support widespread implementation. Institutions are unlikely to adopt blockchain independently without such backing. System integration (M = 4.29) recorded one of the highest mean scores across all items. Institutions already operate multiple digital platforms student information systems, admissions portals, results management software. Blockchain solutions must integrate with these existing tools rather than function as isolated systems that require parallel workflows or complete infrastructural redesign.

The highest single score in the entire study was for awareness and training (M = 4.50). This finding is critical, even the most advanced blockchain solution will not succeed without adequate training for its users. Officers require not only operational training but also conceptual understanding how blockchain works, the value it offers, and how to troubleshoot issues. Training and awareness, therefore, are foundational to adoption rather than supplementary. Overall, the FIAB results convey a clear message, verification officers are open to blockchain adoption, but they emphasize the need to address concrete, practical requirements cost, ease of use, integration with existing systems, institutional capacity building, and strong regulatory support. These factors form the essential groundwork for any successful transition to blockchain based certificate verification.

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

5. Discussion

5.1 Current State: Manual Methods in a Digital Age

The results on existing verification practices (grand mean = 3.34) reveal that many higher education institutions are still operating in a transitional phase. Traditional manual procedures remain the norm (CMCV1: M = 3.64), while truly digital verification systems are still uncommon (CMCV2: M = 2.57). This mirrors the findings of Said et. al. [18] in Tanzania, who also observed that institutions continue to depend heavily on paper-based verification, even though its limitations are well known.

What stands out is the contrast between how far digital transformation has progressed in other areas of education such as online admissions, virtual classrooms, and electronic libraries and how credential verification continues to rely on outdated, paper driven processes. It is already 2025, yet confirming whether someone legitimately earned a degree still requires phone calls, emails, and the examination of physical documents.

The strong dependence on direct communication with issuing institutions (CMCV3: M = 3.57) reflects what Mohammad and Vargas [6] describe as "verification network dependency." In other words, an institution cannot verify a credential without contacting the original issuer. This naturally introduces delays and creates a single point of vulnerability. If the issuing institution has weak record management, responds slowly, or is no longer operational, verification becomes slow, complicated, or even impossible.

Even more troubling is the acknowledgment that the current process is not particularly accurate (CMCV4: M = 3.43). Verification officers those responsible for authenticating academic documents express only moderate confidence in their own systems. Given the sophisticated forgery techniques available today, their concern is understandable. Physical certificates can be replicated with alarming precision, and even verification calls may be hijacked or rerouted to collaborators involved in credential fraud.

5.2 The Challenge Landscape: Why Change Is Needed

The challenges associated with current verification practices received an even higher overall rating than the methods themselves (grand mean = 3.69), showing that these issues are not only recognized but are strongly felt across institutions. Difficulties with remote verification (CICV1: M = 3.71) highlight Nigeria's geographical and infrastructural limitations. When campuses are separated by long distances, unreliable road networks, unstable internet access, and limited courier services, verifying documents from afar becomes slow, frustrating, and sometimes impossible.

Concerns about cost (CICV2: M = 3.64) combined with a clear lack of adequate resources (CICV5: M = 3.86 the highest challenge score) create a difficult paradox. Current methods drain time and manpower, yet institutions still do not have the financial or technical capacity to move to more efficient digital systems. This is consistent with Mohammad and Vargas [6], who found that resource limitations were a major barrier to blockchain implementation even in Europe and Canada. If well-funded universities in developed countries struggle with these costs, it is easy to see why Nigerian institutions feel the strain even more sharply.

The problem of delayed responses (CICV4: M = 3.79) has widespread consequences. Students may miss admission deadlines, employers face hiring delays, and institutions cannot complete transfer or postgraduate admission processes. These are not minor inconveniences they lead to disrupted academic calendars, lost employment opportunities, and interrupted career progress.

The acknowledgment of vulnerability to fraud (CICV3: M = 3.43) also aligns with the concerns raised by Vikhankar et. al. [8] and Kim [9], who highlight how centralized verification systems are prone to manipulation. While those studies focus mainly on technical risks and system design, the findings here reveal another layer, the human side. Verification officers are fully aware that the tools they rely on are inadequate, and that awareness shapes their experiences and decision making every day.

5.3 Awareness: A Foundation for Change

The results on blockchain awareness (grand mean = 3.68) are notably positive. In many technology adoption studies, organizations struggle with basic understanding of new tools, but that is not the case here. Respondents demonstrate a meaningful grasp of blockchain's capabilities and relevance to verification work. The strong agreement that blockchain provides security and tamper proof records (AOBT2: M = 4.07) indicates that officers clearly understand its core strengths. Likewise, the high rating for transparency (AOBT3: M = 4.21 the highest in this category) suggests they can connect technological features with the practical needs of their daily tasks.

This awareness level surpasses what Mohammad and Vargas [6] found in their European and Canadian sample, where limited understanding posed a major barrier to adoption. The difference may stem from Nigeria's vibrant cryptocurrency ecosystem and the visibility of blockchain in African fintech innovations. Regardless of the reason, beginning from a position of relatively strong awareness increases the likelihood of successful adoption. The exact midpoint rating for institutional exploration (AOBT4 = 3.00) is also telling. It suggests some institutions have started preliminary conversations, but systematic investigation is still limited. Essentially, institutions appear to be at a transition stage moving from awareness toward active consideration.

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

5.4 Adoption Factors: The Implementation Reality

Adoption related factors recorded the highest overall mean across the entire survey (grand mean = 4.13), indicating strong consensus on what verification officers believe is necessary for successful implementation. Training and awareness (FIAB5: M = 4.50) emerged as the single highest score among all 20 items. This reinforces an established finding in the Technology Organization Environment (TOE) framework, technology adoption does not depend solely on technical capability. Individuals must feel confident using the system, understand its processes, and trust their ability to resolve issues as they arise. In other words, organizational capacity begins with people. The high value placed on system integration (FIAB4: M = 4.29) reflects practical institutional realities. Universities have already invested heavily in student information systems. A blockchain solution that requires replacing those systems is neither realistic nor efficient. Farabi et. al. [16] attempted to address this through the layered architecture of ShikkhaChain, but implementing such systems requires technical expertise that many institutions do not possess.

User friendliness (FIAB2: M = 4.07) is another essential requirement. Verification officers are administrative professionals, not blockchain specialists. Tools that are overly technical or require blockchain specific knowledge are unlikely to be adopted, no matter how advanced they are. The importance placed on government policy (FIAB3: M = 3.86) underscores the environmental component of the TOE framework. Fragmented, institution by institution adoption cannot solve cross institutional verification challenges. National coordination through policy, standards, and regulatory guidelines is needed to create interoperability and ensure legal recognition.

Finally, cost concerns (FIAB1: M = 3.93) echo earlier findings in the challenges section. Institutions that already struggle to fund their existing verification processes cannot absorb the financial burden of implementing sophisticated blockchain solutions. This creates a familiar dilemma, those most in need of improvement are least able to afford it.

5.5 Interpreting Patterns Through the TOE Framework

Applying the Technology Organization Environment framework helps clarify how these findings interact.

Technological Context: The current verification landscape is inadequate (CMCV grand mean = 3.34), susceptible to fraud (CICV3: M = 3.43), and lacking efficiency. At the same time, officers have a strong understanding of blockchain's advantages (AOBT2: M = 4.07; AOBT3: M = 4.21). The technological benefits are clear. However, integration concerns (FIAB4: M = 4.29) identify a key barrier, blockchain solutions must be compatible with existing systems.

Organizational Context: Resource limitations dominate this dimension (CICV5: M = 3.86; FIAB1: M = 3.93). Institutions acknowledge the need for improved systems but lack the financial and technical capacity to implement them independently. Training (FIAB5: M = 4.50) emerges as critical, emphasizing that organizational readiness depends heavily on human capacity. Although awareness levels are relatively strong (AOBT grand mean = 3.68), awareness alone does not equate to readiness.

Environmental Context: The importance of government policy (FIAB3: M = 3.86) and challenges associated with remote verification (CICV1: M = 3.71) highlight broader environmental constraints. Nigeria's digital infrastructure gaps, regulatory uncertainties, and absence of national credentialing standards all shape the pace and feasibility of adoption. The significant correlation between perceived challenges (CICV) and adoption requirements (FIAB) ($r = .558$, $p < .05$) provides further insight. Those who experience the problems most acutely also have clearer expectations about what successful adoption would require. In other words, officers are not merely identifying problems they are actively thinking through the conditions necessary for meaningful change.

6. Conclusion

This study set out to explore the barriers preventing higher education institutions in Gombe State, Nigeria, from adopting blockchain technology for certificate verification so as to have sustainable education. It focusses on verification officers the individuals who would ultimately operate such systems, allowed us to capture practical, experience-based insights often missing from broader adoption studies. The findings reveal a mix of promising opportunities and significant challenges. On the positive side, verification officers understand the weaknesses of their current processes. They recognize that manual verification is slow, prone to fraud, and expensive in both time and resources. They also demonstrate substantial awareness of blockchain technology and its potential to improve accuracy, transparency, and trust in verification procedures.

However, awareness alone is not enough to drive adoption. The realities facing institutions are serious: financial constraints remain a major barrier; integration with existing student information systems is non-negotiable, and the usability of any proposed blockchain solution will determine whether it is genuinely adopted. Most importantly, respondents consistently emphasized that training and capacity building are fundamental. No technology, regardless of its promise, will succeed without adequately trained personnel. For meaningful progress to occur, systemic support is needed. National bodies such as the Ministry of Education, NITDA, NUC, and

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

NBTE must move beyond general advocacy and provide concrete assistance in the form of funding pathways, regulatory frameworks, integration standards, and comprehensive training programs. While individual institutions can take steps to build internal readiness such as educating staff and evaluating workflows, they cannot overcome structural barriers alone.

Technology developers must also rethink their approach. Instead of prioritizing technical perfection, systems should be designed for ease of use, interoperability, and the realities of resource limited institutions with modest IT capacity. A sophisticated blockchain solution accomplishes little if it cannot integrate with existing data systems or requires specialized expertise institutions do not possess. Overall, this study contributes empirical evidence about adoption readiness from an underexamined but critical stakeholder group. With a validated instrument (Cronbach's $\alpha = 0.813$) and a TOE-based analysis, the study illustrates how technological, organizational, and environmental factors intersect to shape blockchain adoption pathways.

Ultimately, the findings indicate a pivotal moment, blockchain technology is now mature and well-understood, and credential fraud remains a pressing threat to academic integrity. Verification officers recognize both the problems and the potential solutions. What remains is bridging the implementation gap turning possibility into practical, sustainable reality for sustainable education.

6.1 Recommendations for Future Research

Future studies can expand and deepen these findings in several important directions:

Expanded Geographic Coverage: Conduct similar studies across multiple states in Nigeria or other African countries to determine whether these patterns persist in different contexts. Comparative research would help identify universal versus location-specific factors.

Longitudinal Studies: Track institutions over time as awareness grows or implementation efforts begin. This would help identify how attitudes change and which factors predict actual adoption.

Mixed-Methods Approaches: Integrate surveys with interviews or focus groups to capture deeper, more nuanced perspectives. Case studies of institutions attempting real world pilots could reveal challenges that quantitative surveys cannot detect.

Technical Readiness Assessments: Complement attitudinal data with evaluations of infrastructure, network capability, and IT staffing. This would allow researchers to map both human and technical readiness for adoption.

Intervention-Based Research: Design and test interventions training programs, policy frameworks, prototype deployments to identify practical strategies that increase adoption and overcome institutional barriers.

References

[1] Y. Xu, "Development of Blockchain-Based Academic Credential Verification System," *OAlib*, vol. 11, no. 09, pp. 1–20, 2024, doi: 10.4236/oalib.1112130.

[2] D. L. Silaghi and D. E. Popescu, "A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions," *Computers*, vol. 14, no. 4, p. 141, Apr. 2025, doi: 10.3390/computers14040141.

[3] O. S. Oluwaseyi and R. O. Akinyede, "Utilizing Blockchain Technology for University Certificate Verification System," 2024. [Online]. Available: www.ijais.org

[4] P. Gupta and P. Rai, "Can blockchain revolutionize educational practices? an in-depth analysis of applications and challenges," Dec. 01, 2025, *Elsevier Ltd.* doi: 10.1016/j.sftr.2025.101171.

[5] G. H. Harika, B. H. Harshitha, G. A. Akash, and N. Hema, "Academic Credential Verification System Using Blockchain," *Int. J. Innov. Sci. Res. Technol.*, vol. 9, no. 11, Nov. 2024, doi: 10.38124/ijisrt/IJISRT24NOV1597.

[6] A. Mohammad and S. Vargas, "Barriers Affecting Higher Education Institutions' Adoption of Blockchain Technology: A Qualitative Study," *Informatics*, vol. 9, no. 3, Sep. 2022, doi: 10.3390/informatics9030064.

[7] T. Ifeyemi, A. Oyedeji, and F. Adebiyi, "A BLOCKCHAIN-BASED DIGITAL EDUCATIONAL CERTIFICATE VERIFICATION SYSTEM," *Journal of Engineering and Technology for Industrial Applications*, vol. 10, no. 49, pp. 35–41, Oct. 2024, doi: 10.5935/jetia.v10i49.1145.

[8] N. Vikhankar, A. Andhare, I. Barne, A. Dhawale, and S. Kauchali, "E-Certificate Verification Using Blockchain," 2024, [Online]. Available: http://www.ijert.org

[9] S. K. Kim, "Blockchain Smart Contract to Prevent Forgery of Degree Certificates: Artificial Intelligence Consensus Algorithm," *Electronics (Switzerland)*, vol. 11, no. 14, Jul. 2022, doi: 10.3390/electronics11142112.

[10] A. Chaurasia and S. Gangwar, "Blockchain-based Authentication and Verification System for Academic Certificate using QR Code and Decentralized Applications," *Article in International Journal of Computer Applications*, vol. 186, no. 26, pp. 975–8887, Jun. 2024, doi: 10.5120/ijca2024923722.

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026

[11] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," Jun. 26, 2023, *Institute of Electrical and Electronics Engineers Inc.* doi: 10.1109/ACCESS.2023.3289598.

[12] R. Wiputra, A. Gunawan, Ervin, and A. Wijaksana, "Harnessing Blockchain and Generative AI to Prevent Certificate Forgery and Enhance Educational Integrity," in *2024 IEEE 12th Conference on Systems, Process & Control (ICSPC)*, IEEE, Dec. 2024, pp. 233–238. doi: 10.1109/ICSPC63060.2024.10862981.

[13] M. A. C. Quispe and A. Pacheco, "Blockchain ensuring academic integrity with a degree verification prototype," *Sci. Rep.*, vol. 15, no. 1, Dec. 2025, doi: 10.1038/s41598-025-93913-6.

[14] D. K. Kumar and M. D. Kumar, "Educational Certificate Verification System Using Blockchain," *Article in International Journal of Scientific & Technology Research*, 2023, [Online]. Available: www.ijstr.org

[15] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "DIAR: a blockchain-based system for generation and verification of academic diplomas," *Discover Applied Sciences*, vol. 6, no. 6, Jun. 2024, doi: 10.1007/s42452-024-05984-1.

[16] A. Farabi, I. Khandaker, J. Ahsan, I. K. Shanto, N. Jahan, and M. J. Khan, "ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh," Oct. 2025, [Online]. Available: http://arxiv.org/abs/2508.05334

[17] L. G. Tomatzky and M. Fleischer, *The processes of technological innovation*. Lexington MA: Lexington Books, 1990.

[18] S. H. Said, M. A. Dida, E. M. Kosia, and R. S. Sinde, "A Blockchain-based Conceptual Model to Address Educational Certificate Verification Challenges in Tanzania," *Engineering, Technology and Applied Science Research*, vol. 13, no. 5, pp. 11691–11704, Oct. 2023, doi: 10.48084/etasr.6170.

[19] J. W. Creswell, "Educational Research Planning Conducting and Evaluating Quantitative and Qualitative Research (4th ed.)," Lincoln, 2012.

"

Received: 09/02/2026; Revised: 09/03/2026; Accepted: 13/03/2026; Published: 23/03/2026