European Journal of Accounting, Auditing and Finance Research, 14(7),53-70, 2026

Print ISSN: 2053-4086(Print),

Online ISSN: 2053-4094(Online)

Website: https://www.eajournals.org/

Publication of the European Centre for Research Training and Development-UK

Integrating Artificial Intelligence and Blockchain for Real-Time Fraud Detection: Evidence from Financial Sector in Nigeria

Olabisi Bolarinwa Odewole [1]
Augustine University, Ilara-Epe, Lagos state, Nigeria.

Oluwafunmike Ayomide Craig-Olorunda [2]

Adeolu Moses Abolude [3]

Nofisat Azeez [4]

Femi Timothy Ogundeji [5]
Federal University of Technology, Ilaro, Ogun state, Nigeria

Abiodun Samuel Ige [6]

Fransisca Abimbola Oliyide[7]

[2,3,4,6,7] Crescent University, Abeokuta, Ogun state, Nigeria.

doi: https://doi.org/10.37745/ejaafr.2013/vol14n75370 Published September 07, 2026

Citation: Odewole O.B., Craig-Olorunda O.A., Abolude A.M., Azeez N., Ogundeji F.T., Ige A.S., Oliyide F.A. (2026) Integrating Artificial Intelligence and Blockchain for Real-Time Fraud Detection: Evidence from Financial Sector in Nigeria, *European Journal of Accounting, Auditing and Finance Research*, 14(7),53-70

Abstract:

This study determines how integrating artificial Intelligence affects blockchain for real-time fraud detection in financial Sector in Nigeria. Survey research design was adopted by the study. The study employed a well-structured questionnaire to the targeted sample size of 240 respondents: 10 per institution across 15 deposit money banks (150 respondents), 6 per institution across 10 fintech companies (60 respondents), and 6 per institution across 5 other supervised entities (30 respondents). However, only 210 respondents were received which represents the study's sample size. Descriptive statistics, correlation and multiple regressions were used to analyze the data collected. The Cronbach's alpha test was also conducted to test the reliability and validity of the data collected. The findings from the multiple regression results revealed that indicate that the capability of AI, adoption of blockchain, IT infrastructure and regulatory environment are each statistically significant and independent drivers of the variance of fraud detection effectiveness in the Nigerian financial sector. Furthermore, the interaction between artificial intelligence and blockchain was not statistically significant ($p = .259$) notably, while the impact of IT infrastructure is significant ($\beta = .252$). The study concluded that each of the three factors of Artificial Intelligence capability, Blockchain adoption and IT infrastructure quality, and the regulatory environment significantly and independently improves the effectiveness of fraud detection in Nigeria's financial sector.

The non-significant of artificial intelligence and blockchain interaction, however, suggests that, as yet, the two technologies are complementary and not mutually reinforcing each other. The study recommended among others that financial institutions should continue to invest in both AI-based analytics and blockchain infrastructure, as each independently and significantly improves fraud detection effectiveness, rather than deferring one in favour of the other.

Keywords: *Artificial Intelligence, Blockchain adoption, Fincncial sector, IT infrastructure and Regulatory environment.*

INTRODUCTION

Digitalisation of financial services has revolutionised the way financial institutions operate, moving beyond simple digitalisation channel to data driven intelligence (Chen, 2025; Karanina & Skopin, 2025; Kolisnyk & Skiiarov, 2025; Lam, 2024), however, these opportunities introduced new risk areas for fraudulent activities necessitating continuous development in detection and prevention mechanism (Aina, et al., 2024; Ilori, Nwosu & Naiho, 2024; Munira, 2025; Yang, Shukur & Sahran, 2026). Access to financial data and information had gone beyond mobile banking, Internet payment systems, and real-time transfer systems, to opening doors to increased attack from fraudsters through sophisticated schemes like cyber fraud, identity theft and transaction manipulation (Guo & Lui, 2025; Shofi et al., 2026; Supriadi, 2024).

Financial fraud continues at levels which pose a material risk to the stability of banks and public confidence in the banking system in Nigeria despite regulatory framework in place such as CBN's Risk Based Cybersecurity Framework, the NDIC reported high volume of fraud losses within the Deposit Money Banks sector as evidenced in the reports of the Nigeria Deposit Insurance Corporation (NDIC, 2022) and Nigeria Interbank Settlement System (NIBSS, 2023) where a constant rise in electronic fraud cases evidenced the growing severity of fraud challenge with the uptake of digital technology.

The underlying reason is that organizations still don't have a proactive strategy to detect fraud, centralised records are weak in terms of data integrity, no real-time monitoring, inefficient traditional fraud detection methods, poor data integrity and transparency and fraudsters are getting smarter and smarter, as well as the lack of adoption of a unified system of AI and blockchain in the anti-fraud processes of organisations. Bello & Olufemi (2024) stated that effective fraud prevention strategies enhance the security of financial system, economic activity stability and consumer trust. Akintoye et al. (2022) noted that increased investment in cybersecurity has a positive effect on financial innovation within Nigerian DMBs, yet the technological infrastructure to support the implementation of sophisticated fraud analytics is still not matured.

According to Aina et al., (2024) and Akinniyi (2023) financial fraud poses threat and high risk to the stability and integrity of the world financial systems, bringing about continuous developments of advanced measures to detect, prevent and curb the menace that the traditional fraud detection systems cannot curtail.

This is because it relied on rule-based mechanisms and lack the speed, volume, and adaptability needed to handle today's demands for fraud (Ikhsan et al., 2022, Chirumamilla, 2025; Sujana & Laela, 2025). It only mark transactions as fraud when such transaction gets to a certain threshold, creating serious blind spots for fraud to go on without detection, thereby justifying the urgent need for innovative systems that can proffer solutions in real-time (Bello, Idemudia & Iyelola, 2024).

Even though the AI systems, which are based on machine learning and deep learning, are able to analyze transactional data in real-time, preserve the integrity of accounting data, and minimize financial manipulation by doing so, they still have lower usage in the Nigerian financial sector than their potential (Yanjun, 2025; Chen, 2025, Guo & Lui, 2025; Da Silva Robusti, et al., 2025; Zulhelmi et al., 2023). Outside the technological perspective, previous studies stated that a successful implementation of AI and blockchain, demand some other factors that needed to be considered particularly in an accounting information system environment. These factors include IT infrastructural readiness and adaptive regulations and supervisory frameworks (Sidabutar et al., 2026). There is limited empirical evidence on how these technologies influence fraud detection effectiveness in Nigeria. Based on this empirical review. this study therefore seeks to examine the impact of integrating AI and Blockchain on real-time fraud detection in Nigeria’s financial sector.

LITERATURE REVIEW AND HYPOTHESIS DEVELOPMENT

Artificial Intelligence and Fraud Detection

Artificial Intelligence is the term for computer systems that are able to learn, reason, recognize patterns, make decisions and perform other tasks that normally require intelligent human beings. AI's role in the financial industry has been particularly significant in fraud detection, where banks and other financial institutions use AI to continuously learn from past and present transactions, detecting unusual spending patterns, suspicious transactions, and new fraud methods more effectively than ever before (Devan, Prakash & Jangoan, 2023; Shoetan & Familoni, 2024; Suyono et al 2025; Taha & Malebary, 2020).

Unlike conventional systems that rely on predefined rules, AI-based systems adapt to new fraud patterns through continuous learning and can analyse lots of data at the same time, at an unimaginable speed, bringing out patterns that are hidden that traditional system cannot detect (Bello & Olufemi, 2024; Supriadi, 2024). Supervised and unsupervised machine learning techniques are becoming more popular in the financial sector for identity theft detection, credit card fraud, money laundering, cyber fraud and account takeover attacks.

Empirical studies show differences and inconsistencies in the effectiveness of AI, with some studies reporting high level accuracy in detection, and others stating that its effectiveness depends on data quality, the competency of human resources and the complexity of algorithms (Kethra, 2024; Zayed et al., 2024; Arham, 2025; Suyono et al., 2025). AI can help financial institutions identify fraudulent transactions more efficiently, as it can detect complex patterns that traditional systems are unable to. As a result, the effectiveness of fraud detection is anticipated to rise with the increase in the use of AI. We therefore, hypothesized that:

Ho1: There is no significant difference in the effectiveness of fraud detection in the financial sector due to the use of artificial intelligence.

Blockchain Technology and Fraud Detection

Blockchain technology is a decentralized digital ledger that documents transactions in chronological sequence through cryptography methods. Once the information is recorded on the blockchain, it becomes very hard to tamper with, hence improving transparency, accountability, and data integrity. The findings from the research by Thommandru and Chakka (2023) regarding the use of blockchain technology for anti-money laundering compliance show that the characteristics of blockchain greatly enhanced the audit trail's completeness and reliability, solving one of the oldest problems in fraud management that involves the alteration of transactional data prior to investigation. According to Chowdhury et al. (2023), the blockchain technology suffers from regulatory issues as well as compatibility issues when integrated with conventional banking operations, meaning there needs to be regulatory framework guiding the process. Issues with scalability as well as the heavy computational requirements of some consensus algorithms limit the implementation of the blockchain at the scale of operations of large Nigerian banks.

In financial organizations, blockchain will enhance fraud prevention through immutable transaction history, secure information sharing, and less room for transaction (Kernani, et al., 2024; Taher & Ahmed, 2024). Notwithstanding all the benefits, there exist some problems in relation to scalability, energy consumption, interoperability, lack of regulatory clarity, and costliness of the technology implementation. However, despite the problems, the technology is gaining popularity as an effective way of enhancing financial security. Transparency and immutability offered by the blockchain technology create fewer chances for fraud and improve financial transaction security (Chen, et al., 2018; Tian, 2017; Zykind et al 2015). Therefore, increased usage of the technology will lead to better fraud detection effectiveness. We consequently proposed the following hypothesis:

Ho2: Blockchain technology does not have any impact on fraud detection effectiveness in the financial industry.

Integration of Artificial Intelligence and Blockchain

Though the individual use of Artificial Intelligence and Blockchain has advantages in the area of fraud management, their combination yields even more value than each one individually (Shofi et al., 2025). The combination uses the trusted, secure and open data by means of Blockchain and the analysis of such trusted sources through Artificial Intelligence for the detection of suspicious actions.

The combination leads to the enhancement of fraud detection, continuous transaction monitoring, automation of compliance, automatic fraud alerts, improvement of identity and access controls, predictability, integrity of data, immediate threat reaction and intelligent decision-making (Lui, 2023; Shofi, et al., 2025; Tampubolon et al., 2025; Feng, 2019). AI is positively impacted by the data environment that blockchain creates and blockchain is positively impacted by the analytical abilities of AI, which gives the whole fraud detection system (Zhao & Yermack, 2024; Nguyen, Tran & Le, 2023).

Research explicitly analyzing the integration of these two technologies found that there are many positive impacts on fraud detection, accuracy, operational efficiency, cyber-resilience, and enhanced accounting data integrity (Kumar & Yumuna, 2025; Ketha, 2024).

Aslam et al. (2022) showed empirical proof that AI is superior to conventional fraud classification for insurance data. Taher et al. (2024) show that applying ensemble AI in analyzing blockchain data enhances not only accuracy but also explainability. Bello et al. (2024) synthesized both conceptual and empirical knowledge in order to formulate the multi-layered AI and blockchain fraud detection framework. As regards the Nigerian case, Kanu et al. (2023) and Akintoye et al. (2022) analyzed the fraud environment and the process of technological adoption, respectively, but none of them dealt with the integration of AI and blockchain. The synergy between both technologies is increasingly viewed as the future of intelligent financial security systems as their integration creates complementary capabilities that enhance real-time fraud detection beyond what either technology can achieve independently (Ashfaq et al. 2022; Taher et al. 2024). We therefore hypothesized that:

Ho_3: The integration of Artificial Intelligence and Blockchain has no significant effect on real-time fraud detection in the financial sector.

Moderating role of IT Infrastructure and Regulatory Environment

Successful implementation of AI and blockchain depends largely on the availability of adequate technological infrastructure and supportive regulatory frameworks, since robust IT infrastructure makes available the necessary interfaces in the form of computational capacity, secure networks, cloud services, data management systems, agility, security required for AI and blockchain applications (Chen, 2025).

Similarly, effective adaptive regulations and supervisory frameworks encourage technology adoption by establishing standards for cybersecurity, data privacy, digital identity management, and compliance while weak infrastructure and regulatory uncertainty may reduce the effectiveness of these technologies even when organisations invest heavily in them (Chen, 2025; Chukwu, 2025; Kolisnyk & Skliarov, 2025; Kon & Lu, 2025; Natali, et al 2026; Wang et al., 2026).

Organisations operating within strong technological regulatory environments are expected to derive greater fraud detection benefits from AI and blockchain integration than organisations with weak infrastructure and regulatory support. We hereby hypothesized that:

H04: IT infrastructure and regulatory environment do not significantly moderate the relationship between AI-blockchain integration and real-time fraud detection in the financial sector.

METHODOLOGY

The study adopts a descriptive survey research design with an explanatory approach. The population for the study comprises of employees of selected financial institutions in Nigeria, including commercial banks, fintech companies and other licensed financial service providers. The target respondents include staff working in information technology, internal audit, risk management, compliance, cybersecurity, fraud investigation and operations departments because they possess relevant knowledge of fraud detection systems. 26 licensed deposit money banks, approximately 40 licensed fintech companies, and related supervised institutions form the sample size for the study and this was achieved using a stratified purposive sampling technique.

The population is stratified by institution type to ensure representation across contexts in which AI and blockchain adoption may differ. Within each stratum, purposive sampling selects respondents directly involved in or knowledgeable about fraud detection and technology. The target sample is 240 respondents: 10 per institution across 15 deposit money banks (150 respondents), 6 per institution across 10 fintech companies (60 respondents), and 6 per institution across 5 other supervised entities (30 respondents). Structured questionnaire was used to elicit relevant information from the chosen respondents. A face and content validity was done while the cronbach's Alpha coefficient of 0.85 was achieved and the data was analysed using SPSS

Measurement of Variables

Variable	Proxy/Dimension
Artificial Intelligence	AI adoption, Machine learning capability, predictive analytics
Blockchain Technology	Transparency immutability, decentralization, smart contracts
Fraud Detection Effectiveness	Detection speed, detection accuracy, fraud prevention capability
IT infrastructure	Network capability digital infrastructure, computing resources
Regulatory Environment	Compliance requirements, legal framework, regulatory support

The functional relationship is expressed as:
$FDE = f(AI, BC, ITI, REG)$
$FDE = \beta_0 + \beta_1 AI + \beta_2 BC + \beta_3 (AI \times BC) + \beta_4 ITI + \beta_5 REG + \mu$
Where:
FDE = Fraud detection
AI = Artificial Intelligence
BC = Blockchain Technology
AI x BC = Interaction effect between Artificial intelligence and blockchain
ITI = Information Technology Infrastructure
REG = Regulatory Environment
β_0 = Constant
$\beta_1 - \beta_4$ = Regression coefficients
μ = Error

Theoretical Framework

Technology Acceptance Model (TAM)

This theory was propounded by Fred D. Davis (1989) to give explanation to the reason behind human adoption of new technologies. Based on the model, technology acceptance is mainly influenced by two constructs: perceived usefulness (PU) and perceived ease of use (PEOU) to understand financial, functional and attitudinal basis for decisions. Perceived usefulness is the extent to which the individual believes the use of the specific technology would improve job performance, and perceived ease of use is the extent to which the person believes the technology would be easy to use (Venkatesh et al.,2003; Davis, 1989).

Despite its ability to users' privacy (Bonneau, et al., 2015), financial institutions are more likely to adopt AI and Blockchain technologies if employees and management view that these technologies would increase the likelihood of detecting fraud accurately, and decrease the amount of financial loss, operational efficiency and security benefits (Dhanda, Singh & Jindal, 2020). The use of AI-driven fraud detection systems can quickly flag suspicious transactions, and blockchain offers the advantage of a transparent and immutable record of transactions, enhancing trust in fraud prevention tools.

TAM is relevant because it provides a theoretical foundation for understanding the behavioral and organizational dynamics that can impact the adoption of AI and blockchain technology in finance. It offers an insight into the rationale behind and opposition to these innovations by financial institutions (Venkatesh, et al., 2003). The theory has been criticized, though, for focusing solely on user perception and neglecting to consider the role of organizational, environmental, regulatory and technological factors that affect technology adoption. Thus, a number of researchers try to incorporate additional theories in order to include these wider influences in TAM (Bryan & Zuva, 2021; Ali et al., 2022).

Diffusion of Innovation (DOI)Theory

Everett M. Rogers (1962) put forward the theory. The theory has been developed to help understand the process of the spread of new technologies, products, or innovations within organizations and society over time. Rogers' identified five main attributes which affect the rate of innovation adoption: relative advantage, compatibility, complexity, trialability and observability (Rogers, 1995). The theory is that the more that financial institutions believe that AI and Blockchain solutions provide better benefits than conventional fraud detection solutions, the more likely they are to adopt these technologies; the more they can integrate AI and Blockchain technologies with traditional solutions and see the benefits in fraud prevention, the more they will adopt them (Carter & Belanger, 2005; Lean et al., 2009).

The theory also proposes that the rate of adoption is related to organisational readiness, management support, technological infrastructure and communication channels. With growing awareness and the establishment of successful use-cases in the financial sector, it is likely more financial institutions will implement integrated AI-Blockchain fraud detection systems.

The diffusion innovation theory is suitable since it can explain why the innovative fraud detection technology is diffused in financial institutions and also the factors that facilitate or obstruct the diffusion.

Fraud Triangle Theory

Donald R. Cressey (1953) developed this theory. The theory is that fraud is a result of three factors: pressure, opportunity and rationalization.

Pressure is any financial or personal influence that encourages people to defraud others. Fraud opportunity occurs when internal control or monitoring is weak or compromised. Rationalization is when people rationalize unethical action (Cressy, 1953).

By combining Artificial Intelligence and Blockchain, the opportunity arm of the fraud triangle can be enhanced with additional internal controls, enhanced transaction monitoring, more transparency and real-time fraud detection. AI can detect odd transaction activity before it does any harm, and blockchain technology provides an unchangeable record that is hard to manipulate, minimizing fraud opportunities (Al-Hchaimi, Khalifa, & El-Shafai, 2025).

This theory is relevant to the study as they are concerned with technologies that aim to minimize the possibility of frauds in the financial institution.

The study is based on the Technology Acceptance Model (TAM), since it directly addresses the factors that affect the organizational acceptance and use of these technologies. The Diffusion of Innovation theory will help to understand the process of spreading these innovations throughout the financial sector, and the fraud triangle theory will serve as a basis to explain the reduction of opportunities for fraud with the new technological controls. Collectively, these theories provide a comprehensive framework for examining the relationship between AI, Blockchain and real-time fraud detection. Together, this lower perceived opportunity, the most consistently targeted in Nigerian banking fraud according to Kanu et al. (2023).

FINDINGS AND DISCUSSIONS

Response Rate and Respondent Profile

Of the 240 copies of the questionnaire distributed across the sampled institutions, 210 were correctly completed and returned, representing a response rate of 87.5%, while 30 copies (12.5%) were not retrieved on account of respondent unavailability or incomplete entries. A response rate above 70% is generally regarded as adequate for survey-based organisational research; the achieved rate therefore supports the reliability of the analysis that follows.

Table 4.1: Questionnaire Administration

S/N	Questionnaire Status	Frequency	Percentage (%)
1	Retrieved and usable	210	87.5
2	Not retrieved / discarded	30	12.5
	Total	240	100.0

Source: Field Survey, 2026.

Table 4.2 summarises the profile of the 210 respondents by gender, age, institution type, years of working experience, qualification and department. Male respondents formed the larger share (72.4%), and commercial bank staff dominated the sample (57.6%), consistent with their weight in the sampling frame. Most respondents (86.7%) had five or more years of working experience, and a majority (56.2%) held a first degree (HND/B.Sc.), with the remainder holding a Master's degree, professional certification or PhD, indicating that the sample was well positioned to provide informed assessments of institutional AI and blockchain practice.

Table 4.2: Respondent Profile (N = 210)

Category	Classification	Frequency	Percentage (%)
Gender	Male	152	72.4
	Female	58	27.6
Age	Below 25 years	28	13.3
	25 - 34	87	41.4
	35 - 44	64	30.5
	45 - 54	23	11.0
	55 years and above	8	3.8
Type of Institution	Commercial Bank	121	57.6
	Fintech Company	53	25.2
	Microfinance Bank	14	6.7
	Insurance Company	10	4.8
	Others	12	5.7
Years of Working Experience	Less than 5 years	28	13.3
	5 - 10 years	79	37.6
	11 - 15 years	68	32.4
	Above 15 years	35	16.7
Highest Educational Qualification	HND	40	19.0
	B.Sc.	78	37.1
	Master's Degree	62	29.5
	Professional Qualification	24	11.4
	PhD	6	2.9
Department	Risk Management	50	23.8
	Compliance	39	18.6
	Information Technology	46	21.9
	Internal Audit	33	15.7

	Operations	30	14.3
	Other	12	5.7

Source: Field Survey, 2026.

Reliability of Research Instrument

The internal consistency was re-assessed using Cronbach's Alpha, with a minimum acceptable threshold of 0.70 (Hair et al., 2019). As shown in Table 4.3, all five constructs exceeded this threshold, and the overall 25-item instrument returned a coefficient of 0.871, confirming that the instrument was reliable for the purpose of this study.

Table 4.3: Reliability Statistics

Construct	No. of Items	Cronbach's Alpha	Remark
Artificial Intelligence Capability (AI)	5	0.761	Reliable
Blockchain Technology Adoption (BC)	5	0.741	Reliable
Fraud Detection Effectiveness (FDE)	5	0.732	Reliable
IT Infrastructure Quality (ITI)	5	0.762	Reliable
Regulatory Environment (REG)	5	0.769	Reliable
Overall Instrument	25	0.871	Reliable

Source: Field Survey, 2026.

Descriptive Analysis of Study Variables

Table 4.4 presents the descriptive statistics for the twenty-five questionnaire items, all measured on a five-point Likert scale. The item means under the instrument cluster tightly around the scale midpoint, ranging from 2.88 ("AI reduces false fraud alerts") to 3.14 ("adequate digital infrastructure for AI and blockchain"). At the construct level, blockchain adoption recorded the highest composite mean (3.06), followed closely by fraud detection effectiveness (3.04), IT infrastructure (3.03) and regulatory environment (3.02), while AI capability recorded the lowest composite mean (2.96). This pattern indicates a broadly moderate, neutral-leaning perception across all five constructs, with no single dimension standing out as markedly more embedded in institutional practice than the others.

Table 4.4: Descriptive Statistics of Study Constructs (N = 210)

No.	Item	Mean	Std. Dev.
1	AI systems detect suspicious transactions quickly	3.04	1.02
2	AI improves the accuracy of fraud detection	2.96	1.08
3	Machine learning helps identify new fraud patterns	3.00	1.07
4	AI reduces false fraud alerts	2.88	1.13
5	AI enhances decision-making in fraud investigations	2.91	1.00
6	Blockchain improves transaction transparency	2.94	1.05
7	Blockchain prevents unauthorized alteration of records	3.08	1.05
8	Blockchain enhances transaction security	3.10	1.06

9	Blockchain improves traceability of financial transactions	3.09	1.09
10	Blockchain minimizes opportunities for financial fraud	3.11	1.03
11	Fraudulent transactions are detected promptly	3.08	0.98
12	Fraud detection accuracy has improved	2.99	0.94
13	Financial losses resulting from fraud have reduced	3.11	0.95
14	Fraud investigation has become more sufficient	3.00	1.10
15	Overall fraud prevention has improved	3.02	1.05
16	Institution has adequate digital infrastructure for AI/blockchain	3.14	1.07
17	Reliable internet and computing resources support fraud detection	2.99	1.01
18	Employees receive adequate technical support	3.04	1.02
19	Existing IT systems integrate well with AI and blockchain	3.08	1.08
20	Institution regularly upgrades its digital infrastructure	2.91	1.06
21	Existing regulations support AI adoption in fraud detection	3.05	0.97
22	Regulatory guidelines encourage blockchain implementation	3.06	1.07
23	Compliance requirements improve fraud prevention	3.10	1.01
24	Regulators provide guidance on emerging technologies	2.98	1.03
25	The legal framework supports innovation in fraud detection	2.92	1.06

Source: Field Survey, 2026.

Regression Analysis and Test of Hypotheses

To test the study's hypotheses, item scores were averaged into composite construct scores for AI, BC, FDE, ITI and REG, and an interaction term (AI x BC) was computed as the product of the mean-centred AI and BC scores. Multiple regression was estimated using the model: $FDE = \beta 0 + \beta 1AI + \beta 2BC + \beta 3(AI \times BC) + \beta 4ITI + \beta 5REG + \mu$. Variance Inflation Factors for all five predictors ranged from 1.04 to 1.30, well below the threshold of 10, confirming that multicollinearity did not distort the estimates.

Table 4.5: Regression Model Summary

R	R Square	Adjusted R Square	Std. Error of Estimate	F	df1	df2	Sig.
.808[a]	.653	.645	2.087	76.907	5	204	.000

Source: Field Survey, 2026.

The model returned an R Square of 0.653, indicating that AI capability, blockchain adoption, their interaction, IT infrastructure and the regulatory environment jointly explain 65.3% of the variance in fraud detection effectiveness. The Adjusted R Square of 0.645 confirms the model's stability after accounting for the number of predictors.

Table 4.6: ANOVA

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	1674.076	5	334.815	76.907	.000[b]
Residual	888.119	204	4.354		
Total	2562.195	209			

Source: Field Survey, 2026.

The ANOVA result ($F = 76.907$, $p = .000$) confirms that the overall regression model is statistically significant at the 5% level, indicating that the combined predictors meaningfully explain fraud detection effectiveness.

Table 4.7: Regression Coefficients

Variable	B	Std. Error	Beta	t	Sig.	Decision
(Constant)	-3.531	2.157		-1.637	.103	
AI Capability	.586	.152	.635	3.862	.000	Reject $H_0$1
Blockchain Adoption	.354	.116	.408	3.055	.003	Reject $H_0$2
AI x BC (Interaction)	-.009	.008	-.277	-1.131	.259	Fail to Reject $H_0$3
IT Infrastructure	.235	.043	.252	5.438	.000	Reject $H_0$4
Regulatory Environment	.166	.042	.176	3.938	.000	Reject $H_0$5

Source: Field Survey, 2026. Dependent Variable: Fraud Detection Effectiveness.

$H_0$1: AI capability has no significant effect on fraud detection effectiveness. This is rejected ($\beta = .635$, $p = .000$); AI capability is the single strongest predictor in the model, consistent with Aslam et al. (2022) and Xu et al. (2024) on the predictive strength of AI-driven analytics.

$H_0$2: Blockchain adoption has no significant effect on fraud detection effectiveness. This is rejected ($\beta = .408$, $p = .003$), corroborating Thommandru and Chakka (2023) on the contribution of tamper-proof ledgers to fraud control.

$H_0$3: The integration of AI and blockchain has no significant effect on fraud detection effectiveness. This hypothesis is not rejected ($\beta = -.277$, $p = .259$). AI and blockchain contribute to fraud detection effectiveness as independently valuable technologies rather than as statistically reinforcing ones.

$H_0$4: IT infrastructure has no significant effect on fraud detection effectiveness. This is rejected ($\beta = .252$, $p = .000$), confirming that infrastructure adequacy meaningfully strengthens detection outcomes, in line with Akintoye et al. (2022).

$H_0$5: The regulatory environment has no significant effect on fraud detection effectiveness. This is rejected ($\beta = .176$, $p = .000$). The regulatory environment now shows a significant positive effect, suggesting that clearer CBN and NDIC guidance is directly associated with improved detection outcomes rather than functioning purely as a background enabling condition.

DISCUSSION OF FINDINGS

The findings indicate that the capability of AI, adoption of blockchain, IT infrastructure and regulatory environment are each statistically significant and independent drivers of the variance of fraud detection effectiveness in the Nigerian financial sector, accounting for 65.3% of the variance. Though the descriptive mean value (2.96) of AI capability was the lowest among the four substantive constructs, this finding was consistent with Thilagavathi et al. (2024) and Sinha et al. (2022), indicating that institutions are more aware of the significance of AI than its current level of usage.

The substantive constructs showed comparatively stable, but still modest, institutional uptake, with the adoption of Blockchain being the most significant, with a descriptive mean of 3.06, and the highest β value of .408. The interaction between AI and BC was not statistically significant ($p = .259$) notably. At the current rate of adoption, AI and blockchain seem to be contributing to institutions' goals in parallel, not synergistically; an AI system has been able to bring about change in a particular area without, as yet, seeing an additional measurable benefit when combined with blockchain.

The impact of IT infrastructure is significant ($\beta = .252$), thus reinforcing Akintoye et al. (2022) and emphasizing that technology approach in the banking industry in Nigeria is inseparable from investment in IT infrastructure. The influence of regulatory environment, however, is not simply a background enabling condition, as evidenced by the positive influence of CBN and NDIC guidance on the outcome of the fraud-detection process ($\beta = .176$), particularly from the Diffusion of Innovation approach that suggests that a better defined regulatory environment fosters not only adoption, but actual performance.

CONCLUSION AND POLICY RECOMMENDATIONS

The study concluded that each of the three factors of Artificial Intelligence capability, Blockchain adoption and IT infrastructure quality, and the regulatory environment significantly and independently improves the effectiveness of fraud detection in Nigeria's financial sector, with a combined effect of explaining 65.3% of the variance in the outcomes of the fraud detection in the financial sector. The non-significant AI x BC interaction, however, suggests that, as yet, the two technologies are complementary and not mutually reinforcing each other. This adds nuance to the theoretical position that follows from the Technology Acceptance Model and the Fraud Triangle and Diffusion of Innovation Theory: While combined technology adoption may help reduce detection gaps of existing, siloed fraud management systems, achieving a tangible, quantifiable value-add of AI and blockchain will likely take more deliberate technical integration than co-adoption offers at this time. Based on these findings, the following policy recommendations are made:

i. Financial institutions should continue to invest in both AI-based analytics and blockchain infrastructure, as each independently and significantly improves fraud detection effectiveness, rather than deferring one in favour of the other.

ii. Because the AI x BC interaction was not statistically significant, institutions should not assume automatic synergy from co-adoption; deliberate technical integration — such as feeding blockchain-verified data directly into AI fraud models — is needed to realise compounding benefits.
iii. Institutions should continue investing in IT infrastructure, including processing capacity, network bandwidth and core-system integration, given its confirmed role in strengthening detection performance.
iv. The Central Bank of Nigeria and the Nigeria Deposit Insurance Corporation should sustain and expand clear, technology-specific guidance on AI and blockchain deployment in fraud management, given the confirmed positive effect of the regulatory environment on detection outcomes.
v. Institutions should establish continuous AI model retraining and blockchain data-audit routines, and periodically re-test the AI-blockchain interaction as adoption deepens, since a non-significant interaction today does not preclude synergy emerging as integration matures.

REFERENCES

Aina, L. O., Agboola, T. O., Adegede, J., Omonule, T. G., & Oyeniran, O. C. (2024). A review of mobile networks: Evolution from 5G to 6G. International Institute for Science, Technology and Education (IISTE), 15(1).

Akinniyi, J. S. (2023). Enhancing financial fraud detection with AI and cloud-based big data analytics: Security implications. World Journal of Advanced Engineering Technology and Sciences, 9(2), 417–434. https://doi.org/10.30574/wjaets.2023.9.2.0208

Akintoye, R., Ogunode, O., Ajayi, M., & Joshua, A. A. (2022). Cyber security and financial innovation of selected deposit money banks in Nigeria. Universal Journal of Accounting and Finance, 10(3), 643–652. https://doi.org/10.13189/ujaf.2022.100302

Al-Hchaimi, A. A. J., Khalifa, M. A., & El-Shafai, W. (2025). Explainable AI with imbalanced learning strategies for blockchain transaction fraud detection. Engineering Reports, 8, e70545, 1–25. https://doi.org/10.1002/eng2.70545

Ali, O., Murray, P. A., Muhammed, S., Dwivedi, Y., & Rahiti, S. (2022). Evaluating organizational level IT innovation adoption factors among global firms. Journal of Innovation & Knowledge, 7(3). https://doi.org/10.1016/j.jok.2022.100213

Arham, M. W. (2025). Transforming auditing through AI and blockchain: A comprehensive study on adoption, implementation and impact in financial audits, 15(2), 225–241. https://doi.org/10.4236/ajibm.2025.152011

Ashfaq, T., Khalid, R., Yahaya, A. S., Aslam, S., Azar, A. T., Alsafari, S., & Hameed, I. A. (2022). A machine learning and blockchain-based efficient fraud detection mechanism. Sensors, 22(19), 7162. https://doi.org/10.3390/s22197162

Aslam, F., Hunjra, A. I., Ftiti, Z., Louhichi, W., & Shams, T. (2022). Insurance fraud detection: Evidence from artificial intelligence and machine learning. Research in International Business and Finance, 62, 101744. https://www.sciencedirect.com/science/article/am/pii/S0275531922001325

Bello, H. O., Idemudia, C., & Iyelolu, T. V. (2024). Integrating machine learning and blockchain: Conceptual frameworks for real-time fraud detection and prevention. World Journal of Advanced Research and Reviews, 23(1), 056–068. https://doi.org/10.30574/wjarr.2024.23.1.1985

Bello, O. A., & Olufemi, K. (2024). Artificial intelligence in fraud prevention: Exploring techniques and applications, challenges and opportunities. Computer Science and IT Research Journal, 5(6), 1505–1520. https://doi.org/10.51594/csitrj.v516.1252

Bonneau, J. A., Miller, J., Clark, A., Narayanan, J. A. K., & Felten, E. W. (2015). SoK: Research perspectives and challenges for bitcoin and cryptocurrencies. In 2015 IEEE Symposium on Security and Privacy (pp. 104–121). San Jose, CA, USA.

Bryan, J. D., & Zuva, T. (2021). A review on TAM and TOE framework progression and how these models integrate. Advances in Science, Technology and Engineering Systems Journal, 6(3), 137–145. https://doi.org/10.25046/aj060316

Carter, L., & Belanger, F. (2005). The utilization of e-government services: Citizen trust, innovation and acceptance factors. Information Systems Journal, 15(1), 5–25.

Chen, J. (2025). Research on AI-based smart finance innovation models and their impact mechanisms. Advances in Economics, Management and Research, 14(1), 711–715. https://doi.org/10.56028/aemr.14.1.711.2025

Chen, Y., Ding, S., Xu, Z., Zheng, H., & Yang, S. (2018). Blockchain-based medical records secure storage and medical service framework. Journal of Medical Systems, 43(1), 5. https://doi.org/10.1007/s10916-018-1121-4

Chirumamilla, K. R. (2025). Next gen real time fraud detection with cloud scale stream processing. International Journal of Research and Applied Innovations, 8(1), 11675–11689.

Chowdhury, E. K., Stasi, A., & Pellegrino, A. (2023). Blockchain technology in financial accounting: Emerging regulatory issues. Review of Economics and Finance, 21, 862–868. https://doi.org/10.55365/1923.x2023.21.94

Chukwu, B. N. (2025). FinTech innovation and digital security: AI applications for fraud mitigation and regulatory compliance in US financial markets. International Journal of Science and Research Archive, 17(1), 1031–1031. https://doi.org/10.30574/ijsra.2025.17.1.2916

Cressy, D. R. (1953). Other people's money. Montclair, Glencoe, Free Press.

Da Silva Robusti, C., Avelar, A. B. A., Farina, M. C., & Gananca, C. A. (2025). Blockchain and smart contracts: Transforming digital entrepreneurial finance and venture funding. Journal of Small Business and Enterprise Development, 32(3), 739–761. https://doi.org/10.1108/jsbed-12-2023-0584

Davis, F. D. (1989). Perceived usefulness, perceived ease of use, and user acceptance of information technology. MIS Quarterly, 13(3), 319–340. https://doi.org/10.2307/249008

Devan, M., Prakash, S., & Jangoan, S. (2023). Predictive maintenance in banking: Leveraging AI for real-time data analytics. Journal of Knowledge Learning and Science Technology, 2(2), 483–490.

Dhanda, S. S., Singh, B., & Jindal, P. (2020). Lightweight cryptography: A solution to secure IoT. Wireless Personal Communications, 112(4), 1–34. https://doi.org/10.1007/s11277-020-07134-3

Feng, Q., He, Q., Zeadaly, S., Khan, M. K., & Kumar, N. (2018). A survey on privacy protection in blockchain system. Journal of Network and Computer Applications, 126, 45–58. https://doi.org/10.1016/j.jnca.2018.10.020

Guo, H., & Liu, X. (2025). Exploring trust dynamics in finance: The impact of blockchain technology and smart contracts. Humanities and Social Sciences Communications, 12(1). https://doi.org/10.1057/s41599-025-05473-9

Ikhasan, W. M., Ednoer, E. H., Kridantika, W. S., & Firmansyah, A. (2022). Fraud detection automation through analytics and artificial intelligence. Riset, 4(2), 103–119. https://doi.org/10.37641/riset.v4i2.166

Ilori, O., Nwosu, N. T., & Naiho, H. N. N. (2024). Advanced data analytics in internal audits: A conceptual framework for comprehensive risk assessment and fraud detection. Finance & Accounting Research Journal, 6(6), 931–952.

Kanu, C., Nnam, M. U., Ugwu, J. N., Achilike, N., Adama, L., Uwajumogu, N., & Obidike, P. (2023). Frauds and forgeries in banking industry in Africa: A content analysis of Nigeria Deposit Insurance Corporation annual crime report. Security Journal, 36(4), 671–692. https://doi.org/10.1057/s41284-022-00358-x

Karanina, E. V., & Skopin, D. I. (2023). Theoretical aspect of digital finance development. Ekonomika I Upravlenie Problemy Resheniya, 138(6/4), 5–11. https://doi.org/10.26871/ek.up.p.r.2023.06.04.001

Kermani, A. Z., Piri, H., Payan, A., & Sotudeh, R. (2025). Investigating the role of blockchain technology and artificial intelligence in the enhancement and improvement of accounting information systems using an interpretive structural approach. Business Marketing and Finance Open, 2(4), 1–17. https://doi.org/10.61838/bmfopen.2.4.8

Ketha, S., & Provodnikova, A. (2024). Combining blockchain and AI for fraud detection: Building secure, transparent and sustainable financial ecosystems. Global Journal of Business and Integral Security, 7(3). https://gbis.ch/index.php/gbis/article/view/599

Kolisnyk, O., & Skliarov, D. (2025). Transformation of financial accounting: From traditional methods to digitalization. Business Navigator, 79, 30–36. https://doi.org/10.32782/business-navigator.79-36

Kon, G., & Lu, Y. (2025). FinTech: A literature review of emerging financial technologies and applications. Financial Innovation, 11(1). https://doi.org/10.1186/s40854-024-00668-6

Kumar, G., & Yamuna, B. (2025). Blockchain-based fraud detection and prevention system enhanced with AI. International Journal for Research in Applied Science and Engineering Technology, 13(9), 538–544. https://doi.org/10.22214/ijraset.2025.73998

Lam, A. Y. S. (2024). Artificial intelligence applications in financial technology. Journal of Theoretical and Applied Electronic Commerce Research, 20(1), 29. https://doi.org/10.3390/jtaer20010029

Lean, O. K., Zailani, S., Ramayah, T., & Fernando, Y. (2009). *actors influencing intention to use e—government services among citizens in Malaysia*, *6*, 458-475.

Munira, M. S. K. (2025). Digital transformation in banking: A systematic review of trends, technologies, and challenges. Strategic Data Management and Innovation, 2(01), 78–95.

Nguyen, D., Tran, Q., & Le, H. (2023). Cross-chain security threats in decentralized finance. Future Internet, 15(6), 193.

Nigeria Deposit Insurance Corporation. (2022). Annual report and statement of accounts 2022. NDIC Publications. https://www.ndic.gov.ng/publications/annual-reports/

Nigeria Interbank Settlement System. (2023). Annual fraud landscape 2023. NIBSS Publications. https://www.nibss-plc.com.ng/

Nuraeni, R., Natalia, E. A., Hua, C. T., Septiani, N., & Sasono, I. (2026). Decentralized Storage in Smart City Data Infrastructure SWOT Analysis. *Blockchain Frontier Technology*, *5*(2), 112-123. https://journal.pandawan.id/b-front/article/download/872/599

Rogers, E. M. (1983). Diffusion of innovations (3rd ed.). Free Press.

Shoetan, P. O., & Familoni, B. T. (2024). Transforming fintech fraud detection with advanced artificial intelligence algorithms. Finance & Accounting Research Journal, 6(4), 602–625.

Shofi, B., Agustin, A. W., Maydina, S. N., & Dewi, B. K. (2026). Effectiveness of artificial intelligence and blockchain integration for fraud prevention in accounting information systems: A systematic review of empirical evidence. Sinergy, 1, 256–264.

Sidabutar, R. (2026). Strategies for Digitalizing Tourism Services to Support Smart Tourism. *International Journal of Business Innovation and Smart Technologies*, *1*(1), 5-9. https://bimjournal.id/bist/article/download/4/4

Sujana, D. A., & Laela, S. F. (2025). AI for fraud detection and accounting system security: Implementation in Indonesian Islamic banks. Jurnal Akuntansi dan Bisnis, 25(1), 65–86. https://doi.org/10.20961/jab.v25i1.1308

Supriadi, I. (2024). The audit revolution: Integrating artificial intelligence in detecting accounting fraud. Akuntansi dan Teknologi Informasi, 17(1), 48–61. https://doi.org/10.24123/jati.v1711.6279

Suyono, W. P., Puspa, E. S., Anugrah, S., & Finanda, R. (2025). Redefining fraud detection: The synergy between auditor competency and AI-powered audit analytics. RIGGS Journal of Artificial Intelligence and Digital Business, 4(3), 953–960. https://doi.org/10.31004/riggs.v4i3.2066

Taha, A. A., & Malebary, S. J. (2020). An intelligent approach to credit card fraud detection using an optimized light gradient boosting machine. IEEE Access, 8, 25579–25587. https://doi.org/10.1109/ACCESS.2020.2971354

Taher, S. S., Ameen, S. Y., & Ahmed, J. A. (2024). Advanced fraud detection in blockchain transactions: An ensemble learning and explainable AI approach. Engineering, Technology and Applied Science Research, 14(1), 12822–12830. https://doi.org/10.48084/etasr.6641

Tampubolon, E. O., Hutauruk, J. R. O., & Muda, I. (2025). A systematic literature review on the integration of blockchain and artificial intelligence for fraud detection in auditing. https://doi.org/10.56799/peshum.v5i1.12376

Thommandru, A., & Chakka, B. (2023). Recalibrating the banking sector with blockchain technology for effective anti-money laundering compliances. Sustainable Futures, 5, 100107. https://doi.org/10.1016/j.sftr.2023.100107

Tian, F. (2017). A supply chain traceability system for food safety based on HACCP, blockchain & internet of things. In International Conference on Service Systems and Service Management (pp. 1–6). https://doi.org/10.1109/ICSSSM.2017.7996119

Utomo, F. S., Suryana, N., & Azmi, M. S. (2025). Factors influencing user adoption of mobile payment system: an integrated model of perceived usefulness, ease of use, financial literacy, and trust. *Journal of Digital Market and Digital Currency*, *2*(2), 135-156. https://jdmdc.com/index.php/JDMDC/article/download/31/23

Venkatesh, V., Morris, M. G., Davis, G. B., & Davis, F. D. (2003). User acceptance of technology toward a unified view. MIS Quarterly, 27(3), 425–478.

Wang, Y., Rezaei, A., & Hicks, S. J. (2026). Digital twins in the construction industry: A systematic review of current practices and future directions. *Journal of Information Technology in Construction*, *31*, 149-179. https://wrap.warwick.ac.uk/id/eprint/197571/1/2026_07-ITcon-Wang.pdf

Yang, H., Shukur, Z., & Sahran, S. (2026). A review of artificial intelligence for financial fraud detection. Applied Sciences, 16, 1931, 1–32. https://doi.org/10.3390/app16041931

Yanjun, G. (2025). Application of blockchain technology in green finance and evaluation of its economic effects. Journal of Posthumanism, 5(5), 2239–3364. https://doi.org/10.63332/joph.v515.1613

Zayed, L. M. M., Nour, M. I., Al Attar, K., Almubaideen, H., & Abdelaziz, G. A. M. (2024). Role of artificial intelligence (AI) in accounting information systems in detecting fraud. In Artificial Intelligence and Economic Sustainability in the Era of Industrial Revolution 5.0 (pp. 397–409). Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-56586-1_30

Zhao, R., & Yermack, D. (2024). AI fraud detection and financial stability. Journal of Financial Economics. https://doi.org/10.1016/j.jfineco.2023.103640

Zulhelmi, T., Asih, V. S., & Helmiawan, M. A. (2023). Analysis of the application of blockchain and artificial intelligence to overcome accounting fraud in Islamic banking, 4(1), 184–193. http://ur.aeu.edu.my/1182/

Zykind, G., Nathan, O., & Pentland, A. (2015). Decentralizing privacy: Using blockchain to protect personal data. In IEEE Security and Privacy Workshops (p. 18184). https://doi.org/10.1109/SPW.2015.27