FUDMA Journal of Accounting and Finance Research, 4(1). ISSN: 2992-4693 (Online); 2992-2704 (Print)

Impact of smart contracts and cryptographic security on fraud prevention in Nigerian deposit money bank

Oluwaseyi Ayodele Adedipe
Department of Accounting, Ajayi Crowther University, Oyo, Oyo State, Nigeria
Corresponding email : hephzibahfine@gmail.com
https://doi.org/10.33003/fujafr-2026.v4i1.328.250-263

Abstract
Purpose: Cyber fraud and money laundering are growing threats to the integrity of operations in the Nigerian banking sector, which undercuts the confidence of customers. This study examined the influence of FinTech solutions specifically smart contracts and cryptographic security on fraud prevention in Nigerian deposit money banks (DMBs), in view of the increasing incidence of cyber fraud and money laundering in the sector.
Methodology: The study adopted a quantitative research design, underpinned by the Technology Acceptance Model (TAM), agency theory, and control theory. A cross-sectional survey was conducted on 312 management and IT employees drawn from five selected DMBs in Lagos State. Data collected were analyzed using descriptive statistics and multiple regression analysis.
Results and conclusion: The findings revealed that smart contracts have a positive and statistically significant effect on the prevention of cyber fraud ($r = 0.408$, $p < 0.001$), while cryptographic security exerts a strong and significant influence on the prevention of money laundering ($r = 0.433$, $p < 0.001$). The study concluded that these FinTech solutions are effective tools for enhancing fraud prevention and improving the security architecture of Nigerian banks.
Implication of findings: The study implies that deposit money banks should prioritize investment in FinTech innovations, while regulatory authorities should establish supportive frameworks to facilitate their adoption, thereby strengthening financial security and restoring customer confidence in the banking system.

Keywords: Cryptographic security, Cyber fraud, Financial security, FinTech, Money laundering.

1. Introduction

The digital revolution, through the evolution of information technology and the internet, has essentially changed the world of business in its entirety. The period has witnessed the emergence of fully new industries and the revolution of old ones, which have been significantly triggered by the rise of financial technology, or FinTech. FinTech has become a paradigm shift, providing more efficient, safer, and affordable patterns of doing business. The blockchain technology takes the forefront of this change in the financial sector, as it is a revolutionary technology that has the potential to transform the fundamentals of the banking and financial industry. First made well-known as the backbone of fintech of cryptocurrencies such as Bitcoin and Ethereum, blockchain makes possible a decentralised peer-to-peer transaction system. This removes the necessity of a centralised power and creates a financial ecosystem that is more transparent, efficient and trustworthy. Having acknowledged such a game-changing prospect, progressive countries such as Singapore, the U.K., Switzerland, and the UAE are increasingly studying and introducing blockchain to revive their economies and transform their financial sectors (Zheng et al., 2020).

In line with such an international trend, in 2023 the federal government of Nigeria rolled out a policy titled the National Blockchain Policy for Nigeria. This long-term strategic plan is expected to establish a blockchain-enabled economy that helps to ensure safe and transparent value exchange between citizens, businesses, and the state. The expected results are the closer to economic prosperity, the better quality of the business services, employment, and an impetus towards domestic innovation (National Blockchain Policy for Nigeria, 2023). In the case of the Deposit Money Banks (DMBs) in Nigeria, adoption of

FinTechs such as blockchain is no longer a choice but a strategic initiative to survive and thrive. The applicability of blockchain is much wider than cryptocurrencies. It provides a new paradigm of financial operations, especially such operations as payments between countries, where it is supposed to be faster, more secure, and save a lot of money, in contrast to traditional systems that utilise intermediaries (Kocianski, 2018). With the adoption of this potent FinTech innovation, the Nigerian banks will not only have an opportunity to improve the existing processes but also conduct new financial operations, ensure even more secure transactions, and remain competitive in a highly dynamic environment threatened by nimble FinTech start-ups (Cucari et al., 2022; Orumwense et al., 2026; Sanusi, et al. 2026).

Nonetheless, irrespective of the possible advantages, the Nigerian banking industry is under a constant and growing threat of cyber fraud, which severely compromises the integrity of operations and destroys customer confidence. The traditional banking model, which is based on centralised databases and manual verification procedures, is more prone to elaborate cyber-attacks, which translate to huge financial losses. As an example, the Central Bank of Nigeria (CBN, 2022) claimed that the number of fraud cases increased at an alarming rate of 24 per cent in 2021, leading to a loss of about ₦5.6 billion. Although the available literature talks about FinTech in general terms, empirical studies on how transactions can be automated and secured by smart contracts as self-executing agreements with pre-existing rules are essential at the distinct environment of Nigerian Deposit Money Banks (DMBs). This gap creates a need to conduct a dedicated study on the influence of this particular element of fintech.

To worsen the problem of cyber fraud, there is the persistent problem of money laundering, which poses a threat to the stability and integrity of the financial system. The conventional anti-money laundering (AML) controls of the banks of Nigeria tend to grapple with their inefficiencies, forgeries of documents, and inability to trace the illegal transactions of the money in real-time. The nature of the current systems being centralised provides opaque channels through which laundering activities could be carried out. Although past research has been to discuss the potential of fintech in an abstract way, they have not been able to adequately break down the role played by cryptographic security, the encryption and hashing algorithms that ensure data integrity and identity assurance in providing a clear and auditable trail that can play a significant role in the prevention of money laundering.

Prior research often examines fraud prevention in general terms, without distinguishing between specific dimensions such as cyber fraud and money laundering. Similarly, most studies analyze FinTech tools in isolation, with limited attention to their combined effects on fraud prevention. Also, there is limited focus on deposit money banks in Nigeria**, as** many studies are conducted at a broader financial system level. Additionally, insufficient integration of theoretical frameworks such as the Technology Acceptance Model (TAM), agency theory, and control theory weakens the theoretical explanation of FinTech adoption and its impact on fraud prevention. Finally, few studies employ robust quantitative methods, such as multiple regression based on cross-sectional data from banking professionals, thereby limiting the strength of empirical validation. There is also inadequate evidence linking FinTech solutions to specific fraud outcomes, as most studies treat fraud prevention as a generalized concept. These gaps highlight the need for a focused, theory-driven, and empirical investigation into the combined effects of smart contracts and cryptographic security on cyber fraud and money laundering prevention within Nigerian deposit money banks, which this study seeks to address. Hence, this paper fills this gap by discussing the precise ways in which cryptography can strengthen AML systems of Nigerian DMBs. The general objective of the research is to analyse the influence of FinTech innovation in the prevention of fraud in Nigerian Deposit Money Banks (DMBs). The particular objectives of this research focused on: (1) Delineate how smart contracts can address cyber fraud prevention in DMBs, and (2) evaluate how

cryptographic security can be used to address money laundering prevention in DMBs. With the aim of achieving these goals, the paper aims at establishing empirical facts on how particular technological elements can alleviate security threats within the Nigerian financial system.

2. Literature review

Financial Technology (FinTech) is the combination of financial services and recent digital technologies to enhance the efficiency, accessibility, and security of financial transactions. FinTech encourages real-time financial transactions, automated financial transactions, and digital financial transactions, unlike traditional financial systems where physical infrastructure is very important and many intermediaries are used. It includes several innovations that include mobile banking, peer-to-peer lending, artificial intelligence, and blockchain technology. FinTech formation is mostly the reaction against the shortcomings of traditional banking systems such as slow transaction processing, high cost of operation, and susceptibility to fraud (Arner et al., 2020). One of the most important innovations in the FinTech world is blockchain, which is a decentralised registry that stores transactions on a network of computers. The structure guarantees the transparency, immutability and security of financial records and also minimises the use of intermediaries. Consequently, financial operations, especially cross-border payments, will be faster and cheaper than using the traditional banking system (Boehme et al., 2020).

Cyber fraud prevention and smart contracts

Smart contracts are digitalised automated contracts whereby the terms of the contract are coded in computer programs that carry out transactions when particular terms are fulfilled. The idea was initially proposed by Nick Szabo, and it allows the process of financial agreements to be achieved automatically. Smart contracts are used in the FinTech ecosystem to increase the level of transparency, decrease the delays in operations, and minimise the danger of dealing with manual processing. They also play a major role in preventing fraud, whereby transactions are only made to take place when certain conditions are met. Also, blockchain systems have an immutable and decentralised transaction record which may not be easily altered by fraudsters, as they are not able to alter the records of finances. Such a decentralised verification system does not have the single point of failure as in the traditional financial system and improves the overall data security (Khera et al., 2022; Shen and Hou, 2021; Wang et al., 2021).

Cryptographic security and money laundering prevention

Cryptographic security is an essential part of the FinTech systems because it preserves the digital financial data and guarantees the confidentiality, integrity, and authenticity of various transactions. Encryption, public key infrastructure (PKI) and hashing are a few examples of techniques applied to secure financial information and eliminate access by unauthorised people. Such regulatory agencies as the National Institute of Standards and Technology (NIST) offer frameworks that can help organisations to adopt effective cybersecurity (NIST, 2018). Also, FinTech technologies have enhanced the process of detection and prevention of money laundering.

Conventional anti-money laundering systems are frequently manually monitored and detected by rules, with risk of high false positives. Nonetheless, the combination of artificial intelligence and machine learning can help financial institutions to study the behaviour of transactions and identify suspicious behaviour more efficiently. The Financial Action Task Force (FATF, 2021) notes that network analysis and machine learning are advanced technologies that are important in the detection of sophisticated money laundering schemes. Evidence also shows that integrating blockchain and a robust cryptography system can minimise susceptibility to illegal financial operations (Smith & Johnson, 2023; Sanusi, et al. 2026).

Theoretical framework

Agency theory

Agency theory was propounded by Jensen and Meckling (1976) as an understanding of the conflict between the principals (owners or shareholders) and the agents (managers or employees) who provide the resources of the organisation on behalf of the principals. This clash is because they can act in their own interests, in the form of bonuses or convenience, rather than the interests of the organisation, particularly in cases of information asymmetry, where agents have a greater amount of operational information than their principals. This asymmetry in the case of the deposit money banks in Nigeria is usually presented in the form of internal fraud, illegal transactions, and financial data manipulations. The solutions to this ancient issue are proposed by FinTech technologies, in particular, blockchain technology. Transparency of transactions and lack of centralisation in the blockchain facilitate real-time tracking of transactions, thus eliminating chances of agents hiding fraudulent transactions. It provides clear reporting and audit trails which are traceable and align the interests of the managers and the shareholders. This theory as applied to the study offers the basis of how the FinTech transparency tools (such as blockchain-based ledgers and AI-based transaction tracking) can minimise opportunistic behaviour, reinforce surveillance, and enhance accountability provisions in Nigerian banks. (Obumneme, et al 2025; Sanusi, et al. 2026)

Control theory

Both Thomas and Donald (1982) advanced control theory, stating that companies should introduce feedback-related systems that will make sure that the behaviour and performance are not going against the set objectives. Traditional banking has internal control procedures that tend to be manual, periodical audits, and hierarchical approval systems – systems that can be manipulated to misuse their powers. FinTech changes this paradigm by means of automated tamper-proof control systems. Such technologies as smart contracts, biometric authentication, or real-time analytics initiate self-regulating systems that track compliance in real-time. This will not only make the operation more disciplined but also make sure that anomalies are detected early, which will strengthen the control-environment. Therefore, the control theory proves the thesis that automation implemented by FinTech can reinforce internal control systems in Nigerian banks to a high degree. These tools provide the solution to integrity in financial transactions through minimising human interference and making sure that fraudulent practices are corrected as soon as they are detected by the tools.

Empirical review

Empirical studies on fraud prevention in the Nigerian banking sector have evolved from traditional corporate governance mechanisms to advanced FinTech-driven approaches. Erstwhile evidence emphasizes the role of corporate governance structures in mitigating fraud. Obumneme et al. (2025) examined the relationship between governance attributes and fraud likelihood using an ex post facto design and secondary data from 10 listed deposit money banks between 2014 and 2023. The study employed multiple regression analysis and found that board independence and audit committee independence significantly reduce fraud likelihood, while board size showed mixed results. Ownership structure was also significant, with higher institutional ownership linked to lower fraud risk. The model explained a substantial proportion of variation in fraud likelihood ($R^2 = 0.75$), indicating strong explanatory power. However, the study was limited by its narrow scope and failure to incorporate modern fraud detection technologies.

With the advancement of digital technologies, recent studies have shifted focus to artificial intelligence and data-driven tools. Orumwense et al. (2026) explored the impact of AI tools such as predictive

analytics, robotic process automation (RPA), and natural language processing (NLP) on auditing practices in Nigeria. The study reported a 42% improvement in audit quality among firms that consistently adopted AI, highlighting enhanced fraud detection and reduced human error. The study focuses only on Southern Nigeria, leaving out other regions that might have different AI adoption rates or challenges. Long-term impact of AI adoption on audit practices was not examined and though the study mentions challenges like high costs but fails to propose specific solutions to overcome them. Similarly, Sanusi et al. (2026) adopted a hybrid approach combining Partial Least Squares Structural Equation Modelling (PLS-SEM) and Artificial Neural Networks (ANN) to detect fraud patterns in 15 Nigerian deposit money banks (2016–2023), achieving an accuracy rate of 89%. Despite their contributions, these studies paid limited attention to ethical considerations, staff capacity development, and broader sectoral applications.

Further empirical evidence highlights the role of FinTech innovations in fraud prevention. Fatokun et al. (2025) demonstrated that machine learning techniques such as Random Forest and XGBoost significantly improve fraud detection in Nigeria's financial system. Similarly, Adeyemo and Obafemi (2024) found that technological innovations including blockchain, real-time monitoring systems, and data analytics enhance fraud prevention and strengthen banking operations. In the area of blockchain and smart contracts, Ayodele et al. (2025) and Ahmed et al. (2025) reported that smart contracts improve transparency, automate compliance, and reduce fraud risk in financial transactions. Supporting these findings, Kokogho et al. (2025) established that blockchain technology enhances real-time auditing and financial transparency, thereby strengthening fraud detection mechanisms. In addition, Ajayi et al. (2025) found that cryptographic security significantly improves data integrity and reduces cyber threats in banking systems.

Other studies have examined complementary approaches. Akpootu and Yusuf (2025) highlighted the effectiveness of forensic accounting techniques in fraud control, while Sheikh et al. (2025) confirmed through a systematic review that blockchain adoption improves transparency, compliance, and operational efficiency. Akinola (2024) further emphasized the importance of integrating internal control systems with technological solutions to enhance fraud risk management in Nigerian banks. Overall, the empirical literature demonstrates that both traditional governance mechanisms and emerging FinTech solutions contribute significantly to fraud prevention. However, while prior studies provide valuable insights, they largely examine these mechanisms in isolation, thereby necessitating further research on the combined effects of specific FinTech tools such as smart contracts and cryptographic security within Nigerian deposit money banks.

Despite the growing body of literature on FinTech and fraud prevention, several gaps are evident in the reviewed empirical studies. First, existing studies largely adopt a broad approach to FinTech, focusing on general technologies such as blockchain or machine learning (Fatokun et al., 2025; Adeyemo & Obafemi, 2024; Ajayi et al., 2025), without isolating specific components like smart contracts and cryptographic security. These limits understanding of the individual and comparative effects of these technologies on fraud prevention. Second, some studies in the like of Ahmed et al. (2025) emphasize technical and algorithmic improvements in FinTech systems but pay limited attention to their practical application within banking institutions, particularly Nigerian deposit money banks. In addition, several studies adopt conceptual or qualitative approaches, resulting in limited empirical evidence based on organizational-level data, especially from management and IT personnel (Sheikh et al., 2025). Third, certain studies such as Akpootu & Yusuf (2025) focus on forensic accounting techniques, which differ

from modern FinTech innovations, thereby leaving a gap in research specifically addressing emerging FinTech tools. Moreover, many studies are conducted in non-Nigerian or global contexts, reducing their relevance to the Nigerian banking environment, where available studies tend to emphasize internal controls rather than FinTech adoption (Akinola, 2024). These gaps necessitate an empirical investigation into the specific roles of smart contracts and cryptographic security within the Nigerian banking context, leading to the formulation of the following hypotheses:

H1: Smart contracts have no significant impact on cyber fraud prevention.

H2: Cryptographic security has no significant influence on money laundering prevention**.**

3. Methodology

In this research, a quantitative research design was adopted, and a cross-sectional survey design was used. The design is suitable since it will enable the collection of numerical data of a sample of a population at one point in time and analyse the relationships between defined variables (Saunders, Lewis, and Thornhill, 2019). The selection of a survey design will be based on its effectiveness in collecting the information about a big population of respondents in a systematic way so that it will be easy to statistically analyse and test the hypothesis. The given approach is rather appropriate to respond to the research questions and test the formulated null hypotheses since it helps the researcher to measure the perceptions and experiences of banking professionals concerning the influence of different FinTech components. The design is said to be positivist-orientated because it aims to determine the correctness or incorrectness of pre-existing hypotheses through the systematic and controlled collection of factual and objective information (Bell, Bryman, and Harley, 2022).

Lagos State was selected as the study location because it is the financial hub of Nigeria, hosting the headquarters of most Deposit Money Banks (DMBs) and major financial institutions. It also serves as the centre of FinTech innovation and digital banking operations, making it the most suitable environment for examining fraud prevention technologies such as smart contracts and cryptographic security.

The study focuses on Guaranty Trust Bank, First Bank of Nigeria, Zenith Bank, Access Bank, and Stanbic IBTC Bank due to their systemic importance, strong digital infrastructure, and leadership in FinTech adoption within the Nigerian banking sector. These banks are also among the most active in deploying advanced fraud detection and cybersecurity systems. The target population comprises management and IT/operations personnel from key departments such as compliance, risk management, internal audit, finance, and information technology, as they are directly involved in fraud control and digital banking operations. The estimated population of relevant staff across the selected banks in Lagos is approximately 5,000 professionals, making it adequate for robust empirical analysis.

Considering the large and scattered target population, it will require a sampling strategy to make the research viable and affordable. Therefore, to have a representative sample that is not biased, a multi-stage sampling technique was utilised. Stage 1 entailed a purposive sample of five top deposit money banks in Lagos according to their asset size, market share and perceived investments in digital transformation. Stage 2 was stratified random sampling in the banks; the population was stratified based on the main job functions (e.g., management, IT, operations, and compliance). In stage 3, simple random sampling was used, and the respondents were selected through the random number generator in lists that were requested at the Human Resources department.

The sample was calculated using the Taro Yamane formula of finite populations, which is a common way of calculating the sample in social science research (Yamane, 1967). The sample size (n) was

determined with a population size (N) of about 3000 and a required level of precision (e) of 5% (0.05). Out of the 357 questionnaires sent, there were 312 that were returned and were usable in analysis, giving us a response rate of 87.4. This is a sufficient response rate in order to make strong statistical inferences.

Method and instrument of data collection

A structured self-administered questionnaire was used as the main tool of data collection. This tool was selected due to its capability to gather standardised data using a large sample size, reduce interviewer bias, and perform quantitative analysis. The questionnaire was online through such sites as Google Forms, and professionally printed hard copies were provided to ensure that the maximum number of people could respond to the questionnaire. The questionnaire was designed in three different parts: Section A took the demographic details. Section B was used to test the independent variables (smart contracts, cryptographic security) on a 5-point Likert scale. The dependent variables (cyber fraud prevention and money laundering prevention) were measured in section C, on a 5-point Likert scale.

Instrument validity and reliability

Validity and reliability tests were done to make the research instrument sound and credible. Validity is used to refer to the extent to which an instrument is used to measure what it is expected to measure (Heale and Twycross, 2020). To determine the clarity, relevance, and comprehensiveness of the items, the supervisor reviewed the first draft of the questionnaire. Reliability is to do with the stability and consistency of the measuring instrument. The pilot study data were examined in terms of Cronbach's Alpha to determine the reliability of the multi-item scales in measuring each of the constructs. The acceptable Cronbach's alpha coefficient of 0.70 or above is typically regarded as a good internal consistency (Tavakol and Dennick, 2020). According to the reliability statistics displayed in the study, the Cronbach's alpha of all the constructs is 0.868 to 0.918, which is a lot greater than the acceptable level of 0.70. The coefficient of the overall reliability of the whole instrument is 0.927. This means that there is a high degree of internal consistency and reliability.

Data analysis methods

The analysis of the data collected was done with the Statistical Package of the Social Sciences (SPSS) version 21. The summarisation of demographic characteristics was conducted by using descriptive statistics (frequencies, percentages, means and standard deviations). Pearson Product-Moment Correlation (PPMC) was used in the preliminary analysis, and multiple regression analysis was used as the main technique of analysis in testing the hypotheses in the inferential statistics. The analysis presented the R^2 (coefficient of determination) to indicate the value (per cent) of the variation in the dependent variable explained jointly by all the predictors. More to the point, the regression provided the beta coefficients (β) of each independent variable, t-statistic, and p-value. The criterion of rejection of the null hypotheses was a p-value that is lower than 0.05. Multicollinearity (diagnostic tests using Variance Inflation Factor - VIF), normality, linearity and homoscedasticity tests were run to be certain that the data satisfies the major assumptions of multiple regression analysis.

4. Results and discussion

Demographic characteristics of respondents

Table 1: Demographic profile of respondents

Demographic Variable	Category	Frequency	Percentage (%)
Gender	Male	172	55.1%
	Female	140	44.9%
	Total	312	100.0%
Age	18-25 years	28	9.0%
	26-35 years	145	46.5%
	36-45 years	102	32.7%
	46 years and above	37	11.9%
	Total	312	100.0%
Years of Experience	Less than 1 year	15	4.8%
	1-3 years	68	21.8%
	4-6 years	121	38.8%
	Above 6 years	108	34.6%
	Total	312	100.0%
Bank	GTBank	65	20.8%
	First Bank	63	20.2%
	Zenith Bank	62	19.9%
	Access Bank	61	19.6%
	Stanbic IBTC	61	19.6%
	Total	312	100.0%
Department	IT/Digital Innovation	89	28.5%
	Operations	78	25.0%
	Risk Management/Compliance	75	24.0%
	Finance/Audit	70	22.4%
	Total	312	100.0%

Source: Field survey, (2026)

Demographic distribution of the respondents also gives an insight to what the sample used in this study was composed of and its representativeness. The outcome reveals that 172 (55.1) out of 312 respondents were males, whereas 140 (44.9) were females. This shows that there is a slight male dominance of the participants, implying a relatively higher percentage of men as the workforce of the sampled deposit money banks. The analysis also shows that 145 respondents (46.55%) were between the 26-35 age brackets, meaning that we have a young and energetic workforce that is probably flexible to organisational change and innovation and digital transformation in the banking sector. Concerning the level of experience in the field of work, 121 respondents (38.8%) had a period of four to six years of professional experience, and 108 respondents (34.6%) had over six years' experience in the field of work. This distribution indicates a highly experienced workforce, as a majority of the respondents (73.4%) possess more than four years of working experience in the banking industry and are therefore well informed with regard to the operations and reforms as well as the environment that regulates the banking industry in Nigeria. On the institutional affiliation, the answers were quite even among the five chosen deposit money banks (GTBank, First Bank, Zenith Bank, Access Bank, and Stanbic IBTC), giving wide institutional coverage. Lastly, the departmental analysis shows that 89 respondents (28.5%) were

in IT/Digital Innovation departments, 78 respondents (25.0%) in Operations, 75 respondents (24.0%) in Risk Management/Compliance, and 70 respondents (22.4%) in Finance/Audit. This distribution indicates that most of the participants were recruited in technology-orientated and operationally sensitive departments.

Test of hypothesis

To test the study's hypotheses and determine the unique contribution of each FinTech variable to the outcomes, separate regression analyses were performed. For each model, the assumptions of linearity, homoscedasticity, and independence of errors were met. Multicollinearity was assessed using the Variance Inflation Factor (VIF), and all VIF values were below 3.5, well within the acceptable threshold of 10.

H1: Smart contracts have no significant impact on cyber fraud prevention.

Model Summary table for Hypothesis 1

R	R^2	Adjusted R^2	Std. Error of the Estimate
.781	.610	.603	0.44128

Source: SPSS 21

ANOVA table for Hypothesis 1

	Sum of Squares	Df	Mean Square	F	Sig.
Regression	58.912	4	14.728	75.624	.000
Residual	37.688	307	0.195		
Total	96.600	311			

Source: SPSS 21

Coefficients table for Hypothesis 1

	Unstandardized Coefficients	Standardized Coefficients (Beta)	t	Sig. (p-value)	VIF
(Constant)	0.745		3.112	.002	
SC	0.402	**0.408**	6.855	**.000**	2.145
CS	0.291	0.279	4.892	**.000**	2.301
DEC	0.085	0.099	1.721	.086	2.567
DLT	0.121	0.128	2.102	**.036**	2.488

Source: SPSS 21

The model summary in hypothesis 1 above indicates an R-value of 0.781, showing a strong positive correlation between the independent variables and cyber fraud prevention (CFP). The R^2 value of 0.610 suggests that approximately 61.0% of the variance in cyber fraud prevention can be explained by the combined influence of the four blockchain-related variables. The ANOVA table reveals an F-statistic of 75.624 with a corresponding p-value of 0.000 ($p < 0.05$), indicating that the regression model is statistically significant.

The regression coefficients provide deeper insight. The unstandardized coefficient for Smart Contracts ($B = 0.402$, $t = 6.855$, $p = 0.000$) indicates that a one-unit increase in the adoption or effectiveness of smart contracts leads to a 0.402-unit increase in cyber fraud prevention, holding other factors constant. This relationship is statistically significant at the 1% level ($p < 0.01$). Similarly, Cryptographic Security (B =

0.291, t = 4.892, p = 0.000) exhibits a positive and significant influence on cyber fraud prevention. Distributed Ledger Technology (B = 0.121, t = 2.102, p = 0.036) also demonstrates a statistically significant effect. However, Decentralization (B = 0.085, t = 1.721, p = 0.086) was found to have an insignificant effect at the 5% significance level. The regression results collectively demonstrate that smart contracts, cryptographic security, and distributed ledger technology significantly and positively influence cyber fraud prevention in Nigerian deposit money banks. Smart contracts emerged as the most dominant predictor. Therefore, the null hypothesis (H_{01}) is rejected.

H2: Cryptographic security has no significant influence on money laundering prevention.

Model summary table for hypothesis 2

R	R^2	Adjusted R^2	Std. Error of the Estimate
.802	.643	.638	0.47311

Source: SPSS 21

ANOVA table for hypothesis 2

	Sum of Squares	Df	Mean Square	F	Sig.
Regression	67.445	4	16.861	75.321	.000
Residual	37.455	307	0.224		
Total	104.900	311			

Source: SPSS 21

Coefficients table for hypothesis 2

	Unstandardized Coefficients	Standardized Coefficients (Beta)	T	Sig. (p-value)	VIF
(Constant)	0.612		2.445	.015	
SC	0.188	0.171	3.121	**.002**	2.145
CS	0.467	**0.433**	8.112	**.000**	2.301
DEC	0.072	0.074	1.401	.162	2.567
DLT	0.155	0.148	2.654	**.008**	2.488

Source: SPSS 21

The model summary in hypothesis 2 above shows a multiple correlation coefficient (R) of 0.802, indicating a strong positive relationship between the predictor variables and money laundering prevention. The coefficient of determination (R^2) is 0.643, implying that approximately 64.3% of the variation in money laundering prevention is explained by Smart Contracts, Cryptographic Security, Digital Encryption Compliance, and Distributed Ledger Technology. The Adjusted R^2 value of 0.638 confirms the model's goodness of fit after adjustment for the number of predictors. The standard error of the estimate is 0.47311, indicating a relatively low level of prediction error.

The ANOVA result shows that the regression model is statistically significant (F = 75.321, $p < 0.001$). Since the p-value is less than 0.05, the null hypothesis of no joint effect is rejected. This confirms that the independent variables collectively have a significant effect on money laundering prevention in Nigerian Deposit Money Banks.

The coefficients result reveals the individual effects of the explanatory variables: Smart Contracts (SC) have a positive and significant effect on money laundering prevention (B = 0.188, β = 0.171, t = 3.121, p = 0.002). This indicates that increased adoption of smart contracts improves banks' ability to prevent money laundering. Cryptographic Security (CS) shows a positive and highly significant effect (B = 0.467, β = 0.433, t = 8.112, p < 0.001), making it the most influential predictor in the model. This implies that stronger cryptographic mechanisms significantly enhance money laundering prevention. Digital Encryption Compliance (DEC) has a positive but statistically insignificant effect (B = 0.072, β = 0.074, t = 1.401, p = 0.162), suggesting that while it contributes positively, its effect is not statistically supported. Distributed Ledger Technology (DLT**)** exerts a positive and significant effect (B = 0.155, β = 0.148, t = 2.654, p = 0.008), indicating its relevance in strengthening anti–money laundering systems. The constant term (B = 0.612) represents the baseline level of money laundering prevention when all predictors are held constant.

The Variance Inflation Factor (VIF) values range from 2.145 to 2.567, which are within the acceptable threshold (below 10). This indicates that multicollinearity is not a concern in the model, and the estimates are stable and reliable. Conclusively, the regression results lead to the rejection of the null hypothesis (H_{02}), affirming that cryptographic security has a significant influence on money laundering prevention among Nigerian deposit money banks.

Discussion of findings

The results of the initial regression analysis indicates that smart contracts, among other fintech-based schemes, play a major role in deterring cyber fraud in the Nigerian deposit money banks. The model had a high correlation coefficient (R = 0.781) and the power of explanation (R^2 = 0.610). This implies that, technologies facilitated by fintech are all instrumental to ensuring the improvement of digital integrity, transparency, and security in the Nigerian financial environment. Further examination of the coefficients has shown that smart contracts (= 0.402, p = 0.001) have the greatest positive impact overall on cyber fraud prevention. This highlights their practical significance to automate financial operations and do away with human manipulation which in most cases leads to cyber fraud. Smart contracts decrease the chances of internal and external participants manipulating data and money by implementing pre-programmed rules that are self-verifying and enforcing transactions. The findings support previous empirical observations that automation and transparency provided by fintech minimizes the risks of fraud in the financial industry (Khera et al., 2022; Smith, 2024 Obumneme, et al 2025; Sanusi, et al. 2026).

Cryptographic security (= 0.291, p < 0.001) also became a major influencer of cyber fraud prevention. Encryption will protect sensitive banking information where the data cannot be read by unauthorized parties and hence data cannot be stolen at all by unauthorized parties thus probability of system infiltration will be minimized. The fact that it has a huge impact justifies the fact that financial institutions are increasingly relying on encryption systems such as the use of the public to the private key system and sophisticated hashing functions to help in securing digital transactions. On the same note, the distributed ledger technology (= 0.121, p = 0.036) exhibited a moderate, albeit significant positive effect, meaning that the immutability and transparency of fintech networks resulted in improved traceability of financial transactions. Nonetheless, the concept of decentralization (0.085, p = 0.086) did not have statistical significance, implying that the concept of distributing data among multiple nodes lowers the risk of system compromise, although infrastructural and regulatory aspects of the country are limiting to the implementation of these practices and their effects in Nigeria.

In the context of the prevention of money laundering, the most effective predictor was cryptographic security (0.433, $p < 0.001$). It is the bottom layer that guarantees the integrity of data, confidentiality and non-repudiation. The need to invest in an advanced cryptography is an urgent necessity to Nigerian DMBs aiming to comply with international AML standards and secure their systems, which is consistent with the assumptions of the Control Theory since it implies the possibility of creating a self-regulating control environment. This is in accordance with the best global practices that focus on technological financial surveillance and transaction monitoring (FATF, 2021; Smith and Johnson, 2023; Obumneme, et al 2025).

Overall, the findings demonstrate that Smart Contracts, Cryptographic Security, and Distributed Ledger Technology significantly enhance money laundering prevention in Nigerian Deposit Money Banks, with Cryptographic Security emerging as the strongest predictor. However, Digital Encryption Compliance, though positively related, does not show a statistically significant effect. These results confirm that the model is robust and statistically valid, with substantial explanatory power (64.3%). The findings further lead to the rejection of the null hypothesis, thereby affirming that FinTech-based security tools significantly influence money laundering prevention in Nigerian Deposit Money Banks.

5. Conclusion

Judging by the results of this study, a number of conclusions are made with reference to financial security. The research conclusively defines that Smart Contracts is not just a technological enhancement but a strategic pillar to counter cyber defraud acts in the Nigerian banks. They solve the weakness of traditional and manual systems directly by automating contractual executions and integrating security as part of the process logic. This observation confirms the use of the Agency Theory since smart contracts decrease information asymmetry and opportunism. The study finds out that strong Cryptographic Security cannot be compromised to achieve the best money laundering prevention measures. It forms the base layer that provides the integrity, confidentiality and non-repudiation of data. To the wider picture, the study has concluded that the combined implementation of these FinTech solutions provides a comprehensive solution to these problems of security threats that Nigerian DMBs would face simultaneously. A successful adoption of these technologies can go a long way in enhancing the stability, integrity, and global competitiveness of the Nigerian financial system.

Therefore, based on the empirical results obtained from the regression analysis, the study concluded that Smart contracts have no significant impact on cyber fraud prevention in Nigerian deposit money banks. The findings reveal that smart contracts have a positive and statistically significant effect on cyber fraud prevention. Consequently, the null hypothesis is rejected. This implies that smart contracts significantly enhance cyber fraud prevention in Nigerian deposit money banks. Furthermore, cryptographic security has no significant influence on money laundering prevention in Nigerian deposit money banks. The results show that cryptographic security has a positive and highly significant effect on money laundering prevention. Accordingly, the null hypothesis is rejected, indicating that cryptographic security plays a significant role in reducing money laundering activities in Nigerian deposit money banks.

In specific terms, the study concluded that smart contracts significantly improve cyber fraud prevention, while cryptographic security significantly enhances money laundering prevention in Nigerian deposit money banks. Both variables are statistically significant determinants of financial security and play a crucial role in strengthening the resilience of the Nigerian banking sector against financial crimes.

Based on the conclusions of this study which revealed that smart contracts significantly enhance cyber fraud prevention, while cryptographic security significantly improves money laundering prevention in Nigerian deposit money banks, the recommendations below are suggested:

i. FinTech-driven security mechanisms have become essential components of modern banking risk management rather than optional innovations. Consequently, policy direction within the Nigerian banking sector should focus on the structured integration of these technologies into existing fraud prevention frameworks. Regulatory and institutional structures should be strengthened to support the secure adoption of smart contracts in high-risk banking operations, while ensuring continuous upgrading of cryptographic security systems to respond to evolving cyber threats. Overall, regulatory oversight should prioritize enabling secure innovation, particularly in blockchain-based systems and digital encryption practices, rather than imposing restrictive controls.

ii. Deposit money banks should gradually integrate smart contracts into critical operational areas such as loan processing, trade finance, and corporate guarantees, where exposure to fraud risk is relatively high. This should be supported with adequate staff training and strategic collaboration with reputable FinTech providers to ensure effective deployment. In addition, banks are advised to strengthen their cryptographic security systems through the adoption of advanced encryption standards, robust key management frameworks, and continuous investment in cybersecurity expertise to enhance system resilience against money laundering activities.

References

Adeyemo, T., & Obafemi, K. (2024). Technological innovation and fraud prevention in Nigerian deposit money banks. *Journal of Financial Innovation and Risk Management*.

Ahmed, S., Usman, H., & Kadai, M. (2025). Security of blockchain-based smart contracts in financial systems. *FUDMA Journal of Sciences*.

Ajayi, O. A., Bello, M. K., & Ibrahim, T. (2025). Cryptographic security and cyber threat mitigation in banking systems. *International Journal of Digital Finance*.

Akinola, R. O. (2024). Internal control systems and fraud prevention in Nigerian banking sector. *African Journal of Accounting and Finance*.

Akpootu, D., & Yusuf, H. (2025). Forensic accounting techniques and fraud control in financial institutions. *FUDMA Journal of Accounting and Finance Research*.

Arner, D. W., Barberis, J., & Buckley, R. P. (2020). FinTech, RegTech, and the reconceptualization of financial regulation. *Journal of Financial Regulation and Technology*.

Ayodele, S. O., Oye, B. A., Alimi, T. O., & Obitolu, O. (2025). Blockchain-based smart contracts and financial transparency in digital transactions. *International Journal of Emerging Financial Technologies*.

Bell, E., Bryman, A., & Harley, B. (2022). *Business research methods* (6th ed.). Oxford University Press.

Boehme, R., Christin, N., Edelman, B., & Moore, T. (2020). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*.

Central Bank of Nigeria. (2022). *Annual report on fraud and forgery cases in Nigerian banks*. https://www.cbn.gov.ng

Cucari, N., Esposito De Falco, S., & Orlando, B. (2022). Blockchain adoption and financial innovation in banking systems. *International Journal of Bank Marketing*.

Fatokun, B. O., Sikiru, S. A., Balogun, A. A., & Okorie, U. (2025). Machine learning techniques in fraud detection in Nigeria's financial system. *FUDMA Journal of Sciences*.

Financial Action Task Force. (2021). *Money laundering and terrorist financing risks from new technologies*. https://www.fatf-gafi.org

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360.

Khera, P., Ng, S., & Wang, Z. (2022). Smart contracts and blockchain applications in financial systems. *Journal of Digital Banking*.

Kocianski, A. (2018). Blockchain in banking: Opportunities and challenges. *Financial Innovation Review*.

Kokogho, M., Efe, E., & Okpara, C. (2025). Blockchain technology and real-time auditing in FinTech environments. *Journal of Financial Technology Studies*.

Ministry of Communications and Digital Economy. (2023). *National blockchain policy for Nigeria*. Federal Government of Nigeria.

National Blockchain Policy for Nigeria. (2023). *Federal Ministry of Communications and Digital Economy*. Abuja, Nigeria.

National Institute of Standards and Technology. (2018). *Framework for improving critical infrastructure cybersecurity*. https://www.nist.gov

Obumneme, C., Eze, J., & Nwankwo, I. (2025). Corporate governance and fraud likelihood in Nigerian deposit money banks. *FUDMA Journal of Management Sciences*.

Orumwense, A., Ibrahim, T., & Bello, S. (2026). Artificial intelligence and audit quality in Nigerian financial institutions. *FUDMA Journal of Sciences*.

Sanusi, M., Abdullahi, Y., & Garba, A. (2026). Hybrid machine learning approaches for fraud detection in Nigerian banks. *FUDMA Journal of Sciences*.

Saunders, M., Lewis, P., & Thornhill, A. (2019). *Research methods for business students* (8th ed.). Pearson.

Sheikh, A., Bello, M., & Usman, K. (2025). Blockchain adoption and financial transparency: A systematic review. *International Journal of Banking and Finance Research*.

Shen, W., & Hou, J. (2021). Smart contracts and blockchain security applications. *Journal of Financial Technology and Systems*.

Smith, J. (2024). FinTech innovation and fraud risk reduction in financial institutions. *International Journal of Financial Technology Studies*.

Smith, J., & Johnson, L. (2023). Cryptographic systems and financial crime prevention. *Cybersecurity and Finance Journal*.

Tavakol, M., & Dennick, R. (2020). Making sense of Cronbach's alpha. *International Journal of Medical Education, 11*, 53–55. https://doi.org/10.5116/ijme.5dfb.8dfd

Wang, H., Li, X., & Zhang, Y. (2021). Blockchain-based fraud prevention systems in financial services. *International Journal of Information Management*.

Yamane, T. (1967). *Statistics: An introductory analysis* (2nd ed.). Harper & Row.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2020). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*.