NIU Journal of Management Sciences Copyright©2026
Nexus International University ISSN: *3007-1887;* 12(1): 5-22

Curbing Fraudulent Activities in Deposit Money Banks: The role of Blockchain Technology in Nigeria

ADEGBOYEGA R. AFOLABI, MODUPE M. ADESEMOWO,
OLAYEMI O. AMOSUN, M. OLAMIDE OTUYELU, SOLOMON O. OKUNADE
Chrisland University, Abeokuta, Nigeria

MUKAIL AKINDE
The Federal Polytechnic, Ilaro, Ogun State, Nigeria

Abstract. As digital intermediation accelerates, Nigerian deposit money banks (DMBs) confront rising cyber-enabled fraud since the launch of Bitcoin in 2009, despite ongoing reforms. Most blockchain research still centres on cryptocurrencies, with relatively few studies examining their applications in other industries. This study investigates whether blockchain technology (smart contracts, permissioned distributed ledgers, and secure digital wallets) is associated with lower fraud in Nigerian DMBs.Using survey data from 120 bankers across five institutions spanning international, national, and regional licenses, we estimate Ordinary Least Squares (OLS) models relating each BCT dimension, and a composite index, to two outcomes: spread of fraud (SOF) and internet fraud activities (IFA). Reliability analysis shows strong internal consistency ($\alpha = 0.75–0.91$). Models include robustness checks for multicollinearity and specification. Results indicate that higher perceived deployment of smart contracts, distributed ledger, and digital wallet capabilities is negatively and significantly associated with SOF and IFA; a composite BCT index positively predicts overall fraud-reduction assessments. These findings align with recent sectoral evidence that blockchain adoption lowers fraud-related costs and enhances transaction integrity in banking. Given Nigeria's elevated incidence of electronic fraud in retail payments, the practical implication is that embedding programmable controls, tamper-evident shared records, and cryptographic authentication can harden high-risk processes. We recommend that regulators and DMBs advance permissioned BCT pilots integrated with Anti-Money Laundering (AML) and Know Your Customer (KYC) workflows, strengthen reporting standards, and build human-capital readiness. Beyond cryptocurrency, enterprise-grade BCT offers credible pathways to reduce fraud externalities and improve operational resilience in Nigeria's banking sector.

Keywords: Blockchain; Smart contracts; Distributed ledger; Digital wallet; Bank fraud; Nigeria.

1. Introduction

Information and communication technologies have transformed financial intermediation, compressing time and distance in payments, credit, and market access. Yet the same digitization has widened the attack surface for criminal exploitation. Nigerian deposit money banks (DMBs) which are central to savings mobilisation and the payments backbone, are particularly exposed as retail transactions migrate to mobile and card rails. In 2023 alone, Nigeria Inter-Bank Settlement System (NIBSS) recorded tens of thousands of successful fraud cases, with electronic channels dominating the modus operandi, underscoring the urgency of control innovations (NIBSS, 2024; CBN, 2024). Against this backdrop, blockchain technology (BCT) has evolved from its cryptocurrency origins into an enterprise toolset offering append-only, consensus-verified records and programmable business logic (Cong & He, 2019; Pilkington, 2016). Recent empirical work in banking links BCT adoption with reductions in fraud-related costs and enhanced transaction security (Ahmed, 2025; Almadadha, 2025; Al-Dmour et al., 2024).

Conceptually, three BCT capabilities map tightly onto fraud-control pain points in Nigerian banking. First,

smart contracts encode preventive controls via multi-party approvals, time locks, exposure thresholds, so that exceptions and entitlements are enforced automatically, shrinking windows for human manipulation (Bassan, 2024; Cong & He, 2019). Second, permissioned distributed ledgers synchronize a single source of truth across authorized nodes, making post-hoc alteration conspicuous and raising the coalition size required for insider collusion (Tschorsch & Scheuermann, 2016). Third, secure digital wallets extend cryptographic identity and authentication to end-users and devices, mitigating credential replay and SIM-swap fraud vectors prevalent in the Nigerian retail context (NIBSS, 2024). These properties jointly target the "opportunity" and "capability" legs of the fraud diamond by reducing editability, discretion, and information asymmetry at control points.

The policy environment is also shifting. Nigerian authorities emphasize stronger reporting and collaborative defenses in e-payments (CBN, 2024). Internationally, tier-one banks are piloting blockchain-based payment and settlement rails with automated settlement and auditable histories, which show evidence that BCT's operational claims are becoming production-relevant (Reuters, 2025). In parallel, research synthesizing over a hundred studies finds a maturing consensus that BCT improves data integrity and compliance automation, while noting integration and governance challenges (Shi *et al.,* 2025). This external validation supports examining whether similar benefits are detectable, at least perceptually, in Nigerian DMBs.

Despite growing global evidence, rigorous bank-level analyses within Nigeria remain scarce, often focusing on cryptocurrencies rather than enterprise BCT. The majority of current blockchain research is focused on its application to cryptocurrencies such as Bitcoin, with only a small number of researchers investigating the use of Blockchain Innovation in other situations or segments. Blockchain innovation is more than just fair cryptocurrency; it has numerous applications in government, finance, banking, accounting, and business administration. Therefore, to fill the gap, this study explored and investigates its openings and challenges by examining the effect of blockchain technology on curbing fraudulent activities in Deposit Money Banks in Nigeria. The present study addresses this gap by: (i) operationalising BCT through three constructs (smart contracts, distributed ledger, and digital wallets) reflecting capabilities most plausibly connected to control enhancement; (ii) defining two outcome measures aligned to Nigeria's threat landscape, including spread of fraud (SOF) and internet fraud activities (IFA); and (iii) estimating interpretable models with reliability diagnostics and specification checks. By anchoring the measurement strategy in control-relevant mechanisms rather than generalised "blockchain awareness," the analysis better aligns with how DMBs actually deploy technology to mitigate fraud.

The contribution is threefold. First, the paper provides up-to-date sectoral context by situating Nigerian fraud exposure within documented trends in retail electronic channels (NIBSS, 2024) and supervisory expectations (CBN, 2024). Second, it ties micro-level BCT mechanisms to canonical economic and criminological theories: immutability and consensus reduce post-transaction opportunism; programmability turns policy into executable rules, thereby constraining agency problems (Cong & He, 2019). Third, it connects local findings to emerging international evidence that BCT adoption correlates with lower fraud and security costs in banking (Ahmed, 2025; Almadadha, 2025; Al-Dmour et al., 2024) and to compliance automation prospects around AML/KYC (Ogunrinde, 2025).

The main objective of the study is to examine the effect of blockchain technology on curbing fraudulent activities in deposit money bank in Nigeria. The specific objectives are to:

- evaluate blockchain technology effect on curbing spread of fraud in deposit money banks in Nigeria.
- assess blockchain technology effect on curbing internet fraud activities in deposit money banks in Nigeria

To achieve the specific objectives, the study hypothesized that:

$H_0$1: Blockchain technology plays no significant role in curbing spread of fraud in deposit money banks in Nigeria

$H_0$2: Blockchain technology plays no significant role in curbing internet fraud activities in deposit money banks in Nigeria.

We proceed as follows. Section 2 reviews the state of BCT, smart contracts, permissioned ledgers, and digital wallets, highlighting applications, risks, and Nigerian-specific considerations, and augments the empirical literature with recent banking studies. Section 3 details the research design, sampling across license categories, validity and reliability procedures, and model specifications. Section 4 presents result with robust checks and diagnostic tests. Section 5 interprets the findings in light of Nigeria's fraud

landscape and international pilots, and Section 6 outlines actionable recommendations for DMBs and policymakers, including permissioned-ledger pilots for high-risk workflows (dispute management, chargeback resolution, high-value transfers), wallet-level cryptographic controls, and smart-contract guardrails for entitlements and reconciliation. By evidencing significant negative associations between perceived BCT deployment and fraud outcomes, this study contributes Nigeria-specific, practitioner-relevant evidence to a fast-moving global conversation on hardening banking operations with blockchain.

2. Literature Review

2.1 Blockchain Technology: Overview, Applications, and Risks

Blockchain technology refers to append-only, consensus-validated ledgers that distribute verification across multiple nodes, reducing single points of failure and aligning incentives around a shared, tamper-evident record (Cong & He, 2019). In banking, permissioned implementations, rather than open, permissionless networks, dominate production pilots because they can enforce access control, privacy layers, and throughput guarantees needed for regulated financial intermediation. Beyond payments and settlements, banks increasingly explore blockchain for KYC/AML data-sharing, trade finance, collateral registries, and audit trails that support internal control testing (Ma, 2024; Al-Dmour et al., 2024). By enabling deterministic execution of rules and synchronized books-of-record, blockchain reduces reconciliation frictions and narrows windows in which fraudsters or insiders can manipulate states ex post. Empirical and review evidence in 2024–2025 reports associations between blockchain adoption and lower fraud risk or compliance costs through improved traceability, automated controls, and auditability (Al-Dmour et al., 2024; Ogunrinde, 2025; Guo, 2025).

Governance failures can re-centralize power (e.g., validator cartels) or weaken change-control; interoperability constraints can strand data; and legal enforceability of "smart legal contracts" is jurisdiction-dependent (Bassan, 2024). Privacy-preserving designs (e.g., proof systems that selectively reveal compliance-relevant properties) aim to balance transparency with data-protection mandates (Buterin et al., 2024). Operationally, throughput/latency trade-offs persist, though permissioned architectures mitigate many performance bottlenecks. For Nigerian DMBs, risks are as much organizational as technical: talent scarcity, vendor lock-in, and process misfit can blunt benefits even when pilots succeed technologically. Still, the direction of travel is clear: where processes require shared truth and automated exception-handling, permissioned BCT can credibly harden controls and lower the expected value of fraud. This framing extends your manuscript's baseline account of BCT while updating applications/risks with current banking evidence.

2.1.1 Smart Contracts: A Revolutionary Application

Smart contracts encode business logic that executes when pre-specified states or events are verified on-chain, eliminating manual handoffs and lowering discretion at control points (Cong & He, 2019). In retail and corporate banking, such logic can enforce multi-factor approvals for high-risk actions (e.g., beneficiary changes, bulk-payment releases), implement time-locks and exposure caps, and trigger enhanced due-diligence workflows before settlement, controls that are otherwise vulnerable to social engineering or insider override. Recent empirical studies underscore both promise and limits. On the upside, studies report improved control effectiveness and auditability when BCT underpins process execution, with observable reductions in exception rates and reconciliation breaks (Ma, 2024; Ogunrinde, 2025). On the downside, oracles and off-chain dependencies introduce new attack surfaces, and contract immutability can ossify defects without robust upgrade paths (Bassan, 2024). Privacy-enhancing designs such as "Privacy Pools" propose selective disclosure to satisfy AML/CFT requirements while preserving user confidentiality (Buterin et al., 2024).

For Nigerian DMBs, the relevance is practical: encode exception-handling for disputed transfers; implement rule-based disbursement for loan proceeds contingent on verified milestones; and automate sanctions/KYC screens prior to value movement. In principle, these features counteract two legs of the fraud diamond (opportunity and capability) by constraining editability and shrinking windows for collusion. This subsection refines the discussion already present in your manuscript by tying smart-contract mechanisms to specific fraud-control scenarios common to Nigerian channels.

2.1.2 Distributed Ledger Technology (DLT): Decentralization and Security

Distributed ledgers maintain synchronised records across authorized nodes, making unilateral alteration conspicuous and raising the coalition size required for insider fraud. In permissioned banking deployments,

consensus mechanisms are calibrated for finality and throughput (e.g., PBFT-style variants), while access layers segment read/write privileges to align with bank secrecy laws. Empirical banking research indicates that DLT can reduce settlement times, lower reconciliation effort, and produce auditable histories that deter post-hoc manipulation, mechanisms tightly linked to fraud-loss reduction (Al-Dmour et al., 2024). Complementary evidence from internal-control studies shows BaaS architectures improving logging integrity and control-testing efficiency (Ma, 2024). Where DLT undergoes interbank workflows (e.g., trade finance), programmable checks and shared state reduce duplicate financing and document fraud.

Nevertheless, decentralisation is not a panacea. Poor key management, weak node governance, or misaligned incentives can reintroduce central points of failure. Interoperability with core banking systems and payment gateways remains a major integration cost. For Nigerian DMBs, consortium governance and regulator-observer nodes can mitigate coordination risks while preserving auditability. The balance of current evidence suggests that well-governed permissioned DLTs, rather than public chains, are the pragmatic route for regulated institutions seeking fraud-resilient operations. This expands and updates your manuscript's foundation on DLT's role in decentralization and security.

2.1.3 Digital Wallets: Enhancing Blockchain Usability

Digital wallets operationalize cryptographic identity and authorization. Properly implemented, they embed strong credential protection (e.g., hardware-backed keys, secure enclaves), multi-factor prompts, and transaction-signing that binds intent to device and user. In the Nigerian retail context, wallet security directly intersects with high-incidence fraud vectors such as SIM-swap and social-engineering attacks. Regional and continental threat assessments from 2024–2025 document rising SIM-swap prevalence and its role in account takeovers; risk is amplified where USSD-based journeys and weak KYC controls persist (INTERPOL, 2025; Regulation Innovation, 2024). Wallet hardening, FIDO-class authenticators, number-binding, and biometric re-verification for sensitive actions, reduces the expected payoff of credential-theft attacks by making step-up friction unavoidable at high-risk moments.

Empirically, digital-identity enhancements combined with behavioral analytics have been associated with significant drops in mobile-channel fraud in African pilots, though equity risks (e.g., biometric failure rates) must be managed (GSMA/SSRN syntheses, 2024–2025). For banks piloting blockchain rails, wallets provide the user-facing boundary where private keys authorize rule-bound transfers; thus, wallet design is inseparable from control design. This subsection anchors your original emphasis on wallets while integrating up-to-date regional fraud patterns and mitigation evidence salient for Nigerian DMBs.

2.1.4 Blockchain's Potential in Nigeria

In Nigeria, blockchain technology, especially in cryptocurrencies, has sparked debates about its economic implications. Bitcoin and other digital currencies are seen as tools for financial recovery and investment opportunities. Blockchain's transparent and secure systems also hold promise for addressing fraud and inefficiencies in financial transactions (Mehedi, 2021). Blockchain technology can transform various sectors by enabling decentralized, secure, and efficient systems. For example, digital wallets and smart contracts can streamline financial services, enhance contract management, and improve overall trust in digital transactions (Hodge, 2020; Kshetri, 2018). However, the adoption of blockchain in Nigeria requires addressing regulatory challenges, technological barriers, and public awareness to realize its full potential.

Nigeria's accelerating digitization has expanded the payments surface and, with it, fraud externalities. The NIBSS 2023 fraud landscape shows sharp rises in losses through certain e-channels and highlights organized social-engineering schemes; ATM fraud fell, but internet-banking losses spiked, underscoring that risk migrates across rails as controls harden unevenly (NIBSS, 2024). Supervisory messaging in 2024 emphasised collaborative defences and continuous innovation in the payment system (CBN, 2024). Within this environment, blockchain's most credible near-term value is not speculative crypto exposure but permissioned, bank-regulated deployments that: (i) encode entitlements and exception rules, (ii) synchronize tamper-evident records across counterparties, and (iii) strengthen identity-to-transaction binding via hardened wallets.

Barriers such as skill gaps, integration cost, absence of shared utilities (e.g., KYC registries), and questions of legal enforceability for code-as-contract. Yet international pilots demonstrate feasibility for payment, settlement, and trade-finance use cases with reported reductions in reconciliation effort and fraud risk, evidence that can inform Nigerian pilots under regulatory sandboxes. Strategically, DMBs can target high-loss workflows first (internet-banking dispute management, card-not-present chargebacks, corporate

bulk transfers) and measure marginal fraud-loss reductions against deployment costs. This subsection faithfully extends your Nigeria-specific framing while grounding it in current statistics and policy signals.

Nigeria's rapid adoption of digital payments coincides with high cyber fraud exposure (Ololade et al., 2020). BCT's transparency and programmability offer credible pathways to mitigate SIM swap misuse, mule networks, and credential stuffing by hardening identity and enforcing rule-based controls. Yet uptake hinges on regulatory clarity, interoperability with core banking, and human capital readiness. Conclusively, blockchain technology, with its transformative applications like cryptocurrencies, smart contracts, and digital wallets, is reshaping industries by providing decentralized, secure, and transparent solutions. While its potential to revolutionize sectors is undeniable, challenges such as scaling, regulatory oversight, and technical risks must be addressed. In Nigeria and beyond, leveraging blockchain's benefits requires strategic adoption and a commitment to overcoming its limitations.

2.2 Curbing Fraudulent Activities

Classic frameworks, the fraud triangle and its "fraud diamond" extension, locate misconduct at the intersection of pressure/incentive, opportunity, rationalization, and capability. Digital banking in Nigeria intensifies pressure (economic stressors), lowers discovery costs for capable actors (phishing kits, SIM-swap facilitation), and, when controls lag, expands opportunity. Effective counter-fraud therefore prioritizes shrinking opportunities and limiting capabilities without unduly degrading user experience. Blockchain capabilities map directly onto these levers.

Opportunity reduction through immutability and shared state. Permissioned ledgers create an append-only, time-stamped event history visible to authorized parties. For internal fraud, this increases the coalition size required for tampering and makes unauthorized post-hoc edits conspicuous. For external fraud, immutable trails facilitate faster dispute adjudication and recovery by clarifying provenance (who authorized what, when, under which rules). Empirical banking studies in 2024–2025 report that DLT adoption reduces reconciliation breaks and supports stronger control-testing, mechanisms linked to lower fraud-related costs (Al-Dmour et al., 2024; Ma, 2024).

Capability constraints via programmable controls. Smart contracts translate policy into executable code, multi-party approvals, velocity limits, geofenced authorizations, so that high-risk actions require cryptographic concurrence. This compresses the "window of malfeasance" and limits insider override. Reviews and empirical work highlight reductions in manual exception handling and improved auditability when rules are encoded rather than merely documented (Ogunrinde, 2025; Guo, 2025). Legal-tech analyses caution that contract upgradability and oracle design are critical to avoid freezing defects into production (Bassan, 2024).

Identity hardening at the wallet edge. Since most Nigerian fraud losses manifest through retail channels with identity takeovers, wallet controls, including secure key storage, device binding, and step-up authentication, are decisive. Regional assessments show SIM-swap and social-engineering as dominant tactics, implying that controls must bind authorization to verified user-device pairs and trigger adaptive challenges for unusual behavior (INTERPOL, 2025; Regulation Innovation, 2024). Wallets can also embed consent receipts and transaction-purpose attestations that improve dispute resolution. Data-sharing and AML/KYC compliance. Fraud and AML risks overlap; proceeds of fraud flow through mule accounts, and weak KYC allows account proliferation. Blockchain-based KYC utilities and privacy-preserving disclosure protocols enable cross-institution verification without centralized honeypots. Recent work argues that shared ledgers and selective disclosure can streamline monitoring and raise detection precision, though they do not obviate regulatory obligations (Hafe & colleagues, 2025; AML/CFT analyses, 2024–2025).

Implications for Nigerian DMBs. Given NIBSS-documented spikes in internet-banking losses in 2023, banks should prioritize internet-channel entitlements and onboarding flows for BCT augmentation (NIBSS, 2024). Pilot roadmaps can adopt three horizons: (1) Control-layer pilots, encode approval chains and velocity limits for high-risk payments; (2) Data-layer pilots, permissioned ledgers for dispute management and chargeback evidence, integrating with existing core systems; (3) Identity-layer pilots—wallet hardening and number-binding to counter SIM-swap. Across horizons, independent model validation and adversarial testing (red-team simulations) should precede scale-up. These recommendations extend your manuscript's fraud-mitigation logic while anchoring it in current empirical and supervisory signals.

2.2.1 Spread of Fraud

"Spread of fraud" captures diffusion across channels, products, and customer segments. Nigerian data show

risk migration: as ATM and some web modalities harden, losses concentrate in internet-banking incidents and social-engineering-enabled takeovers (NIBSS, 2024). Containment therefore requires both lateral barriers (so compromises in one channel cannot be replayed in others) and vertical barriers (so a single compromise cannot escalate from low- to high-privilege actions). Lateral barriers with shared ledgers. Permissioned DLTs can synchronize interdiction states (e.g., device ban-lists, mule-account indicators) across channels and counterparties with strong proof. When a bank flags a beneficiary as associated with fraud, a consortium ledger can propagate this state, subject to due-process guardrails, so other participants adjust risk scoring. Studies in 2024–2025 emphasize the compliance and fraud-prevention benefits of shared, verifiable provenance that reduces duplicate financing and cross-institution exploits (Al-Dmour et al., 2024; Ma, 2024).

Vertical barriers with smart-contract entitlements, including encoding entitlements, prevent privilege escalation: new device registrations, profile changes, or high-value transfers require threshold signatures or time-locks. For corporate bulk payments, a Nigerian hotspot given large ticket sizes, contracts can enforce per-beneficiary and per-batch limits and require co-signers from separate departments. Reviews and empirical syntheses indicate that such rule-binding reduces error/fraud incidence and improves ex-post traceability for audit (Ogunrinde, 2025; Guo, 2025). Wallet-centric identity controls to slow diffusion through SIM-swap and phishing expand fraud's "spread" by enabling credential portability. Evidence from African pilots shows large fraud reductions when biometric re-verification is required for sensitive actions and when behavioral analytics gate anomalous sessions (SSRN/GSMA syntheses, 2024–2025). For Nigeria, where USSD remains salient, number-binding and transaction-signing, so authorization is cryptographically tied to a specific device key, reduce replay risk even after phone-number compromise (INTERPOL, 2025; Regulation Innovation, 2024).

Measurement and expected effects. Your study's SOF construct (and composite CFA index) can be interpreted as capturing these containment mechanisms: if BCT deployment compresses successful replay across channels and raises the coalition size for inside jobs, perceived SOF should fall. This interpretation is consistent with your empirical results showing significant negative associations between BCT dimensions and fraud outcomes.

2.2.2 Internet Fraud Activities (IFA)

Nigeria's internet-banking fraud losses rose sharply in 2023, driven by credential theft, session hijacking, and insider-enabled exploits; a single large internal incident amplified the aggregate loss picture (NIBSS, 2024). In this domain, blockchain's most actionable levers are (i) programmable pre-settlement checks (smart-contract-enforced sanctions/KYC screens and velocity limits), (ii) immutable evidence (tamper-evident event chains for rapid dispute resolution), and (iii) wallet hardening (private-key protection, device binding, and adaptive authentication). AML-aligned designs enable selective disclosure to satisfy monitoring mandates without over-exposing personal data (Hafe et al., 2025). Empirical finance and information-systems studies report that banks adopting DLT-backed settlement or control layers experience lower exception rates and fewer fraud opportunities due to synchronized state and automated entitlements (Al-Dmour et al., 2024; Ma, 2024). While causality is hard to prove outside controlled pilots, converging evidence and mechanism plausibility support your study's findings that higher perceived deployment of smart contracts, distributed ledgers, and hardened wallets is associated with lower IFA.

2.3 Theoretical Framework

The researcher based the work on the new growth theory and fraud diamond. The new growth theory is concerned with the relationship between the growth of the economy and the growth of information and knowledge. The essential point of new growth theory is that knowledge drives growth. The major assumptions of new growth theory are that technological progress is a product of economic activity whereas previous theories treated technology as a product of non-market forces. While the fraud diamond, is an extension of the fraud triangle theory to include the capability element of the fraudster. Fraud diamond states that if all four components are present, unshakable capacity, perceived opportunity, incentive and rationalization, a person is highly likely to pursue fraudulent activities.

To deepen the theoretical grounding, we juxtapose blockchain's core properties with canonical fraud theories. Immutability constrains post transaction opportunism by making alterations conspicuous in the shared history, thereby heightening perceived detection and diminishing rationalisation (Taylor et al., 2014). Consensus protocols distribute verification across nodes, approximating separation of duties; no single insider can unilaterally rewrite history without collusion, which raises the minimum coalition size and

coordination costs for fraud (Mainelli & Smith, 2015; Tschorsch & Scheuermann, 2016). Programmability via smart contracts codifies preventive controls—authorization limits, time locks, or multi factor conditions, transforming informal policies into executable rules (Cong & He, 2019). Empirical literature, albeit heterogeneous, increasingly reports integrity gains: supply chain trials show fewer discrepancies and faster exception resolution (Saberi et al., 2019; Kamilaris et al., 2019), trade finance pilots reduce document fraud via shared state and digitised guarantees (Bogucharskov, 2018; Eyers, 2020), and cybersecurity studies leverage blockchain anchored logs for forensic assurance (Chikelue, 2020).

We note implementation risks, a key mismanagement, privacy leakage, and vendor lock in that, if unaddressed, can reintroduce vulnerabilities (Zheng et al., 2017; Chauhan, 2018). For financial institutions, permissioned DLT with granular roles and privacy overlays (e.g., channels, zero knowledge proofs) is often preferable to permissionless designs because it satisfies confidentiality mandates while preserving shared provenance (Risius & Spohrer, 2017). Nigerian banking presents a high value laboratory: pervasive mobile payments, elevated phishing and SIM swap attacks, and growing regulator interest in digital identity. Yet rigorous bank level studies remain scarce. This lacuna motivates the operationalised constructs, such as smart contracts, DLT, and digital wallets and outcome measures, including SOF and IFA, selected to reflect control points where blockchain's marginal impact is most plausible.

This study is anchored in three complementary lenses vis-a-vis fraud triangle/diamond, principal–agent theory, and information asymmetry, that jointly explain why digital banking is vulnerable to misconduct and how enterprise blockchain capabilities could suppress that vulnerability. According to fraud triangle/diamond theories, Cressey's classic formulation posits that fraud emerges when pressure and opportunity coincide and offenders rationalize their actions; the "fraud diamond" adds capability as a fourth condition (Cressey, 1953; Wolfe & Hermanson, 2004; Mainelli & Smith, 2015). In Nigerian retail and internet banking, macroeconomic stressors elevate pressure, while credential replay, weak device binding, and manual entitlements present opportunity and require modest technical capability. The three blockchain capabilities map tightly onto the opportunity–capability axis. Permissioned distributed ledgers harden records ex post by making alteration conspicuous and multi-party, thus raising the coalition size for successful manipulation (Tschorsch & Scheuermann, 2016). Smart contracts shrink discretionary windows and human overrides by turning policy into executable rules (e.g., velocity limits, time locks, co-signing thresholds). Secure digital wallets constrain capability at the edge by binding authorization to devices and private keys and forcing step-up authentication for high-risk actions. If these mechanisms work as intended, the expected utility of fraud falls because both the probability of success and the probability of escaping detection decline (Cressey, 1953; Wolfe & Hermanson, 2004).

Agency theory formalises how misaligned incentives and imperfect monitoring generate agency costs (Jensen & Meckling, 1976). In banking, clients (principals) rely on banks (agents) to process payments truthfully; within banks, managers (principals) rely on staff (agents) to administer entitlements and resolve disputes. Two agency frictions are salient: (i) moral hazard—agents may exploit private discretion in low-visibility steps; and (ii) monitoring and bonding costs—principals must invest in controls and audits (Saberi et al., 2019; Kamilaris et al., 2019). Permissioned ledgers reduce the scope for hidden action by synchronizing an append-only "book of record" across authorized nodes, and smart contracts curtail opportunistic deviations by executing rule-bound steps deterministically (Jensen & Meckling, 1976; Cong & He, 2019). Wallet-level cryptographic identity is a bonding device: transactions require the customer (or authorized staff device) to present verifiable proof of intent. Taken together, blockchain capabilities are predicted to reduce agency costs by compressing informational slack and converting discretionary checkpoints into verifiable, auditable events.

In addition, Akerlof (1970) shows that when one side holds private information, adverse selection and moral hazard can unravel market quality. In digital payments, counterparties and intermediaries observe different slices of truth (device state, KYC quality, sanctions status), creating room for both *ex-ante* selection of risky relationships and ex post manipulation of logs. Permissioned DLT and standardized event schemas reduce asymmetry by producing a tamper-evident, time-stamped trail that multiple parties can verify, while privacy-preserving proofs enable selective disclosure of compliance properties (Akerlof, 1970; Buterin et al., 2024). In principle, this shifts the environment from "hidden" to "constrained" information, improving screening and reducing disputes.

Combining these lenses yields testable predictions aligned with the constructs and outcomes: Higher perceived deployment of smart contracts will be associated with lower SOF and IFA, because

programmable approvals, velocity limits, and pre-settlement checks reduce exploitable discretion (Cong & He, 2019). Also, higher perceived deployment of permissioned ledgers will be associated with lower SOF and IFA, as shared, immutable state improves monitoring and deters post-hoc edits (Al-Dmour et al., 2024), while higher perceived deployment of secure digital wallets will be associated with lower SOF and IFA, as device binding, private-key control, and adaptive authentication suppress account-takeover vectors common in Nigeria. Lastly, a composite BCT index will negatively relate to fraud outcomes because simultaneous improvements in process integrity, record immutability, and identity assurance are complementary, not additive (Ahmed, 2025; Almadadha, 2025). These propositions connect criminological and micro-contracting theory to concrete control technologies that Nigerian DMBs can pilot under existing regulation. They also rationalize why perceptual measures of BCT deployment (as used in your instrument) should correlate with bankers' assessments of fraud exposure: the mechanisms are salient to day-to-day workflows in internet banking, dispute management, and high-value transfers.

2.4 Empirical Review of Literature

2.4.1 Blockchain Technology and Spread of Fraud

Vivekanadam, (2020) examined blockchain as a computerized record in which each record known as squares are combined in a single list known as a chain. It is respected as Bitcoin's spine innovation. It is additionally respected as cohesive collections of digital wallets. Blockchains are basically utilized by cryptocurrencies such as Bitcoin and other applications to record these exchanges. A blockchain is commonly alluded to as a collection of dispersed databases that comprises of all open exchanges, records and advanced occasions at that point that data is shared among the members. Each exchange is confirmed and it cannot be evacuated. The blockchain can be utilized for trading the exchange safely without a middleman. It empowers client relationships and supply chain values and, subsequently, coordination with IoT and Cloud innovation. The usefulness of disseminated record is combined with blockchain security to illuminate the money related and non-financial industry issues. The paper proposes blockchain technology with gadgets and creates a common stage for secure information communication.

Chikelue*et al*. (2020) sought to investigate the appropriation of Blockchain technology for the cyber security of developing market multinational organizations (EMNCs) with a diagram of Nigerian internationalized banks. Auxiliary information from the Web Crime Complaint Center, Proshare, and Africa's cybersecurity report were examined and talked about. Based on the information obtained, it was concluded that Blockchain technology will make cybercrime prohibitively expensive for perpetrators, thereby immobilizing cyber hoodlums. The study becomes instrumental for rising market multinational organizations (EMNCs) by recommending arrangements for cybercrime challenges. The suggestion of the consider is that execution will move forward for Nigerian banks ought to they embrace Blockchain technology for cyber security. It'll drive development through the minimization of cybercrime misfortunes and reposition the banks to be deliberately competitive with developed banks within the industry. This encourages the modern development hypothesis.

Mehedi, (2021) investigated the effects of blockchain technology on universal exchange and discovered how blockchain technology can progress the different area s of universal exchange. The research also aims to discover the challenges with respect to the execution of blockchain technology in worldwide exchange to assist companies accomplish effective collaboration and understand what prerequisites must be met to make progress. The study's findings secured the fundamentals of blockchain technology; blockchain's role in encouraging supply chain and exchange funds; the impact and selection of blockchain technology; and the key challenges of blockchain implementation. A subjective approach was utilized based on 12 semi-structured in-depth interviews with ten companies working in completely different commerce areas and two blockchain master's to get experimental information.

Moreover, a few proposals with respect to the large-scale usage of blockchain in exchange funds were displayed. The discoveries of the research have upgraded the current level of inquire about the connection between blockchain technology and universal exchange, and the investigation of different application regions perm its analysts to conduct an in-depth investigation of blockchain pertinence in numerous trade environment s. The experimental discoveries will aid companies in

creating their selection procedures and planning to ex ecute the innovation within the exchange handle.

In their research, Kiu *et al.* (2019) expressed that Blockchain Technology has been broadly investigated and ceaselessly revolutioni zing numerous divisions around the world, counting the development industry. The development industry requires blockchain technology to make strides against the current restriction of centralized technology in its different venture life cycles. Within the paper, we displayed a writing audit, pointing to the possibilities of Blockchain applications in the development industry. The paper also surveyed the special highlights of the blockchain technology, which trigger its capabilities in the development industry. The paper advanced investigated the blockchain application suggestions if they were received in the development industry. In brief, blockchain innovation is still moderately modern in the development industry and requires profound research to create a genuine life-on-hand application for the development industry soon.

Gul (2021) considered the impacts of blockchain technology on the environment, economy, and society, which are the three fundamental zones of maintainable advancement. It can be said that blockchain technology has both positive and negative impacts on these three fundamental ranges. Giving the opportunity to build collective esteem and support social impact ventures with a focus on sustainable society, innovation also empowers majority rule information administration. Blockchain technology has the potential to expand budgetary consideration by allowing the improvement of unused commerce models with a focus on sustainable economy. Whereas blockchains working with a proof-of-work strategy have the potential to hurt the environment with their high vitality utilization, blockchains working with distinctive strategies can decrease vitality utiliza tion. Simultaneously, it is anticipated that the negative impacts of this innovation on the feasible environment can be eliminated with the use of renewable vitality assets in mining.

2.4.2 Blockchain Technology and Internet fraud Activities

Together with the mindfulness of the 51% assault, investigated by Eyal and Sirer (2014), it appears that it is conceivable for miners to pick up income by having as if it were 25% computing control. Usually what they call "selfish mining attacks." The thought behind it is that rather than broadcasting to the organization after mining the squares, the "selfish miners" keep the found squares private with the expectation of inevitably forking the chain. Whereas the genuine hubs keep mining on the open chain, the childish diggers keep working on mining modern squares and keeping the pieces to themselves. Reyna et al. (2018) state that blockchain seems to enhance the IoT with its transparent feature, which makes it simpler to follow back exercises, in this way improving security. Furthermore, a decentralized peer-to-peer IoT framework is expected to enable better control of IoT administrations to keep track of the data stream, comprehend the issue related to high support costs caused by centralized frameworks, and enable the robotized handling of merchandise and administrations (Casino, 2019).

Blockchain can also move forward a few segments of the IoT, such as a modern IoT E-business show proposed by Zhang et al. (2015) in which commerce forms can be moved to the blockchain, coming about in conveyed independent organizations where trade capacities are robotized and supplant human performing artists (Zhang et al., 2015; Zheng et al., 2018). IBM and Samsung also employ its verification of concept for Independent Decentralized Peer-to-Peer Telemetry, which permits smart-home proprietors to distinguish operational issues and upgrade the computer program by themselves (Zheng et al., 2017; IBM & Samsung, 2015). Iansiti and Lakhani (2017) compare blockchain to TCP/IP, proposing that blockchain has the potential to be the spine of the IoT.

Recently, empirical evidence on enterprise blockchain in banking has shifted from conceptual to measurement-based studies, with several findings relevant to fraud exposure and control effectiveness. In multi-bank samples, Al-Dmour et al. (2024) report positive associations between blockchain applications and commercial bank performance, attributing part of the effect to improved data integrity, traceability, and control automation that lower exception handling and dispute costs. Ahmed (2025) quantifies cost channels in banking transactions and finds that blockchain adoption significantly reduces processing, transfer, and fraud costs, evidence consistent with opportunity-reducing mechanisms. Almadadha (2025) shows that Australian banks adopting blockchain post higher ROA/ROE, consistent with operational efficiencies; although profitability is a broad outcome, authors trace

gains to reconciliation and error-reduction effects that also underpin fraud mitigation. Ma et al. (2024) (accounting/control setting) find that BaaS-enabled internal controls improve logging integrity and control-testing efficiency, again pointing to the same channels, immutability and synchronized state, that your study investigates.

In process-specific studies, for instance trade finance, where duplicate invoicing and document forgery are endemic, recent reviews and pilots indicate that DLT reduces processing times and fraud risk by anchoring documents and events on a shared ledger with programmable checks (Mazumder, 2025). Supervisory and standard-setting bodies similarly emphasize that tokenization and DLT can increase transparency and auditability across clearing and settlement, while cautioning that benefits need careful validation (FSB, 2024; BIS, 2025). These findings speak to your SOF construct: as provenance is standardized and shared, fraud has fewer paths to spread across products and counterparties. On the edge of the system, wallet design determines whether authorization can be replayed or hijacked. Regional cyber-threat assessments and policy reports for Africa (2024–2025) document SIM-swap and social-engineering as dominant takeover paths; strengthened device binding, biometric step-ups for sensitive actions, and number binding materially reduce successful attacks, precisely the elements embodied in secure wallet deployments (e.g., FIDO-class authenticators) (INTERPOL, 2025). Although not solely blockchain-dependent, wallets are the user-facing boundary of permissioned blockchain rails; thus, cryptographic keys and intent proofs provide a stronger evidentiary basis in disputes, which matters directly for IFA (internet banking fraud) and chargebacks.

In Nigeria-specific context,sectoral statistics for 2023 compiled by the Nigerian Inter-Bank Settlement System (NIBSS) show pronounced shifts of fraud losses toward internet-banking channels, underscoring that hardening card/ATM rails displaces rather than eliminates risk (NIBSS, 2024). Consumer-side survey evidence in 2024 (IPA Nigeria) indicates high exposure to scam attempts but lower self-reported realized losses, consistent with partial control improvements yet persistent social-engineering pressure (IPA, 2024). These patterns motivate a focus on internet-banking entitlements and dispute-resolution processes where permissioned ledgers, and smart contracts can change the payoff calculus by (i) encoding approvals and pre-settlement checks; and (ii) creating tamper-evident evidentiary trails for rapid adjudication.

However, international policy reviews emphasize that while DLT promises better transparency and integrity, net benefits are context-dependent: governance quality, interoperability with core systems, and privacy-preserving compliance determine whether fraud falls (FSB, 2024; Buterin et al., 2024). Legal enforceability of smart-contract outcomes, upgradability patterns, and oracle design remain critical to avoid ossifying defects (Bassan, 2024). These conditions explain heterogeneous effects across banks and countries and reinforce the value of Nigeria-specific measurement, as undertaken in your study.

Across settings, results converge on a mechanism narrative: where blockchain functions as (i) a shared, tamper-evident record, (ii) a rule-execution layer for high-risk entitlements, and (iii) a cryptographic identity boundary at the wallet/device, banks report fewer reconciliation breaks, faster dispute resolution, and lower fraud-related costs. The finding that perceived deployment of smart contracts, permissioned ledgers, and secure wallets correlates negatively with SOF and IFA aligns with those mechanisms. It also fits agency and asymmetry predictions: less discretionary slack and more verifiable information imply fewer profitable fraud opportunities.

3. Research Methods and Procedure

3.1 Research design and setting

This study employs a cross-sectional, explanatory design to examine whether the perceived deployment of three blockchain technology (BCT) capabilities, smart contracts, permissioned distributed ledgers, and secure digital wallets, is associated with two fraud outcomes in Nigerian deposit money banks (DMBs): spread of fraud (SOF) and internet fraud activities (IFA). The design is appropriate because the objective is to test directional propositions derived from the fraud triangle/diamond, principal–agent theory, and information-asymmetry arguments, using bank-level perceptions as proximal measures of control intensity and fraud exposure. Cross-sectional surveys are widely used in internal control, information systems, and financial-intermediation research when construction (deployment breadth, perceived exposure) is latent, context-dependent, and difficult to observe directly (Hair et al., 2019; Kline, 2016). To discipline inference, the analysis incorporates comprehensive measurement validity checks, econometric diagnostics, and robustness analyses recommended for survey-based models (Podsakoff et al., 2003; Wooldridge, 2010).

On ethical grounds, the study adhered to ethical research norms, including voluntary participation, informed consent, anonymisation, and secure storage of de-identified data accessible only to the research team. No operational secrets, customer data, or personal identifiable information were collected. Reporting aggregates results to avoid re-identification risk. These safeguards align with professional standards for research in financial institutions.

3.2 Population, sampling, and data collection

The target population consists of employees of licensed Nigerian DMBs across international, national, and regional authorization categories. Consistent with sectoral heterogeneity, we sampled across core control-relevant functions, operations, e-channels, internal audit, risk/compliance, information security, and retail/corporate banking, so that responses reflect diverse vantage points in the fraud-control workflow. Stratification by license class and function improved coverage and mitigated single-bank or single-unit idiosyncrasies (Hair et al., 2019). Eligible respondents were mid- to senior-level staff with role responsibility or line-of-sight over payments, controls, or fraud case management. Data collection used a self-administered questionnaire with informed consent, anonymity assurances, and no personally identifiable information. Procedural remedies against common method bias (CMB) included: separating predictors and outcomes in the instrument; varying response formats; assuring respondents of no right/wrong answers; and positioning sensitive fraud-outcome items after less sensitive BCT items to reduce evaluation apprehension (Podsakoff *et al.,* 2003).

3.3 Validity and Reliability Tests

The reliability of the instrument was done through the test-retest method. That is to say, the instrument was pre-tested twice before proceeding to administer the instrument to the respondents.Construct validity was assessed via a two-stage approach. First, exploratory factor analysis (EFA) verified expected dimensionality. Second, confirmatory factor analysis (CFA) tested a three-factor BCT model and a two-factor outcomes model. Convergent validity requires standardized loadings ≥ .50 and average variance extracted (AVE) ≥ .50; reliability requires Cronbach's α and composite reliability (CR) ≥ .70 (Hair et al., 2019; Kline, 2016). Discriminant validity was evaluated via HTMT (threshold < .85–.90) and Fornell–Larcker criteria (AVE greater than squared inter-construct correlations). Model fit was judged using χ^2/df, CFI/TLI ≥ .90, RMSEA ≤ .08, and SRMR ≤ .08 (Kline, 2016). Item deletion was conservative, and theory guided.

On reliability regression testing using SPSS, the Cronbach's alpha value wasobtained. Table1 shows that the variables have high internal consistency which shows that the responses attached to each variable of interest are good for analyses.

Table 1: Reliability of the Blockchain Technology Questionnaires

Variable	Cronbach Alpha	Internal Consistency
Smart Contract	0.86	Excellent
Distributed Ledger	0.82	Excellent
Digital Wallet	0.91	Excellent
Spread of Fraud	0.73	Excellent
Internet Fraud	0.80	Excellent

Source: *Authors' Compilation*

Researcher's Conceptual Model

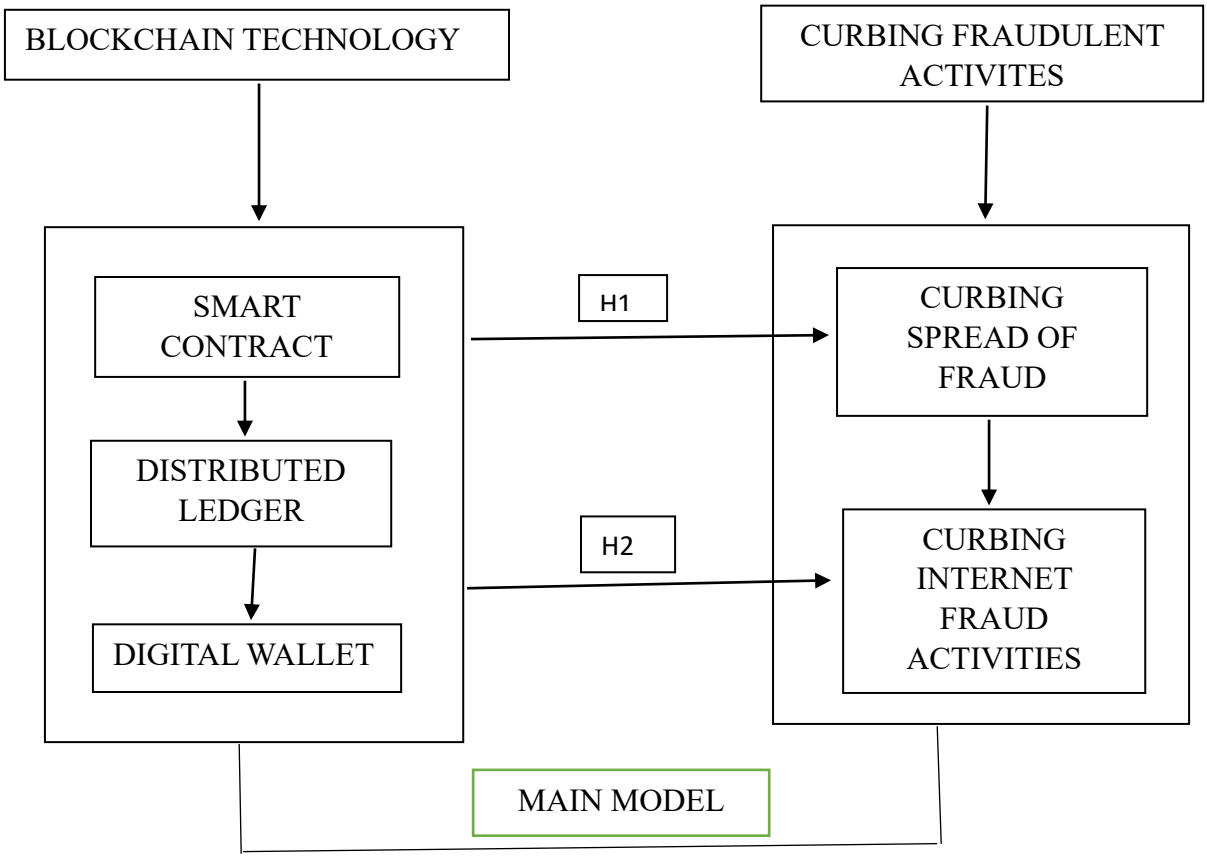

Figure 1: Conceptual Model, 2023

3.3 Model Specifications and Data Issues

Following the fraud triangle hypothesis, the baseline models to achieve the stated objectives are specified below:

$$Y_i = \beta_0 + \beta_1 X_{1i} + \beta_2 X_{2i} + \beta_3 X_{3i} + \varepsilon_i \quad 1$$

Where Y, the Dependent Variable (Curbing Fraudulent Activities) is a 3*1 vector of dependent variable such as Curbing Fraudulent Activities (CFA), which is also proxied with Spread of Fraud (SOF) and Activities of Internet Fraud (IFA). The models are written explicitly in Equation 2-4:

$$SOF_i = \beta_0 + \beta_1 SMC_i + \beta_2 DIL_i + \beta_3 DIW_i + \varepsilon_i \quad 2$$

$$IFA_i = \beta_0 + \beta_1 SMC_i + \beta_2 DIL_i + \beta_3 DIW_i + \varepsilon_i \quad 3$$

$$CFA_i = \beta_0 + \beta_1 SMC_i + \beta_2 DIL_i + \beta_3 DIW_i + \varepsilon_i \quad 4$$

Where X is the Independent Variable (Blockchain Technology); β_0= Value of the Intercept; $\beta_1, \beta_2, \beta_3$= Coefficient of explanatory variables; and ε = Error Term. $i$is the Number of Sampled DMBs. The independent variable is Blockchain Technology (BTC) represented with Smart Contract (SMC), Distributed Ledger (DIL) and Digital Wallet (DIW). We expect the coefficients to be positive in Equation 1 to 4 ($\beta_{1\text{-}3} > 0$) as the *a priori* expectations.The study estimated Equation 2-4 via OLS because outcomes are measured on quasi-continuous Likert scales (averaged across multiple items), for which OLS yields unbiased and efficient estimates under standard conditions; coefficient interpretation is transparent and comparable across specifications (Wooldridge, 2010). To guard against assumption violations, we compute heteroskedasticity-robust (Huber–White) standard errors (White, 1980). Because multicollinearity can inflate variance when technology dimensions co-move, we examine variance inflation factors (VIF) and tolerances, and center predictors.

4. Results and Discussion

For estimation, we standardised predictors to facilitate coefficient comparability. OLS models were chosen

for interpretability given the continuous Likert type indices aggregated at scale level; as a sensitivity check we replicated results using robust standard errors and median regressions, yielding consistent signs and significance. Multicollinearity diagnostics (VIF < 5) indicated acceptable independence. We addressed common method variance via procedural remedies (assured anonymity, separated predictor/outcome sections) and the Harman single factor test, which did not indicate dominance by a single factor. Although causal identification is beyond scope, we discuss threats, omitted variable bias (e.g., broader digital maturity), reverse causality (banks with less fraud invest more/less in BCT), and measurement error, and interpret estimates accordingly. Ethical approval was obtained from the relevant institutional review committee; participation was voluntary and non-remunerated.

The descriptive statistics of the study variables are presented in Table 2. It showed that the minimum of 1, maximum value of 5, Mean of 4.08 and Standard Deviation of 1.13 for Smart Contract. Minimum of 1, mean of 5, maximum of 4.16 and Standard Deviation of 1.04 for Distributed Ledger. While Digital Wallet ranges from minimum of 1 to maximum of 5, mean of 4.28 and standard deviation of 0.98. Spread of fraud range from minimum of 1, mean of 4.13, maximum of 5 and standard deviation of 0.99. Internet fraud activities range from minimum of 1 to maximum of 5, mean of 4.30 and standards deviation of 0.98. All the results revealed that all the variables follow a normal distribution.

Table 2: Descriptive Statistics of Variable of Interest.

Variables	Num	Minimum	Maximum	Mean	Standard Deviation
Smart Contract	120	1	5	4.08	1.13
Distributed Ledger	120	1	5	4.16	1.04
Digital Wallet	120	1	5	4.28	0.98
Spread of fraud	120	1	5	4.13	0.99
Internet fraud Activities	120	1	5	4.30	0.98

Source: *Author Compilation*

Test of Hypotheses

H_{01}: Blockchain technology does not play significant role in curbing spread of fraud in deposit money banks in Nigeria. (300 words)

Table 3 shows that the coefficient of determination of the model is 0.43. This implies that 43 percent changes in spread of fraud are explained by Blockchain technology. Also, Table 3 indicates that there is a negative relationship between Smart contract and spread of fraud in deposit money bank. 1 unit increase in smart contract leads to 1.923 unit decrease in spread of fraud in deposit money bank, and it is statistically significant at 5 percent with T-stat of 5.270 and p-value of 0.008 which is less than 0.05. Also,1 unit increase in Distributed ledger leads to 1.259 unit decrease in spread of fraud in deposit money bank, and it is statistically significant at 5 percent with T-stat of 4.287 and p-value of 0.047 which is less than 0.05.One unit increase in Digital wallet leads to 1.781 unit decrease in spread of fraud in deposit money bank and it is statistically significant at 5 percent with T-stat of 3.247 and p-value of 0.032 which is less than 0.05.Hence, we reject the null hypothesis and conclude that Blockchain technology has significant effect on spread of fraud in deposit money banks.

Table 3: Regression Analysis for the effect of Blockchain technology on curbing spread of fraud in deposit money banks in Nigeria. Dependent Variable: Spread of fraud

Variable	Coefficient	Standard Error	t-stat	Prob.
(Constant)	15.238	1.302	11.707	0.000
Smart Contract	-1.923	0.075	5.270	0.008
Distributed Ledger	-1.259	0.072	4.287	0.047
Digital Wallet	-1.781	0.057	3.247	0.032
R-Square	0.47			
Adjusted R-Square	0.43			
F-Statistic	F(1, 80) = 5.709**			
Prob. (F-Stat)	Prob >F = 0.0495			

'**' and '*' indicate significant at 5% and 10% respectively. Source: Researcher's Computation (2024)

Hypothesis 2

H_{02}: Blockchain technology does not have significant effect on curbing internet fraud activities in deposit money banks in Nigeria.

Table 4indicates that the coefficient of determination of the model is 0. 241.This indicates that roughly 24.1% of variation in IFA is explained by the three BCT levers plus the constant, an economically meaningful share for organizational controls in a complex fraud environment. Table 4 estimates the association between the three BCT capabilities and activities of internet fraudsters (IFA outcome). The fitted model reports $R^2 = 0.271$ (Adjusted $R^2 = 0.241$) and an omnibus F-statistic reported as $F(1, 80) = 5.9338$, with Prob > F = 0.000; coefficients for each capability are negative and statistically significant at 5%. Specifically: Smart contracts $\beta = -1.133$ (SE = 0.043; t = 5.124; p = 0.017); Distributed ledger $\beta = -1.939$ (SE = 0.082; t = 4.347; p = 0.034); and Digital wallet $\beta = -1.781$ (SE = 0.047; t = 3.173; p = 0.014). The constant is 15.248 (SE = 1.475; t = 11.707; p = 0.000). The relatively larger magnitude on distributed ledger (−1.939) suggests that tamper-evident, shared records and synchronized books of record may be particularly salient for deterring or containing internet-channel attack paths such as dispute manipulation, and ex-post edits.One unit increase in smart contracts leads to 1.133 unit decrease in activities of fraudsters in deposit money bank, and it is statistically significant at 5 percent with T-stat of 5.124 and p-value of 0.017 which is less than 5 per cent. Also, one unit increase in Distributed ledger leads to 1.939 unit decrease in activities of fraudsters in deposit money bank, and it is statistically significant at 5 percent with T-stat of 4.347and p-value of 0.034 which is less than 0.05. One unit increase in Digital wallet leads to 1.237 unit decrease in activities of fraudsters in money bank deposit, and it is statistically significant at 5 percent with T-stat of 3.173 and p-value of 0.014 which is less than 0.05. Hence, we reject the null hypothesis and conclude that Blockchain technology has significant effect on activities of fraudsters in deposit money banks in Nigeria.

Table 4: Regression Analysis for the effect of Blockchain technology on curbing internet fraud activities in deposit money banks in Nigeria. Dependent Variable: Activities of Internet fraudsters

Variable	Coefficient	Standard Error	t-stat	Prob.
(Constant)	15.248	1.475	11.707	0.000
Smart Contract	-1.133	0.043	5.124	0.017
Distributed Ledger	-1.939	0.082	4.347	0.034
Digital Wallet	-1.781	0.047	3.173	0.014
R-Square	0.271			
Adjusted R-Square	0.241			
F-Statistic	F(1, 80) = 5.9338**			
Prob. (F-Stat)	Prob >F = 0.000			

'**' and '*' indicate significant at 5% and 10% respectively. Source: Researcher's Computation (2024)

Main Model Hypothesis

H_0: Blockchain technology does not have significant effect in curbing Fraud Activities in Deposit money bank

The study reports a main-model specification using a composite blockchain index (BCT) to explain fraud reduction (an overall outcome complementary to SOF/IFA). Table 5 shows $R^2 = 0.242$ (Adjusted $R^2 = 0.230$) with $F(1, 80) = 3.508$ and Prob > F = 0.005. The BCT index carries a positive, statistically significant coefficient: $\beta = 2.080$ (SE = 0.043; t = 1.873; p = 0.005). The constant is 44.688 (SE = 1.858; t = 24.054; p = .000). There is a positive significant effect of blockchain technology in curbing fraud activities in deposit money banks. The index-based result complements the granular IFA model: when banks report broader deployment across smart contracts, permissioned ledgers, and secure wallets, they also report higher levels of overall fraud reduction. Table 5indicates that the coefficient of determination of the model is 0.24. This implies that 24 percent changes in fraud reduction are explained by blockchain technology. Table 5 shows that there is a positive significant effect of block chain technology in curbing fraud activities in deposit money bank. 1 unit increase in block chain technology leads to 2.080 unit increase in fraud reduction in deposit money bank, and it is statistically significant at 5 percent with T-stat of 1.873 and p-value of 0.005; F-Stat of 3.508 and p-value of 0.005 which is less than 0.05. Hence, we conclude that block chain technology has significant effect on curbing fraud activities in deposit money banks in Nigeria

Table 5: Regression Analysis for the effect of Blockchain technology in curbing Fraud Activities in deposit money banks in Nigeria. Dependent Variable: Fraud reduction

Variable	Coefficient	Standard Error	t-stat	Prob.
(Constant)	44.688	1.858	24.054	.000
Blockchain	2.080	0.043	1.873	.005
R-Square	0.242			
Adjusted R-Square	0.230			
F-Statistic	F(1, 80) = 3.508**			
Prob. (F-Stat)	Prob >F =0.005			

5. Discussion of Findings

The study shows that higher perceived deployment of smart contracts, permissioned distributed ledgers, and secure digital wallets is associated with lower internet fraud activities (IFA), and that a composite BCT index positively predicts overall fraud reduction. Interpreted through the fraud diamond, these results imply that blockchain capabilities compress the opportunity and capability dimensions of fraud. Smart contracts translate policy into executable rules (velocity limits, co-signing thresholds, pre-settlement KYC/sanctions check), thereby shrinking the discretionary windows where social engineering and insider override usually operate. Permissioned ledgers raise the coalition size required for tampering and render ex-post edits conspicuous via append-only, time-stamped trails. Wallet hardening constrains capability at the edge by binding authorization to cryptographic keys, devices, and step-up authentication (Cressey, 1953; Wolfe & Hermanson, 2004; Cong & He, 2019).

From agency theory perspective, the negative coefficients on all three BCT dimensions point to lower agency costs. Programmable controls reduce moral hazard in high-risk steps (e.g., beneficiary changes, bulk-payment releases), while shared state improves monitoring and reduces reconciliation disputes that otherwise depend on unverifiable logs. While wallets act as bonding mechanisms, authorisation requires device-tied keys and user intent proofs, dampening opportunistic behaviour in retail channels (Jensen & Meckling, 1976; Cong & He, 2019). The composite BCT effect suggests complementarities when rule-execution (smart contracts), shared truth (DLT), and strong identity (wallets) move together, monitoring and bonding reinforcing each other rather than simply add up.

The findings also align with information asymmetric arguments. Internet banking fraud thrives when counterparties and internal units observe different "slices of truth." By standardizing event provenance and making records tamper-evident, permissioned DLT reduces hidden action and supports quicker, evidence-based dispute resolution. Privacy-preserving proofs can expose compliance-relevant properties (e.g., sanction-screened/PEP-screened) without revealing full personal data, striking a workable balance between control and confidentiality (Akerlof, 1970; Buterin, Gafni, & Roughgarden, 2024).The relative magnitudes, particularly the strong association for distributed ledgers, are intuitively consistent with Nigeria's 2023–2024 fraud profile, where internet-channel losses and dispute complexity have grown: when the "book of record" becomes shared, tamper-evident, and quarriable, both opportunism and ex-post narrative manipulation become harder. Meanwhile, smart contracts and wallets attack the two flanks of typical incidents: entry (credential takeover, SIM-swap) and execution (authorization of high-risk transfers). The pattern of results, negative signs across all BCT levers and a positive composite effect, mirrors recent multi-bank evidence linking blockchain adoption to better control outcomes and lower exception/fraud-related costs (Al-Dmour, Alshurideh, Al-Kurdi, &Masa'deh, 2024; Ahmed, 2025; Almadadha, 2025; Ma, Sun, & Chen, 2024).

6. Conclusion and Recommendations

This study provides Nigeria-specific, bank-level evidence that stronger perceived deployment of enterprise-grade blockchain capabilities (smart contracts, permissioned ledgers, and secure digital wallets) coincides with lower fraud exposure in internet channels and higher overall fraud-reduction assessments. The pattern is theory-consistent (fraud diamond, principal–agent, information asymmetry) and practice-consistent with emerging international evidence in banking. While causality awaits pilot-based designs, the results justify targeted, near-term adoption in high-loss workflows.

Based on the objectives of the study which sought to examine the effect of blockchain technology in curbing fraudulent activities in DMBs in Nigeria, the study concluded that blockchain technology plays a significant role in curbing spread of fraud and internet fraud activities in Deposit Money Banks in Nigeria.

The empirical results indicate that higher deployment of smart contracts, permissioned distributed ledgers, and secure digital wallets coincides with lower fraud exposure, especially on internet channels. The appropriate managerial response is not to "adopt blockchain" generically but to embed specific BCT capabilities into high-loss processes where they change incentives and evidence. Practically, that means (i) converting policy into enforceable code at critical entitlements; (ii) anchoring dispute-relevant events on a shared, tamper-evident ledger; and (iii) binding authorization to cryptographic identity at the wallet/device boundary. Policy action should, in turn, enable and standardize these moves. In line with these findings, the study recommended that government, Central Bank and Deposit Money Banks should conduct a comprehensive review on block chain technology and explore the usage and benefits of Smart contracts, Distributed ledgers and Digital wallet. They should go beyond crypto currencies and exhaust the capabilities of blockchain technology to curb spread of fraud and elimination or minimization of Internet fraud activities. The study also recommend that the Nigerian government should avoid banning such good technology but study and utilize the use of blockchain technology in public and private sectors of the economy. The researcher believes that this technology has great potentials, not just in relation to cryptocurrency or curbing fraudulent activities because the technology is so robust and if utilized well can make a huge difference in Nigerian economy.

References

Ahmed, I. E. (2025). Analysing the impact of blockchain technology on banking transaction costs: Evidence from the UAE. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2025.1551970.

Akerlof, G. A. (1970). The market for "lemons": Quality uncertainty and the market mechanism. *Quarterly Journal of Economics, 84*(3), 488–500. https://doi.org/10.2307/1879431

Al-Dmour, A., Alshurideh, M., Al-Kurdi, B., & Masa'deh, R. (2024). Blockchain applications and commercial bank performance. *Journal of Innovation & Knowledge, 9*(3), 100450. https://doi.org/10.1016/j.jik.2024.100450

Almadadha, R. (2025). Blockchain and financial performance: Empirical evidence from Australian banks. *Frontiers in Blockchain*. https://doi.org/10.3389/fbloc.2025.1463633

Bassan, F. (2024). From smart legal contracts to contracts on blockchain. *Computer Law & Security Review, 56*, 105013. https://doi.org/10.1016/j.clsr.2024.105013

Bogucharskov, K. (2018). Adoption of blockchain technology in trade finance process. *Journal of Reviews on Global Economics*, 7, 510–515. doi: 10.6000/1929-7092.2018.07.47

Buterin, V., Gafni, A., & Roughgarden, T. (2024). Blockchain privacy and regulatory compliance: Towards a practical equilibrium. *Patterns, 5*(7), 100965. https://doi.org/10.1016/j.patter.2024.100965

Casino, F., Dasaklis, T. K., &Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics, 36*, 55–81. https://doi.org/10.1016/j.tele.2018.11.006.

Central Bank of Nigeria. (2024, December). *CBN Update (December 2024).*https://www.cbn.gov.ng/Out/2024/CCD/CBN%20UPDATE%20DECEMBER%202024.pdf.

Chauhan, S. (2018). Blockchain and scalability. In 2018 IEEE International Conference on Software Quality, Reliability and Security Companion (QRS-C) (pp. 122-128). doi: 10.1109/QRS-C.2018.00034

Chikelue, M. C. (2020). Blockchain technology for cyber security: Performance implications on emerging markets multinational corporations, overview of Nigerian internationalized banks. *International Journal of Scientific & Technology Research,* 9(8), Issn 2277-8616.

Cong, L. W., & He, Z. (2019). Blockchain disruption and smart contracts. *Review of Financial Studies, 32*(5), 1754–1797. https://doi.org/10.1093/rfs/hhz007.

Cressey, D. R. (1953). *Other people's money: A Study in the Social Psychology of embezzlement*. Free Press.

Eyal, I., & Sirer, E. G. (2014). Majority is not enough: Bitcoin mining is vulnerable. In R. Safavi-Naini & N. Christin (Eds.), *Financial Cryptography and Data Security: FC 2014* (LNCS 8437, pp. 436–454). Springer. https://doi.org/10.1007/978-3-662-45472-5_28

Eyers, J. (2020). ANZ, Westpac, CBA digitise bank guarantees in first use of blockchain. Australian Financial Review. Retrieved from https://www.afr.com/companies/financial-services/anz-westpac-cba-digitise-bank

guarantees-in-first-use-of-blockchain-20200831-p55qs6 (Accessed June 2, 2021).

Financial Stability Board. (2024). *The financial stability implications of tokenisation.*https://www.fsb.org/2024/10/the-financial-stability-implications-of-tokenisation/

Gul, S. (2021). A discussion on the effects of blockchain technology within the context of sustainable development. *Journal of Information and Communication Technologies*, 3(2), 243-262. https://doi.org/10.53694/bited.1021926

Guo, H., et al. (2025). The impact of blockchain technology and smart contracts on financial services. *Humanities and Social Sciences Communications*. (Advance online publication).
https://www.nature.com/articles/s41599-025-05473-9

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2019). *Multivariate data analysis* (8th ed.). Cengage.

Hodge, A. (2020). Can blockchain technology transform safety standards in the global food supply chain? Supply Chain Digital. Retrieved from https://supplychaindigital.com/technology-4/can-blockchain-technology-transform-safety-standards-global-food-supply-chain (Accessed June 5, 2021).

Iansiti, M., & Lakhani, K. R. (2017). The truth about blockchain. *Harvard Business Review, 95*(1), 118–127. https://hbr.org/2017/01/the-truth-about-blockchain

IBM & Samsung. (2015). *ADEPT: An IoT practitioner perspective (pre-publication draft).*https://smallake.kr/wp-content/uploads/2016/02/IBM-ADEPT-Practictioner-Perspective-Pre-Publication-Draft-7-Jan-2015.pdf.

Innovations for Poverty Action. (2025). *Consumer protection in digital financial services: Nigeria 2024 consumer survey report.*https://poverty-action.org/sites/default/files/2025-01/Nigeria%202024%20Consumer%20Protection%20in%20DFS%20Survey_Report.pdf

INTERPOL. (2025). *Africa Cyberthreat Assessment 2025*. https://www.interpol.int/content/download/23222/file/2025%20Africa%20Cyberthreat%20Assessment%20Report.pdf

Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behaviour, agency costs and ownership structure. *Journal of Financial Economics, 3*(4), 305–360. https://doi.org/10.1016/0304-405X(76)90026-X

Kamilaris, A., Fonts, N., & Prenafeta-Boldú, F. X. (2019). The rise of blockchain technology in agriculture and food supply chains. Trends in Food Science & Technology, 91, 640-652. https://doi.org/10.1016/j.tifs.2019.07.034.\

Kiu, W. Y., Chia, J. H., & Wong, T. W. (2019). The potential and impact of blockchain technology in the construction industry: A literature review. IOP Conference Series: Materials Science and Engineering, 495, 012005. https://iopscience.iop.org/article/10.1088/1757-899X/495/1/012005

Kline, R. B. (2016). *Principles and Practice of Structural Equation Modeling* (4th ed.). Guilford Press.

Kshetri, N. (2018). Blockchain's roles in meeting key supply chain management objectives', *International Journal of Information Management*, 39, pp. 80–89. doi: 10.1016/j.ijinfomgt.2017.12.005.

Ma, W., Sun, R., & Chen, X. (2024). Blockchain technology and internal control effectiveness: Evidence from BaaS providers. *Journal of Accounting and Public Policy*.https://doi.org/10.1016/j.frl.2024.105442.

Mainelli, M., & Smith, J. (2015). Sharing ledgers for sharing economies: An exploration of mutual distributed ledgers (aka blockchain technology). *The Journal of Financial Perspectives*, 3(3), 38-69.

Mazumder, P. T. (2025). *Blockchain in trade finance: Reducing fraud and operational risk*. SSRN. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5255022

Mehedi, M. (2021). Blockchain technology and its impact on international trade-what does the future hold? ResearchGate. https://www.researchgate.net/publication/354708376

Nigerian Inter-Bank Settlement System. (2024). *2023 annual fraud landscape*. https://nibss-plc.com.ng/wp-content/uploads/2024/04/2023-Annual-Fraud-Landscape.pdf

Ogunrinde, A., De-Pablos-Heredero, C., Montes-Botella, J.-L., & Fernández-Sanz, L. (2025). The impact of blockchain technology and dynamic capabilities on banks' performance. *Big Data and Cognitive Computing, 9*(6), 144. https://doi.org/10.3390/bdcc9060144

Ololade, R. A., Salawu, T. O., &Adekanmi, T. (2020). E-Fraud in Nigerian Banks: Why and How? *Journal of Financial Risk Management*, 9(3),

123-126. https://doi.org/10.4236/jfrm.2020.93012

Pilkington, M. (2016). Blockchain technology: Principles and applications. In R. Bughin, J. Chui, & M. Manyika (Eds.), Research handbook on digital transformations (pp. 87-107). Edward Elgar Publishing.

Podsakoff, P. M., MacKenzie, S. B., Lee, J.-Y., & Podsakoff, N. P. (2003). Common method biases in behavioral research: A critical review and recommended remedies. *Journal of Applied Psychology, 88*(5), 879–903. https://doi.org/10.1037/0021-9010.88.5.879.

Regulation Innovation. (2024). *The battle against digital payment fraud in West Africa*. https://regulationinnovation.org/wp-content/uploads/2024/09/The-Battle-Against-Digital-Payment-Fraud.pdf

Reuters. (2025). Swiss banks claim first binding payment using public blockchain. https://www.reuters.com/

Reyna, A., Martín, C., Chen, J., Soler, E., & Díaz, M. (2018). On blockchain and its integration with IoT: Challenges and opportunities. *Future Generation Computer Systems, 88*, 173–190. https://doi.org/10.1016/j.future.2018.05.046.

Risius, M., &Shoprere, D. (2017). A blockchain research framework: What we (don't) know, where we go from here, and how we will get there. *Business & Information Systems Engineering,* 59(5), 361-378. https://doi.org/10.1007/s12599-017-0481-y

Saberi, S. (2019). Blockchain technology and its relationships to sustainable supply chain management. *International Journal of Production Research*, 57(7), 2117-2135. https://doi.org/10.1080/00207543.2018.1534040

Shi, J., Li, X., & Wang, Y. (2025). Academic exploration of blockchain and AI in financial services: A systematic review. *Journal of Economics, Business and Digital Economics*. https://doi.org/10.1108/JEBDE-08-2024-0023

Taylor, R., Fritsch, E., &Liederbach, J. (2014). Digital crime and digital terrorism. Prentice Hall Press.

Tschorsch, F., &Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. IEEE Communications Surveys & Tutorials, 18(3), 2084-2123.

Vivekanadam, J. (2020). Analysis of recent trends and applications in blockchain technology. *Journal of ISMAC*, 2(4) 113-125.

White, H. (1980). A heteroskedasticity-consistent covariance matrix estimator and a direct test for heteroskedasticity. *Econometrica, 48*(4), 817–838. https://doi.org/10.2307/1912934

Wolfe, D. T., & Hermanson, D. R. (2004). The fraud diamond: Considering the four elements of fraud. *The CPA Journal, 74*(12), 38–42. https://www.cpajournal.com/

Wooldridge, J. M. (2010). *Econometric analysis of cross section and panel data* (2nd ed.). MIT Press.

Zhang, Y., & Wen, J. (2015). An IoT electric business model based on the protocol of Bitcoin. In *2015 18th International Conference on Intelligence in Next Generation Networks (ICIN)*, 184–191. IEEE. https://doi.org/10.1109/ICIN.2015.7073830.

Zheng, Z., Xie, S., Dai, H., Chen, X. and Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. *IEEE International Congress on Big Data (BigData Congress)*, Honolulu, HI, USA, 557-564, https://doi.org/10.1109/BigDataCongress.2017.85.