

Cryptocurrency Regulation and Financial Crime in Nigeria

Dr. Usiere Ekere Nelson

Centre for Peace and Security Studies, University of Port Harcourt

DOI: <https://doi.org/10.51244/IJRSI.2026.1308000279>

Received: 05 September 2026; Accepted: 10 September 2026; Published: 21 September 2026

ABSTRACT

The rapid expansion of cryptocurrency in Nigeria has generated significant opportunities for financial innovation, digital entrepreneurship, financial inclusion and alternative forms of value transfer. At the same time, the pseudonymous, decentralised and transnational characteristics of cryptocurrency transactions have created new challenges for the prevention and control of financial crime. This article examines the relationship between cryptocurrency regulation and financial crime in Nigeria, with particular attention to money laundering, fraud, terrorist financing, tax evasion and illicit financial flows. It critically analyses Nigeria's evolving regulatory framework and the roles of key institutions, particularly the Central Bank of Nigeria, the Securities and Exchange Commission, the Nigerian Financial Intelligence Unit and the Economic and Financial Crimes Commission. The article argues that the historical tendency to approach cryptocurrency primarily through restriction or prohibition is inadequate for addressing the complexities of contemporary digital-asset activities. While regulation is necessary to protect financial-system integrity, investors and consumers, excessive restrictions may encourage informal markets, regulatory evasion and the migration of cryptocurrency activities beyond effective oversight. The study therefore advocates a coordinated, risk-based and technology-sensitive regulatory framework that distinguishes legitimate cryptocurrency activities from their criminal exploitation. It recommends stronger know-your-customer and beneficial-ownership requirements, improved blockchain-analytics capacity, enhanced inter-agency cooperation, effective digital-asset investigation and recovery mechanisms, and stronger international collaboration. The article concludes that Nigeria can effectively combat cryptocurrency-related financial crime without undermining legitimate innovation by combining proportionate regulation, technological capacity, institutional coordination and robust enforcement.

Keywords: Cryptocurrency; Regulation; Financial Crime; Money Laundering; Blockchain; Virtual Assets; Nigeria.

INTRODUCTION

The emergence of cryptocurrency has become one of the most significant developments in the contemporary transformation of the global financial system. Built largely on blockchain and related distributed-ledger technologies, cryptocurrencies enable the transfer and storage of value through digitally mediated systems that can operate across conventional institutional and geographical boundaries. Unlike traditional fiat currencies, cryptocurrencies generally rely on decentralized networks and cryptographic verification rather than central monetary authorities for the validation of transactions. The increasing diffusion of these technologies has consequently challenged conventional assumptions about money, financial intermediation, payment systems and regulatory oversight. In Nigeria, this transformation has been particularly pronounced. The country has emerged as one of the world's major cryptocurrency markets, with cryptocurrency increasingly incorporated into investment, savings, commerce, remittance and cross-border payment activities. Chainalysis (2021) observed that Nigeria was among the countries with strong grassroots cryptocurrency adoption in Africa, while its subsequent assessments placed Nigeria among the leading cryptocurrency-adopting countries globally.

The growth of cryptocurrency in Nigeria cannot be adequately understood without reference to the country's broader socioeconomic and financial environment. Economic pressures, currency depreciation, inflation, difficulties associated with international payments and the search for alternative channels of financial activity

have contributed to the attractiveness of digital assets. Chainalysis (2023) reported that Nigeria's cryptocurrency economy continued to expand despite considerable volatility in global cryptocurrency markets and domestic economic difficulties. Its analysis indicated that cryptocurrency, particularly Bitcoin and stablecoins, had increasingly become relevant to Nigerians seeking alternatives in the context of naira depreciation and economic uncertainty. (Chainalysis) More recent evidence reinforces the significance of this development. Chainalysis (2024) estimated that Nigeria received approximately \$59 billion in cryptocurrency value between July 2023 and June 2024, placing the country second globally on its cryptocurrency adoption index. The same assessment noted that approximately 85 percent of the value of cryptocurrency transfers received in Nigeria during the period involved transactions below \$1 million, indicating substantial participation beyond large institutional transactions.

One of the principal arguments for the continued development of cryptocurrency is its potential contribution to financial innovation and inclusion. Digital assets can facilitate financial transactions without requiring all participants to depend upon conventional banking structures. They may also provide alternative mechanisms for cross-border transfers, particularly where conventional international payment systems are costly, slow or inaccessible. The CBN's 2026 Fintech Report acknowledges that stakeholders view cryptocurrency as potentially useful for cost-effective cross-border transactions, financial inclusion and the development of new digital-asset markets. At the same time, the report identifies illicit financial flows, speculative risks and consumer protection as significant concerns. This dual character of cryptocurrency—simultaneously an instrument of financial innovation and a potential channel for financial abuse is central to the regulatory debate in Nigeria.

Accordingly, this article examines the relationship between cryptocurrency regulation and financial crime in Nigeria, focusing on the country's evolving legal and institutional framework and its capacity to address emerging digital-financial risks. It considers the roles of the CBN, SEC, Nigerian Financial Intelligence Unit and relevant law-enforcement institutions, while examining the challenges posed by money laundering, fraud, terrorist financing, illicit financial flows and cross-border digital transactions. The article ultimately argues that effective cryptocurrency regulation should seek to achieve a principled balance between financial innovation, financial inclusion, consumer protection, financial-system integrity and crime prevention. Nigeria's experience demonstrates that the objective of regulation should not simply be to restrict cryptocurrency, but to create an accountable digital-financial environment in which technological innovation can develop without becoming a convenient infrastructure for financial crime.

Conceptualizing Cryptocurrency and Financial Crime

A clear conceptual understanding of cryptocurrency and financial crime is necessary for assessing the regulatory challenges associated with digital assets in Nigeria. Cryptocurrency operates at the intersection of finance, information technology and decentralized digital networks, while financial crime encompasses a broad range of unlawful activities through which individuals or organized groups obtain, conceal, transfer or legitimize illicit financial gains. The relationship between the two concepts is therefore neither automatic nor exclusively criminal. Rather, the technological characteristics that make cryptocurrency attractive for legitimate financial innovation can, under particular circumstances, also be exploited for illicit purposes. This section consequently clarifies the principal concepts underpinning the cryptocurrency–financial crime relationship.

Meaning and Nature of Cryptocurrency

Cryptocurrency may broadly be understood as a privately issued digital representation of value that uses cryptographic techniques and distributed-ledger technology to record, validate and secure transactions. The International Monetary Fund (IMF) describes crypto assets as privately issued digital representations of value that are cryptographically secured and deployed through distributed-ledger technology (IMF, 2023). The concept therefore encompasses more than the popular understanding of cryptocurrency as simply “digital money.” It includes a range of digitally represented assets whose economic functions and underlying structures differ considerably. Similarly, the Financial Action Task Force (FATF) defines a virtual asset as a digital representation of value that can be digitally traded or transferred and can be used for payment or investment

purposes, while excluding digital representations of fiat currencies and financial assets already covered by other regulatory frameworks (FATF, 2021).

The fundamental characteristics of cryptocurrency derive from its technological architecture. First, transactions are secured through cryptographic mechanisms that make unauthorized alteration of the transaction record extremely difficult. Second, cryptocurrencies generally operate through distributed networks rather than depending upon a single central institution to maintain the transaction ledger. Blockchain, a particular form of distributed ledger, records transactions in linked blocks and distributes the ledger across network participants. The IMF (2025) explains that a distributed ledger is a database shared and synchronized across a computer network, while blockchain represents a specific form of distributed ledger in which information is structured into linked blocks.

Understanding Financial Crime

Financial crime can be referred broadly to unlawful activities involving the acquisition, movement, concealment, conversion or use of money and other financial assets for illicit purposes. It is not confined to one particular offence but encompasses different forms of criminal conduct whose common feature is the exploitation of financial systems, transactions or assets for unlawful gain or purposes. In the context of cryptocurrency, the concept is especially significant because digital assets can become involved at different stages of criminal activity: as the proceeds of an offence, as a means of transferring illicit value, as an instrument for concealing assets or as a target of fraudulent schemes.

Money laundering represents one of the most significant forms of financial crime associated with virtual assets. In general terms, money laundering involves processes through which proceeds derived from criminal activity are disguised, transferred or transformed in an attempt to conceal their illicit origin and make them appear legitimate. Cryptocurrency can become relevant to money laundering where criminals attempt to move illicit proceeds through digital wallets, exchanges or multiple transactions in order to obscure the connection between the proceeds and their original criminal source. Nigeria's National Inherent Risk Assessment of Money Laundering (2022) identified virtual assets as an emerging area of money-laundering risk and reported that a substantial proportion of virtual-asset-related suspicious reports received by the NFIU between 2019 and 2021 concerned suspected money laundering.

The Cryptocurrency–Financial Crime Nexus

The relationship between cryptocurrency and financial crime is seen to arise principally from the interaction between the technological characteristics of digital assets and the objectives of criminal actors. Cryptocurrency is not inherently criminal, nor is every cryptocurrency transaction suspicious. Indeed, blockchain-based systems can provide legitimate financial and technological benefits. The FATF recognizes that virtual assets can make payments faster, cheaper and more accessible to persons who lack access to conventional financial products, while simultaneously warning that inadequate regulation can create opportunities for criminal and terrorist misuse (FATF, 2021). The issue, therefore, is the potential misuse of a legitimate technology, rather than the inherent criminality of cryptocurrency itself.

Several characteristics may nevertheless make cryptocurrency attractive to financial criminals. The first is pseudonymity. Although transactions on many public blockchains are visible, the identities associated with wallet addresses are not necessarily apparent from the blockchain itself. Criminal actors may therefore attempt to exploit multiple wallet addresses or other technological mechanisms to make attribution more difficult. FATF (2026) notes that pseudonymous peer-to-peer transactions involving unhosted wallets can make attribution more difficult, particularly when individuals repeatedly generate new addresses. The second factor is the speed and cross-border character of cryptocurrency transactions. Digital assets can be transferred across jurisdictions without necessarily passing through the conventional correspondent-banking infrastructure. This creates legitimate opportunities for international commerce and remittances, but it can simultaneously complicate the work of regulators and law-enforcement agencies. The FATF's recent work emphasizes that cross-border transactions involving virtual assets can create jurisdictional difficulties, particularly where

service providers are located offshore or outside the direct supervisory authority of the jurisdiction in which users reside (FATF, 2026).

A third concern is the growth of peer-to-peer transactions and unhosted wallets. Where transactions occur directly between users without the involvement of a regulated virtual asset service provider, conventional customer-identification and transaction-monitoring mechanisms may be less effective. FATF (2026) specifically identifies peer-to-peer transactions through unhosted wallets as presenting heightened illicit-finance risks because they may occur outside the obligations normally imposed on regulated intermediaries. This issue is particularly relevant to Nigeria, where peer-to-peer cryptocurrency activity forms an important part of the broader digital-asset ecosystem. A fourth vulnerability concerns cryptocurrency exchanges, wallets and other intermediaries. These entities can serve legitimate economic functions by facilitating the purchase, sale, transfer and custody of virtual assets. At the same time, inadequately regulated or offshore providers may become points through which illicit funds enter, move through or exit the cryptocurrency ecosystem. FATF (2021) consequently recommends that jurisdictions assess and mitigate risks associated with virtual-asset activities, license or register relevant service providers and subject them to appropriate supervision. Nigeria's NFIU has similarly emphasized the importance of virtual-asset service providers within the country's AML/CFT framework and has identified cooperation with the SEC as important to strengthening oversight.

In this respect, the conceptual relationship can be expressed as follows: cryptocurrency does not cause financial crime; rather, particular technological and institutional characteristics of cryptocurrency may create opportunities, vulnerabilities and new channels through which existing forms of financial crime can be committed. This distinction provides an essential foundation for evaluating whether Nigeria's current regulatory framework is sufficiently capable of managing digital-asset risks without unnecessarily suppressing legitimate financial innovation.

The Growth of Cryptocurrency and Its Implications for Nigeria

The growth of cryptocurrency in Nigeria represents an important dimension of the country's rapidly changing digital-financial landscape. Over the past decade, the use of crypto assets has moved from a relatively specialized activity associated with technology enthusiasts to a broader phenomenon involving individuals, businesses, investors, remittance recipients and digital entrepreneurs. Nigeria's position is particularly notable within Africa because cryptocurrency has increasingly been used not only as an investment instrument but also as a means of transferring value, accessing international markets and responding to weaknesses within conventional financial arrangements. Chainalysis (2024) ranked Nigeria second globally in its Global Crypto Adoption Index, while estimating that the country received approximately \$59 billion in cryptocurrency value between July 2023 and June 2024. The report also identified Nigeria as one of the major markets for stablecoins and noted the growing importance of cryptocurrency for commercial and cross-border financial activity.

The expansion of cryptocurrency adoption in Nigeria is driven by a combination of technological, economic and socioeconomic factors. Increasing smartphone penetration, expanding internet access, the growth of fintech services and the emergence of digitally oriented businesses have lowered some of the barriers to participation in digital-asset markets. At the same time, the limitations of conventional financial systems have encouraged some Nigerians to explore alternative mechanisms for storing and transferring value. Cryptocurrency therefore occupies a distinctive position within Nigeria's financial environment: it represents both a product of digital transformation and a response to perceived deficiencies in existing financial infrastructure.

The relevance of cryptocurrency is particularly evident in relation to cross-border payments and remittances. Nigeria is one of Africa's major recipients of remittances, and the cost, speed and accessibility of conventional international money-transfer systems remain important policy concerns. Digital assets, especially stablecoins, can facilitate rapid transfers across geographical boundaries and may reduce dependence on traditional intermediaries in certain circumstances. The Central Bank of Nigeria's recent fintech research acknowledges that stakeholders perceive digital assets as having potential benefits for cross-border transactions, including increased efficiency and reduced transaction costs. At the same time, the CBN recognizes that these benefits

must be balanced against concerns relating to illicit financial flows, fraud, consumer protection and financial stability (CBN, 2026). This dual assessment is important because the same characteristics that make cryptocurrency attractive for legitimate international payments—speed, accessibility and global transferability may also make it attractive for illicit financial movements.

The economic significance of cryptocurrency therefore presents a dual-edged phenomenon. On one side, digital assets can support technological innovation, facilitate certain cross-border transactions, create new entrepreneurial opportunities and contribute to the development of financial technologies. Blockchain applications may also have uses beyond cryptocurrency, including tokenisation, digital identity, payment settlement and automated contractual arrangements. On the other side, cryptocurrency markets may generate substantial risks, including consumer losses, fraud, money laundering, terrorist financing, tax-related challenges, market manipulation and illicit capital movements. The Financial Action Task Force (2021) consequently emphasizes that virtual-asset activities should be subject to risk-based anti-money-laundering and counter-terrorist-financing controls.

The growth of cryptocurrency in Nigeria should be understood within the broader transformation of the country's financial economy. Cryptocurrency has emerged partly because of technological progress and partly because users perceive practical advantages in digital forms of value transfer. Its growth therefore reflects both innovation and structural pressures within the Nigerian economy. The central regulatory challenge is to ensure that these benefits are not undermined by financial crime, while preventing concerns about criminal misuse from producing regulation so restrictive that legitimate innovation is driven outside the formal financial system. This balance provides the foundation for examining Nigeria's evolving regulatory response to cryptocurrency and the extent to which that framework can effectively address financial crime without suppressing the legitimate development of the digital economy.

Evolution of Cryptocurrency Regulation in Nigeria

The regulatory history of cryptocurrency in Nigeria reflects a gradual movement from caution and restriction towards recognition, supervision and institutional regulation. This evolution has been shaped by the rapid growth of digital-asset activities, concerns about money laundering and terrorist financing, consumer and investor protection, monetary stability, and the increasing recognition that prohibition alone cannot eliminate cryptocurrency-related activities. The trajectory is particularly significant because it illustrates a broader transformation in regulatory philosophy: from attempting to prevent financial institutions from interacting with cryptocurrency towards developing mechanisms through which cryptocurrency-related businesses can operate within identifiable legal and supervisory structures.

Nigeria's initial regulatory response to cryptocurrency was predominantly precautionary. Before the emergence of a comprehensive digital-asset regulatory framework, the Central Bank of Nigeria (CBN) repeatedly warned financial institutions and members of the public about the risks associated with virtual currencies. The concerns included the absence of sovereign backing, price volatility, consumer vulnerability, money laundering and terrorist financing. The underlying regulatory position was that cryptocurrency transactions existed outside the conventional monetary and banking framework and therefore created significant risks for the financial system. The restrictive approach became particularly pronounced in February 2021, when the CBN issued circular directing banks, non-bank financial institutions and other regulated financial institutions to identify and close accounts belonging to persons or entities involved in cryptocurrency transactions. The directive instructed regulated institutions not to facilitate cryptocurrency-related transactions and warned of regulatory sanctions for non-compliance (CBN, 2021).

The CBN's position was grounded principally in financial-system risk. Cryptocurrency transactions could occur without the conventional oversight associated with regulated financial institutions, thereby raising concerns about the movement and concealment of illicit funds. The Bank's earlier warnings had specifically connected virtual currencies with potential money-laundering and terrorist-financing risks, while also emphasizing the absence of legal protection for persons who invested in them. The 2021 directive consequently represented the culmination of a precautionary approach in which limiting the connection between banks and cryptocurrency was regarded as a means of protecting the formal financial system.

Again, Nigeria's subsequent regulatory trajectory demonstrates a significant shift from outright restriction towards regulated engagement. This change reflects both the increasing economic importance of digital assets and the recognition that cryptocurrency-related activities could not realistically be addressed through banking restrictions alone. Instead, the regulatory objective increasingly became the identification of digital-asset operators, establishment of compliance obligations and integration of relevant activities into the broader anti-money-laundering and financial-supervision architecture.

An important legal development was the Money Laundering (Prevention and Prohibition) Act 2022. The Act expanded Nigeria's anti-money-laundering framework and expressly brought Virtual Asset Service Providers (VASPs) within the scope of relevant financial-sector obligations. This development was significant because it moved virtual-asset activities from an area characterized primarily by regulatory uncertainty towards one in which participants could be subjected to formal AML/CFT requirements. The recognition of VASPs is particularly important because exchanges, custodians and other intermediaries constitute critical points at which customer identification, transaction monitoring and suspicious-transaction reporting can occur.

The regulatory shift became more explicit with the CBN's Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers, issued on 22 December 2023. Rather than maintaining the earlier blanket restriction on banking relationships, the Guidelines established conditions under which financial institutions could provide designated banking services to VASPs. The Guidelines require financial institutions to monitor activities conducted through designated accounts and impose specific controls on the use of those accounts. They also require relevant VASPs to satisfy requirements relating to AML, counter-terrorist financing and counter-proliferation financing policies. The significance of this development lies in the change in regulatory philosophy. The CBN moved from “do not transact with cryptocurrency-related entities” towards “permit regulated banking relationships subject to specified controls.” This is not equivalent to unrestricted acceptance of cryptocurrency as money or legal tender. Rather, it represents an attempt to establish controlled points of contact between the conventional banking system and the virtual-asset sector.

Also, the Securities and Exchange Commission (SEC) has played a complementary and increasingly important role in the evolution of Nigeria's cryptocurrency regulatory framework. While the CBN's principal concerns relate to monetary, banking and financial-system stability, the SEC approaches digital assets substantially from the perspective of securities regulation, capital-market integrity and investor protection. The SEC's foundational intervention came in 2020, when it issued its Statement on Digital Assets and Their Classification and Treatment. The Commission adopted the position that virtual crypto assets would generally fall within its regulatory jurisdiction where the characteristics of the investment qualified them as securities. It also placed the burden on issuers or sponsors to demonstrate that a particular digital asset did not constitute a security.

The 2020 framework was significant because it represented a move away from treating cryptocurrency exclusively as a monetary or banking issue. Instead, it recognised that certain digital assets could operate as investment products and therefore required the protections associated with the capital market. The framework covered digital-asset offerings conducted within Nigeria, offerings by Nigerian issuers or sponsors, and foreign issuers targeting Nigerian investors. This approach was developed further through the SEC's Rules on Issuance, Offering Platforms and Custody of Digital Assets, issued in 2022. The rules created distinct regulatory categories and requirements for several components of the digital-asset ecosystem. These included Digital Asset Offering Platforms (DAOPs), Digital Asset Custodians (DACs), Virtual Asset Service Providers (VASPs) and Digital Asset Exchanges (DAXs).

The Nigerian experience therefore suggests that the central regulatory question is no longer whether cryptocurrency can simply be prohibited. Rather, it is how digital-asset activities can be brought within a sufficiently transparent and enforceable regulatory framework without undermining legitimate innovation. The answer requires a continuing balance between financial innovation and financial integrity, with regulation capable of adapting as the technology, market structure and methods of financial crime continue to evolve.

Cryptocurrency as a Vehicle for Financial Crime in Nigeria

The expansion of cryptocurrency in Nigeria has created new opportunities for financial innovation, but it has also introduced vulnerabilities that can be exploited for financial crime. The characteristics that make virtual assets attractive for legitimate purposes speed, global reach, programmability, accessibility and the ability to transfer value without conventional intermediaries can equally be exploited by criminals seeking to conceal, move or convert illicit proceeds. The Financial Action Task Force (FATF) has repeatedly identified virtual assets as presenting money-laundering and terrorist-financing risks, particularly where transactions involve anonymity-enhancing technologies, peer-to-peer arrangements, weakly regulated jurisdictions and unusual transaction patterns (FATF, 2025). It is therefore important to distinguish between cryptocurrency as a technology and criminal conduct involving cryptocurrency. The existence of financial crime within the cryptocurrency ecosystem does not establish that cryptocurrency itself is inherently criminal. Rather, the problem concerns the exploitation of particular technological and institutional characteristics by individuals and networks engaged in unlawful activities. Consequently, effective regulation requires the identification of specific risks and vulnerabilities rather than a blanket characterization of all cryptocurrency activity as illicit.

First Money laundering, money laundering represents one of the most significant financial-crime risks associated with cryptocurrency in Nigeria. In its conventional form, money laundering involves processes through which proceeds derived from criminal activities are concealed, disguised, transferred or transformed so that they can eventually appear legitimate. Cryptocurrency can potentially facilitate these processes because digital assets permit value to move rapidly across borders and between different addresses without necessarily revealing the real-world identity of the person controlling each address.

The first major vulnerability concerns the concealment of criminal proceeds. A person who obtains funds through fraud, corruption, cybercrime or other predicate offences may attempt to convert the proceeds into virtual assets and subsequently transfer them through multiple wallets or platforms. Although transactions recorded on a public blockchain may be visible, the blockchain address does not automatically reveal the natural person who controls it. Consequently, the distinction between transaction visibility and identity visibility is crucial. A transaction may be permanently recorded while the beneficial owner behind the transaction remains difficult to establish without additional information from exchanges, wallet providers, telecommunications companies, banks or other relevant institutions.

A related technique involves layering, whereby funds are moved through a series of transactions and addresses in an attempt to complicate the reconstruction of the original source and ultimate destination of the funds. FATF identifies unusual transaction patterns, rapid movement of virtual assets, peer-to-peer transfers, anonymity-enhancing technologies and transactions involving high-risk jurisdictions as indicators that may warrant closer scrutiny. (FATF) The difficulty is therefore not necessarily that blockchain transactions cannot be traced, but that establishing the identity, purpose and beneficial ownership associated with a sequence of transactions can require sophisticated blockchain analysis and information from multiple jurisdictions.

Again, Cryptocurrency has also become associated with different forms of fraud in Nigeria. The rapid expansion of digital-asset markets, combined with limited financial literacy among some participants, creates opportunities for fraudulent actors to exploit expectations of quick financial returns. Cryptocurrency-enabled fraud can take several forms, including fraudulent investment schemes, Ponzi arrangements, impersonation, social-engineering attacks, fake trading platforms and unauthorized token offerings.

Investment and cryptocurrency scams are particularly problematic because fraudulent operators can present themselves as legitimate investment professionals or digital-asset entrepreneurs. They may promise unrealistic or guaranteed returns, manufacture evidence of successful trading and encourage participants to recruit others. In a Ponzi-type arrangement, payments to earlier participants may be funded substantially from contributions made by later participants rather than from genuine investment returns. The digital environment can make such schemes easier to advertise widely and can permit fraudulent operators to reach potential victims through social-media and messaging platforms. Consequently, combating cryptocurrency-enabled fraud requires more than conventional policing. It requires regulatory monitoring of digital-asset service providers, public verification mechanisms, financial and digital literacy, effective disclosure requirements, technological

surveillance and cooperation among the SEC, CBN, NFIU, EFCC, law-enforcement agencies and relevant international authorities. The SEC's 2026 warning concerning unregistered online investment schemes further illustrates the importance of monitoring investment opportunities promoted through social-media platforms and other digital channels.

Also, the potential use of cryptocurrency for terrorist financing represents another important dimension of the financial-crime problem. Terrorist organizations and their supporters require mechanisms through which resources can be collected, transferred and used without attracting the attention of financial institutions or law-enforcement authorities. Virtual assets may create vulnerabilities because they can facilitate rapid cross-border transfers and can operate through decentralized or offshore infrastructures. The FATF has consistently identified terrorist financing as one of the principal risks associated with virtual assets. Its analysis emphasizes that virtual assets may be exploited because of their speed, global accessibility and certain features that can increase transactional anonymity. At the same time, FATF's risk-based approach recognizes that not every cryptocurrency transaction represents a terrorist-financing threat. The appropriate response is therefore the identification and mitigation of specific risks through effective regulation, supervision and intelligence gathering.

Nigeria's national risk assessment also demonstrates the relevance of virtual assets to broader illicit-finance concerns. The NFIU reported that virtual assets had appeared in cases involving organized crime and fraud and noted their capacity to facilitate rapid international transfers. Such findings are significant within the Nigerian context because financial crime frequently possesses a transnational character, making cooperation between domestic institutions and foreign counterparts essential.

For Nigeria, the issue extends beyond tax collection to the broader problem of illicit financial flows. Where cryptocurrency is used to transfer proceeds of fraud, corruption, tax evasion or other unlawful activity across borders, the resulting transactions may reduce the ability of government institutions to monitor the movement of capital. The problem is intensified where funds are converted between digital assets, fiat currencies and other forms of value across multiple jurisdictions.

Institutional and Legal Framework for Combating Cryptocurrency-Related Financial Crime

The effectiveness of cryptocurrency regulation in Nigeria depends not only on the existence of substantive laws but also on the institutional capacity to implement, supervise and enforce those laws. Cryptocurrency-related financial crime cuts across banking, securities regulation, financial intelligence, taxation, cybercrime, national security and criminal justice. No single institution therefore possesses the capacity to address the entire spectrum of risks associated with virtual assets. Rather, effective regulation requires a coordinated institutional architecture in which the mandates of financial regulators, intelligence agencies, law-enforcement bodies, tax authorities and technology institutions complement one another. Nigeria's current framework reflects this increasingly interconnected approach. The Money Laundering (Prevention and Prohibition) Act 2022 (MLPPA), the Terrorism (Prevention and Prohibition) Act 2022, the Investments and Securities Act 2025, the Central Bank of Nigeria's regulatory framework for virtual-asset service providers and the Securities and Exchange Commission's digital-asset rules collectively provide important legal foundations. The Nigerian Financial Intelligence Unit (NFIU), Economic and Financial Crimes Commission (EFCC), Nigeria Police Force and other agencies provide complementary intelligence, investigative and enforcement functions. The effectiveness of the framework, however, ultimately depends on the ability of these institutions to exchange information and respond to the technological and transnational nature of cryptocurrency transactions.

Central Bank of Nigeria

The Central Bank of Nigeria (CBN) occupies a central position in the regulation of cryptocurrency-related risks because of its statutory responsibilities for monetary policy, banking supervision, payment systems and financial-system stability. Although the CBN does not regulate every aspect of cryptocurrency activity, its oversight of banks and other regulated financial institutions is critical because conventional financial institutions constitute important gateways through which cryptocurrency-related funds enter and leave the formal financial system.

The CBN's approach to virtual assets has evolved considerably. In February 2021, the Bank directed regulated financial institutions to identify and close accounts associated with persons or entities transacting in or operating cryptocurrency exchanges. The directive reflected concerns regarding money laundering, terrorism financing, consumer protection and the potential risks posed by cryptocurrency to the formal financial system. Subsequently, however, the regulatory approach shifted toward controlled engagement. On 22 December 2023, the CBN issued the Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers, establishing conditions under which banks and other financial institutions could provide designated accounts for registered VASPs. Thus, the CBN's contribution to combating cryptocurrency-related financial crime extends beyond simply permitting or restricting cryptocurrency activity. It involves ensuring that the points of interaction between virtual assets and the regulated financial system remain subject to appropriate identification, monitoring, reporting and risk-management requirements.

Securities and Exchange Commission

The Securities and Exchange Commission (SEC) is the principal regulator of Nigeria's capital market and plays a central role in regulating digital assets that fall within the securities and investment-services domain. Its involvement is particularly important because cryptocurrency-related financial crime frequently occurs through investment schemes, token offerings, digital-asset exchanges and other activities that may expose investors to fraud and market abuse. The SEC first established its regulatory position on digital assets in 2020, stating that crypto-token or crypto-coin investments would fall within its jurisdiction where their characteristics qualify them as securities. The Commission also adopted the position that virtual crypto assets would be treated as securities unless the issuer or sponsor established otherwise. This approach brought digital-asset activities within the broader framework of securities regulation and investor protection.

The Commission subsequently developed more detailed rules. Its 2022 Rules on Issuance, Offering Platforms and Custody of Digital Assets established requirements relating to digital-asset issuance, Digital Assets Offering Platforms (DAOPs), Digital Assets Custodians (DACs), Virtual Asset Service Providers (VASPs) and Digital Assets Exchanges (DAXs). The framework also addressed registration and operational requirements for relevant digital-asset businesses. This regulatory architecture gives the SEC several mechanisms for combating cryptocurrency-related financial crime. Licensing and registration requirements enable the Commission to identify legitimate operators and distinguish them from unregistered entities. This is especially important in an environment in which fraudulent operators can establish online platforms and solicit investments without maintaining a transparent corporate or regulatory identity.

The SEC's role is therefore multidimensional: it involves licensing, supervision, investor protection, market integrity, enforcement and the development of regulatory standards for an evolving digital-asset market. Its effectiveness will depend substantially on its ability to coordinate with the CBN, NFIU, EFCC and other institutions whose mandates intersect with digital-asset activities.

Nigerian Financial Intelligence Unit

The Nigerian Financial Intelligence Unit occupies a distinctive position within Nigeria's AML/CFT architecture. Its principal function is not conventional criminal prosecution but the collection, analysis and dissemination of financial intelligence capable of assisting law-enforcement, regulatory and security institutions in identifying and responding to financial crime. The NFIU receives suspicious transaction reports (STRs) and threshold-based transaction reports from reporting entities. Its mandate is grounded in the NFIU Act 2018, the Money Laundering (Prevention and Prohibition) Act 2022 and the Terrorism (Prevention and Prohibition) Act 2022. Importantly for cryptocurrency regulation, Virtual Asset Service Providers fall within the category of reporting entities recognized under the MLPPA.

The STR mechanism is particularly important in detecting cryptocurrency-related money laundering and terrorist financing. Reporting entities are required to identify transactions or activities that generate reasonable suspicion and report them to the NFIU in accordance with applicable legal requirements. The NFIU then analyzes the information and may generate financial intelligence reports for relevant law-enforcement

agencies. It also maintains databases and shares intelligence with foreign financial-intelligence units under appropriate arrangements.

The importance of the NFIU is heightened by the fact that cryptocurrency-related financial crime often involves transactions extending beyond the jurisdiction of a single institution. A suspicious transaction may begin through a Nigerian financial institution, move through a virtual-asset platform in another jurisdiction and ultimately reach a beneficiary in a third country. Financial intelligence therefore provides the connective mechanism through which information from different reporting entities and jurisdictions can be analyzed collectively.

Economic and Financial Crimes Commission

The Economic and Financial Crimes Commission (EFCC) is one of Nigeria's principal law-enforcement institutions for investigating and prosecuting economic and financial crimes. Its relevance to cryptocurrency regulation arises from the increasing use of digital assets in fraud, money laundering, cyber-enabled financial crime and other forms of illicit financial activity. The EFCC's investigative function is particularly important once financial intelligence indicates that cryptocurrency may have been used in connection with a criminal offence. Whereas the CBN and SEC primarily exercise regulatory and supervisory functions within their respective sectors, the EFCC can investigate suspected economic and financial crimes, trace assets and support prosecution in appropriate cases.

Cryptocurrency presents distinctive challenges for asset tracing because digital assets may be distributed across numerous wallet addresses, exchanges and jurisdictions. Nevertheless, the transparent transaction records associated with many public blockchains can provide investigative leads when combined with blockchain-analysis tools and conventional evidence. The EFCC can therefore potentially connect blockchain transaction histories with bank records, telecommunications information, exchange records, identity documentation and other evidence to establish the movement and ownership of illicit proceeds.

Other Relevant Institutions

The institutional framework for combating cryptocurrency-related financial crime extends beyond the CBN, SEC, NFIU and EFCC. The complexity of digital financial crime makes inter-agency cooperation indispensable, with different institutions contributing according to their statutory responsibilities. The Nigeria Police Force (NPF) remains important in investigating fraud, cyber-enabled offences, identity-related crimes and other criminal conduct in which cryptocurrency may constitute the means of payment or transfer. Its investigative role is particularly relevant at the level of individual complaints and offences that may not fall exclusively within the specialized jurisdiction of financial regulators.

The Nigeria Customs Service (NCS) may also become relevant where cryptocurrency-related financial activity intersects with cross-border movement of goods, trade-based financial crime or other customs offences. As illicit financial flows increasingly combine physical and digital components, customs intelligence can complement information obtained from financial institutions and digital-asset platforms. The Federal Inland Revenue Service (FIRS) has an important role in the taxation of income and transactions associated with digital assets. Cryptocurrency can create difficulties for tax administration because taxpayers may transact through multiple wallets, peer-to-peer markets and foreign platforms. Cooperation between FIRS, financial regulators and financial-intelligence authorities can therefore contribute to identifying taxable economic activity and detecting potential tax evasion.

The National Information Technology Development Agency (NITDA) is relevant from the broader perspective of Nigeria's digital-technology ecosystem. Although its role is not equivalent to that of the CBN, SEC, NFIU or EFCC in financial-crime enforcement, technological standards, digital governance and cybersecurity-related institutional development can influence the security and reliability of the wider digital environment in which virtual-asset services operate. The Office of the National Security Adviser (ONSA) and other national-security institutions are also relevant where cryptocurrency-related activities intersect with terrorism financing,

organized crime, proliferation financing or other threats to national security. Such cases require financial intelligence to be integrated with security and intelligence information.

The broader institutional framework can therefore be understood as a network rather than a hierarchy. The CBN provides banking and payment-system supervision; the SEC regulates relevant digital-asset and investment activities; the NFIU receives and analyzes financial intelligence; the EFCC investigates and prosecutes economic and financial crimes; tax authorities address fiscal implications; security agencies address national-security dimensions; and technology-related institutions contribute to the digital governance environment.

The effectiveness of Nigeria's institutional and legal framework should be measured not merely by the number of regulations enacted or institutions established, but by their ability to identify suspicious activity, prevent financial crime, trace illicit assets, protect legitimate investors and users, prosecute offenders and recover criminal proceeds. Cryptocurrency regulation therefore requires an integrated institutional architecture in which prevention, intelligence, supervision, investigation, prosecution, taxation, asset recovery and national security are treated as interconnected elements of financial-crime governance.

Effectiveness of Nigeria's Cryptocurrency Regulatory Framework

The effectiveness of Nigeria's cryptocurrency regulatory framework should be assessed not merely by the number of laws, regulations and institutions that have been established, but by their capacity to prevent financial crime while preserving legitimate technological and economic activity. Nigeria's regulatory trajectory demonstrates a significant movement from an initially restrictive approach toward a more structured system of recognition, registration, supervision and risk management. The Money Laundering (Prevention and Prohibition) Act 2022, the Central Bank of Nigeria's framework for banking relationships with Virtual Asset Service Providers (VASPs), the Securities and Exchange Commission's digital-asset regulatory framework and the Investments and Securities Act 2025 collectively provide a stronger legal foundation than existed during the earlier prohibition-oriented period. Nevertheless, important challenges remain concerning regulatory coordination, technological capacity, beneficial ownership, peer-to-peer transactions, enforcement and the effective supervision of offshore and decentralized platforms.

Nigeria's current legislation provides a considerably more comprehensive basis for addressing cryptocurrency-related financial crime than the earlier regulatory environment. The recognition of VASPs within the anti-money-laundering framework is particularly important because it brings relevant virtual-asset businesses within formal reporting and compliance obligations. The Investments and Securities Act 2025 also strengthens the capital-market foundation for regulating digital and virtual assets that fall within the SEC's jurisdiction. The adequacy of legislation, however, should not be measured solely by formal legal recognition. Cryptocurrency develops more rapidly than conventional legislative processes, creating a persistent risk of regulatory lag. New forms of decentralized finance, tokenization, stablecoins, non-custodial arrangements and automated financial services may generate risks that existing rules were not originally designed to address. The SEC's exposure of proposed rules on Digital and Virtual Asset Operations, Custody and Markets in August 2026 illustrates the continuing process of regulatory adaptation. The proposed framework covers issuance, tokenisation, trading, custody, transfer and settlement, as well as investment and advisory services, and extends to persons operating in Nigeria, providing services to Nigerian residents or targeting Nigerian investors through digital channels.

The existence of multiple institutions with overlapping interests creates both an advantage and a potential weakness. The CBN is principally concerned with banking, payment systems and financial stability; the SEC regulates capital-market activities and relevant digital-asset businesses; the NFIU focuses on financial intelligence; and the EFCC investigates and prosecutes economic and financial crimes. Other institutions, including tax and security agencies, possess complementary responsibilities. This division of labour is necessary because cryptocurrency-related financial crime is multidimensional. However, institutional overlap can produce uncertainty concerning which agency should take the lead in particular cases. The effectiveness of the framework consequently depends upon clear delineation of responsibilities and efficient information-

sharing mechanisms. A suspicious cryptocurrency transaction, for example, may simultaneously raise questions concerning money laundering, securities regulation, tax liability, cybercrime and national security.

Licensing and registration constitute important preventive mechanisms because they enable regulators to identify legitimate operators before they provide services to the public. The SEC's registration framework for VASPs, digital-asset exchanges, custodians and related operators creates an institutional gateway through which businesses must demonstrate compliance with regulatory requirements. The SEC's Accelerated Regulatory Incubation Programme (ARIP) represents an important innovation in this regard. Rather than forcing emerging business models into a regulatory framework without testing their technological characteristics, ARIP provides a controlled environment in which qualifying VASPs and other digital investment service providers can be assessed. The program includes operational, risk-management, investor-protection and compliance considerations and provides a pathway toward full registration.

Know-Your-Customer (KYC) and Customer Due Diligence (CDD) are among the most important tools for preventing anonymous or pseudonymous financial activity from becoming a vehicle for crime. Their purpose is to establish the identity of customers, understand the nature and purpose of their activities, assess risk and monitor transactions for suspicious patterns. The inclusion of VASPs within Nigeria's AML framework strengthens the legal basis for applying these controls to virtual-asset activities. The NFIU identifies VASPs among reporting entities and requires suspicious transactions to be reported in accordance with the applicable legal framework.

Suspicious Transaction Reporting (STR) is an essential link between regulated entities and financial-intelligence authorities. The NFIU states that reporting entities, including VASPs, are required to submit suspicious transaction reports and that the Unit analyzes these reports and generates intelligence for relevant law-enforcement agencies. It also facilitates information exchange with foreign financial-intelligence units. The effectiveness of this system depends upon the quality, timeliness and sophistication of the reports received. Cryptocurrency creates particular challenges because suspicious activity may involve numerous small transactions, multiple wallets, rapid movement of assets or transfers between regulated and unregulated platforms. A reporting system based exclusively on conventional banking indicators may therefore fail to identify emerging cryptocurrency typologies.

Major Challenges to Cryptocurrency Regulation in Nigeria

Despite the substantial progress made in establishing a legal and institutional framework for cryptocurrency regulation, Nigeria continues to face significant obstacles in controlling cryptocurrency-related financial crime. These obstacles arise from the structure of the regulatory system, the technological characteristics of digital assets, their international reach, differences between regulatory jurisdictions, institutional limitations and the vulnerability of users. These challenges are interconnected, but each presents a distinct problem requiring a specific regulatory response.

A major challenge is the fragmentation of regulatory responsibility among several institutions. Cryptocurrency activities can fall within the mandates of the Central Bank of Nigeria (CBN), Securities and Exchange Commission (SEC), Nigerian Financial Intelligence Unit (NFIU), Economic and Financial Crimes Commission (EFCC), tax authorities and security agencies. Although this institutional diversity reflects the multidimensional nature of cryptocurrency-related crime, it can also create uncertainty concerning responsibility for particular activities.

Another challenge is the technological structure of cryptocurrency presents a fundamentally different regulatory challenge from conventional financial activity. Blockchain networks can operate without a central administrator, while decentralized finance, smart contracts, cross-chain transactions and privacy-enhancing technologies continually expand the range of digital-asset activities requiring regulatory attention.

Cryptocurrency also challenges the territorial foundations of national regulation. A Nigerian user can transact with an exchange incorporated in another country, transfer assets through a globally distributed blockchain and

ultimately interact with a counterparty located elsewhere. The transaction may therefore involve several legal systems without requiring the physical movement of money across a national border.

A related but distinct challenge is regulatory arbitrage. Cryptocurrency businesses and users may take advantage of differences in national regulatory requirements by locating activities in jurisdictions where compliance obligations are less demanding. Criminal actors can similarly exploit these differences by routing transactions through platforms or jurisdictions with weaker AML/CFT controls. The problem is intensified by the ease with which digital businesses can provide services to users in other countries without establishing a substantial physical presence there. Consequently, a jurisdiction may impose stringent requirements on domestic operators while users continue to access comparable services through foreign platforms.

The existence of legislation does not automatically produce effective enforcement. Cryptocurrency investigations require specialized capabilities that differ from conventional financial investigations. Investigators must be able to identify wallet addresses, reconstruct transaction histories, connect digital addresses with real-world identities and preserve electronic evidence. Asset recovery presents an additional difficulty. Digital assets can be transferred rapidly, divided among several wallets or moved through multiple platforms. Where assets are located outside Nigeria, recovery may depend on foreign cooperation and the legal procedures applicable in the relevant jurisdiction.

Institutional resources are therefore critical. Regulators and law-enforcement agencies require adequately trained personnel, appropriate forensic tools and reliable technological infrastructure. The CBN's 2026 fintech assessment and recent Nigerian regulatory initiatives indicate growing recognition of the importance of artificial intelligence and blockchain analytics in financial-crime detection. However, technological acquisition must be accompanied by sustained institutional training and the development of specialist expertise.

Having an Effective Regulatory Model for Nigeria

The preceding analysis demonstrates that cryptocurrency regulation in Nigeria cannot be adequately assessed by asking whether digital assets should be permitted or prohibited. The more fundamental question is what kind of regulatory architecture is capable of controlling financial-crime risks while preserving the legitimate economic and technological functions of cryptocurrency. Nigeria's experience shows the limitations of a purely prohibitive approach. Restricting formal financial-sector access may reduce the visibility of cryptocurrency transactions without necessarily eliminating their existence. Users can migrate toward peer-to-peer arrangements, offshore platforms and informal channels, potentially making transactions more difficult for regulators to monitor. An effective regulatory model should therefore move beyond the binary opposition between prohibition and unrestricted liberalization. It should regulate cryptocurrency according to the activities undertaken, the functions performed and the risks generated. This requires an integrated framework in which licensing, AML/CFT obligations, blockchain intelligence, inter-agency cooperation, international collaboration and innovation policies operate as mutually reinforcing components. The central argument of this article is that Nigeria should adopt a risk-based, technology-responsive and institutionally coordinated model of cryptocurrency regulation. Such a model should distinguish legitimate digital-asset activity from conduct that presents significant risks of money laundering, terrorist financing, fraud, illicit financial flows and other forms of financial crime. At the same time, regulatory interventions should remain proportionate and consistent with privacy, property, due process and legitimate economic activity.

From Prohibition to Risk-Based Regulation

The first requirement of an effective regulatory model is a decisive movement from regulation based primarily on the technological identity of cryptocurrency toward regulation based on the nature, function and risk of the activity involved. Cryptocurrency is not a single homogeneous phenomenon. The risk associated with a regulated exchange, a stablecoin issuer, a custodial service, a blockchain-development enterprise, a decentralized application and an informal peer-to-peer transaction may differ considerably. A regulatory framework that treats all cryptocurrency activity as equally dangerous is therefore unlikely to be either effective or proportionate. The relevant question should be whether a particular activity creates identifiable risks and, if so, what regulatory measures are appropriate for controlling those risks. This functional approach

is consistent with the broader risk-based philosophy promoted by the Financial Action Task Force (FATF), under which countries are expected to identify, assess and mitigate risks associated with virtual assets and virtual-asset service providers (FATF, 2025).

For Nigeria, this means distinguishing between legitimate cryptocurrency activities and high-risk activities. A properly licensed exchange that performs KYC, maintains adequate records and reports suspicious transactions should not necessarily be subjected to the same regulatory treatment as an unregistered platform designed to facilitate anonymous transactions or evade AML/CFT requirements.

Strengthening AML/CFT Controls

The second pillar of an effective regulatory model is the strengthening of anti-money-laundering and counter-terrorist-financing controls. Nigeria's recognition of virtual-asset service providers within its AML/CFT framework represents an important development, but formal inclusion within the regulatory system must be accompanied by effective implementation. Enhanced customer due diligence should constitute a central requirement for higher-risk cryptocurrency activities. VASPs should be capable of establishing and verifying the identity of customers, understanding the nature and purpose of customer relationships and identifying circumstances that warrant enhanced scrutiny. Customer due diligence should not, however, be understood as a one-time exercise. Risk profiles can change as transaction behaviour changes, requiring continuous review.

Beneficial ownership identification is equally important. Cryptocurrency businesses may be structured through corporate entities, trusts or other arrangements that make it difficult to determine the natural persons who ultimately own or control an organization. Regulators should therefore require VASPs to establish and maintain reliable beneficial-ownership information and should ensure that such information can be made available to competent authorities in accordance with law. Suspicious transaction reporting should also be strengthened. The objective should not simply be to increase the number of reports submitted but to improve their quality, relevance and analytical usefulness. VASPs need clear guidance concerning cryptocurrency-specific indicators of suspicious activity, while the NFIU requires sufficient analytical capacity to transform reports into actionable financial intelligence.

Strengthening Blockchain Intelligence

The third pillar is the development of stronger blockchain intelligence and digital-forensics capacity. Traditional financial investigation techniques remain important, but they are insufficient on their own for investigating complex cryptocurrency transactions. The structure of blockchain transactions requires investigators to understand wallets, addresses, transaction histories, smart contracts, exchanges, cross-chain movements and other technological features. Nigeria should therefore make sustained investment in blockchain-analytics capabilities. Such systems can assist authorities in identifying transaction patterns, tracing the movement of digital assets, detecting links between apparently separate addresses and identifying transactions associated with known risk indicators. However, analytical technology should be treated as an investigative tool rather than as an automatic substitute for human judgment.

Digital-forensics capacity should also be strengthened. Investigators need the ability to preserve, authenticate and analyse digital evidence in ways that satisfy applicable legal standards. This includes evidence obtained from exchanges, devices, wallets, communications and blockchain records. The evidentiary chain connecting a digital asset to a particular individual or criminal activity must be established carefully rather than assumed merely because a suspicious transaction has been identified. The objective should be to create an institutional environment in which Nigerian authorities are not merely reacting to technological developments but possess sufficient expertise to anticipate emerging methods of financial crime.

Strengthening Inter-Agency Cooperation

No single Nigerian institution possesses all the powers or expertise necessary to regulate cryptocurrency effectively. The CBN, SEC, NFIU and EFCC occupy different positions within the regulatory and enforcement architecture, and their effectiveness depends partly upon their ability to exchange information and coordinate

their respective activities. A more effective model should therefore institutionalize cooperation among these agencies. Information concerning licensed VASPs, suspicious transactions, regulatory violations, criminal investigations and identified risk patterns should be capable of being shared through secure and legally authorized mechanisms.

The CBN can contribute banking and payment-system intelligence; the SEC can contribute information concerning licensed digital-asset operators and market activities; the NFIU can contribute financial intelligence and suspicious transaction analysis; and the EFCC can translate relevant intelligence into criminal investigation, prosecution and asset-recovery processes. The value of these functions is significantly increased when information can move efficiently across institutional boundaries.

Nigeria should consequently develop stronger information-sharing mechanisms, including interoperable databases where legally appropriate. Such systems should allow authorized agencies to obtain relevant information without creating unnecessary duplication or compromising data-protection safeguards. At the same time, coordination should preserve institutional accountability. Cooperation should not mean that statutory responsibilities become indistinguishable. Each agency should retain clearly defined powers while operating within a framework that facilitates timely information exchange and coordinated action.

International Cooperation

The transnational nature of cryptocurrency makes international cooperation indispensable. A Nigerian investigation may involve an exchange incorporated abroad, a wallet controlled from another jurisdiction, assets transferred across several blockchain networks and criminal proceeds ultimately converted through a foreign financial institution. Domestic regulation alone cannot adequately address such circumstances. Nigeria should therefore continue aligning its AML/CFT framework with relevant FATF standards concerning virtual assets and VASPs. International standards provide a common basis for customer due diligence, licensing and registration, supervision, suspicious transaction reporting and international cooperation (FATF, 2026).

Cooperation with foreign regulators should also be strengthened. Where an offshore VASP provides services to Nigerian residents or targets the Nigerian market, Nigerian authorities may require information concerning the operator, its beneficial owners, customers, transactions and compliance arrangements. Regulatory cooperation can facilitate the lawful exchange of such information. Cross-border financial-intelligence sharing is equally important. The NFIU and relevant foreign financial-intelligence units should maintain effective channels for exchanging intelligence concerning suspicious cryptocurrency transactions. Such cooperation can assist in identifying international transaction patterns that would remain invisible if each jurisdiction examined only the transactions occurring within its own territory.

Mutual legal assistance should also be strengthened in cryptocurrency cases. Investigations may require foreign evidence, identification of persons, preservation of digital records, freezing of assets or enforcement of judicial orders. Efficient legal-assistance procedures can significantly improve the ability of Nigerian authorities to pursue proceeds that have moved outside the country.

An Integrated Model for Nigeria

The preceding dimensions should not operate as independent reforms. Their effectiveness depends upon their integration into a coherent regulatory model. A useful framework can therefore be understood as a chain: Risk Identification → Licensing and Registration → KYC/CDD → Beneficial Ownership Identification → Continuous Monitoring → Suspicious Transaction Reporting → Blockchain Intelligence → Financial Intelligence → Investigation → Prosecution/Enforcement → Asset Recovery. This chain should be supported horizontally by data protection, inter-agency cooperation, international cooperation, consumer protection and regulatory innovation.

The significance of this integrated approach is that financial-crime prevention does not occur at a single point in the cryptocurrency ecosystem. Licensing without supervision may create only formal compliance. KYC without transaction monitoring may identify customers without identifying suspicious conduct. Suspicious

transaction reporting without financial intelligence may produce large volumes of information without actionable results. Blockchain analytics without investigative expertise may produce leads without admissible evidence. Enforcement without asset recovery may punish offenders without effectively removing the economic benefits of crime. Nigeria therefore needs to understand cryptocurrency regulation as an ecosystem of mutually dependent controls rather than a collection of isolated rules. Each stage should reinforce the others, while weaknesses at one stage should be identified and corrected through feedback from the wider regulatory system.

CONCLUSION

The relationship between cryptocurrency and financial crime in Nigeria is complex. Cryptocurrency is not inherently criminal; rather, its technological characteristics, including pseudonymity, decentralization, speed and cross-border transferability, can be exploited for legitimate economic purposes as well as for money laundering, fraud, terrorist financing and other illicit financial activities. The central regulatory challenge is therefore to distinguish legitimate digital-asset activity from its criminal misuse. Nigeria has made significant progress in developing a regulatory framework for cryptocurrency. The transition from an initially restrictive approach toward a system involving licensing, supervision and AML/CFT obligations represents an important institutional development. The roles of the Central Bank of Nigeria, Securities and Exchange Commission, Nigerian Financial Intelligence Unit and Economic and Financial Crimes Commission provide important foundations for addressing cryptocurrency-related financial crime. However, the framework continues to face weaknesses arising from regulatory fragmentation, technological complexity, cross-border transactions, offshore operators, limited enforcement capacity and rapidly evolving digital-asset technologies. The analysis demonstrates that prohibition alone cannot effectively address cryptocurrency-related financial crime. Restrictive measures may limit cryptocurrency activity within the formal financial system without eliminating its use. Instead, users may move toward peer-to-peer transactions, informal markets or offshore platforms, thereby reducing regulatory visibility. A prohibition-centred approach can consequently displace rather than resolve the underlying risks.

The more appropriate approach is a risk-based regulatory model. Regulation should focus on the nature, function and risk of particular cryptocurrency activities rather than treating the technology itself as inherently problematic. Legitimate digital-asset businesses should be permitted to operate within a clearly defined regulatory environment, while high-risk activities and operators should be subjected to enhanced scrutiny and effective enforcement. Such differentiation would allow regulatory resources to be concentrated where the risks of financial crime are greatest.

The effectiveness of this approach depends upon the capacity of Nigerian institutions to work together and to employ appropriate technological tools. Rather than creating an ever-expanding collection of overlapping rules, Nigeria should strengthen the implementation of its existing framework through coordinated institutional action, effective AML/CFT supervision, blockchain intelligence, digital-forensics capacity and international cooperation. These measures should operate within appropriate safeguards for privacy, due process and legitimate economic activity.

The central argument of this article is therefore that Nigeria should regulate cryptocurrency ecosystems according to risk rather than prohibit them on the basis of technology. A proportionate, coordinated and technologically informed framework offers a more sustainable means of combating financial crime than blanket restriction. The objective should be to suppress the illicit use of cryptocurrency while preserving its legitimate contribution to financial innovation, economic activity and the development of Nigeria's emerging digital economy.

REFERENCES

1. Central Bank of Nigeria. 2017. Circular on Virtual Currency Operations in Nigeria. Abuja: Central Bank of Nigeria.
2. Central Bank of Nigeria. 2021. Letter to All Deposit Money Banks, Non-Bank Financial Institutions and Other Financial Institutions on Cryptocurrency Operations. Abuja: Central Bank of Nigeria.

3. Central Bank of Nigeria. 2023. Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers (VASPs). Abuja: Central Bank of Nigeria, December 22, 2023.
4. Central Bank of Nigeria. 2024. CBN Update: Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers. Abuja: Central Bank of Nigeria.
5. Economic and Financial Crimes Commission. Various years. Annual Reports and Publications. Abuja: Economic and Financial Crimes Commission.
6. Federal Republic of Nigeria. 1999. Constitution of the Federal Republic of Nigeria 1999 (as Amended). Abuja: Federal Government of Nigeria.
7. Federal Republic of Nigeria. 2022. Money Laundering (Prevention and Prohibition) Act, 2022. Abuja: Federal Government of Nigeria.
8. Federal Republic of Nigeria. 2023. Nigeria Data Protection Act, 2023. Abuja: Federal Government of Nigeria.
9. Federal Republic of Nigeria. 2025. Investments and Securities Act, 2025. Abuja: Federal Government of Nigeria.
10. Financial Action Task Force. 2019. Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF.
11. Financial Action Task Force. 2020. Virtual Assets Red Flag Indicators of Money Laundering and Terrorist Financing. Paris: FATF.
12. Financial Action Task Force. 2021. Updated Guidance for a Risk-Based Approach to Virtual Assets and Virtual Asset Service Providers. Paris: FATF.
13. Financial Action Task Force. 2023. Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Paris: FATF.
14. Financial Action Task Force. 2024. Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Paris: FATF.
15. Financial Action Task Force. 2026. Targeted Update on Implementation of the FATF Standards on Virtual Assets and Virtual Asset Service Providers. Paris: FATF.
16. International Monetary Fund. 2021. Global Financial Stability Report: COVID-19, Crypto Assets and Financial Stability. Washington, DC: International Monetary Fund.
17. International Monetary Fund. 2023. Global Financial Stability Report: Safeguarding Financial Stability amid Tightening Conditions. Washington, DC: International Monetary Fund.
18. Nigerian Financial Intelligence Unit. 2022. National Inherent Risk Assessment of Money Laundering in Nigeria. Abuja: Nigerian Financial Intelligence Unit.
19. Nigerian Financial Intelligence Unit. 2022. National Inherent Risk Assessment of Terrorist Financing in Nigeria. Abuja: Nigerian Financial Intelligence Unit.
20. Nigerian Financial Intelligence Unit. 2022. National Inherent Risk Assessment of Proliferation Financing in Nigeria. Abuja: Nigerian Financial Intelligence Unit.
21. Nigerian Financial Intelligence Unit. 2022. National Inherent Risk Assessment of Legal Persons and Legal Arrangements in Nigeria. Abuja: Nigerian Financial Intelligence Unit.
22. Securities and Exchange Commission. 2020. Statement on Digital Assets and Their Classification and Treatment. Abuja: Securities and Exchange Commission, Nigeria.
23. Securities and Exchange Commission. 2022. Rules on Issuance, Offering Platforms and Custody of Digital Assets. Abuja: Securities and Exchange Commission, Nigeria.
24. Securities and Exchange Commission. 2024. Accelerated Regulatory Incubation Programme (ARIP) Framework. Abuja: Securities and Exchange Commission, Nigeria.
25. Securities and Exchange Commission. 2025. Digital and Virtual Asset Regulatory Framework and Related Regulatory Materials. Abuja: Securities and Exchange Commission, Nigeria.
26. Securities and Exchange Commission. 2026. Public Notice on Unregistered Online Investment Schemes. Abuja: Securities and Exchange Commission, May 2026.
27. United Nations Office on Drugs and Crime. 2021. Cryptocurrency and Criminality: Money Laundering, Terrorist Financing and Other Illicit Uses of Virtual Assets. Vienna: United Nations Office on Drugs and Crime.
28. World Bank. 2022. The Global Findex Database 2021: Financial Inclusion, Digital Payments, and Resilience in the Age of COVID-19. Washington, DC: World Bank.