



An Assessment of the Impact of Cryptocurrency on Terrorism Financing in Nigeria

By

PRINCEWILL Okwara, Ph.D

**Department of Political Science & International Relations,
Nile University of Nigeria, Abuja
&**

NJOKU Hyacinth Tochukwu, Ph.D

Miva Open University, Nigeria

&

EMMANUEL Ochogwu

Nile University of Nigeria, Abuja

Abstract

This study assesses the impact of cryptocurrency on terrorism financing in Nigeria focusing on the growing use of digital financial technologies and their implications for national security. The rapid adoption of cryptocurrencies has transformed financial transactions globally, offering efficiency and innovation while also creating new avenues for illicit financial activities. In Nigeria, concerns have emerged regarding the potential exploitation of cryptocurrencies by terrorist groups and criminal networks to facilitate terrorism financing and evade regulatory oversight. The objectives of the study are to examine the extent to which cryptocurrencies are used in financing terrorist activities in Nigeria, identify vulnerabilities within the country's financial and regulatory systems, and evaluate the effectiveness of existing countermeasures. The study is anchored on Technology Determinism Theory, popularized by Marshall McLuhan in 1964, which emphasizes the role of technology in shaping social behavior and institutional responses. A mixed-method research design was adopted, drawing on both primary and secondary data sources, including interviews with officials from key regulatory institutions such as the Economic and Financial Crimes Commission, the Central Bank of Nigeria, and the Securities and Exchange Commission. Findings reveal that while cryptocurrencies are increasingly being considered as a tool for terrorism financing, they remain secondary to traditional cash-based methods in Nigeria. However, their anonymity, speed, and borderless nature present emerging security risks. The study concludes that strengthening regulatory frameworks, enhancing institutional capacity, and aligning national policies with the standards of the Financial Action Task Force are essential for effectively combating terrorism financing in the digital era.

Key Words: Cryptocurrency, Terrorism Financing, Digital Currency, Financial Crime.



1. Introduction

The emergence of cryptocurrency has significantly transformed the global financial system by introducing decentralized digital currencies that operate outside traditional banking structures. Cryptocurrencies, particularly Bitcoin and other blockchain based assets, enable fast, secure, and borderless transactions without the need for intermediaries. While these innovations have improved financial inclusion and efficiency, they have also created new challenges for governments and regulatory authorities, especially in relation to financial crimes and terrorism financing (Nakamoto, 2008; Böhme et al., 2015). The rapid growth of digital financial technologies has raised concerns about their potential misuse by criminal and terrorist organizations seeking to conceal financial transactions and evade detection (FATF, 2021).

Terrorism financing remains a major security challenge in Nigeria, particularly due to the activities of extremist groups such as Boko Haram and the Islamic State West Africa Province (ISWAP), which have relied on diverse funding sources, including ransom payments, illegal trade, and informal financial networks (Onuoha, 2014; United Nations Office on Drugs and Crime [UNODC], 2020). The evolving nature of financial technology has introduced additional channels through which terrorist organizations may obtain, transfer, and store funds. Consequently, the increasing adoption of cryptocurrency has attracted the attention of security agencies and financial regulators concerned about its potential role in facilitating illicit financial flows and undermining national security (Chainalysis, 2023).

The Nigerian government, through institutions such as the Central Bank of Nigeria, the Economic and Financial Crimes Commission, and the Securities and Exchange Commission, has implemented regulatory measures to address the risks associated with cryptocurrency transactions. For instance, the Central Bank of Nigeria issued directives in 2021 restricting financial institutions from facilitating cryptocurrency transactions, citing concerns about money laundering and terrorism financing (Central Bank of Nigeria, 2021). Despite these efforts, regulatory gaps, technological limitations, and inconsistencies in policy frameworks continue to hinder effective monitoring and control of cryptocurrency-related activities in Nigeria (Financial Action Task Force [FATF], 2022). Between 2019 and 2025, Nigeria witnessed significant digital transformation in financial services alongside persistent security threats related to terrorism and cybercrime. This period was marked by increased public debate



over cryptocurrency regulation and the need to balance technological innovation with national security considerations. The global and decentralized nature of cryptocurrency transactions has made it increasingly necessary to assess their implications for counter-terrorism financing and financial governance (Kethineni & Cao, 2020). Therefore, this study seeks to assess the impact of cryptocurrency on terrorism financing in Nigeria between 2019 and 2025 by examining the extent of cryptocurrency usage in terrorist financing, identifying vulnerabilities within Nigeria's financial and regulatory systems, and evaluating the effectiveness of existing countermeasures. The findings of this study are expected to contribute to policy development, academic discourse, and national security strategies aimed at strengthening Nigeria's response to emerging financial crimes in the digital age.

1.2 Research Questions

From the statement of problem, this article provide answer to the following research questions.

- i. To what extent are cryptocurrencies used in financing terrorism in Nigeria?
- ii. What vulnerabilities exist within Nigeria's financial and regulatory systems that may facilitate the use of cryptocurrencies for terrorism financing?
- iii. How effective are the existing countermeasures implemented by regulatory and security agencies in combating cryptocurrency-related terrorism financing in Nigeria?

1.3 Research Objectives

- i. To examine the extent to which cryptocurrencies are used in financing terrorism in Nigeria.
- ii. To identify and analyze the vulnerabilities within Nigeria's financial and regulatory systems that may enable the misuse of cryptocurrencies for terrorism financing.
- iii. To evaluate the effectiveness of countermeasures adopted by relevant institutions such as the Central Bank of Nigeria and the Economic and Financial Crimes Commission in addressing cryptocurrency-related terrorism financing.



1.3. Conceptual Analysis: Cryptocurrency and Terrorist Financing

Cryptocurrencies have increasingly been exploited by terrorist groups for illicit activities, such as drug and weapons trading on black markets. A notable example is the dark web platform “Fund the Islamic Struggle without Leaving a Trace”, which facilitates the anonymous transfer of Bitcoin to jihadist organizations. Extremists have even authored publications like Bitcoin wa Sadaqat al Jihad, which provides detailed instructions on how to send Bitcoin from North America and Western Europe to jihadists (Weimann, 2016). In one high-profile case, Bahrin Naim, the mastermind behind the 2016 Jakarta terrorist attacks, reportedly used Bitcoin to finance militant operations (Hasbi & Mahzam, 2018).

The Islamic legal perspective on cryptocurrencies remains unclear. National sharia authorities have yet to establish definitive rulings on the permissibility of cryptocurrencies. Although global Islamic finance institutions offer guidance, they lack the authority to enforce standards. Consequently, many Muslim-majority governments remain hesitant torn between the fear of financial instability and the desire to harness the benefits of emerging technologies (Al Jazeera, 2018). This ambiguity has led to the partial acceptance of cryptocurrencies as alternatives to conventional financial systems among certain Muslim populations. Further illustrating this trend, a U.S. teenager in 2015 admitted to instructing Islamic State supporters on how to create Bitcoin wallets and use privacy-enhancing tools like 'dark wallet' to shield transactions (Irwin & Milad, 2016). The Islamic State has also reportedly used Bitcoin for ransom payments after kidnapping Europeans in Syria (Teichmann, 2018). Additionally, terrorists have employed cryptocurrencies in blackmail schemes, including threats to disclose sensitive data unless payments of up to 1,000 BTC were made (Hampton & Baig, 2015). Other incidents include a failed ransomware attack on the Lincoln Group in 2016, and threats against three Greek banks in 2015 demanding hundreds of thousands of euros in Bitcoin (Brown, 2016).

Global Overview of Cryptocurrency Use and Its Extent in Terrorism Financing

Cryptocurrencies have emerged as a transformative force in the global financial system, enabling secure, fast, and decentralized transactions without reliance on traditional banking institutions. Since the introduction of Bitcoin in 2009, digital currencies have grown exponentially, both in terms of market capitalization and user adoption, with thousands of cryptocurrencies now in circulation (Böhme et al., 2015). This global adoption has been driven



by the promise of financial inclusion, reduced transaction costs, cross-border transfers, and blockchain-based transparency. However, alongside these benefits, the anonymity, decentralization, and borderless nature of cryptocurrencies have created potential avenues for illicit activities, including money laundering, cybercrime, and terrorism financing (FATF, 2021). Globally, terrorist organizations have begun exploring cryptocurrencies as alternative funding mechanisms, though the extent of their usage varies widely across regions. For example, research indicates that extremist groups in the Middle East, such as ISIS, experimented with Bitcoin and other digital assets to fund operations and procure resources, leveraging peer-to-peer networks and online fundraising campaigns (Weimann, 2016). Similarly, in Europe and North America, law enforcement agencies have documented cases where cryptocurrencies were used to facilitate donations to extremist groups through online crowdfunding platforms, social media, and privacy-enhancing digital currencies such as Monero and Zcash (Europol, 2020; Chainalysis, 2023).

Despite these instances, studies show that cryptocurrencies remain a secondary tool for terrorism financing globally. Traditional methods, such as cash transfers, informal hawala networks, smuggling, and trade-based money laundering, continue to dominate due to accessibility and established operational networks (UNODC, 2020). Nevertheless, the global trend indicates an increasing awareness and experimentation by terrorist actors with cryptocurrencies, primarily because digital assets provide anonymity, speed, and borderless transferability features that can help circumvent traditional financial monitoring and regulatory controls. International regulatory bodies, including the Financial Action Task Force, have recognized the potential misuse of cryptocurrencies and have issued guidance to member countries to implement Anti-Money Laundering (AML) and Counter-Terrorism Financing (CTF) measures. This includes requiring cryptocurrency exchanges to comply with “know-your-customer” (KYC) regulations, reporting suspicious transactions, and enhancing blockchain forensics to track illicit financial flows (FATF, 2022).

Cryptocurrency Use and Terrorism Financing in Nigeria

In Nigeria, the adoption of cryptocurrencies has grown rapidly over the past decade, driven by increased smartphone penetration, internet accessibility, and a growing digital economy. According to Chainalysis (2023), Nigeria consistently ranks among the top countries globally for peer-to-peer cryptocurrency transactions, with Bitcoin, Ethereum, and USDT (Tether)



being the most widely used digital assets. The decentralized and borderless nature of these currencies has made them attractive for legitimate purposes such as remittances, e-commerce, and investment. However, these same features also present potential vulnerabilities for illicit activities, including money laundering, fraud, and terrorism financing. Terrorism financing in Nigeria remains a critical security concern, particularly in the North-East region, where extremist groups such as Boko Haram and the Islamic State West Africa Province (ISWAP) operate. These groups rely on multiple funding sources, including ransom payments from kidnappings, illegal trade, donations from sympathetic networks, and informal financial systems such as hawala or underground banking (Onuoha, 2014; UNODC, 2020). Between 2019 and 2025, there has been growing concern that cryptocurrency could supplement these traditional funding mechanisms, offering terrorists anonymity, speed, and cross-border transferability that cash-based methods cannot provide.

Evidence from Nigerian regulatory and security agencies indicates that cryptocurrencies have been used sporadically in terrorism financing. Officials from the Economic and Financial Crimes Commission and the Securities and Exchange Commission reported ongoing investigations where digital wallets were linked to individuals or networks suspected of financing extremist activities. However, hard evidence admissible in Nigerian courts remains limited, highlighting challenges in tracking and prosecuting cryptocurrency-related offenses. Cybersecurity experts further note that while cryptocurrencies are not yet the primary method for terrorism financing, they are increasingly explored by illicit actors seeking to evade regulatory oversight (CBN, 2021; FATF, 2022). The Nigerian government has implemented measures to regulate cryptocurrency usage and combat financial crimes. For instance, the Central Bank of Nigeria in 2021 issued directives restricting banks and financial institutions from facilitating cryptocurrency transactions. Simultaneously, the Securities and Exchange Commission has sought to develop licensing frameworks for crypto exchanges to promote compliance while supporting innovation. Despite these efforts, inconsistencies in policy, limited technological capacity, and the cross-border nature of cryptocurrency transactions continue to hinder effective monitoring and enforcement (Chainalysis, 2023; FATF, 2022). Overall, the period from 2019 to 2025 demonstrates a complex intersection between digital financial innovation and national security in Nigeria. Cryptocurrencies remain a secondary channel for terrorism financing compared to cash-based networks, but their anonymity and



global reach pose emerging risks that require proactive regulation, technological capacity building, and inter-agency cooperation to prevent misuse by terrorist and criminal actors.

1.4 Theoretical Framework: Technology Determinism Theory (TDT)

This study adopts Technology Determinism Theory (TDT) as its theoretical foundation to examine the impact of cryptocurrency on terrorism financing in Nigeria. Technology Determinism Theory, popularized by Marshall McLuhan in 1964, posits that technological innovations are the principal drivers of societal change and human behavior. According to TDT, technology is not merely a tool used by society; rather, it shapes social structures, institutions, and the ways people interact, often in ways that are independent of human intention (McLuhan, 1964; Smith & Marx, 1994). In the context of this study, cryptocurrencies represent a disruptive technological innovation that has altered traditional financial systems. Their characteristics decentralization, anonymity, speed, and cross-border transferability have created new possibilities for financial transactions while simultaneously introducing risks related to illegal activities, including terrorism financing. By applying TDT, the study emphasizes how the emergence and adoption of digital currency technology can influence social behavior and institutional practices, potentially enabling terrorist organizations to exploit these systems for illicit financial flows.

The theory also provides a lens through which to understand the responses of regulatory and security institutions in Nigeria. As technology advances, institutions such as the Central Bank of Nigeria, the Securities and Exchange Commission, and the Economic and Financial Crimes Commission must adapt their policies and enforcement strategies to the evolving technological environment. TDT thus supports the analysis of both the enabling effects of cryptocurrency technology on terrorism financing and the institutional adaptations aimed at mitigating associated risks. In summary, Technology Determinism Theory is appropriate for this study because it explains how technological innovation in this case, cryptocurrency can independently drive changes in behavior, social interaction, and institutional responses, all of which are critical to understanding the emergence and regulation of cryptocurrency-based terrorism financing in Nigeria.



Cryptocurrency and terrorism financing in Nigeria

The rise of cryptocurrencies has fundamentally altered the global financial landscape, providing a decentralized, digital, and borderless means of transferring value. Cryptocurrencies, such as Bitcoin, Ethereum, and Tether (USDT), are secured through blockchain technology, allowing for peer-to-peer transactions without the need for traditional financial intermediaries (Böhme et al., 2015). These features particularly decentralization, speed of transfer, and relative anonymity make cryptocurrencies attractive not only for legitimate purposes, such as investment, remittances, and e-commerce, but also for illicit activities, including money laundering, cybercrime, and terrorism financing (FATF, 2021). In Nigeria, the adoption of cryptocurrencies has grown rapidly due to high smartphone penetration, increasing internet access, and interest in alternative investment opportunities. According to Chainalysis (2023), Nigeria consistently ranks among the top countries in peer-to-peer cryptocurrency trading, reflecting both the growing digital economy and the accessibility of cryptocurrencies to the general population. This digital transformation presents both opportunities and risks, especially as terrorist organizations seek new ways to fund their operations.

While cash-based transactions and informal financial networks such as hawala and underground banking remain the predominant methods for terrorism financing in Nigeria, evidence suggests that cryptocurrencies are gradually being explored as supplementary channels. Reports from the Economic and Financial Crimes Commission and the Securities and Exchange Commission indicate ongoing investigations where digital wallets have been linked to suspected terrorist groups. These cases highlight that terrorist actors recognize the potential of cryptocurrencies to provide anonymity, rapid cross-border transfers, and reduced reliance on intermediaries, which can circumvent traditional monitoring mechanisms (CBN, 2021). However, the extent of cryptocurrency adoption for terrorism financing in Nigeria remains limited. Several factors contribute to this: first, many terrorist groups lack the technical expertise to manage digital currencies securely and convert them into cash for operational use. Second, regulatory restrictions, such as the Central Bank of Nigeria's 2021 directive prohibiting banks from facilitating cryptocurrency transactions, have constrained the integration of digital currencies into mainstream financial channels. Third, cryptocurrency exchanges operating within Nigeria are increasingly subject to oversight and reporting requirements, limiting the ease with which illicit actors can use these platforms (FATF, 2022).



Despite these limitations, cryptocurrencies are increasingly recognized as a potential threat to national security due to their ability to bypass traditional financial oversight. The decentralized and pseudonymous nature of digital currencies makes it difficult for authorities to trace transactions, identify beneficiaries, or freeze assets once funds are moved across borders. Experts in cybersecurity and financial intelligence note that while cryptocurrencies are not yet the primary method of terrorism financing in Nigeria, they are likely to become more attractive to terrorist networks as adoption grows and new technologies (e.g., privacy coins and decentralized finance platforms) expand the options for covert fund transfers (Onuoha, 2014; UNODC, 2020). Cryptocurrencies currently serve as a secondary but emerging channel for terrorism financing in Nigeria. Their adoption reflects broader global trends in digital finance and the need for terrorist organizations to explore innovative funding mechanisms. The extent of their use is still constrained by technical, operational, and regulatory challenges, yet the potential for exploitation continues to grow. This underscores the importance of continuous monitoring, strengthened regulatory frameworks, technological capacity building, and inter-agency collaboration to prevent terrorist actors from exploiting cryptocurrencies to fund extremist activities.

Analyzing Vulnerabilities within Nigeria's Financial and Regulatory Systems Enabling Cryptocurrency Misuse for Terrorism Financing

One of the critical objectives of this study is to identify and analyze the vulnerabilities within Nigeria's financial and regulatory systems that may facilitate the misuse of cryptocurrencies for terrorism financing. Despite efforts by regulatory agencies such as the Central Bank of Nigeria (CBN), the Securities and Exchange Commission (SEC), and the Economic and Financial Crimes Commission (EFCC), several structural and operational weaknesses persist.

i. Regulatory Fragmentation: Nigeria's cryptocurrency regulatory environment is marked by conflicting policies. While the CBN has prohibited banks and financial institutions from facilitating cryptocurrency transactions (CBN, 2021), the SEC has encouraged the development of licensing frameworks for cryptocurrency exchanges. This lack of harmonization creates loopholes that can be exploited by illicit actors. Terrorist networks could take advantage of regulatory ambiguities to transfer or conceal funds across multiple platforms, undermining enforcement efforts (FATF, 2022).



ii. Limited Technological and Analytical Capacity: Effective monitoring of cryptocurrency transactions requires sophisticated blockchain analytics and cybersecurity expertise. Nigerian regulatory institutions face limitations in technological infrastructure and skilled personnel, reducing their ability to track suspicious transactions, identify wallet ownership, and trace funds moving across borders. This capacity gap creates vulnerabilities that may be exploited by actors seeking to use cryptocurrency for illicit purposes (Chainalysis, 2023).

iii. Informal Financial Systems: A significant portion of Nigeria's economy operates through informal financial networks, including hawala systems and peer-to-peer cryptocurrency platforms. These unregulated networks are difficult to monitor and can be used to launder funds or transfer resources discreetly. Terrorist organizations could exploit these informal channels, integrating them with cryptocurrency to obscure the origin and movement of funds (Onuoha, 2014; UNODC, 2020).

iv. Weak Cross-Border Oversight: Cryptocurrencies are inherently global and borderless. Nigeria's regulatory institutions face challenges in coordinating with international counterparts, limiting the tracking of illicit transfers across jurisdictions. Weak cross-border cooperation and inadequate data sharing exacerbate vulnerabilities, allowing terrorist actors to move funds undetected (FATF, 2021).

v. Evolving Methods of Illicit Actors: Terrorist groups continuously innovate to exploit weaknesses in financial systems. The adoption of privacy coins, decentralized finance (DeFi) platforms, and crypto mixers allows them to further conceal transactions. These technological developments outpace current regulatory capabilities, highlighting the need for adaptive and proactive policy measures (Chainalysis, 2023).

Evaluating the Effectiveness of Countermeasures Adopted by Nigerian Institutions in Addressing Cryptocurrency-Related Terrorism Financing

A critical objective of this study is to evaluate the effectiveness of countermeasures implemented by Nigerian regulatory and enforcement institutions, particularly the Central



Bank of Nigeria (CBN) and the Economic and Financial Crimes Commission (EFCC), in combating the potential misuse of cryptocurrencies for terrorism financing.

i. Regulatory Measures by the Central Bank of Nigeria: In 2021, the CBN issued a directive prohibiting banks and other financial institutions from facilitating cryptocurrency transactions. The objective was to prevent the use of digital currencies for money laundering, terrorism financing, and other illicit activities (CBN, 2021). This measure had the immediate effect of limiting the entry points through which cryptocurrencies could be converted into fiat currency via regulated channels. By restricting access to mainstream banking infrastructure, the CBN aimed to reduce the risk of terrorist groups exploiting crypto for funding operations. However, this approach has limitations: it primarily targets formal financial institutions while leaving peer-to-peer (P2P) transactions and decentralized exchanges largely unregulated, which are increasingly popular channels in Nigeria (Chainalysis, 2023).

ii. Enforcement and Investigations by the EFCC: The EFCC has undertaken investigations into cryptocurrency wallets linked to suspected terrorist networks and illicit financial activities. The agency has leveraged intelligence gathering, monitoring of suspicious transactions, and collaboration with domestic financial institutions to identify potential cases of cryptocurrency misuse (EFCC, 2022). These enforcement actions demonstrate a proactive approach to detecting and disrupting illegal financing. Nonetheless, challenges persist due to the pseudonymous nature of digital assets, limited blockchain analytics capacity, and the difficulty of securing admissible evidence for prosecution in Nigerian courts.

iii. Coordination and Policy Gaps: While both the CBN and EFCC have made strides in countering cryptocurrency misuse, the effectiveness of their measures is affected by regulatory fragmentation and limited inter-agency coordination. Conflicting policies between the CBN, which restricts cryptocurrency, and the SEC, which licenses exchanges, create gaps that can be exploited by illicit actors. Additionally, the lack of formalized data sharing and collaboration with international financial intelligence units limits the ability to track cross-border transactions associated with terrorism financing (FATF, 2022).



iv. Capacity Building and Technological Limitations: Efforts to enhance the technical capabilities of enforcement agencies have begun, including training personnel in blockchain forensics and adopting monitoring software. However, these initiatives are still insufficient to keep pace with the rapidly evolving cryptocurrency ecosystem. Terrorist networks can exploit newer technologies, including privacy coins and decentralized finance platforms that evade traditional surveillance methods (Chainalysis, 2023).

1.5. Conclusion and Recommendations

Strengthening Regulatory and Legal Frameworks: The Nigerian government should establish and continuously update comprehensive regulations governing cryptocurrency operations to address emerging risks associated with terrorism financing. Regulatory agencies such as the Central Bank of Nigeria (CBN) should ensure strict compliance with licensing, monitoring, and reporting requirements for cryptocurrency exchanges and digital financial service providers.

Enhancing Institutional Capacity and Technological Capability: Security and financial regulatory bodies, including the Economic and Financial Crimes Commission (EFCC) and the Nigerian Financial Intelligence Unit (NFIU), should invest in advanced digital forensic tools, blockchain analytics systems, and specialized training for personnel to improve their ability to detect, investigate, and prevent cryptocurrency-related terrorism financing.

Promoting National and International Collaboration: Nigeria should strengthen collaboration among domestic agencies and international partners to enhance intelligence sharing and coordinated responses to terrorism financing. Cooperation with global regulatory bodies such as the Financial Action Task Force (FATF) will help Nigeria align its policies with international standards and improve the effectiveness of counter-terrorism financing measures.

References

AbdulMalik Oladipupo, A. O. (2025). *Cryptocurrency, terrorism financing, and the dark web: An exploratory study of the role of anonymous transactions in supporting terrorist activities*. *African Journal of Stability and Development (AJSD)*, 17(2), 971–988. <https://doi.org/10.53982/ajsd.2025.1702.09-j>



Anggriawan, R., & Susila, M. E. (2024). *Cryptocurrency and its nexus with money laundering and terrorism financing within the framework of FATF recommendations*. *Novum Jus*, 18(2), 249–277. <https://doi.org/10.14718/NovumJus.2024.18.2.10>

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of Economic Perspectives*, 29(2), 213–238. <https://doi.org/10.1257/jep.29.2.213>

Boyode, F. E. (2024). *Evaluating Nigeria's cryptocurrency regulatory framework: Pathway to boosting investors' confidence* (Unpublished manuscript). SSRN. <https://papers.ssrn.com/sol3/Delivery.cfm/4956760.pdf?abstractid=4956760&mirid=1>

Central Bank of Nigeria. (2021). *Circular on cryptocurrency and financial institutions operations*. CBN. <https://www.cbn.gov.ng>

Chitimira, H., & Animashaun, O. (2023). The adequacy of the legal framework for combating money laundering and terrorist financing in Nigeria. *Journal of Money Laundering Control*, 26, 110–126. <https://doi.org/10.1108/jmlc-12-2022-0171>

Dawodu-Sipe, O. A. (2025). *The role of cryptocurrency in terrorism financing: The Nigerian context*. *Journal of Commercial and Property Law*, 12(1). <https://journals.unizik.edu.ng>

EFCC. (2022). *Annual report on financial crimes and investigations in Nigeria*. Economic and Financial Crimes Commission. <https://www.efccnigeria.org>

FATF. (2021). *Virtual assets and virtual asset service providers*. Financial Action Task Force. <https://www.fatf-gafi.org/publications>

FATF. (2022). *Guidance for a risk-based approach to virtual assets and virtual asset service providers*. Financial Action Task Force. <https://www.fatf-gafi.org>

International Monetary Fund. (2025). *Regulating the crypto market in Nigeria* (Selected Issues Paper No. 096). IMF. <https://www.imf.org/en/Publications/selected-issues-papers/Issues/2025/07/11/Regulating-the-Crypto-Market-in-Nigeria-568580>



Onuoha, F. C. (2014). *Terrorism and security in Nigeria: Boko Haram and the state response*. Al Jazeera Centre for Studies.

Peters, T. Y. S., Oladeji, F. O., & Lawal, Q. A. (2022). *Anti-money laundering and combating the financing of terrorism: Is the accounting system effective? SADI International Journal of Management and Accounting*. <https://sadijournals.org/index.php/SIJMA/article/view/977>

Udenta, S. C. (2024). *Overview of terrorist financing in Nigeria: Legal and institutional framework for combating terrorism financing*. SSRN. <https://papers.ssrn.com/sol3/Delivery.cfm/4870234.pdf?abstractid=4870234&mirid=1>

UNODC. (2020). *Global report on terrorism financing trends*. United Nations Office on Drugs and Crime. <https://www.unodc.org>

Weimann, G. (2016). *Terrorism in cyberspace: The next generation*. Columbia University Press.