International Journal of Multidisciplinary Department
Published by: International Journal & Research Global Publisher
ISSN: 3108-2718

Research Article

Dismantling the Myth of Cryptocurrency as a Safe Haven for Illicit Wealth: Virtual Assets, Conflict Minerals, Terrorism Financing, and Grand Corruption, with Nigeria as a Global Case Study

Iyeru Godglory Oluwole

Independent Corrupt Practices and Other Related Offences Commission, Nigeria Polygraph Examiner

Email: oluwoleiyeru@gmail.com

Article History:
Received: 27 Oct 2026 | **Accepted:** 02 Nov 2026 | **Published:** 05 Nov 2026
DOI: https://doi.org/10.5281/zenodo.23969819

** *Related declarations are provided in the final section of this article.*

Abstract

Conventional wisdom among investigators, prosecutors, and the wider public holds that once illicit proceeds are converted into cryptocurrency, they effectively vanish beyond the reach of the state. This article challenges that assumption. Public blockchains are permanent, transparent ledgers; what criminals conceal is identity, not the movement of funds — a distinction properly understood as pseudonymity rather than anonymity, and one that trained investigators can routinely defeat through blockchain forensics, legal process, and international cooperation. Drawing on Nigeria as an in-depth case study, the article demonstrates that virtual-asset-enabled crime rarely operates in isolation. It is frequently embedded in a wider, converging criminal ecosystem that also encompasses illicit artisanal mineral extraction, armed banditry, terrorism financing, and grand corruption by politically exposed persons (PEPs) and senior public officers. Comparable convergences of conflict minerals, informal value-transfer systems, and virtual assets are documented in other jurisdictions, including the Sahel, suggesting the Nigerian pattern is an instance of a broader global phenomenon rather than a uniquely national one. The article reviews the relevant technology, forensic methodology, and international and Nigerian legal frameworks, and closes with policy recommendations for building investigative capacity, closing regulatory

This article is licensed under a Creative Commons Attribution 4.0 International License.

gaps between mineral and financial oversight, strengthening the PEP due-diligence regime, and deepening cross-border cooperation.

Keywords: cryptocurrency; blockchain forensics; terrorism financing; conflict minerals; politically exposed persons; anti-money laundering; Nigeria; FATF

1. Introduction

Across anti-corruption and law-enforcement circles internationally, a persistent and costly misconception has taken hold: that cryptocurrency offers criminals a permanent hiding place for stolen wealth. This belief discourages investigators from opening cases involving virtual assets, and it emboldens corrupt actors and armed groups to believe they have found an escape route from accountability.

The reality is the opposite. Public blockchains such as Bitcoin and Ethereum are, by design, permanent and transparent ledgers. Every transaction is timestamped, recorded, and viewable by anyone, indefinitely. What is concealed is not the transaction but the real-world identity behind a wallet address — properly described as pseudonymity rather than anonymity. Pseudonymity can be, and routinely is, defeated through a combination of technical analysis, legal process, and international cooperation. Cash, once it changes hands, leaves no trail; cryptocurrency leaves a trail that lasts forever and can be revisited years later with better tools, as demonstrated by United States authorities' 2022 recovery of billions of dollars in bitcoin stolen from the Bitfinex exchange in 2016 — traced and seized roughly six years after the theft using blockchain analytics that did not exist, or were far less mature, at the time of the crime (U.S. Department of Justice, 2022).

This article makes that case at two levels. First, it sets out, for an academic and policy audience, the technical foundation and investigative methodology needed to pursue virtual-asset-enabled corruption, money laundering, and terrorism-financing cases. Second, it examines Nigeria as a detailed case study of how virtual assets, illicit mineral extraction, terrorism financing, and elite corruption converge into a single criminal ecosystem rather than remaining separate problem areas. Nigeria is not sui generis in this respect. Comparable convergences of conflict minerals, informal value transfer, and digital finance are documented elsewhere — notably in the central Sahel, where gold mining increasingly finances jihadist groups linked to al-Qaeda and the Islamic State (Nsaibia, 2026; International Crisis Group, 2022) — which suggests the Nigerian evidence has wider explanatory value for how such ecosystems form and how they might be disrupted.

This article is licensed under a Creative Commons Attribution 4.0 International License.

2. Understanding the Technology: How Cryptocurrency Works

A firm grasp of the underlying technology is a precondition for meaningfully tracing illicit flows.

2.1 The Blockchain

A blockchain is a distributed, cryptographically secured ledger maintained simultaneously by thousands of independent computers ("nodes") worldwide, rather than by a single central authority such as a bank. New transactions are grouped into "blocks," cryptographically linked to the previous block, and validated through a consensus mechanism — historically "Proof of Work" (Bitcoin) or, increasingly, the more energy-efficient "Proof of Stake" (Ethereum and most newer networks). Once recorded, a block cannot be altered without redoing the computational work for every subsequent block across a majority of the network, which is what makes the ledger effectively immutable and permanently auditable.

2.2 Wallets, Keys, and Addresses

A cryptocurrency "wallet" does not store coins as a physical wallet stores cash; it stores cryptographic keys. A public key (or the address derived from it) is visible on the blockchain and functions like an account number; a private key is the secret credential that authorizes spending, comparable to a PIN or signature. Wallets are either custodial (held by a third party such as an exchange, which typically requires identification) or non-custodial/self-hosted (the user alone holds the keys). This distinction is critical for investigators: custodial wallets at regulated exchanges are where identity can most readily be attached to an address.

2.3 On-Ramps and Off-Ramps

Cryptocurrency becomes useful to an illicit actor only when it can be converted to or from something spendable in the real economy. The conversion points — centralized exchanges, peer-to-peer (P2P) platforms, over-the-counter (OTC) desks, and cryptocurrency ATMs — are the chokepoints where virtual assets meet identity, banking records, and regulatory obligations, and are consequently the single most important investigative target in almost every case.

2.4 Privacy-Enhancing Tools Investigators Must Understand

This article is licensed under a Creative Commons Attribution 4.0 International License.

- Mixers/Tumblers: services (e.g., historically Tornado Cash on Ethereum) that pool and scramble multiple users' funds to obscure the link between sender and recipient.
- Privacy coins: cryptocurrencies such as Monero and Zcash that use advanced cryptography to conceal sender, recipient, and amount by default, unlike Bitcoin or Ethereum, where transaction details are public.
- Chain-hopping and cross-chain bridges: moving value rapidly between different blockchains to break simple tracing heuristics.
- Decentralized exchanges (DEXs): peer-to-peer trading platforms that typically perform no identity verification, complicating attribution.
- Stablecoins (e.g., USDT, USDC): tokens pegged to a fiat currency, now the preferred vehicle for many launderers because they hold stable value — but also among the easiest to freeze, since issuers such as Tether and Circle can and do blacklist addresses at law enforcement's request.

A recurring theme in Nigerian terrorism-financing typologies is the specific preference of extremist financiers for Monero because of its enhanced privacy features, a pattern examined further in Section 5.

3. Blockchain Forensics: The Investigative Toolkit

3.1 Core Analytical Techniques

- Address clustering: grouping multiple addresses that behave as though controlled by a single entity, based on heuristics such as shared transaction inputs and predictable "change" address patterns.
- Fund-flow (taint) tracing: following the movement of specific coins across multiple hops, wallets, mixers, and swaps to their eventual destination — typically an exchange where they are converted to fiat or another asset.
- Entity attribution and tagging: cross-referencing addresses against databases of known exchanges, darknet markets, sanctioned entities, ransomware wallets, and previously identified criminal actors.
- Behavioural and temporal analysis: correlating the timing, size, and pattern of on-chain transactions with off-chain events (bank withdrawals, travel, communications) to build corroborating evidence.

This article is licensed under a Creative Commons Attribution 4.0 International License.

3.2 Tools of the Trade

Commercial blockchain-analytics platforms — Chainalysis (Reactor and KYT), Elliptic, TRM Labs, and CipherTrace among them — provide investigators with visual transaction-graphing, automated entity attribution, and risk-scoring capabilities. Access is often arranged through government grants, donor-funded capacity building, or direct licensing by a financial intelligence unit or anti-corruption agency. Where budgets are constrained, open-source and free tools remain valuable: public block explorers (Etherscan, Blockchain.com) and community-maintained clustering and visualization tools such as GraphSense and OXT. A credible national strategy should not assume every agency can afford commercial licenses, and should build baseline capability using open-source tools supplemented by targeted commercial access for complex cases.

3.3 Honest Limits

Analysts and prosecutors should be candid about the limits of forensic tracing. Privacy coins and well-implemented mixing services can defeat standard clustering heuristics. In these situations, technical analysis alone is often insufficient, and the case must be built through legal process — subpoenas, exchange KYC records, cooperating witnesses, and traditional financial and human intelligence — working from the known on-ramp or off-ramp inward, rather than attempting to force a technical breakthrough that may not exist.

4. Linking Virtual Assets to Fiat Currency and Traditional Bank Accounts

This is the step that determines whether a blockchain trace becomes a prosecutable case.

4.1 The FATF Travel Rule

Financial Action Task Force Recommendation 16 — commonly called the "Travel Rule" in its virtual-asset application — requires Virtual Asset Service Providers (VASPs) to collect, verify, and transmit originator and beneficiary information for transfers above USD/EUR 1,000, first extended to virtual assets in 2019. At its June 2025 Plenary, the FATF agreed further refinements, due to take effect by the end of 2030, that standardize the identity information (name, address, date of birth) required for cross-border peer-to-peer virtual-asset transfers and clarify where responsibility begins in the payment chain (FATF, 2025). This is the single most important international standard tying pseudonymous wallets to verified identity.

4.2 Practical Investigative Steps

This article is licensed under a Creative Commons Attribution 4.0 International License.

1. Identify the exchange or VASP through which funds entered or exited the blockchain (the on-ramp/off-ramp).
2. Issue a formal production order, subpoena, or — for foreign-headquartered exchanges — a Mutual Legal Assistance Treaty (MLAT) request or direct law-enforcement data request, seeking KYC records, IP logs, device fingerprints, and linked bank account or card details.
3. Correlate the timestamps and amounts of fiat deposits/withdrawals at the exchange with the timestamps and amounts of the on-chain transactions under investigation, to build a continuous fiat-to-crypto-to-fiat chain.
4. Where the exchange is domestic and licensed, engage the exchange's compliance and legal team directly for expedited voluntary account freezes pending formal process.
5. For stablecoins, contact the issuer (e.g., Tether, Circle) directly; issuers can and do blacklist specific addresses on legitimate law-enforcement request, effectively freezing the asset in place even before formal forfeiture proceedings conclude.

4.3 International Cooperation Channels

- Mutual Legal Assistance Treaties (MLATs) for compelling foreign-held exchange records and account information.
- The Egmont Group of Financial Intelligence Units, enabling rapid, informal FIU-to-FIU information sharing that can precede and support formal MLAT requests.
- Direct law-enforcement liaison relationships with major global exchanges' compliance and investigations teams, which frequently respond faster than treaty-based requests for urgent freezes.

5. The Nigerian Case: A Converging Criminal Ecosystem

Nigeria offers an unusually clear window onto how virtual assets, illicit minerals, terrorism financing, and elite corruption interact. These are frequently treated by investigators and the media as separate problem areas; the evidence reviewed below shows they are financially and operationally interlinked — and, as Section 5.6 discusses, structurally similar to convergences documented in other resource-rich, conflict-affected regions.

5.1 Nigeria's Cryptocurrency Landscape and Regulatory Evolution

Nigeria has one of the largest cryptocurrency user bases and peer-to-peer transaction volumes in the world, driven substantially by the naira's volatility and citizens' use of crypto as an inflation hedge and remittance tool. This scale is precisely why the space is attractive to launderers: high genuine transaction volume provides cover for illicit flows. The regulatory

This article is licensed under a Creative Commons Attribution 4.0 International License.

environment has shifted markedly: after the Central Bank of Nigeria's 2021 directive barring banks from servicing crypto exchanges, policy reversed course. The CBN's December 2023 VASP guidelines permitted banks to again serve licensed virtual-asset businesses, and the Investments and Securities Act 2025 formally classified digital assets as securities under Securities and Exchange Commission (SEC) oversight, requiring VASPs, Digital Asset Offering Platforms, and exchanges to obtain licenses and comply with KYC/AML obligations. By late 2025, the EFCC reported that roughly 40 virtual-asset platforms had been licensed in Nigeria, giving the Commission a growing capacity to trace registered wallets.

5.2 The Solid Minerals Sector: Illegal Gold Mining, Banditry, and Elite Complicity

Nigeria's solid minerals sector — particularly artisanal and small-scale gold mining concentrated in Zamfara, Katsina, Kaduna, and neighbouring North-West states — has become deeply entangled with organized armed banditry. An estimated 80 percent of mining activity in the North-West is conducted illegally on an artisanal basis, and gold from the region is routinely smuggled across the border into Niger and Togo. Gold's portability, high value-to-weight ratio, and difficulty of tracing once smuggled make it an ideal store and mover of illicit value, functioning in many respects as a parallel, physical "anonymity" system that complements digital laundering channels.

Research and public statements from Nigerian officials identify a troubling pattern of collusion between armed bandit groups and politically or institutionally connected elites. Nigeria's Minister of Solid Minerals stated in late 2024 that powerful individuals engaged in illegal mining were sponsoring banditry, while a sitting senator publicly alleged that retired senior security officers were coordinating illegal mining operations nationwide. Field research conducted in Katsina and Zamfara documented recurring accounts of collusion between bandits and elites, with a joint 2024 report by the Global Initiative Against Transnational Organised Crime and the Armed Conflict Location and Event Data Project finding that banditry-related deaths in Zamfara and Kaduna states between 2018 and 2023 exceeded 4,750 — surpassing fatalities attributable to violent extremist groups in Nigeria's North-East over the same window (GI-TOC & ACLED, 2024). Nigeria is estimated to lose over $9 billion annually to illegal mining activity, a meaningful share of it tied to the gold sector.

The federal government's 2019 suspension of mining activity in Zamfara, intended to cut off bandit financing, has had limited durable effect, underscoring that enforcement focused solely

This article is licensed under a Creative Commons Attribution 4.0 International License.

on the mine site — without dismantling the financial and elite-protection networks that monetize the gold — cannot succeed alone.

5.3 Terrorism Financing: The Crypto–Hawala–Gold Nexus

Nigeria's North-East insurgency, driven principally by Boko Haram and its offshoot, the Islamic State West Africa Province (ISWAP), has evolved a financing model that blends traditional and digital methods. Historic revenue sources — extortion, kidnapping for ransom, and the taxation of fishing, cattle, and agricultural trade in territory the groups influence — are increasingly supplemented by two channels of particular concern to financial investigators:

- Hawala and informal value-transfer systems, and bureaux de change, which move funds through networks of trust with minimal documentary trail. The United States Treasury sanctioned several Nigerian bureaux de change in 2026 for allegedly facilitating fund transfers linked to ISIS-West Africa, part of a wider international network also using cryptocurrency channels to move money to ISIS associates (OFAC, 2026).
- Direct solicitation and use of cryptocurrency — with Monero specifically favoured by ISWAP-affiliated financiers for its enhanced transaction privacy, mirroring a global pattern among Islamic State-linked networks that has seen affiliated propaganda channels openly solicit Monero donations on the dark web.

The Nigerian Financial Intelligence Unit's Typologies Report on Terrorism Financing in Nigeria (NFIU, 2023) documents these evolving methods across Boko Haram, ISWAP, and other militant and secessionist groups, and calls for stronger, coordinated detection measures across financial institutions and law enforcement. The practical implication for investigators is that a single financing network may simultaneously use gold smuggling, hawala transfers, and Monero — meaning an investigation confined to only one channel will systematically understate, and likely fail to disrupt, the group's true financial capacity.

5.4 Politically Exposed Persons and Senior Public Officers

Nigeria's Money Laundering (Prevention and Prohibition) Act 2022 significantly strengthened the country's framework for identifying and monitoring Politically Exposed Persons — defined broadly to include individuals who are or have been entrusted with prominent public functions, domestically or abroad, along with their close associates and immediate family members. The Act imposes mandatory enhanced due diligence, reporting to the Nigerian Financial Intelligence Unit (NFIU) and the Special Control Unit Against Money

This article is licensed under a Creative Commons Attribution 4.0 International License.

Laundering (SCUML), and strict thresholds and timelines for reporting large or cross-border transactions.

Despite this framework, senior public officers and their proxies continue to exploit gaps between traditional banking oversight and the newer virtual-asset ecosystem. The EFCC's own chairman disclosed in September 2026 that a case under investigation involved a local government transferring public funds to a private company, which then moved the funds into cryptocurrency wallets — funds that, once converted, could not be traced back to any tangible physical asset. The Commission further disclosed that some public officials now use young people as intermediary "fronts" to move stolen funds into and through crypto wallets, often within 24 hours of diversion, before eventually spending the proceeds abroad on real estate and luxury goods. In response, the Nigerian government approved a national confiscation wallet — dedicated infrastructure for the secure custody of virtual assets seized by law enforcement — addressing what had previously been an acknowledged accountability gap in handling confiscated digital assets, including proceeds recovered from the collapsed CBEX cryptocurrency investment scheme.

This pattern — rapid conversion of stolen public funds into crypto through intermediaries, followed by conversion to offshore assets — represents the clearest evidence that PEP-driven grand corruption in Nigeria has adapted to, rather than been deterred by, the growth of virtual assets, and that investigative capacity must adapt correspondingly.

5.5 Illustrative Enforcement Cases

- 2021: EFCC disclosed approximately $20 million in cryptocurrency recovered from cybercriminals, held in a dedicated agency e-wallet — an early acknowledgment that crypto proceeds of crime could be recovered, not merely written off.
- December 2024 / 2025: Following the arrest of 792 suspects (including 599 Nigerians and 193 foreign nationals) in a cryptocurrency investment and romance-fraud syndicate financed through a Nigerian-registered company, a Federal High Court in Lagos ordered interim and, in July 2025, final forfeiture of digital assets valued at approximately $222,729.86 in USDT.
- 2025: EFCC recoveries connected to the collapsed CBEX Ponzi scheme, in which investor losses were estimated as high as ₦1.3 trillion, illustrating both the scale of crypto-enabled fraud and the technical difficulty of converting recovered crypto assets back into usable fiat currency.

This article is licensed under a Creative Commons Attribution 4.0 International License.

• 2026: EFCC disclosure of a local-government-to-private-company-to-crypto-wallet diversion scheme, and the establishment of a national confiscation wallet for seized virtual assets — evidence of institutional adaptation to PEP-linked, crypto-enabled corruption.

5.6 Global Parallels: Beyond Nigeria

The Nigerian ecosystem is best understood as one instance of a broader pattern in which armed or extremist groups monetize conflict minerals alongside informal and digital financial channels. In the central Sahel, ACLED analysis of more than 1,000 mining-adjacent violent incidents between 2015 and mid-2026 found that nearly 90 percent occurred outside mining concessions, concentrated instead around transport routes, artisanal sites, and commercial hubs — evidence that armed groups value gold-producing regions for territorial control and revenue as much as for the mineral itself (Nsaibia, 2026). Groups affiliated with al-Qaeda, including Jama'at Nusrat al-Islam wal-Muslimin (JNIM), and with the Islamic State have been found to levy in-kind gold taxes on artisanal miners, using the proceeds to store wealth and purchase operational resources (Global Initiative Against Transnational Organized Crime, as cited in ADF, 2026). The International Crisis Group has similarly documented jihadist groups seizing or taxing gold-mining sites across Mali, Burkina Faso, and Niger since 2016, fuelled by the discovery of a trans-Saharan gold vein in 2012 (International Crisis Group, 2022).

The structural resemblance to the Nigerian case is notable: in both settings, weak state presence in mineral-rich peripheries, the portability and traceability challenges of gold, and the availability of informal or digital value-transfer channels combine to let armed actors convert extractive resources into operational financing with relative ease. This suggests that policy responses calibrated narrowly to a single jurisdiction or a single channel (mining interdiction alone, or financial-sector regulation alone) are unlikely to succeed anywhere in the region, and that the recommendations developed from the Nigerian case in Section 7 have relevance beyond Nigeria's borders.

6. Legal and Institutional Frameworks

6.1 International and Regional Standards

Instrument / Body	Relevance
FATF Recommendations 15	Global AML/CFT standards for virtual assets and VASPs,

This article is licensed under a Creative Commons Attribution 4.0 International License.

& 16	including the Travel Rule requiring identity data on transfers.
UNCAC	UN Convention Against Corruption — provisions on international cooperation and asset recovery applicable to proceeds moved through virtual assets.
Egmont Group	Global network enabling rapid, informal information sharing between Financial Intelligence Units, including Nigeria's NFIU.
GIABA	Inter-Governmental Action Group Against Money Laundering in West Africa — FATF-style regional body coordinating AML/CFT standards and mutual evaluations for Nigeria and its neighbours.
EU Transfer of Funds Regulation (TFR)	The European Union's implementation of the Travel Rule — a useful model for a harmonized national framework.

6.2 Nigerian Legal and Institutional Framework

Instrument / Agency	Relevance
Money Laundering (Prevention and Prohibition) Act, 2022	Repeals the 2011 Act; strengthens PEP identification and due diligence, mandates NFIU/SCUML reporting for transactions above ₦5m (individuals) / ₦10m (corporates), and shortens cross-border transfer reporting to one day.
Terrorism (Prevention and Prohibition) Act, 2022	Primary statute criminalizing terrorism financing, enforced jointly with the Money Laundering Act by the EFCC and NFIU.
Investments and Securities Act, 2025	Classifies digital assets as securities; requires VASPs, Digital Asset Offering Platforms, and exchanges to register and be licensed by the SEC.
NFIU Act, 2018	Establishes the Nigerian Financial Intelligence Unit as an autonomous agency for receiving, analyzing, and disseminating

This article is licensed under a Creative Commons Attribution 4.0 International License.

	financial intelligence.
EFCC / SCUML	Lead investigative and prosecutorial agency for economic and financial crimes, including crypto-enabled fraud and corruption; SCUML supervises designated non-financial businesses and professions.
CBN VASP Guidelines (Dec. 2023)	Permit licensed banks to again provide services to SEC-licensed virtual-asset businesses, reversing the 2021 blanket restriction.

Taken together, this framework gives Nigeria most of the statutory tools needed to pursue crypto-enabled corruption and terrorism-financing cases. The persistent gap, as the case evidence in Section 5 shows, lies less in legislation than in operational capacity: forensic tooling, inter-agency coordination, timely cross-border cooperation, and the technical sophistication of investigators relative to increasingly adaptive offenders.

Policy Recommendations

7.1 Building National Investigative Capacity

1. Establish or expand dedicated inter-agency crypto-asset task forces bringing together the EFCC, NFIU, SEC, CBN, the Nigeria Police Force, the Department of State Services, and the Nigerian Customs Service (for mineral-smuggling interdiction).
2. Institutionalize blockchain forensics training and certification for investigators and prosecutors, combining commercial-platform training (e.g., Chainalysis Reactor Certification) with open-source tool proficiency to ensure capability is not dependent on licensing budgets alone.
3. Operationalize and audit the national confiscation wallet announced in 2026, with clear custody, valuation, and disposal protocols to prevent the accountability gaps previously acknowledged by the EFCC.

7.2 Closing the Solid Minerals–Terrorism Financing Gap

1. Formalize artisanal and small-scale gold mining rather than relying solely on blanket suspensions, paired with mandatory buyer/exporter licensing and gold provenance documentation to interrupt the smuggling-to-arms pipeline.

This article is licensed under a Creative Commons Attribution 4.0 International License.

2. Extend financial investigation techniques — not just physical interdiction — to the elites and intermediaries alleged to be sponsoring or profiting from illegal mining, applying the same PEP due-diligence standards to any officials or retired security personnel implicated.

3. Integrate solid-minerals trade data with NFIU and EFCC financial intelligence to detect the layering of gold-smuggling proceeds into the formal banking and crypto systems.

7.3 Strengthening the PEP and Senior Public Officer Regime

1. Mandate that PEP due-diligence obligations under the 2022 Money Laundering Act explicitly extend to virtual-asset transactions and VASP-held accounts, not solely traditional bank accounts.

2. Require licensed Nigerian VASPs to implement real-time transaction monitoring keyed to politically exposed persons and known front-operator typologies (e.g., rapid transfer of public funds through intermediary companies into personal wallets).

3. Strengthen whistleblower protections for the young intermediaries reportedly recruited as crypto "fronts" by public officials, incentivizing early disclosure rather than prosecution-only enforcement.

7.4 Deepening International and Regional Cooperation

1. Formalize expedited information-sharing protocols with major global exchanges and stablecoin issuers to enable rapid freezing ahead of formal MLAT processes.

2. Strengthen Nigeria's engagement with GIABA and the Egmont Group to align typologies reporting and accelerate cross-border FIU requests, particularly for funds moved to neighbouring Niger, Togo, and beyond.

3. Pursue harmonized regional VASP licensing standards across the Economic Community of West African States (ECOWAS), and comparable coordination among Sahel and West African states more broadly, to prevent regulatory arbitrage in which illicit actors simply route transactions through the least-regulated jurisdiction.

7.5 Public Communication and Research

1. Sustain public and institutional communication efforts — of which this article is a part — to retire the myth that cryptocurrency provides permanent impunity, both to deter prospective offenders and to build political and judicial confidence in pursuing crypto-asset recovery cases.

2. Encourage comparative research examining whether the mineral–terrorism–crypto convergence documented in Nigeria and the Sahel is replicated in other conflict-affected,

This article is licensed under a Creative Commons Attribution 4.0 International License.

resource-rich regions, to build a stronger evidentiary base for regional and international policy design.

8. Conclusion

Cryptocurrency is not a permanent hiding place for looted funds — it is a forensic goldmine for investigators equipped with the right knowledge, tools, and legal process. The Nigerian case demonstrates that virtual assets do not operate in isolation from other established vectors of grand corruption and instability: they are intertwined with illegal gold mining and banditry in the North-West, with terrorism financing by Boko Haram and ISWAP in the North-East, and with the diversion of public funds by politically exposed persons and senior public officers across the country. Similar convergences of conflict minerals, informal finance, and digital assets in the Sahel indicate that this is not a uniquely Nigerian pathology but a pattern with regional and potentially global relevance. Treating these as a single, converging criminal ecosystem — rather than as separate silos — is essential to any effective response, in Nigeria and beyond.

With updated legislation already in place, a maturing regulatory framework for virtual-asset service providers, and a growing body of successful recovery cases, Nigeria has the foundation needed to lead on this issue regionally. What remains is sustained investment in technical capacity, inter-agency coordination, and international cooperation to convert that foundation into consistent enforcement outcomes — and to permanently retire the myth that once stolen funds enter the crypto world, they are gone forever.

Article Publication Details

This article is published in the **International Journal of Multidisciplinary Department**, **ISSN 3108-2718 (Online).** In Volume 2 (2026), Issue 6 Nov-Dec)

The journal is published and managed by **IJRGP**.

Acknowledgements

We sincerely thank the editors and the reviewers for their valuable suggestions on this paper.

References

1. Armed Conflict Location & Event Data Project (ACLED), & Global Initiative Against Transnational Organised Crime (GI-TOC). (2024). Report on banditry-related fatalities in Zamfara and Kaduna states, 2018–2023.
2. Africa Defense Forum (ADF). (2026). Control of gold mines fuels Sahel terrorism.

This article is licensed under a Creative Commons Attribution 4.0 International License.

3. Central Bank of Nigeria. (2023, December). VASP guidelines.
4. Economic and Financial Crimes Commission (EFCC). (2021–2026). Public statements and press releases, including disclosures on cryptocurrency recovery, the CBEX case, and the national confiscation wallet.
5. Federal Republic of Nigeria. (2022). Money Laundering (Prevention and Prohibition) Act.
6. Federal Republic of Nigeria. (2022). Terrorism (Prevention and Prohibition) Act.
7. Federal Republic of Nigeria. (2025). Investments and Securities Act.
8. Financial Action Task Force (FATF). (2025). Recommendation 16 and updated guidance for a risk-based approach to virtual assets and VASPs; June 2025 Plenary outcomes.
9. HumAngle, & Africa Defense Forum (ADF). (2025). Reporting on Boko Haram/ISWAP financing typologies, including cryptocurrency (Monero) solicitation and hawala usage.
10. Institute for Security Studies (ISS) / ENACT Africa. (n.d.). Research on illegal mining, banditry, and elite complicity in Nigeria's North-West.
11. International Crisis Group. (2022). Jihadists are rolling in gold in the Sahel.
12. Nigerian Financial Intelligence Unit (NFIU). (2023, December). Typologies report on terrorism financing in Nigeria.
13. Nsaibia, H. (2026). Gold and conflict in the Sahel. Armed Conflict Location & Event Data Project (ACLED).
14. U.S. Department of Justice. (2022). Statements on the recovery of bitcoin linked to the 2016 Bitfinex exchange hack.
15. U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC). (2026). Sanctions designations relating to ISIS-West Africa financing networks and Nigerian bureaux de change.
16. Chainalysis, Elliptic, & TRM Labs. (n.d.). Publicly available methodology overviews on blockchain forensic analysis (referenced for descriptive purposes only).

This article is licensed under a Creative Commons Attribution 4.0 International License.

This article is licensed under a Creative Commons Attribution 4.0 International License.