SUNTEXT REVIEWS

SunText Review of Arts & Social Sciences
ISSN: 2766-4600

Open Access
Research Article
Volume 7:2

Encrypted Markets, Decentralised Trust: Technology and the Reconfiguration of Illicit Drug Networks in Nigeria

Obaji-Akpet IO[1] and Uduo TA[2,*]

[1]*Political Science, University of Calabar, Nigeria*
[2]*ICEST Resource Centre, Lagos, Nigeria*

[*]**Corresponding author:** Uduo TA, ICEST Resource Centre, Lagos, Nigeria; E-mail: achutu@gmail.com

Received date: 15 October 2026; **Accepted date:** 05 November 2026; **Published date:** 15 November 2026

Citation: Obaji-Akpet IO, Uduo TA (2026) Encrypted Markets, Decentralised Trust: Technology and the Reconfiguration of Illicit Drug Networks in Nigeria. SunText Rev Arts Social Sci 7(2): 214.

DOI: https://doi.org/10.51737/2766-4600.2026.114

Copyright: © 2026 Obaji-Akpet IO, et al. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Abstract

Traditional narratives describe Nigeria as a transit point in the transatlantic cocaine trade because of its coastlines, transport routes, and courier movements. This article argues that such explanation misses the social contexts in which actors organise drug trade, manage risk, and sustain routine exchange. To explain how digital technology is reshaping illicit drug networks from within, the article draws together four literatures, West African trafficking, darknet crypto markets, encrypted communication in organized crime, and Nigeria's digital finance economy. The findings show that drug markets are shaped by communication, payment, surveillance, and concealment. The framework introduces decentralized trust, which it defines as the shift of the assurance on which illegal exchange depends on persons to protocols. In Nigerian trafficking, trust has long rested on ethnicity, confraternity, encrypted channels, blockchain settlement, and digital reputation systems. By bringing this scholarship together, the article shows how platform logics flatten network structure, how encryption reshapes coordination, and how digital value transfer changes settlement and laundering. It also argues that these developments create resilience through their interaction, which none of them produces. Beyond the transit-state model that overlooks it, the article reframes the governance of an African drug economy and recommends ways that future research should test.

Keywords: Illicit drug markets; Nigeria; Decentralised trust; Crypto markets; Encrypted communication; Organised crime; Digital criminology

Introduction

In September 2022, officers of Nigeria's National drug law enforcement agency (NDLEA) raided a warehouse on the outskirts of Lagos and removed roughly 1.8 tonnes of cocaine, a consignment valued at around US$278 million and described by the agency as the largest single seizure in its history [1,2]. The raid made national headlines, and the revealing detail surfaced when agency estimated that it represented two per cent of what passes through the country in a single year. What it conceals is the calm structure has been assembled as consignments, the messaging channels, the digital wallets through which value moves, and the dispersed set of actors who coordinate without physical meeting. This article examines this mechanism and its implications on how drug trafficking in Nigeria should be understood. For close to two decades, research and policy have studied Nigeria's place in the global drug trade through the language of transit. From 2005, as European cocaine demand climbed and direct Atlantic routes came under pressure, South American suppliers began staging shipments through West Africa, and Nigeria emerged as the consolidating centre of the sub-region [3-5]. The transit model did important work and explain why traffickers favoured the region's limited interdiction capacity, it ties the trade to corruption and institutional fragility, and it placed West Africa squarely on the agenda of the United Nations Security Council and the Economic Community of West African States [6]. What that model did not anticipate, because scholars formulated it largely before the digital turn, was how quickly the organizational substrate of trafficking would migrate online.

This migration is consequential in Nigeria than in most other African countries for a specific reason: the country combines a

large and expanding drug economy with one of the highest levels of digital adoption in the world. Nigeria has ranked at or near the summit of global grassroots cryptocurrency adoption for several consecutive years, second only to India in 2024, and the sole African economy in the global top twenty, receiving tens of billions of dollars in cryptocurrency value annually through peer-to-peer channels [7]. Because Nigeria combines a mature mobile money ecosystem with a globally notorious online fraud sector, it provides a strong African case for examining whether, and how, digital technology is reshaping illicit drug networks [8,9]. By contrast, the classical account, with its focus on coastlines and couriers, does not address this dimension of the problem effectively. It explains where drugs go, but it is much less clear on how contemporary networks coordinate, settle accounts, and decide whom to trust. This article therefore pursues three questions. First, how do digital platforms and encrypted communications restructure the organisation of drug networks operating in and through Nigeria? Second, how does the migration of value into cryptocurrency and mobile money change the way these networks settle debts, launder proceeds, and enforce obligations? Third, and most consequentially, what happens when these technologies interact: do they merely add convenience, or do they together alter the very basis of trust on which illegal exchange depends?

The argument advanced here is that they alter it. Illegal markets cannot summon courts to enforce their bargains, so they must build trust by other means (Gambetta) [10,8]. In Nigerian trafficking, those means have historically been personal, drawing on kinship, ethnic affiliation, university confraternity membership, and reputation built over years of repeated dealing [8]. These bonds do not disappear with digital tools. Instead, systems supplement them and, at times, replace them with built-in assurances such as escrow scripts, rating mechanisms, cryptographic identities, and the irreversible settlement of block chain transactions. We call this shift decentralised trust, and we argue that it is the under-theorized, reason Nigerian drug networks have become dispersed and coordinated than the transit model would predict. Because the empirical picture of this transformation remains thin (systematic data on technology use within African drug networks barely exists), this article proceeds conceptually. It brings together four disconnected bodies of research, grounds them in the established sociology of trust in illegal markets, interprets them against agency recording and publicly documented cases, and builds from that combination a framework for understanding how technology reconfigures the governance of illicit drug markets in Nigeria. The contribution is therefore theoretical: a new observation, and a set of propositions, intended both to make sense of present developments and to guide the empirical research that should follow. The remainder of the article reviews the four literatures it combine together, theorises trust in illegal markets, sets out the conceptual framework and its component dynamics, explains the conceptual approach and its evidentiary basis, discusses the theoretical and policy implications alongside the strongest counter-arguments, and concludes by pointing towards the trafficking extremism nexus in the Sahel as the natural next frontier of inquiry.

The View from Transit: Four Literatures and a Gap

The contribution of this article sits at the intersection of four bodies of work that have developed in isolation from one another. Bringing them into contact is itself part of the argument because the gap this study addresses is precisely the space between them.

The West African transit-state literature

The first and most directly relevant literature treats West Africa, and Nigeria within it, as a transit zone in the transatlantic cocaine economy. Its canonical statements come from the UNODC's threat assessments and the West Africa Commission on Drugs, which established that large cocaine volumes began transiting the region around 2005, that the southern centered on Nigeria consolidated these flows, and that the trade corroded already fragile institutions [4-6]. Ellis added historical depth, tracing Nigerian involvement back several decades and locating it within longer patterns of diaspora, informal commerce, and state decay [3,8], while Klantschnig situated drug control within the Nigerian state itself, showing enforcement and trafficking to be long entangled rather than opposed [9]. Comparative scholarship has debated how far the vocabulary of organised crime fits African realities and traced the rise of West African criminal networks [11-13]. This literature is indispensable for understanding flows, routes, and the political economy of complicity. Yet its authors wrote it before the digital shocks, so it treats technology as incidental, a phone here, a wire transfer there, instead as a force reorganizing the trade. It tells us where the drugs go and who carries them; far less concerning how contemporary networks coordinate and trust. The literature also records the distinctive social composition of Nigerian trafficking, and that documentation is important for the present argument. Observers have long noted the prominence of networks rooted in the country's south-east and in its Igbo diaspora, whose breadth and mobility, a legacy in part of the dislocations of the 1967–1970 civil war, furnished ready-made channels of trust and communication across continents [3,8,5]. University confraternities, originally elite fraternal societies, have in several accounts supplied disciplined, vetted membership to criminal enterprises, and Nigerian groups have established durable footholds in European distribution markets [8,9]. In the vocabulary of this article, these are embedded-trust institutions par excellence: they make betrayal costly by binding members into dense, enduring social structures that punish defection through exclusion and sanction. They are precisely the institutions a digital account must

take seriously instead of wish away because decentralised trust does not arrive to replace them so much as to layer upon them.

The cryptomarket and darknet literature

This is quite different literature, has grown up around online drug markets in the global North. Since Silk Road launched in 2011, researchers have shown that cryptomarkets fused three technologies (anonymising networks such as Tor, cryptocurrency, and encrypted communication) to let strangers transact drugs across great distances without meeting [14-16]. Three of its debates bear directly on the present argument. The first is resilience: closing a marketplace rarely destroys the trade, because participants migrate to successor platforms and aggregate activity recovers, a pattern measurement studies have placed on firm empirical footing and that even publicised takedowns interrupt only briefly [17-19]. The second is trust: these markets build it through reputation systems, vendor signalling, and the cross-context transfer of standing, even as ratings can be gamed and administrators periodically abscond in "exit scams" that show protocol-based assurance solving some problems while creating others [15,20,21]. The third is structure: network analytic and vendor-level studies map how these markets spread risk across many small connections against a few brokers, and how revenue concentrates among a section of sellers [22,23]. The limitation, for present purposes, is geographic. Built entirely from the United States, Western Europe, and Oceania, including its qualitative strand on risk and community, this research leaves Africa a blank space on the map [24,25]. Whether its insights travel to Nigeria, with different infrastructure, trust traditions, and a wholesale rather than retail role, remains an open and unasked question.

Encryption, messaging, and operational security in organized crime

A third strand examines how encrypted messaging has migrated from the dark net to the everyday smartphone. Studies of platforms such as Telegram and other encrypted applications show that they have become attractive tools for drug coordination because they combine easy creation and dissolution of closed groups, strong anonymity features, and constant mobile availability [26-28]. This work is relevant for Nigeria because it describes a far lower technological threshold than Tor-based cryptomarkets: any actor with a smartphone and a data bundle can participate, which fits a context of high mobile penetration but uneven fixed-internet access. The literature on operational security and signalling complements this, showing how digital offenders construct credible personas, communicate covertly, and manage the constant risk of exposure and infiltration [29-31]. Wider cybercrime research has examined how illicit online trades become commoditised and how anonymous offenders gauge one another's reliability [32,33]. Yet here too the empirical Centre of gravity sits in Europe and North America, and the interaction between encrypted messaging and the older, relationship-based architecture of West African trafficking has so far escaped examination.

Digital value transfer in Nigeria: crypto and mobile money

The fourth literature is the most locally grounded and the least connected to the other three. It documents Nigeria's remarkable embrace of digital value: sustained top-tier rankings in grassroots cryptocurrency adoption, heavy reliance on peer-to-peer trading as a hedge against inflation and currency controls, the contested introduction of the eNaira central bank digital currency, and a deep mobile-money culture [7]. Read alongside long-standing accounts of Nigerian fraud networks and informal value-transfer systems, this literature describes exactly the financial bedrock that a digitally reconfigured drug trade would exploit [8,31]. What it has not done is connect that bedrock to drug-network operations specifically as scholars reveal the financial-technology story and the drug-trafficking story in separate extents.

The gap in literature

Set side by side, these literatures reveal their shared blind spot because the transit-state literature sees Nigeria but not technology; the cryptomarket and encryption literatures see technology but not Nigeria; the fintech literature sees Nigeria's digital economy but not its drug trade. None examines how encrypted markets, encrypted messaging, and digital value transfer interact within a single African network to reconstitute the basis of trust. That interaction is the object of this study. To analyse it, however, we first need a theory of what trust does in an illegal market, and what changes when its source moves from persons to protocols.

Theorising Trust in Illegal Markets

Trust is the central problem of any market that operates beyond the protection of law. A legal firm that is cheated can sue; an illegal one cannot. Every participant in a drug transaction therefore faces a double exposure, to the counterparty who might take the goods or the money and disappear, and to the counterparty who might be, or might become, an informant. The history of organised crime is in large part a history of improvised solutions to this problem, and the sociology of illegal markets has long treated the production of trust as the discipline's core analytical question [34,10,11]. That embedded trust lends illegal markets much of their resilience is by now well established [35-37]. The classical solutions are social as Diego Gambetta's account of the Sicilian mafia famously reframed the organisation not as a conspiracy of violence but as an industry

that builds and sells trust where the state fails to provide it [34]. Mark Granovetter's broader argument about the embeddedness of economic action supplies the general principle as concrete, ongoing social relations, as opposed to abstract institutions, are what generate the confidence that allows exchange to proceed, and this is true with special force where formal enforcement is absent [34]. In applying to criminal networks, the implication is that trust is produced through repetition, kinship, shared ethnicity, common membership, and reputations that travel by word of mouth, mechanisms that bind individuals into networks dense enough to punish betrayal through exclusion and inferior [38,11]. Nigerian trafficking has been a textbook case of exactly this embedded model, organised through familial ties, ethnic networks, and the disciplined solidarity of university confraternities [8,9]. A complementary strand explains how such trust is communicated because criminals cannot advertise openly, they rely on signals, displays that are credible precisely because they are costly or hard to fake [30]. Membership of a confraternity, a shared hometown, a record of consignments delivered without loss: each function as a costly signal that a counterparty is reliable and is not an infiltrator, because each is difficult for an impostor to counterfeit and expensive for a member to betray. Signalling theory thereby specifies the micro-mechanics of embedded trust, and it sets up the central question the digital turn poses. When a network moves onto encrypted channels and settles in cryptocurrency, what replaces the costly signal of the shared confraternity or the face known for years? Part of the answer, as the cybercrime literature shows, is that offenders rebuild signalling online through reputation scores, vouching by established members, and the accumulated history of successful trades [29,39]. Part of the answer is that the protocol itself absorbs work the signal used to do, where settlement is irreversible, a counterparty's honesty about payment no longer needs to be signalled at all.

Embedded trust is robust but expensive, it is slow to build, it does not scale easily, it ties the network to particular people and places, and it concentrates risk. When a trusted broker is arrested or turns, the relationships that ran through that person are compromised at a stroke. Digital systems promise a different settlement of the same problem, and a parallel literature on cybercrime has examined how online offenders generate trust without the dense social ties on which embedded trust depends [39,31]. Part of the answer is that they reconstruct familiar social mechanisms in digital form, reputation, vouching, and signalling migrate onto forums and encrypted channels [29,30]. Part of it is genuinely new as the cryptographic systems offer what some have called 'trustless' exchange, since a settled blockchain transaction is irreversible by design, so a buyer need not trust a seller's honesty about payment, only the integrity of the protocol [40,41]. Escrow scripts and platform-administered ratings likewise convert interpersonal confidence into system-level assurance, allowing strangers to transact on the strength of the architecture as opposed to the acquaintance [42,20].

Table 1: *Embedded trust and decentralised trust compared.*

Dimension	Embedded trust (traditional)	Decentralised trust (digital)
Basis of assurance	Persons: kinship, ethnicity, confraternity, reputation	Protocols: escrow, ratings, cryptographic identity, settlement
How it is built	Slow, through repeated face-to-face dealing	Fast, through system design and verified history
Network shape	Hierarchical chains of brokers	Flat, modular, interchangeable cells
Effect of losing a node	Fractures the chain; trust must be rebuilt	Absorbed; a replaceable module is swapped out
Geographic reach	Bounded by personal relationships	Extended across jurisdictions by code
Key vulnerability	Identifiable people who can be turned or arrested	Conversion seams where value re-enters the formal economy

This is the conceptual crux on which the article relies, hence the crypto market literature has tended to present the move from embedded to engineered trust as a substitution, reputation systems replacing personal ties [15]. We argue that in Nigeria the relationship is better understood as layering. Protocol-based assurance does not arrive on a blank slate; it enters a market already saturated with embedded trust and combines with it. Decentralised trust, the concept developed in the next section, names this layered condition as a regime in which assurance is increasingly distributed across systems and protocols than concentrated in persons, but in which the personal attach persists and continues to do work. Theorising trust this way is significant because it predicts a different outcome from the northern model, not the disappearance of kinship and reputation, but their recombination with code, and that prediction is, in principle, empirically testable. It is suggested that there is a reason, trust signal repays attention and so

historically, the production of trust has also been the point of greatest vulnerability that the state has exploited. Conventional enforcement against embedded networks works in large part by attacking trust, turning a member into an informant, inserting an undercover officer, or so degrading confidence that the network turns on itself. Each tactic depends on the fact that embedded trust runs through people who can be identified, pressured, or impersonated [30,11]. This is what makes the passage towards engineered trust strategically consequential than merely technical. Where assurance is vested in a protocol than a person, there is less for an informant to betray and less for an undercover officer to penetrate, because the transaction does not rely on the counterparty's good faith in the first place. Decentralised trust, in other words, does not only reorganise the network from within; it erodes the specific seam that enforcement has long pried open. That is a central reason the framework treats the shift as a transformation of governance instead of an upgrade of equipment (Table 1).

The Conceptual Framework: Encrypted Markets and Decentralised Trust

Two concepts anchor the framework, and both require localisation before they can do useful work in the Nigerian context. In encrypted markets we mean trading environments, whether full darknet marketplaces, semi-open channels on encrypted messaging applications, or hybrids of the two, in which cryptographic tooling lowers the cost of transacting without face-to-face contact. The defining feature is not any single platform but the substitution of cryptographic and infrastructural anonymity for physical co-presence. In the global North, this substitution produced the classic cryptomarket; in Nigeria, where Tor penetration is thinner, but smartphone messaging is ubiquitous, the same logic expresses itself through encrypted channels than through hidden-service marketplaces. The concept travels since its material form adapts. In decentralised trust we mean the migration of assurance from persons to protocols in the layered sense developed above. The traditional answer to the trust problem in Nigerian trafficking was personal and social; decentralised trust offers a complementary and partly competing settlement in which escrow scripts hold value until delivery is confirmed, rating systems convert past behaviour into portable reputation, cryptographic keys establish persistent identity without disclosing personhood, and the irreversibility of a settled transaction removes the need to trust a counterparty's willingness to pay at all [40,41].

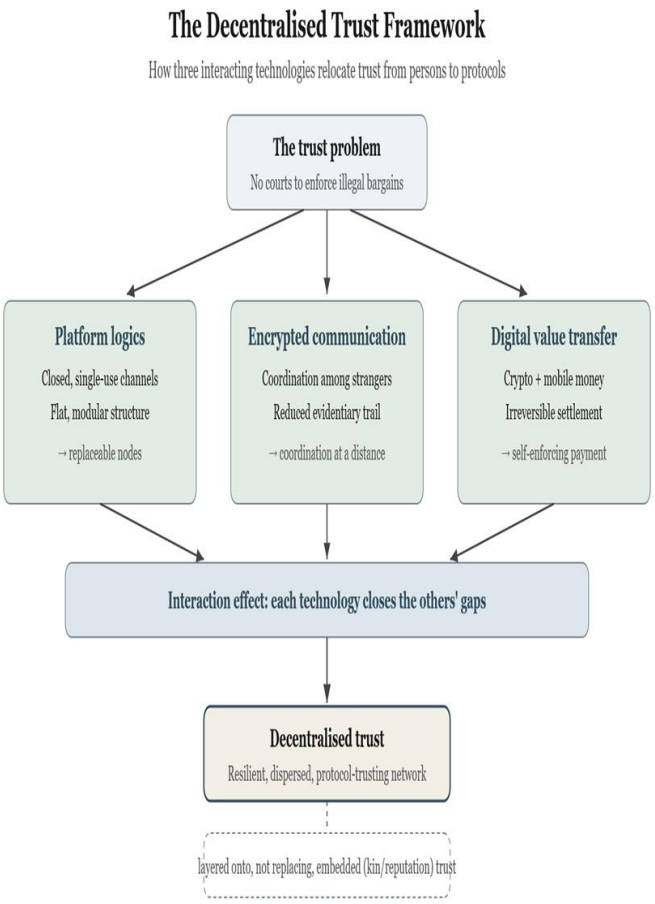


Figure 1: *The Decentralised Trust Framework. Three interacting technologies relocate assurance from persons to protocols, producing a resilient, dispersed network layered onto enduring embedded trust.*

Trust, in this model, is engineered into the protocol than invested solely in the person, but it coexists against erasing, the embedded trust that preceded it. From this framing follow three propositions, developed through the component dynamics that follow. Proposition 1: platform and messaging technologies flatten and modularise network structure, reducing dependence on any single broker. Proposition 2: encrypted communication and digital value transfer substitute protocol-based assurance for personal assurance, but partially, producing hybrid trust arrangements than wholesale replacement. Proposition 3: the technological developments generate organisational resilience in combination that none generates in isolation. The remainder of the section develops four interlocking dynamics, structure, communication, value, and trust, before turning to the institutional challenge they collectively pose. These dynamics are analytical components grounded in the published literature and in publicly documented patterns, not findings from primary data (Figure 1).

The digital transformation of operations and network structure

The first dynamic concern structure designed for the transit-era picture of Nigerian trafficking was hierarchical, as a consignment moved through a recognisable chain of brokers, each a potential point of failure and each commanding trust through accumulated reputation [8,38]. Platform and messaging technologies loosen this structure. When tasks can be assigned and dissolved through closed channels created for a single transaction, the network comes to resemble a set of interchangeable modules than a fixed pyramid, and the removal of any one node does less damage to the whole. The cryptomarket literature documents an analogous pattern in the global North, where network-analytic studies find risk distributed across many small participants and where marketplace closures prompt migration than to collapse [17,22,18]. The Nigerian expression differs in form, closed messaging channels instead of hidden-service marketplaces, but the structural logic, and its consequence for enforcement, converge, hence an arrest that would once have fractured a network removes a replaceable module instead. The 2022 Lagos seizure illustrates the point in negative as result of officers interdicted a consignment of that scale, yet the trade it belonged to continued, which is precisely what a modular, redundant structure predicts and what a brittle hierarchy would not. This structural transformation has a transnational dimension that the framework must register, hence Nigerian trafficking has never been confined to Nigeria. The trade's documented architecture spans continents, source relationships with South American suppliers, a diaspora presence that reaches European distribution markets, and well-recorded alliances between Nigerian groups and major Latin American organizations [8,5]. In the embedded model, holding such a farflung structure together demanded exactly the trust-intensive institutions described earlier: the diaspora tie, the confraternity bond, the broker known on both sides of an ocean and digital coordination changes the economics of distance. Encrypted channels and self-executing settlement allow a Lagos point, a São Paulo point, and a European point to act in concert without the dense interpersonal scaffolding that long-range cooperation once required, easing the coordination problems that previously throttled transcontinental collaboration through the same tools that flatten the domestic network [45,22]. The result is not abolition of the diaspora structure but its augmentation since the network can now combine the deep trust of established ethnic and fraternal ties with the reach and redundancy of digital coordination formidable combination than either alone. Decentralised trust, in short, does not only modularise the network internally; it extends the radius over which a modular network can operate (Figure 2).

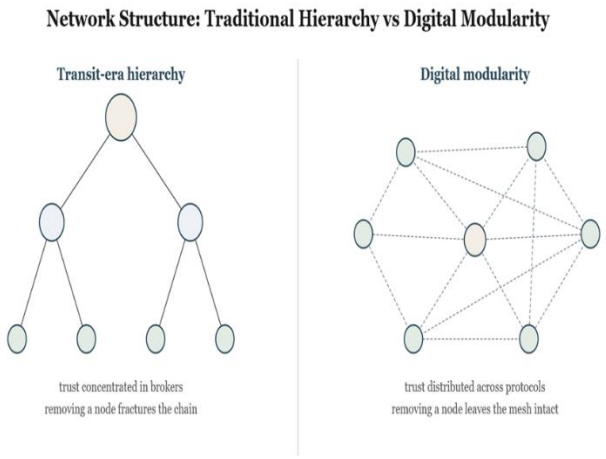


Figure 2: *Network structure compared: the transit-era hierarchy concentrates trust in brokers, whereas digital modularity distributes it across a redundant mesh.*

Encrypted communication and operational security

The second dynamic look at coordination and concealment as encrypted messaging changes the calculus of operational security. It shrinks the evidentiary trail, allows communities to open and close at will, and lets participants who have never met coordinate with confidence that their exchanges are shielded [27,28]. The conceptual point is that encryption does not merely protect existing relationships, but it makes a different kind of relationship possible, in which coordination no longer presupposes acquaintance. Yet the framework insists on a qualification that the northern literature, working in higher-trust-in-systems environments, can afford to underplay. In Nigeria, admission to an encrypted channel is still governed by the older currencies of kinship, confraternity membership, and reputation, and signalling within those channels still draws on offline credentials [29,8, 30]. Encryption carries the traffic and personal vetting still guards the gate. Decentralised trust, in other words, arrives as a hybrid, and that hybridity than being a weakness in the argument, is the framework's distinctive claim and the feature that clearly separates the Nigerian case from the Euro-American model.

Digital value transfer: cryptocurrency and mobile money

The third dynamic follows the money since cryptocurrency and mobile money reshape how networks settle accounts, move proceeds, and enforce payment. The irreversibility of a settled blockchain transaction removes a classic risk, the counterparty who takes delivery and refuses to pay, by engineering finality into the protocol itself [40,41] (Figure 3).

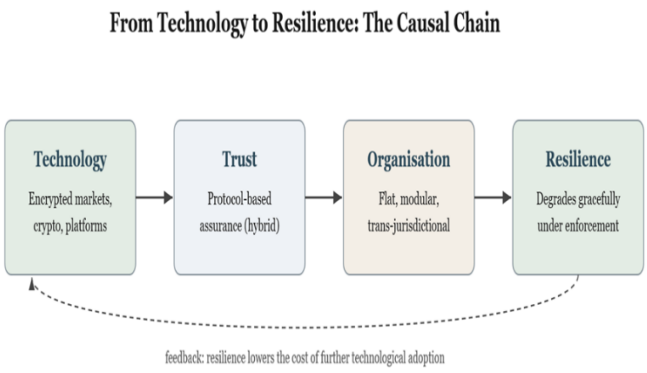


Figure 3: *The causal chain linking technology, trust, organisation, and resilience, with a feedback loop in which resilience lowers the cost of further adoption.*

Nigeria's exceptional depth of peer-to-peer crypto and mobile-money activity means the rails are already laid and heavily used for licit purposes, which lowers both the technical and the social threshold to illicit use [7]. Two qualifications keep the claim honest. First, public blockchains cut both ways as result of the finality that reassures counterparties also leaves a permanent, documented record, and this is the reason sophisticated actors turn to privacy coins, mixers, stablecoins, and rapid conversion, the very techniques international bodies catalogue as red flags of virtual-asset laundering, and which traceability research shows are rarely perfect [7,43-46]. Second, cryptocurrency rarely operates alone, it interlocks with mobile money and cash, and the interesting object is the seam between these systems, the cash-in and cash-out points where value crosses between digital and physical economies than any one in isolation. Therefore, laundering deserves emphasis, because it is where the framework's claims about value and trust meet concretely. In the embedded model, moving and cleaning proceeds depended on trusted intermediaries (bureaux de change, complicit businesses, couriers) each of whom had to be known and relied upon, and each a point of exposure. Digital value transfer partially dissolves this dependence, reason that proceeds can be fragmented across wallets, converted into stablecoins, swapped through decentralised exchanges, and reassembled elsewhere with far less reliance on any single human node [7,41]. Yet the dissolution is only partial at some stage value must re-enter the formal economy, to buy property, pay personnel, or fund the next consignment, and at that cash-out seam the older requirements reassert themselves. A trusted exchanger, a complicit account, a person who can be identified. The hybrid regime is thus legible precisely where it is most vulnerable and this is why the seam, not the encrypted core, is the framework's candidate for productive site of analysis and intervention.

Decentralised trust as an organising principle

The fourth dynamic is the combination, and the decisive claim of the framework: these developments produce resilience in combination that none produces alone. Individually, each tool is incremental, encrypted messaging shields a conversation, a modular structure absorbs an arrest, a crypto settlement removes a payment risk. Bringing these together they reconstitute the network's trust architecture so that it no longer depends on any person. The mechanism is worth stating precisely because each tool compensates for the others' weaknesses. The modularity that disperses the network would, in a purely personal-trust world, strain coordination beyond breaking point, but encrypted messaging restores coordination at a distance. The anonymity that makes counterparties unknowable would, without engineered settlement, make payment unenforceable, but blockchain finality makes payment self-executing. The closing of each gap by another technology yields a network simultaneously dispersed and coordinated than the transit model can explain. This is where the framework parts company with the cryptomarket literature's simpler substitution opinion, and where the personal-trust regime persists, as in Nigeria technology has not erased it but freed the network from total dependence on it, producing a hybrid in which embedded and engineered trust reinforce one another [47,39,11].

Harm, violence, and the limits of the analogy

It should be noted that this framework borrows from the cryptomarket literature, and it must engage that literature's best striking claim. This is because moving exchange online reduces interpersonal violence, as geographic separation and reputational enforcement displace the territorial competition that drives killings in street markets [48,49,42]. As such, two features of the Nigerian case complicate the analogy. First, the trade is heavily wholesale and logistical, hence cocaine still arrives in tonnes, warehoused, and transfer physically, so the frictions over consignments, debts, and territory that have long produced violence do not vanish for coordination has gone digital. Second, the persistence of embedded trust means disputes may still be settled through the older, sometimes violent machinery of confraternity and network discipline than a platform arbitration. Decentralised trust may therefore redistribute violence, easing it at the dispersed coordination layer while leaving it intact at the physical logistics layer as opposed to reducing it. Whether digitalisation pacifies the Nigerian trade, displaces its violence, or leaves it unchanged is an open and consequential question the new framework examined.

The institutional challenge

A framework built on decentralised trust carries a direct implication for the state, which belongs in the framework rather

than only in the policy discussion. If a network's resilience rests on modular structure, encrypted coordination, and protocol-based settlement, then the pace of technological change tends to outrun institutional adaptation, and capacities honed for an earlier era, interception of conventional communications, pursuit of identifiable kingpins, seizure of physical consignments, deliver diminishing returns. The challenge is not merely resourcing but conceptual, agencies organized to dismantle hierarchies' networks that have, in effect, dispensed with the hierarchy. This is the analytical bridge to the discussion, which takes up what the framework implies for security governance in Nigeria, and the counterarguments it must answer.

Approach and Evidentiary Basis

As a conceptual contribution, this article does not report primary fieldwork; it builds and defends a framework through structured synthesis. That choice is deliberate and, given the state of the field, warranted. Systematic empirical data on the use of digital technologies within African drug networks barely exists: the cryptomarket literature that has measured such practices in detail is overwhelmingly concerned with the global North, while the West African trafficking literature that knows the Nigerian terrain predates the digital turn [15,5]. In a field at this stage of development, premature empiricism risks measuring the wrong things; the prior task is conceptual, to specify what is happening and why it matters, so that subsequent empirical work knows what to look for. The framework is accordingly constructed from three kinds of evidence, used not as data to be coded but as materials to be combined and interpreted. The first is peer-reviewed work across the four literatures and the trust theory reviewed above, which supplies the mechanisms, embeddedness, reputational substitution, protocol-based settlement, modularity, whose applicability to Nigeria the article assesses. The second is institutional and policy reporting from bodies such as the UNODC, the Global Initiative Against Transnational Organized Crime, and blockchain-analytics firms, which supplies contemporary detail on flows, adoption, and enforcement [7,1,50]. The third is publicly documented cases, such as the 2022 Lagos seizure, which serve as illustrations that anchor the argument in observable events than as a representative sample. Throughout, the reasoning is analytical as the article asks which mechanisms documented elsewhere credibly operate in Nigeria, what the Nigerian context modifies, and what follows for theory and policy. The limitation intrinsic to this approach is stated plainly, which is a conceptual framework that would establish coherence, plausibility, and significance, but not prevalence. How widespread these dynamics are within Nigerian drug networks is an empirical question the framework is designed to make researchable, and the conclusion returns to it.

The combination proceeds in three deliberate steps rather than as an unstructured review. First, it extracts from each literature the specific causal mechanism that body of work has established, modularity and resilience from the cryptomarket studies, embeddedness and reputational governance from the trust literature, protocol-based settlement from the work on cryptocurrency. Second, it appraises each mechanism for portability, asking which features of the Nigerian context, the wholesale role, the embedded-trust institutions, the depth of digital finance, would amplify, dampen, or reshape it. Third, it recombines the portable mechanisms into a single account and tests that account for internal consistency against the documented features of the Nigerian trade. The sources carry weight accordingly, so peer-reviewed empirical studies bear the analytical load, agency and policy reporting supplies context and contemporary detail, or single-case material illustrates rather than evidence. This procedure cannot deliver the representativeness of primary data, but it makes the path from existing evidence to new framework explicit and auditable, which is the appropriate standard for a conceptual contribution. As the choice of Nigeria to conduct analytical work, a brief note on case selection is warranted for Nigeria is not presented as typical of West Africa or the global South; rather, it is selected as an extreme, or case for the mechanism specified by the framework. If decentralised trust is reshaping any African drug network, it should appear most clearly where a large, internationally connected drug economy coincides with one of the world's deepest levels of grassroots digital finance adoption and a mature culture of online illicit enterprise. Nigeria exhibits this combination to an unusual degree [7,8,31]. A most-likely case is the appropriate site for establishing that a mechanism operates at all and for tracing how it works, which is the proper ambition of a conceptual contribution; it is correspondingly ill-suited to claims about average prevalence, which require representative sampling the design does not attempt. The logic cuts in a useful direction for what follows as if the framework's mechanisms could not be shown to operate even here, under conditions maximally favorable to them, the argument would be in serious doubt. That they are plausible here licenses the framework as a hypothesis to be tested elsewhere, under less favorable conditions, rather than as a settled description of the trade.

Discussion: Counter-Arguments, Theory, and Security Governance

A framework of this kind is only as strong as its answers to the obvious objections, so it is worth meeting the three most serious head-on. The first objection is deflationary: nothing fundamental has changed, and traffickers have simply swapped landlines for encrypted apps and cash couriers for wallets, leaving the

underlying trade intact. The framework's reply is that the interaction effect is not reducible to tool-swapping. A new phone does not change a network's structure; the combination of modular organisation, encrypted coordination, and self-executing settlement does, because together they relocate the source of trust and thereby alter what the network can survive [22,11]. The claim is about architecture, not gadgets. The second objection runs the other way: the framework overstates the digital, when cash and personal relationships plainly still dominate much of the Nigerian trade. This objection is partly right, and the framework concedes it by design. The hybridity thesis does not claim that embedded trust has vanished; it claims that engineered trust has been layered onto it, freeing the network from total dependence on any single person [47,39]. The cash-in and cash-out seams where cryptocurrency meets the physical economy are, on this account, not embarrassments to the argument but among its most important analytical objects, the points where the hybrid regime is most visible and most vulnerable. To insist that cash still matters is to restate the framework, not to refute it.

The third objection is theoretical: if trust remains personal, is "decentralised trust" really a new phenomenon, or merely the old reputation system with extra steps? Here the cryptomarket literature's own findings correct the answer. Engineered trust is demonstrably not identical to reputational trust, escrow can enforce a bargain between parties who have no reputation with one another, and blockchain finality can complete a payment that no amount of reputation would otherwise secure, even as ratings can be gamed and administrators can abscond, which shows the new mechanisms have failure modes of their own [15,42,20]. Decentralised trust is therefore genuinely distinct from embedded trust, while remaining, in the Nigerian case, entangled with it. That entanglement is the contribution, not a concession. With the objections answered, the theoretical contribution comes into focus. The framework extends network-governance and trust accounts of illegal markets by specifying how the foundational problem of trust is being re-engineered in an African setting the cryptomarket literature has ignored, and by showing that the global-North model of clean substitution does not travel intact. In Nigeria it becomes hybridisation, in which protocol-based and kin-based assurance coexist and reinforce one another [15,8,47]. For the transit-state literature, the implication is a needed update than a refutation. Nigeria remains a transit centre; the flows, the UNODC and the West Africa Commission on Drugs described are actual and persistent [5,6]. But the organisational bedrock beneath those flows has changed, and an account that stops at routes and couriers now misses the layer where coordination and trust are produced.

The framework also speaks to digital criminology's conversation about the platform of crime, the migration of illicit activity onto digital infrastructures that reshape how offenders organise, communicate, and transact. That conversation has drawn on global North cases and has tended to treat the move online as a clean break with prior forms [14,15]. The Nigerian case offers a corrective political platform, which can be partial and additive rather than substitutive, grafting digital coordination and settlement on durable pre-digital institutions instead of dissolving them. A general criminology of digital illicit markets therefore needs the global South not as an afterthought but as a source of cases that reveal what the technology does when it meets a different social substrate. The conditions that produce hybridity in Nigeria, strong, durable embedded-trust institutions meeting rapid, grassroots digital adoption, are not unique to it. Comparable configurations arise wherever kinship, clan, or fraternal structures have long organized illicit exchange and mobile-first finance has spread quickly, from parts of South and Southeast Asia to other mobile-money-dense African economies. The framework predicts layering than substitution in such settings, with the local balance between embedded and engineered trust tracking the strength of the pre-digital institutions the technology meets: where embedded trust is weak, engineered trust may approach the clean substitution the northern literature describes; where it is strong, as in Nigeria, hybridity should dominate. Stating that comparative hypothesis is itself part of the contribution, turning a single-case argument into a programme.

Practical implications for Nigerian institutions

The policy implication follows directly and is uncomfortable. If a network's resilience rests on modular structure, encrypted coordination, and protocol-based settlement, then enforcement built around removing key individuals and seizing key consignments, the takedown model, is poorly matched to its target, because removing a replaceable module imposes a cost the network is designed to absorb [17,18]. This is not an argument for acceptance but for reorientation. Hence, in relation to the financial layers where cryptocurrency, mobile money, and cash convert into one another, where the trail is legible and the hybrid regime exposed; infrastructural choke points than human ones; towards the specialised competencies, blockchain analytics, digital forensics, cyber-enabled financial investigation, that a protocol-trusting trade demands; and the integrated inter-agency and cross-border intelligence sharing that a trans-jurisdictional network requires [7,1]. The deeper point is conceptual as agencies built to dismantle hierarchies must reorganise around networks that have dispensed with hierarchy. A regulatory dilemma sharpens the policy challenge, Nigeria's authorities have oscillated between restricting cryptocurrency, at one point curtailing banks' dealings with crypto exchanges, and promoting digital finance through initiatives such as the eNaira, while peer-to-peer adoption surged notwithstanding [7]. The framework suggests why blunt prohibition is unlikely to

dislodge decentralised trust because the same rails serve a vast licit economy of remittances, savings, and inflation hedging, so suppression imposes heavy costs on ordinary users while pushing illicit value towards less visible instruments. A more promising posture works with the grain of the technology, strengthening the regulated where digital value re-enters the formal economy, building the analytic capacity to follow public ledgers, and treating financial-intelligence integration as the principal front than an afterthought. The implication is not that the state is helpless, but that its leverage lies at the seams of the hybrid system than at its strongest points.

These principles translate into distinct mandates across the Nigerian institutional landscape. The National Drug Law Enforcement Agency (NDLEA) should pair interdiction with embedded digital-forensic and open-source capacity, treating a seized phone or wallet as the entry point to a network instead of the end of a case. The Economic and Financial Crimes Commission (EFCC) and the Nigerian Financial Intelligence Unit (NFIU) should make the cryptocurrency mobile-money cash conversion seam their priority, building blockchain-analytic capability and operationalising the virtual-asset red-flag typologies that international bodies have already codified [43,46]. The Nigerian Communications Commission (NCC), together with the telecommunications operators it regulates, sits at the chokepoint of mobile identity and connectivity, where enforcing know-your-customer rules on SIM registration and mobile-money onboarding raises operational costs for networks more durably than any single takedown. Financial institutions and licensed virtual-asset service providers should be resourced, and required, to perform meaningful transaction monitoring at the regulated on- and off-ramps, the points where pseudonymous value must re-enter the formal economy. Policymakers, finally, should resist the reflex of blunt prohibition, which displaces than removes, and legislate instead for graduated, intelligence-led oversight that concentrates scarce capacity on these seams. None of this promises to dismantle a protocol-trusting network; the realistic aim is to raise its costs and reclaim visibility where the architecture is most exposed.

Limitations

Four limitations bound the contribution and should be understood alongside its claims. The first is the reliance on secondary sources because the article synthesises published scholarship, agency reporting, and documented cases rather than generating primary data, its account is only as current and complete as those materials, which were produced for other purposes and rarely capture the Nigerian digital layer directly. The second is the limited visibility intrinsic to clandestine networks. Encrypted, anonymised, and deliberately concealed activity resists observation by design, so even the best available evidence illuminates fragments, a seizure, a prosecution, a defector's account than the whole. The framework is built to reason carefully from such fragments, but it cannot see what the network successfully hides. The third is the difficulty of measuring prevalence because the analysis establishes that decentralised trust can operate in the Nigerian trade and traces how; it cannot say how common the mechanism is, which segments it has reached, or how quickly it is spreading. Those are quantitative questions that a conceptual design is not equipped to answer and that the framework deliberately hands to future fieldwork. The fourth is the pace of technological change, the tools at the centre of the argument, messaging platforms, coins, mixing services, settlement rails, evolve faster than scholarship can track, so specific claims about any one technology risk dating quickly.

Conclusion

This article set out to ask whether technology is reshaping illicit drug networks in Nigeria, and how. Conceptually, it has argued that technology does so consequentially not through any single tool but through their interaction, which shifts the basis of trust from persons to protocols. Platform logics flatten and modularise the network; encrypted messaging sustains coordination across distance and disruption; cryptocurrency and mobile money engineer settlement that no longer requires interpersonal trust. Collectively, these developments produce a network at once dispersed and coordinated than the transit-state model anticipated, and they do so by layering a system-based assurance on replacing reputation-based assurance that has long underwritten the Nigerian trade. That layered, hybrid character is the framework's central claim and its principal contribution to a literature that has seen either Nigeria or technology, but rarely both at once, and that has theorised trust in illegal markets without reference to the African networks where it is now being rebuilt. As a conceptual framework, the argument's value lies partly in what it makes researchable. It specifies mechanisms, modularity, reputational substitution, protocol-based settlement, hybrid trust, that empirical work can now look for, test, and measure in the Nigerian network and beyond. The most pressing of those empirical questions concerns prevalence, how far, and in which segments of the trade, decentralised trust has taken hold. The framework establishes that it operates and why it matters; it does not establish how widespread it is, and that is the proper task of the fieldwork this article is intended to support. Comparative work would be valuable, testing whether the hybridity observed in Nigeria recurs in other settings where embedded trust traditions are strong and digital adoption is rapid.

The framework's limits should be acknowledged as its claims because it is built for a single, theoretically motivated case, chosen

why it maximises the conditions under which decentralised trust should be visible; that very feature limits how far its specifics generalise. It theorises a mechanism and argues for its operation and significance, but it cannot decide magnitude, how much of the Nigerian trade now runs on engineered trust, and how much remains personal. Nor can a conceptual blend capture the texture that interviews and case files would reveal for the actual vetting rituals of an encrypted channel, the precise path of a laundered payment, the lived negotiation between confraternity discipline and platform arbitration. These are not weaknesses to be hidden but the agenda the framework hands to the empirical research that should follow it. Five directions are especially pressing. First, blockchain-analytic studies could trace how Nigerian networks route value across chains, stablecoins, and conversion points, turning the framework's claims about settlement into measurable patterns. Second, as machine-learning tools enter both trafficking and enforcement, research should examine AI-enabled trafficking, automated vendor interactions, synthetic identities, and algorithmic layering of proceeds, alongside the counter-analytics it provokes. Third, the migration of retail and mid-level dealing on encrypted messaging platforms such as Telegram and Signal deserves dedicated empirical attention in the Nigerian and West African setting, where it remains undocumented. Fourth, the cross-border digital-finance dimension, how decentralised trust binds Lagos, São Paulo, and European centre into a single settlement space, invites multi-sited, follow the money designs. Fifth, comparative work across other African states, from mobile money dense East Africa to the conflict adjacent Sahel would test how far the hybridity thesis travels and what local trust institutions do to it when arrive. That agenda can be made concrete for testing the framework call for the evidence a conceptual remedy cannot supply. The court and prosecution records that reveal how specific networks coordinated and paid; interviews with investigators, financial-intelligence analysts, and where possible former participants, that surface the vetting and signalling practices of encrypted channels; and, handled with appropriate ethical and legal care, traces of the digital infrastructure itself, from blockchain flows to the architecture of messaging groups. Mixed designs that triangulate these sources against one another would be best placed to estimate not only whether decentralised trust operates, which the framework already argues, but how far it has spread, which segments of the trade it has reached, and how the balance between embedded and engineered trust is shifting over time. Each of the framework's mechanisms translates into a researchable question, which is the practical sense in which a conceptual contribution earns its place as it tells the next study what to look for. A further frontier also emerges in the argument, which shows that technological reconfiguration is underway in the Nigerian core of West African trade. Yet it raises a question it cannot answer, what happens when these dispersed, resilient, protocol-trusting networks enter zones of violent contestation? In the Sahel, where trafficking, armed groups, and chronic instability already intersect, one can most clearly ask this question. A substantial regional scholarship already documents how trafficking, armed groups, and political authority intertwine across the Sahel; what remains contested and underexplored is the causal intensity of the drug extremism relationship, whether illicit drug economies drive extremist violence, merely coexist with it, or are bound to it through the very logics of protection and trust traced in this article [50,52-58]. Whether the decentralised-trust architecture traced here travels northward into that contested space, and what it does to the relationship between illicit finance, extremist violence, and regional instability when it arrives, is the natural next inquiry, and one this study is intended to make possible.

Declaration of Conflicting Interests

The author declares no potential conflicts of interest with respect to the research, authorship, and/or publication of this article.

Funding

The author received no financial support for the research, authorship, and/or publication of this article.

Data Availability Statement

This article is based on publicly available academic literature, policy documents, institutional reports, and documentary material. No original interview or survey data were generated for this study.

References

1. Global initiative against transnational organized crime. Global Organized Crime Index 2023. GI-TOC. 2023.
2. Global Investigative Journalism Network. Guide to investigating organized crime in Africa: Drug trafficking. GIJN. 2023.
3. Ellis S. West Africa's international drug trade. African Affairs. 2009; 108: 171-196.
4. United Nations Office on Drugs and Crime. The coca/cocaine market. World Drug Report 2011. World Drug Report. 2011; 85-126.
5. Transnational organized crime in West Africa. United Nations Office on Drugs and Crime. 2013.
6. West Africa Commission on Drugs. Not just in transit: Drugs, the state and society in West Africa. WACD. 2014.
7. Chainalysis. The 2024 global crypto adoption index. Chainalysis. 2024.
8. Ellis S. This present darkness: A history of Nigerian organized crime. Oxford University Press, USA. 2016.

9. Klantschnig G. Crime, drugs and the state in Africa: The Nigerian connection. Brill. 2013.
10. Reuter P. Disorganized crime: The economics of the visible hand. Michigan Law Review. 1984; 82: 1127.
11. Von Lampe K, Ole Johansen P. Organized Crime and Trust: On the conceptualization and empirical relevance of trust in the context of criminal networks. Global Crime. 2004; 6: 159-184.
12. Aning K. Are there emerging West African criminal networks? The case of Ghana. Global Crime. 2007; 8: 193-212.
13. Ellis S, Shaw M. Does organized crime exist in Africa? African Affairs. 2015; 114: 505-528.
14. Aldridge J, Decary-Hetu D. Not an'Ebay for Drugs: the Cryptomarket Silk road'as a paradigm shifting criminal innovation. Available at SSRN 2436643. 2014.
15. Barratt MJ, Aldridge J. Everything you always wanted to know about drug cryptomarkets (but were afraid to ask). Inter J Drug Policy. 2016; 35: 1-6.
16. Martin J. Lost on the silk road: Online drug distribution and the crypto market. Criminology & Criminal Justice. 2014; 14: 351-367.
17. Decary-Hetu D, Giommoni L. Do police crackdowns disrupt drug cryptomarkets? A longitudinal analysis of the effects of Operation Onymous. Crime, Law Soc Change. 2017; 67: 55-75.
18. Ladegaard I. Crime displacement in digital drug markets. Inter J of Drug Policy. 2019; 63: 113-121.
19. Soska K, Christin N. Measuring the longitudinal evolution of the online anonymous marketplace ecosystem. In 24th USENIX security symposium (USENIX security 15). 2015; 33-48.
20. Munksgaard R, Tzanetakis M. Uncertainty and risk: a framework for understanding pricing in online drug markets. Inter J Drug Policy. 2022; 101: 103535.
21. Norbutas L, Ruiter S, Corten R. Reputation transferability across contexts: Maintaining cooperation among anonymous cryptomarket actors when moving between markets. Inter J Drug Policy. 2020; 76: 102635.
22. Duxbury SW, Haynie DL. The network structure of opioid distribution on a darknet cryptomarket. J Quantitative Criminology. 2018; 34: 921-941.
23. Paquet-Clouston M, Decary-Hetu D, Morselli C. Assessing market competition and vendors' size and scope on AlphaBay. Inter J Drug Policy. 2018; 54: 87-98.
24. Demant J, Munksgaard R, Decary-Hetu D, Aldridge J. Going local on a global platform: A critical analysis of the transformative potential of cryptomarkets for organized illicit drug crime. Inter Criminal Justice Review. 2018; 28: 255-274.
25. Hout MCV, Bingham T. Surfing the Silk Road: A study of users experiences. Inter J Drug Policy. 2013; 24: 524-529.
26. Demant J, Bakken SA, Oksanen A, Gunnlaugsson H. Drug dealing on facebook, snapchat and instagram: A qualitative analysis of novel drug markets in the Nordic countries. Drug Alcohol Review. 2019; 38: 377-385.
27. Dewey M, Buzzetti A. Easier, faster and safer: The social organization of drug dealing through encrypted messaging apps. Sociology Compass. 2024; 18: 13175.
28. Moyle L, Childs A, Coomber R, Barratt MJ. # Drugsforsale: An exploration of the use of social media and encrypted messaging apps to supply and access drugs. Inter J Drug Policy. 2019; 63: 101-110.
29. Bakken SA. Drug dealer's gone digital: Using signalling theory to analyse criminal online personas and trust. Global Crime. 2021; 22: 51-73.
30. Gambetta D. Codes of the underworld: How criminals communicate. Princeton University Press. 2009.
31. Lusthaus J. Industry of anonymity: Inside the business of cybercrime. Harvard University Press. 2018.
32. Van Wegberg R, Tajalizadehkhoob S, Soska K, Akyazi U, Ganan CH, Klievink B, et al. Plug and prey? measuring the commoditization of cybercrime via online anonymous markets. In Proceedings of the 27th USENIX Security Symposium. USENIX Association. 2018; 1009-1026.
33. Yip M, Webber C, Shadbolt N. Trust among cybercriminals? carding forums, uncertainty and implications for policing. Policing and Society. 2013; 23: 516-539.
34. Gambetta D, Sugden R. The Sicilian mafia: The business of private protection. J Eco Literature. 1995; 33: 863-864.
35. Bouchard M. On the resilience of illegal drug markets. Global Crime. 2007; 8: 325-344.
36. Kleemans ER, Van de Bunt HG. The social embeddedness of organized crime. Transnational organized crime. 1999; 5: 19-36.
37. Von Lampe K. Organized crime. SAGE Publications. 2016.
38. Morselli C. Inside criminal networks. Springer New York. 2009.
39. Lusthaus J. Trust in the world of cybercrime. Global Crime. 2012; 13: 71-94.
40. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system [White paper]. 2008.
41. Werbach K. The blockchain and the new architecture of trust. The MIT Press. 2018.
42. Morselli C, Decary-Hetu D, Paquet-Clouston M, Aldridge J. Conflict management in illicit drug cryptomarkets. Inter Criminal Justice Review. 2017; 27: 237-254.
43. Force FAT. Virtual assets red flag indicators of money laundering and terrorist financing. Consultadoen. 2020.

44. Force FAT. Updated guidance for a risk-based approach to virtual assets and virtual asset service providers. FATF. 2021.
45. Moser M, Soska K, Heilman E, Lee K, Heffan H, Srivastava S, et al. An empirical analysis of traceability in the monero blockchain. Proceedings on Privacy Enhancing Technologies. 2018; 3: 143-163.
46. Moneyval. Virtual assets: Typologies report on money laundering and terrorist financing risks in the world of virtual assets. Council of Europe. 2023.
47. Granovetter M. Economic action and social structure: The problem of embeddedness. American J Soci. 1985; 91: 481-510.
48. Decary-Hetu D, Paquet-Clouston M, Aldridge J. Going international? Risk taking by cryptomarket drug vendors. Inter J Drug Policy. 2016; 35: 69-76.
49. Barratt MJ, Ferris JA, Winstock AR. Safer scoring? Cryptomarkets, social supply and drug market violence. Inter J Drug Policy. 2016; 35: 24-31.
50. United Nations Office on Drugs and Crime. World drug report 2024. United Nations. 2024.
51. International Crisis Group. Drug trafficking, violence and politics in northern Mali (Africa Report No. 267). International Crisis Group. 2018.
52. Lacher W. Organized crime and conflict in the sahel-sahara region. Perilous Desert. 61-85. Carnegie Endowment Inter Peace.1999.
53. Makarenko T. The crime-terror continuum: tracing the interplay between transnational organized crime and terrorism. Global Crime. 2004; 6: 129-145.
54. Micallef M, Farrah R, Bish A, Tanner V. After the storm: organized crime across the Sahel-Sahara following upheaval in libya and mali. Global Initiative against Transnational Organized Crime. 2019.
55. Scheele J. Smugglers and saints of the sahara: Regional connectivity in the twentieth century. Cambridge University Press. 2012.
56. Aldridge J, Decary-Hetu D. Hidden wholesale: The drug diffusing capacity of online drugcryptomarkets. Inter J Drug Policy. 2016; 35: 715.
57. Bakken SA, Moeller K, Sandberg S. Coordination problems in cryptomarkets: Changes in cooperation, competition, and valuation. European J Criminology. 2017; 15: 442-460.
58. Werbach K. The blockchain and the new architecture of trust. The MIT Press. 2018.