e-ISSN 2690-3458 ISSN 2690-3431

JOURNAL
OF
ACADEMICS STAND AGAINST POVERTY

Volume 6, 2025: pages 103-126

Research Paper

Digital Shadows in Illicit Financial Flows: Unraveling Nigeria's Cryptocurrency Paradox and Illuminating Pathways to Financial Integrity

Wisdom Essien

University of Passau, Germany, DAAD Alumni Forum, Nigerian Scholars in Germany (NiSiG), ORCID: 0009-0002-9776-5060.
Email: *essien01@ads.uni-passau.de*

Abstract: Nigeria's lead in global cryptocurrency adoption amidst a slumping economy presents a fascinating paradox. This raises, inter alia, concerns about the factors driving cryptocurrency adoption and its potential for illicit financial flows in the country. Consequently, this study aims to identify the key factors facilitating the use of cryptocurrency for illicit financial flows in Nigeria, assess its impact on the country's economy, and propose workable solutions to address the challenges. Leveraging extant literature, an interview, and Davis' Technology Acceptance Model (TAM) for empirical analysis, the paper identifies the decentralized nature of the blockchain and the anonymity provided by mixers, tumblers, and privacy coins as "perceived usefulness", and the relatively higher cost and delays of international transactions with commercial banks in comparison to the blockchain as the "perceived ease of use". The paper further submits that a porous legal framework guides the use of cryptocurrency in Nigeria, which is part of the enabling factors of on-chain illicit financial flows in the country. This is despite recent policy shifts, including the introduction of Nigeria's Central Bank Digital Currency (CBDC), which have not effectively addressed these issues. The research concludes that, notwithstanding the risks associated with cryptocurrencies, they also present opportunities for financial inclusivity.

Keywords:
1. Nigeria
2. Cryptocurrency
3. Illicit Financial Flows
4. Finance
5. Blockchain
6. Paradox

2025 Journal ASAP

DOI: 10.5281/zenodo.17967591

Received 10 June 2025
Revised 10 December 2025
Accepted 15 December 2025
Available online 17 December 2025

1. Introduction

Today's interconnected world and evolving technological ecosystem have made combating illicit financial flows (IFF) difficult for countries and international authorities. While digital technology has long been utilized in finance, the rise of distributed ledger technology (DLT) like the blockchain has catalyzed the creation and widespread adoption of new digital currencies. These encompass private and public forms, including central bank digital currencies (CBDCs), e-money[1] and cryptocurrencies (Kim et al. 2024, p. 2). Alongside this novel shift to digital finance, is developing economies' burgeoning adoption of cryptocurrencies. A report by Chainalysis (2023, pp. 5-85), posits that the continued regulatory clarity of cryptocurrency worldwide has given rise to developing countries taking their place as global leaders in cryptocurrency adoption. According to which, it also ranks Nigeria in 2nd place, just after India, on the 2023 global cryptocurrency adoption index.

Historically, Bitcoin remains the first cryptocurrency invented. The maiden cryptocurrency was introduced in 2008 through a paper posted to a cryptography mailing list under the pseudonym "Satoshi Nakamoto" titled "Bitcoin: A Peer-to-Peer Electronic Cash System" (Grover et al., 2019, p. 772). The posted paper described establishing a decentralized peer-to-peer system of transactions devoid of interference from the government and financial institutions. The system sought to supplant conventional trust, accountability, and oversight components inherent in commercial and traditional exchange practices. Nakamoto's vision for Bitcoin transactions materialized with the release of the open-source "Bitcoin-Client" and the mining of the initial block[2] of Bitcoins, known as the "genesis block". Over time, Bitcoin gained prominence as a means of transaction, finding utility within global organizations such as WikiLeaks and the Electronic Frontier Foundation. Further underscoring its influence, the foundation pivoted towards the coin's standardization, protection, and promotion (Jejelola, 2021, pp. 12-13).

Akin to cryptocurrency, transnational financial crimes, while longstanding, have taken on new forms and increased magnitude in recent times. In Nigeria, cryptocurrency plays an increasingly significant role in these crimes (Jejelola, 2021, p. 23). The emergence of cryptocurrencies in mainstream markets has transformed conventional ways of money laundering and fraudulent transactions. Technology such as blockchain now plays a crucial role in enabling clandestine acquisition and cross-border transfer of illicit funds. In 2023, the total value of cryptocurrencies sent from illicit addresses on the blockchain amounted to $22.2 billion[3], slightly lower than the $31.5 billion recorded in 2022 (Padalkar, 2023, p. 2; Chainalysis, 2024, p. 23). The United Nations Conference on Trade and Development (UNCTAD) (2020, pp. 155-171) estimated an annual loss of $88.6 billion between 2013 and 2015 in Africa through IFF–trade misinvoicing and other balance-of-payment transactions, with the single largest share of about $41 billion accruing to Nigeria. Thus, posing a substantial economic challenge for the country, and by extension, the continent.

Considering the above challenges, this essay uses a qualitative research approach to unravel the enabling factors of illicit financial flows on blockchain technology, the consequent impact in Nigeria, and the practical solutions to mitigate its unethical usage. Hence analyzing, inter alia, the intrinsic complexities of decentralization and anonymity of cryptocurrencies cum blockchain, and the porous legal framework that drives its use for illegal financial cross-border transfers in Nigeria. As a scientific effort, the essay adopts Fred Davis' Technology Acceptance Model (TAM), which lends clarity to the reasons why technology, in this case, cryptocurrency, is becoming a mainstay channel for IFF in Nigeria and is used by criminal entities to obscure

[1] E-money as used here refers to a digital form of cash/currency electronically stored and used for payment transactions.

[2] Cryptocurrency block is a record of the most recent cryptocurrency transactions.

[3] The designated currency symbol '$' as used here and on other pages refers to the United States' dollar.

cross-border financial fraud. The theoretical indicators of TAM, "Perceived usefulness[4]" and "Perceived ease of use[5]", explain reasons for adopting blockchain technology for IFF in Nigeria. To help inform the discussion, data were collated from Chainalysis - a foremost blockchain research firm; the Economic and Financial Crimes Commission (EFCC); the Nigerian Financial Intelligence Unit (GFIU); and the Central Bank of Nigeria (CBN) to ascertain the use of cryptocurrency for IFF in Nigeria. More so, in establishing other enabling conditions for the use of cryptocurrencies for IFF, a key informant interview (see Appendix 1) was conducted with a staff of the United Bank for Africa (UBA) to evaluate the "ease" of international transactions on the blockchain as against centralized financial institutions (CFI).

Furthermore, there is a paucity of academic literature regarding cryptocurrency adoption, payment and usage in Nigeria. However, when it comes to the subject of cryptocurrency, two contrasting scholarly perspectives have gained significant acceptance. On the one hand, cryptocurrencies are seen by some scholars as the future of payment systems, facilitating swift and efficient transactions between users. On the other hand, others argue that cryptocurrencies provide criminals with a method to store and transfer illegal funds and evade detection by financial authorities. Chen and Bellavitis (2019, pp. 1-2) argue that decentralized finance can reduce transaction costs, broaden financial inclusion, increase access to basic financial services, encourage permissionless payments, and create new opportunities. Buttressing this point further, Oyeyemi et al. (2024, p. 182) affirm that decentralized finance can reshape the structure of modern finance and create a new landscape for entrepreneurship and business innovation. On the flip side, Schär (2021, pp. 153-154) fears that decentralized finance is a segment of financial markets with certain risks, even though it offers efficiency, transparency, accessibility, and interoperability advantages. Upholding Schär's polemic, Zetzsche, Arner, and Buckley (2020, p. 172) argue that decentralized finance has the potential to undermine traditional forms of accountability and erode the effectiveness of traditional financial regulation and enforcement.

Moreover, the significance of this essay to extant literature is its specific study on the complex instigators of blockchain technology and its concomitant currencies for IFF in Nigeria; the succinct comparative analysis of the blockchain and centralized financial institutions (banks) in Nigeria to ascertain the "ease of use" of these channels for IFF; the practicable recommendations, and the variable of its data recency as compared to other studies.

2. Historical overview of illicit financial flow in Nigeria

IFF represents the portion of finance with illicit origin and usage, such as tax evasion, trade mispricing and misinvoicing, currency counterfeiting, terror financing, drug and human trafficking, etc., that either crosses borders or is transferred out of a country (Okojie, 2018, pp. 3-4). Following the decline in oil prices during the 1980s and the subsequent austerity measures linked to Nigeria's Structural Adjustment Programme (SAP), the country witnessed a surge in money laundering activities. This period spurred unprecedented greed and avarice, leading to severe financial crimes among Nigerians (Sanusi, 2023, p. 1). Despite international efforts to combat money laundering, the crime exacerbated and continued to erode Nigeria's economic stability. In 2000, Nigeria was identified by the Financial Action Task Force (FATF) as one of the non-cooperative countries or territories (NCCTs) in the fight against money laundering. Equally, the United Kingdom's (UK) financial supervisory authorities estimated that illicit transactions in UK accounts originating from Nigeria totalled approximately $1.3 billion between 1996 and 2000 (Kama, 2005, p. 31).

Recognizing the detrimental impact of these criminal activities on the economy, especially during the country's pursuit of economic revitalization, the Federal Government of Nigeria established the Independent Corrupt Practices and other Offences Commission (ICPC) in

[4] An indicator that implies people will use technology mainly because of its usefulness.

[5] An indicator that explains that technology will be adopted based on the ease experienced while using it.

September 2000 and the Economic and Financial Crimes Commission (EFCC) in March 2003 (Micah et al., 2022, p. 88). These agencies were tasked with the investigation of economic and financial crimes within the country, aiming to hold perpetrators accountable. The EFCC was saddled with the authority to confront economic and financial crimes, having been established through an enabling Act of the National Assembly in December 2002. According to Section 7(2) of the EFCC (Establishment) Act, 2001, the Commission serves as the coordinating body for the enforcement of the Money Laundering (Prohibition) Act, 2004 (Kama, 2005, p. 32). Despite the constituted authorities and enacted Acts to mitigate against financial crime, IFFs in Nigeria persisted. According to Ngwakwe (2015, p. 124), leveraging data from Global Financial Integrity (GFI), Nigeria's IFF between 2004 and 2012 was well over $150 billion:

Table 1: Illicit Financial Flow in Nigeria 2004 – 2012

Year	Amount ($)	Percentage of GDP	Percentage increase/decrease
2004	1.6 billion	-	-
2005	17.8 billion	6.8%	1012.5%
2006	19.1 billion	6.8%	7.30%
2007	19.3 billion	1.2%	1.05%
2008	24.1 billion	7.4%	24.87%
2009	26.3 billion	7.7%	9.13%
2010	20.7 billion	4.9%	21.29%
2011	20.1 billion	3.8%	2.90%
2012	7.9 billion	1.2%	60.70%

Source: Ngwakwe (2015, p. 124) and Joseph (2019, p. 9).

The data presented above demonstrates the variability in illicit financial flows within Nigeria before the widespread adoption of cryptocurrency. In 2004, a few years after the SAP, IFF totalled $1.6 billion, rising significantly to $17.8 billion in 2005. Subsequent increments were more moderate, ranging from about 1% to 25%. Subsequently, after peaking at $26.3 billion, the values begin to decline, with a $21.3% decrease to $20.7 billion and a further slight drop to $20.1 billion. The most substantial decrease is observed from $20.1 billion to $7.9 billion, amounting to a 60.7% reduction. These variations suggest periods of high and low illicit flows. Also represented are the percentages of IFFs fluctuations to the Gross Domestic Product (GDP) of Nigeria for each year (Ngwakwe, 2015, p.124; Joseph, 2019, p. 9).

3. Cryptocurrency and illicit financial flow in Nigeria: The adoption, impact, and trends

Cryptocurrency, a decentralized and encrypted digital currency, has emerged as a groundbreaking innovation globally, including in Nigeria. Derived from blockchain technology - a revolutionary subset of distributed ledger technology, cryptocurrency operates on a network of interconnected computer servers known as nodes. This decentralized system facilitates the secure recording and sharing of data across multiple ledgers, ensuring transparency, immutability, and security. Users' wallets must possess private and public encryption keys to transact within the cryptocurrency network. The private key, often backed up by seed phrases, is used to authorize transactions, prove ownership of wallets and funds, etc., while the public key functions as an address on the blockchain network and can be used in verifying sender's identity (Jejelola, 2021, pp. 10-11; Oladipupo and Amodu, 2022, p. 116). Cryptocurrencies fulfil distinct roles for users, primarily functioning as speculative investment vehicles or mediums of exchange. While some cryptocurrencies serve both purposes, others are specialized

in one function. For instance, Bitcoin—commonly regarded as "digital gold"—is predominantly held as a store of value for capital appreciation. In contrast, stablecoins such as USDT (Tether)[6] are designed to facilitate transactions due to their price stability, pegged to fiat currencies like the United States dollar (Griffin, 2025, p. 30).

3.1 Adoption

In recent times, Nigeria has witnessed a surge in cryptocurrency adoption and blockchain technology. A large segment of the country's tech-savvy youth has embraced digital assets, contributing to Nigeria's position as a leading adopter of cryptocurrencies. Factors such as limited financial services, high inflation, currency depreciation, and a young demographic have also fueled this growth (Greenfield, 2020, p. 5). Besides being ranked 2nd on the 2023 global cryptocurrency adoption index, Nigeria ranks 1st on peer-to-peer (P2P) exchange trade volume, 2nd in centralized service value received and 3rd in retail centralized service value received globally (see Figure 1). Recording over $50 billion worth of Bitcoin and stablecoins volume received by indigenous exchanges between August 2021 and July 2023. The nation maintains a significant 9.0 % year-over-year (YoY) volume growth between 2021 and 2023 globally, placing it third globally based on YoY and the studied period (Chainalysis, 2023, pp. 83-86). However, alongside these outstanding adoption indices of cryptocurrency in Nigeria are the challenges of huge illicit financial flows, cybercrimes, and tax evasion, resulting in economic instability and poverty in the nation.

Figure 1: The 2023 Global Crypto Adoption Index Top 16

Country	Region	Overall index ranking	Centralized service value received ranking	Retail centralized service value received ranking	P2P exchange trade volume ranking	DeFi value received ranking	Retail DeFi value received ranking
India	Central and Southern Asia and Oceania	1	1	1	5	1	1
Nigeria	Sub-Saharan	2	3	2	1	4	4
Vietnam	Central and Southern Asia and Oceania	3	4	4	2	3	3
United States	North America	4	2	8	12	2	2
Ukraine	Eastern Europe	5	5	3	11	10	10
Philippines	Central and Southern Asia and Oceania	6	6	6	19	7	7
Indonesia	Central and Southern Asia and Oceania	7	13	13	14	5	5

[6] USDT is the symbol for Tether, a cryptocurrency that is pegged to the U.S. dollar

Pakistan	Central and Southern Asia and Oceania	8	7	7	9	20	20
Brazil	Latin America	9	9	11	15	11	11
Thailand	Central and Southern Asia and Oceania	10	8	15	44	6	6
China	Eastern Asia	11	10	5	13	23	23
Turkey	Middle East and North Africa	12	11	9	35	12	12
Russia	Eastern Europe	13	12	10	36	9	9
United Kingdom	Central, Northern and Western Europe	14	15	20	38	8	8
Argentina	Latin America	15	14	12	29	19	19
Mexico	Latin America	16	17	18	30	16	16\

Source: Chainalysis (2023, p. 5)

3.2 Impact

In 2023, the Central Bank of Nigeria (CBN) imposed stringent regulatory measures against Binance, a US-based cryptocurrency exchange, to stabilize the Nigerian naira[7] and bolster the national economy. The CBN alleged that Binance was being exploited by malevolent actors engaged in illicit activities such as money laundering, terrorism financing and market manipulation, which have significantly distorted Nigeria's economy and contributed to the naira's depreciation. This is evidenced in the plummeted exchange rate of the naira against the US dollar[8] from around ₦461 per dollar in May 2023 to over ₦1500 per dollar in August 2024. Additionally, the CBN accused Binance of providing services in Nigeria without remitting taxes, thus depriving the nation of crucial revenue. Dr. Olayemi Cardoso, the CBN Governor, revealed that an estimated $26 billion had been transacted without tax through Binance in Nigeria by unidentified sources within a year, consequently prompting concerns regarding its impact on economic stability (Ogege, 2024, pp. 19-20).

Consequently, according to the World Bank Group (2024, p. 1), Nigeria's current economic inflation rate has reached a 24-year apex of 31.7% in February 2024, indicating a dire economic quagmire facing the country. Ruth and Ismail (2024) lend credence to this, stating:

> "Nigeria is facing its worst economic crisis in decades, with skyrocketing inflation, a national currency in free-fall and millions of people struggling to buy food. The pain is widespread. Unions strike to protest salaries of around $20 a month [see Figure 2]. People die in stampedes, desperate for

[7] Naira, designated "₦", is the official currency of Nigeria

[8] Google Finance (2024) https://www.google.com/finance/quote/USD-NGN?window=5Y

free sacks of rice. Hospitals are overrun with women wracked by spasms from calcium deficiencies"

Figure 2: Nigerians and unionists during the 2024 "End Bad Governance and Hunger" protest

Source: Voice of Liberty (2024, p. 1)[9]

From an appraisal viewpoint, the current economic crisis faced by Nigeria presents a paradoxical juxtaposition: Nigeria simultaneously occupies a prominent position in global cryptocurrency adoption while being among the worst economies globally. Given the country's well-documented issues with systemic corruption [10] and economic mismanagement, this incongruity between Nigeria's lead in cryptocurrency adoption and its severe economic difficulties suggests a potential correlation. Specifically, it raises the hypothesis that cryptocurrency may be serving as a robust conduit for illicit financial transactions and potentially intensifying the nation's economic challenges. This could be so because the impact of IFFs on Nigeria's socio-economic landscape is huge. For example, Nigeria has more than 83 million citizens (about 40 % of the population) living in extreme poverty of less than $1.9/day[11] as per a 2019 estimate, while the number of unemployed Nigerians has reached 23.2 million (33.3 %) in the fourth quarter of 2020 as against 21.77 million in the second quarter[12].

Mobilizing resources lost through IFFs, which manifest as both outflows and inflows of funds, can provide the needed funds to improve the Nigerian economy. The outflows of illicit funds, which occur when funds are illegally moved abroad through tax evasion by multinational corporations, embezzlement by corrupt officials, oil theft, or money laundering, deprive the government of critical revenue needed for public investment. Meanwhile, inflows—such as illicitly repatriated profits, laundered money recycled through fake investments or smuggled goods—distort markets, fuel corruption, and create a bad reputation for the nation, which further weakens the economy. For instance, when stolen funds re-enter Nigeria disguised as foreign investment, they often bypass proper taxation and regulation, perpetuating a cycle of

[9] Voice of Liberty NG (2024) https://voiceoflibertyng.com/endbadgovernance-organisers-plan-million-man-grand-finale-protest-across-nigeria/

[10] Ranks 145 on the Global Corruption Perception Index, 2023 https://www.transparency.org/en/cpi/2023

[11] Akwagyram, Alexis (2020). Forty percent of Nigerians live in poverty: Stats office. www.reuters.com

[12] Adegboyega, Ayodedeji (2021). Nigeria's unemployment rate rises to 33.3% - highest in over 13 years. www.premiumtimesng.com

graft and lost revenue. Both types of IFFs drain resources that could otherwise fund infrastructure, education, and healthcare, while also discouraging legitimate investment.

According to the Mbeki Panel report (2015), it would have taken about 10 years between 2000 and 2011 to meet the MDG goal of reducing child mortality to 77 from 186 per 100,000 if IFFs were eliminated, as against 28 years it would take based on current arrangement (ANEEJ, 2018, p. 20). Illicit financial flows through cryptocurrency divert public resources intended for public welfare, resulting in both immediate and long-term consequences. Nigeria's experience with recovering Abacha's stolen funds highlights the significant costs associated with addressing IFFs. Despite recovering $2.4 billion[13] after a twenty-year process, the government incurred substantial expenses, including foreign jurisdiction levies and recovery agent fees. Additionally, the recovered funds often represent only a fraction of their potential value due to lost interest, while the government incurs significant costs for recovery efforts. For example, the second recovered loot of Abacha, worth $322.5 million, only accrued $1.5 million in interest, representing a mere 0.46 percent. Meanwhile, Nigeria paid 4 percent of the recovered loot, amounting to $96 million (4% of $2.4 billion), to the recovery agent. Also, the long-term impact in terms of the absence of infrastructure, unavailable social services and denied opportunities, which the stolen funds could have generated, cannot be quantified (Africa Network, 2018, p. 21).

3.3 Trends:

The recent trends of illicit financial flows facilitated by cryptocurrency in Nigeria have manifested in a diverse array of activities, encompassing tax evasion, fraud and Ponzi schemes, money laundering, and the financing of illegal activities. As evidenced in Table 2, these illicit activities have had a profound and detrimental impact on Nigeria's economy and its citizens. The widespread use of cryptocurrency has made it easier for people and businesses to engage in illegal activities, harming financial systems and public trust. To this day, reports on financial crimes by the Economic and Financial Crimes Commission (EFCC) involving cryptocurrencies persist, as seen in reported cases of huge IFFs involving Nigeria and other countries below:

[13] BBC (2021). Sani Abacha: the hunt for the billions stolen by Nigeria's ex-leader. www.bbc.co.uk

Table 2: Recent Trends of Illicit Financial Flow using Cryptocurrency in Nigeria

[14]S/N	Jurisdictions	Amount	Report details
1	Kenya/ Nigeria	$349,000	In 2021, the EFCC received a report from a foreign law enforcement agency regarding an alleged fraud case of $349,000 involving two suspected Nigerian fraudsters who had relocated to Kenya. Analysis of the suspects' bank statements uncovered regular payments from the same source, leading to the discovery that a final-year university student in Nigeria had a turnover exceeding N1.2 billion (approximately $1.6 million) in one of his accounts. The student, arrested as the money handler, confessed to knowingly exchanging fiat currency for cryptocurrency for various fraudsters, including the two initial suspects under investigation.
2	Vietnam/Nigeria	$2,000,000	The EFCC received an Intelligence Report from the Nigerian Financial Intelligence Unit (NFIU) regarding the account activities of "Chinelo"[15], a waitress at "Jans Hotels" in Nigeria, prompting an immediate investigation. Bank account intelligence linked to the suspect was gathered, and further information was requested from competent authorities, including the regulated crypto exchange**,** Binance where the suspect held a wallet account. Investigations uncovered that the suspect was a legitimate crypto exchange service provider engaged by an individual named "Henry" to convert crypto valued at over $2,000,000 to cash for someone identified as "Jerry" purportedly residing in Vietnam. "Henry", the principal suspect, used the proceeds to purchase properties valued at over N315,000,000 (approximately $416,000). "Jerry" is presently evading apprehension due to suspicions surrounding the source of the sold cryptocurrency.
3	USA/Nigeria	$95,000	In 2021, the EFCC conducted a sting operation leading to the arrest of a fraud suspect identified as "Mr. Jackson" after a victim filed a complaint about a suspected romance scam. Forensic analysis of "Mr. Jackson's" device revealed his impersonation as an American Surgeon on a UN Mission to the Middle East, targeting a Korean American victim. He manipulated her into financially supporting him through crypto payments, claiming that cash transactions were challenging. "Mr. Jackson" falsely promised marriage upon his return and cited an expected $5 million payment to start a life together. Upon arrest, over $95,000 worth of Bitcoins were seized. "Mr. Jackson" was convicted and the assets were ordered to be forfeited to the victim.
4	South Africa/ Norway/United Kingdom /Barbados	$1,600,000	In 2022, Benjamin Ikaa was convicted and sentenced to five years in prison for his involvement in a $1.6 million cryptocurrency fraud. Ikaa pleaded guilty to a one-count amended charge under Section 14(2) of the Cybercrime (Prohibition Prevention etc.) Act 2015. His arrest by the EFCC stemmed from his operation of a fictitious cryptocurrency investment website (www.mcharveycapital.com), through which he promised significant investment returns. This led to unsuspecting victims from South Africa, Norway, the United Kingdom, and Barbados incurring a loss of about 26 bitcoins, equivalent to $1.6 million as of February 2023.

[14] The font size and page format used for Table 2 is 10 and landscape respectively. This is to allow for a fuller capture of more case reports.

[15] All names in inverted commas used in these case reports are pseudonyms, as the EFCC withheld the names of some individuals involved in these crimes.

5	China/Nigeria	$72, 000,000	In 2022, the EFCC conducted a sting operation in Lagos, resulting in the apprehension of a suspect involved in romance scams while his brother managed to escape. Interrogations with the captured brother revealed their joint involvement in the scams, with the escapee brother providing foreign accounts to store the proceeds. An investigation into the escapee brother's account uncovered a suspicious inflow of thirty million naira (approx. $39,628.91), originating from a company, which reported an unusually high turnover of fifty-seven billion naira (approx. $75,294,938.20) within a year. Seven other companies were identified for making significant deposits into the account. A Chinese woman operated the account from China, engaging in cryptocurrency transactions and making naira payments. It was discovered that the escapee's brother was involved in selling cryptocurrency to the Chinese woman. The Chinese suspect was later arrested, and the investigation remains ongoing.
6	Nigeria, UK, US, Thailand	-	In 2020, three suspects were apprehended in Lagos, Nigeria as part of a joint INTERPOL-Group-IB and Nigeria Police Force cybercrime investigation. They were accused of creating phishing links, domains, and mass mailing campaigns to impersonate organization representatives, deploying 26 malware programs, spyware, and remote access tools. According to Group-IB, the group had targeted government and private sector entities in over 150 countries since 2017, operating through various subgroups with several individuals still at large. The investigation further revealed that the suspects utilized bank and cryptocurrency accounts belonging to their foreign associates to receive illicit payments, with a particular focus on a bank account provided by their counterparts in the UK, US, and Thailand to receive criminal proceeds from victim companies. The monetary amount of their nefarious activities over the years was not given.
7	Kenya, Nigeria, USA, UAE, Europe	$220,000,000	On April 27, 2022, a report of a multi-billion-dollar money laundering syndicate surfaced from the asset recovery agency, drawn from the financial crime and investigation unit, involving top companies and directors from both Nigeria and Kenya. The suspects were said to have used Bitcoin to conceal their transactions. According to a statement filed by European investigators, the Nigerians involved in the scandal were Mr. Olubunmi Akinyemiju, Mr. Eghosasere Nehikhare and Mr. Olufemi Olukunmi Demuren. The three Nigerians were linked to Ksh25.6 billion (US$220 million) moved into Kenya between October and November 2020. The trio were alleged to have first bought 1,113 Bitcoins worth KSh5 billion (US$43 million) in the UAE, the United States, and several other European countries, including Kenya's cryptocurrency exchange platform, BitPesa. European investigators further believe that the Nigerians may have transacted in Kenya long before setting off alarm bells in Europe. The cryptocurrency purchase appears to have happened a month before the three wired Sh25.6 billion (US$220 million) from Lagos to a network comprising more than ten companies in Nairobi.[16]

Source: Compiled by author from EFCC website[17] and NFIU (2023, pp. 24-54).

[16] Business Daily (2021) ''Kenyan politician, Nigerians bought Sh5 billion Bitcoins in two months'' https://www.businessdailyafrica.com/bd/economy/how-nigerians-bought-sh5-billion-bitcoins-in-two-months-3798408

[17] Economic and Financial Crimes Commission (2024) https://www.efcc.gov.ng/efcc/other-pages/smart-search?q=cryptocurrency (Official website of the EFCC of Nigeria)

4. Intrinsic enablers of on-chain illicit financial flow in Nigeria

The nexus between illicit financial flows and cryptocurrency hinges on both intrinsic and extrinsic factors. According to Padalkar (2023, p. 8), "One of the core principles of criminal transactions revolves around increased anonymity. Three blockchain features enabling anonymity are elliptical key cryptography, secure hashing, and decentralization. In addition to these features [are], blockchain mixer, chain hopping, and stealth addressing [which make] detecting the real actors in the transactions become nearly impossible." It is important to state that while these services and privacy coins may guarantee some level of anonymity for users, on-chain experts and authorities can detect illicit funds on centralized exchanges (CEXs) through user errors (reusing addresses and leaking of IPS[18]), spending patterns and exchange compliance measures such as KYC documentations. To establish clarity, this section of the paper only analyses blockchain's internal enablers for IFF, excluding external factors such as an inadequate legal framework, the bottleneck of the centralized financial sector, and the absence of a universal legal framework and collaboration among international economic crime authorities, among others. It is equally imperative to note that while there are no universal legal frameworks on the regulation of cryptocurrency, there are extradition treaties, collaborations across borders between law enforcement agencies, etc..

4.1 Decentralization

Blockchain technology offers a significant advantage by streamlining the execution of various transactions that typically necessitate a third party's involvement, such as a bank, securities settlement system, broker-dealers, or trade repository. Essentially, blockchain promotes trust and facilitates decentralized transaction authentication. In simple terms, it enables the elimination of intermediaries, often referred to as the "middleman" (Houben and Snyers, 2018, p. 17). It is this elimination of centrality and supervision on distributed ledger technology that fosters the susceptibility of cryptocurrencies to illicit financial flows. Thus, it remains a perceived useful channel for money launderers. In Nigeria, despite the implicit ban[19] on cryptocurrency, the use of Bitcoin and other cryptocurrencies continues due to the elusive element of decentralization (Padalkar, 2023, pp. 6-34). Along this line, decentralization, especially in terms of decentralized exchanges, presupposes that cryptocurrencies are useful for concealed cross-border transactions in Nigeria, especially as they help in eliminating third-party supervision and cost.

4.2 Anonymity

There appears to be a widespread misconception regarding anonymity in virtual currencies. While cryptocurrencies are often perceived as entirely anonymous, their true nature is better described as pseudonymous. This distinction arises from the public and transparent characteristics of blockchain technology (Balaskas and Franqueira, 2018, p. 5). Balaskas and Franqueria's assertion on the default pseudonymous nature of cryptocurrencies is worthy of semantic clarity. It is essential to note that anonymity is not an inherent characteristic of the blockchain. As Bancroft (2020, p. 1) puts it, "Anonymity must be produced by the user. Even then, anonymity is contingent and temporary. It is contingent on the ability of the user to hide in the crowd […]." This means that privacy coins and mixing services enable users' anonymity on the blockchain and not the other way around. The blockchain itself does not shield illicit activity, as its ledgers are transparent. However, users can obscure the origin, amount, and destination of illicit funds through privacy tools and covert services; transactions that might otherwise go undetected except by on-chain experts or advanced analytics like that of Coinbase,

[18] Internet Protocol addresses refer to the unique identifiers assigned to devices participating in peer-to-peer (P2P) networks.

[19] An implicit ban is a ban that aims at preventing the use of cryptocurrency without directly outlawing it.

Chainalysis, Fireblocks etc. Equally, the anonymity of payments enabled on the blockchain has not only made it easier to perpetrate illicit transnational transactions like tax evasion but also cybercrimes like the "Yahoo-Yahoo"[20] of Nigeria (Jejelola, 2021, p. 30).

4.3 Privacy coins

Transactions carried out on the blockchain, particularly those using public ledgers that are visible to the general public, can be traced. Through blockchain analysis, investigators can follow suspected funds on the blockchain and identify the wallets they have passed through (Balaskas and Franqueira, 2018, p. 1). Sadly, according to the Inter-governmental Action Group against Money Laundering in West Africa (GIABA) (2020, p. 4): ''To increase the level of privacy [in other words, anonymity] that users have while transacting in crypto, an emerging form of cryptocurrency is gaining popularity. These are referred to as privacy-enabling cryptocurrencies, otherwise known as privacy coins. These types of coins differ from other cryptocurrencies in the sense that they provide their users with a degree of transactional privacy, while also providing the benefits of decentralization.'' Privacy coins have gained profound acceptance stemming from their use for nefarious activities like illicit trades, money laundering, drugs, weapons and human trafficking (Harvey and Branco-Illodo, 2019, p. 6).

Monero, Zcash, and Mimblewimble are examples of popular privacy coins gaining huge usage. Monero is popular for mixing the sender's transaction with past transactions (decoys), generating a one-time address for each transaction, and encrypting transaction amounts. Zcash proves a transaction is valid without revealing sender, receiver or amount, and offers users the option of shielded or transparent transactions, thus delivering flexibility. Mimblewimble encrypts amounts by combining confidential transactions and merging transaction data to ensure both privacy and scalability (Gopi et al., 2024, p. 7). Since CEXs often impose restrictions on some privacy coins, especially those that are hard to detect (See Table 3), P2P platforms and decentralized exchanges that are mostly KYC noncompliant serve as more viable alternatives for users seeking anonymity. Unscrupulous users who have accounts with these exchanges can transact with privacy coins by purchasing them with funds stored in stablecoins or received via other cryptocurrencies. Some may go as far as employing a virtual private network (VPN) during transactions for extra privacy.

Table 3: Privacy Coins on Centralized Exchanges

Privacy Coin	Centralized Exchange	Examples
Monero (XMR)	Mostly banned	Previously: Binance, Huobi
Zcash (ZEC)	Some exchanges	Binance, KuCoin, CoinEx
Mimblewimble(Grin/BEAM)	Few exchanges	Gate.oi, TradeOgre

Source: Scharnowski (2024, p. 6)

4.4 Tumblers, mixers and others

Tumblers are cryptocurrency services utilized when anonymity is not guaranteed, potentially revealing the owner of virtual coins. The legality of cryptocurrency tumblers is often considered a "grey zone" because even cryptocurrencies themselves are not universally legalized, and the process of "mixing" in tumblers represents a specific aspect of this legal uncertainty (Moslavac, 2019, p. 205). Criminal networks often employ tools and services such as mixers, bridges, swap services, and coin-join to enhance privacy and obscure the source of illegal funds. These mechanisms are considered useful as they significantly help in concealing the origin and flow of illicit assets by pushing them through a series of transactions (Padalkar, 2023, p. 8). According to a report by the Financial Services Agency (2022, p. 30), other factors enabling IFF with cryptocurrencies include:

[20] "Yahoo-Yahoo" is the popular name for cyber fraud in the local parlance of Nigerians. It is derived from Yahoo mail, the earliest channel used in perpetrating such crimes.

- Chain Hopping: This involves replacing crypto-assets with other crypto-assets, therefore making it difficult to trace the history of a transaction from one crypto-asset to another. For example, an individual wanting to chain hop $1000 worth of Bitcoin could do this by swapping it to Monero (XMR) for privacy, then convert it to Ethereum (ETH), and finally back to Bitcoin. Since Monero transactions are untraceable, the link between the original BTC and the final ETH is broken, making it harder for anyone to follow the money's path. This method leverages the features of privacy coins like XMR or ZEC to disrupt blockchain forensics.
- The use of decentralized exchanges (DEXs) and decentralized applications (DApps) remains the holy grail of criminal networks when it comes to on-chain IFFs. For example, a user can swap $1000 of Ethereum for Monero on a DEX like Uniswap, the trade executes automatically via code, and without a central authority. Since DEXs don't require KYC, and DApps operate on encrypted ledgers, the user maintains greater privacy compared to centralized platforms. According to Coingecko (2025), DEXs attract nearly 250 million users monthly[21].
- CoinJoin: This method involves pooling coins and combining multiple transactions to obscure the relationship between the originator's and beneficiary's addresses, thereby enhancing anonymity. For example, if senders A, B, and C each send $1000 in a joint transaction using tools like Wasabi Wallet or JoinMarket to automate this process, their inputs are mixed, and outputs are shuffled. Blockchain observers see a single transaction with three inputs and outputs, but can't determine who sent funds to whom. This breaks transactional links, making tracking difficult.

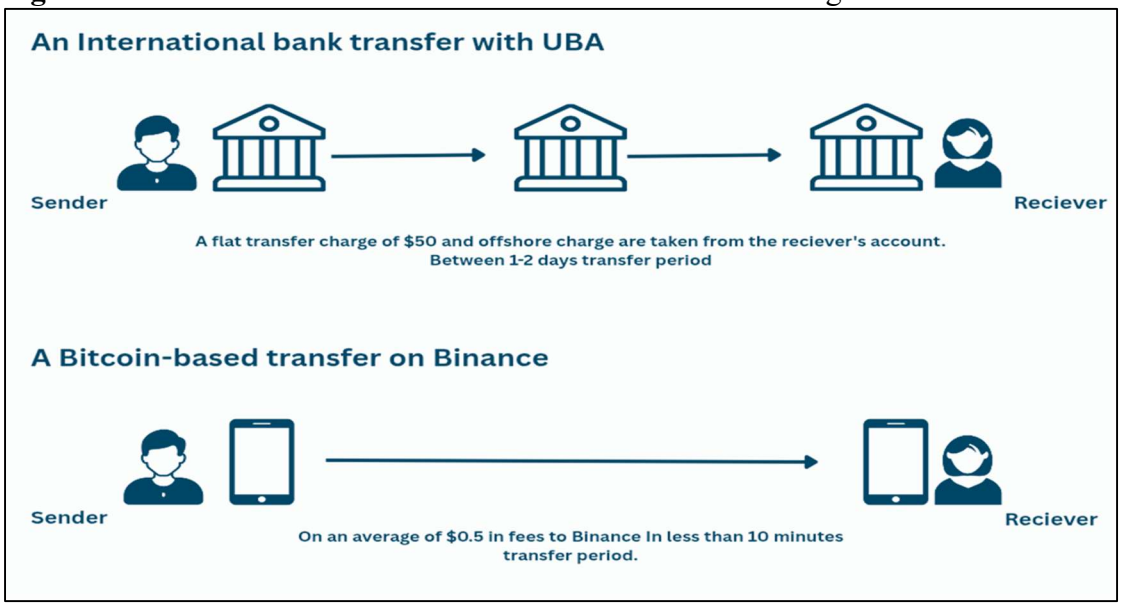
5. Ease of cross-border transactions on the blockchain vis-a-vis banks in Nigeria

According to available financial records, approximately sixty million Nigerians may not have bank accounts, and those who do face restrictions on daily international transactions, often limited to $100 due to the CBN regulations. These factors have prompted a shift towards internet banking and cryptocurrency investment. With a significant number of Nigerians having access to mobile phones and the internet, there has been a movement towards cryptocurrency, facilitated by exchange platforms that allow Nigerians to convert their funds into cryptocurrencies like "stablecoin", with minimal transaction fees and added protection from fund devaluation. Consequently leading to financial inclusion for Nigerians, particularly the youth (Jejelola, 2021, p. 21). In 2021, according to a report by the Deutsche Bank Research (2021, p. 15), cryptocurrency (Bitcoin) held a market capitalization of $1 trillion, making it the third largest currency in the world after the United States dollar and the euro based on currency circulation. Mid-year of the same year, cryptocurrency transactions in sub-Saharan Africa surged to $20 billion per month. This is equivalent to 13% of the region's monthly GDP of around $150 billion[22], 38% of annual remittance inflows of around $53 billion, and surpassing volumes of major national currencies like the West African CFA (XOF), South African Rand (ZAR) and the Nigerian naira (NGN) in cross-border flows (Fuje et al., 2022, p. 2; IMF, 2021)

This surge in the use of cryptocurrency is attributed to the advantages derived from using cryptocurrencies for transactions over the weak fiat currencies the banks transact with. As opposed to commercial banks, cryptocurrency payments offer instant international transactions, easy accessibility, faster processing, and significantly reduced transaction fees. Unlike cryptocurrency, large transactions at the banks often lead to account blockage or the incurrence of high commissions from banks (Jokić et al., 2019, pp. 73-75). The following is an infographic of cross-border transfers within banks and on the blockchain:

[21] Coingecko (2025) https://www.coingecko.com/en/exchanges/decentralized
[22] International Monetary Fund website (2025): https://www.imf.org/external/datamapper/profile/SSA

Figure 3: Ease of Cross-border Transfer: the Blockchain and Nigerian Banks



Source: informed from the Binance website[23] and the author's interview with a UBA staff.

Figure 3 shows the ease of cross-border transfer on the blockchain (Binance) as compared to a Nigerian bank (United Bank for Africa). While there are intermediaries with relatively higher international transfer charges using commercial banks, the blockchain is without an intermediary, except for the DAOP. Following an interview held with a staff of UBA domiciled in Nigeria, a Nigerian wanting to make an international transfer through the bank must have to go to a bank. This is because international transactions cannot be initiated on the bank's mobile application. At the bank, he/she must pick up a foreign currency (FCY) transfer form, fill it up, submit it to a teller officer, and wait for 1 – 2 days for a completed transfer. The transfer charge for an international transaction is a $50 flat rate plus 0.05% of the amount transferred, and there is an additional 0.075% value-added tax charge. Also noted from the interview is that the receiver will also bear the brunt of the transfer charges called "offshore charges". Contrarily, according to the Binance crypto transfer web page, the cost of transfer on the blockchain is within minutes and with as little as $0.50 and a minimum $0.10 - $2 conversion, depending on the cryptocurrency or network used. This is besides the ease of transacting anywhere and anytime with the use of the Binance mobile application on one's phone.

As earlier established in the introduction, "Perceived ease of use" (PEOU) signifies the extent to which users of technological products can use the technology with minimal or no guidance (Ogunode et al. 2023, p. 16). The unlimited access via a mobile device, higher transfer speed, lower cost of transfers, enhanced security of financial transactions, and absence of too much documentation contribute to making the blockchain a resort for international transfer. These perceived advantages remain an enabler for illicit financial flows, as criminal entities not only have a seamless and unregulated channel to exploit, but one that may also give them value in return, particularly in cases where the market volatility of transacted cryptocurrency is favourable (Chen et al., 2020, p. 8). This is what Davis (1989, p. 320) highlights as "ease," meaning "freedom from difficulty or significant effort", which is a finite resource allocated by individuals to their responsibilities. Therefore, it is argued that an application perceived as easier to use than another is more likely to be embraced for use, whether used ethically or not.

[23]Binance (2024) https://www.binance.com/en/fee/cryptoFee

6. Legal framework for the use of cryptocurrency in Nigeria

Transacting in cryptocurrencies indeed represents one of the least regulated markets globally. Research indicates that the surge in unregulated capital flow contributes to heightened financial and overall economic volatility. However, other studies propose that, with appropriate policy frameworks, it's feasible to allow cryptocurrency usage and adoption without undue negative impacts on the economies of the countries permitting them. In some instances, digital token transactions have evolved into substantial capital market hubs, reinforcing the notion that judiciously managed cryptocurrency usage can coexist positively within economies (Ogunode et al., 2022, p. 12).

In contrast to other jurisdictions where digital token transactions have evolved into significant capital market hubs, the Central Bank of Nigeria (CBN) has adopted a stringent stance against cryptocurrencies. In January 2017, the CBN issued a circular prohibiting financial institutions from engaging in any form of transactions involving virtual currencies. Thereafter, on 5th February 2021, the Central Bank of Nigeria, through banks and other financial institutions, declared that dealing in cryptocurrencies and facilitating cryptocurrency exchange were prohibited (Oni and Oyedokun 2025, p. 83). The CBN's rationale centered on the anonymity and lack of Know Your Customer (KYC) protocols, which render cryptocurrencies susceptible to illegal use and in contradiction to existing laws, hence not recognized as legal tender. The CBN emphasized the need to shield Nigerians from fraud, investment risks, money laundering, terrorism financing, illicit funds, and criminal activities associated with unregulated and unlicensed entities (Oladipupo and Amodu, 2022, p. 114).

Following the implicit ban on cryptocurrency by the Central Bank of Nigeria, this apex bank of Nigeria introduced its digital currency, the e-Naira, on October 25, 2021. This marks the first CBDC in Africa and the second globally. The e-Naira is a digital currency sanctioned by Nigerian law, intended for use as a digital version of the naira. Essentially, it serves as an electronic equivalent of the physical naira issued by the Central Bank of Nigeria, designed to offer a secure and efficient alternative method of payment. It is not meant to replace cash but to complement it, functioning as a government-issued digital currency with the same value as physical naira notes, and which is obtainable through financial institutions and transferred into users' e-wallets (Ree 2023, pp. 4-10). Apparently, according to Oladipupo and Amodu (2022, p. 113), although the ban on cryptocurrency played a significant role in introducing e-Naira, there is still no increase in the purchase and usage of e-Naira. This is because the ban generated a lot of controversies and anger among Nigerians, who see cryptocurrencies as a haven in a battered economy. And the e-Naira, unlike other cryptocurrencies like stablecoins, does not protect the users against the very high value loss of the Naira due to inflation.

In 2023, following a new political regime, the Central Bank of Nigeria reversed its position on crypto assets within the country and instructed banks to disregard its previous ban on crypto transactions. This directive was outlined in a circular dated December 22, 2023, bearing reference number FPR/DIR/PUB/CIR/002/003 and signed by the Director of the apex bank's Financial Policy and Regulation Department, Haruna Mustafa. Titled "Circular to all Banks and other Financial Institutions Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers (VASPs)". The circular highlighted the necessity for crypto regulation in response to global trends. The Central Bank emphasized that the need to regulate VASPs, including cryptocurrencies and crypto assets, has become apparent globally (CBN, 2023, pp. 0-5).

This shift in policy slightly aligns with international standards, such as the Financial Action Task Force's (FATF) 2019 update of Recommendation 15, requiring the regulation of VASPs to prevent misuse of virtual assets for money laundering, terrorism financing, and proliferation financing (GIABA, 2020, p. 1). Additionally, the Securities and Exchange Commission issued rules in May 2022 to provide a regulatory framework for the operations of VASPs in Nigeria (SEC Rules, 2022, p. 1). The new guideline supersedes previous directives from 2017 and 2021

while reiterating that banks and financial institutions are still prohibited from holding, trading, and/or transacting in virtual currencies on their account. The circular emphasized that immediate compliance with the new guideline is required (CBN, 2023, p. i). From the following, it is apparent that the regulatory policies of cryptocurrency in Nigeria have not been consistent and comprehensive, thus allowing for the noncompliance of crypto exchanges and users in Nigeria with the ethical use of the digital currency. This regulatory gap elucidates why Zaccheus Adedeji, Chairman of the Federal Inland Revenue Service (FIRS), asserted in a 2024 interview regarding a new executive bill on taxation sent to the parliament: "As we stand today, there is no law anywhere to actually regulate or monitor cryptocurrency."

7. Mitigating on-chain illicit financial flow and eradicating poverty

As previously highlighted, illicit financial flows (IFFs) using cryptocurrency contribute significantly to tax evasion and capital flight, both of which are major contributing factors to underdevelopment, stunted economic growth and poverty in Nigeria. The China-Nigeria case involving a Nigerian who laundered money from suspicious companies through cryptocurrency (Table 2, Case 5) buttresses this point. Also, worth mentioning is the ongoing lawsuit between the Federal Government of Nigeria (FGN) and Binance, where the FGN, through the FIRS, is suing the crypto giant for 81.5 billion in economic losses, back taxes, and complicity in helping customers to evade taxes through its platform[24]. While one can argue that on-chain IFFs may be generating wealth inflows into Nigeria through fraud-targeted foreign victims, it should be noted that such gains are economically unsustainable, distort formal markets, and ultimately damage Nigeria's financial reputation, as a result, outweighing any short-term benefits.

Addressing the challenge of illicit financial flows involving cryptocurrency in Nigeria requires a multi-faceted approach, combining legal frameworks, technological advancements, international and local collaboration, upholding AML/CFT regulatory laws, and public awareness.

7.1 Cooperation with fintech companies and leveraging technological solutions

Most transactions involving illicit funds go through fintech accounts rather than commercial banks, especially as the former possess an online advantage and less scrutiny. Collaboration and not just regulation between fintech companies like Flutterwave, Kuda, Opay, etc. and the Economic and Financial Crimes Commission (EFCC), could enhance regulatory oversight and enforcement of a clampdown regarding unregulated cryptocurrency transactions and fiat currency conversions. Such partnerships may facilitate more effective monitoring and intervention in illicit financial flows within the cryptocurrency ecosystem, thus, mitigating risks associated with the informal conversion of digital assets to the Nigerian naira. This cooperative approach could leverage the technological innovations of the fintech companies and the expertise of regulatory bodies to strengthen the implementation of anti-money laundering frameworks in the rapidly evolving landscape of digital finance.

7.2 Tackling the menace of corruption

Corruption undoubtedly serves as a primary catalyst for illicit financial flows (IFFs) in Nigeria. IFFs originate first from the ability to acquire wealth through illicit means, rather than merely facilitating the transfer of illicit funds. Therefore, addressing the root cause of IFFs- corruption is essential to reducing the prevalence of illicit financial flows, whether it be through cryptocurrency or other mediums. Addressing corruption in Nigeria would seem like a lifelong journey, it will involve, inter alia, the guarantee of the independence of the judiciary and enforcement agencies, the establishment of transparency and accountability within government institutions and the meting out of severe and unbiased penalties to offenders to deter others.

[24] The Guardian (2025) https://www.theguardian.com/technology/2025/feb/19/nigeria-binance-crypto-lawsuit

Additionally, promoting a culture of integrity and ethical behaviour devoid of self-interestedness is also essential. This can be achieved through formal and informal re-education, awareness campaigns, and the fostering of a strong civil society that monitors and exposes corruption

7.3 Poverty and unemployment

Poverty and unemployment continue to be significant drivers of crime, inclusive of cybercrime involving cryptocurrencies in Nigeria. As the biblical verse of Proverbs 16:17a[25] suggests, "Idle hands are the devil's workshop", individuals facing economic hardship with no meaningful economic engagements may resort to desperate measures to survive. This accounts for why a large percentage of Nigerian youths resort to cybercrimes like "yahoo-yahoo" to make ends meet. Poverty alleviation should be prioritized in the battle against cyber fraud in Nigeria. The governments of Nigeria should facilitate the provision of institutional and infrastructural development, such as a reliable power supply, adequate road networks, and a business-friendly regulatory environment such as access to bank accounts, soft loans, grants and skill acquisition, workshops to encourage SMEs, as it is impossible to adequately provide jobs for the ever teeming youthful population of the largest black nation on earth. The citizens can use the benefits of these provisions to generate income. This would, by extension, help to eliminate poverty, which is one of the primary reasons for crime involving blockchain technology.

7.4 Revisiting and implementing a comprehensive legal and monitoring framework

To ensure regulatory continuity and mitigate the challenges posed by IFFs through cryptocurrency, a comprehensive and detailed legal and monitoring framework is indispensable. The implicit ban on cryptocurrency and exchanges like Binance is not a viable solution. Instead, a licensing and regulatory approach similar to that applied to commercial banks should be adopted for exchanges. This would involve mandatory registration and verification with the Central Bank of Nigeria (CBN), implementation of know-your-customer (KYC) and anti-money laundering (AML) controls, and regular reviews and audits of on-chain transactions. By establishing such a framework and deploying a robust monitoring and enforcement team, the $26 billion transacted without tax through Binance could have been prevented.

Effective regulation necessitates a strong emphasis on monitoring, supervision, and enforcement. While many jurisdictions have begun to introduce regulatory frameworks, the implementation and enforcement of these frameworks through examinations and active supervision are still in their early stages. Strict monitoring of compliance with enacted cryptocurrency regulations by exchanges is crucial. Authorities should require crypto-asset issuers and service providers to establish frameworks for collecting, storing, safeguarding, and accurately reporting detected illicit transactions. This can be achieved through working with on-chain experts (See Table 4) and employing technological solutions, especially as funds of illegal origin are usually transacted using privacy coins and on-chain masking services. Ensuring that users also declare their source(s) of income upon registering for an account will help detect when the amounts received or sent do not match the stated source(s). Furthermore, authorities should have the legal authority to access necessary data during investigations, like full KYC documentation, account activity logs, and P2P chat records.

[25] Bible Gateway https://www.biblegateway.com/passage/?search=Proverbs%2016%3A27-29&version=TLB

Table 4: Leading Blockchain security and analytical firms
Source: Monovm (2025)[27]

Firms	Strengths	Methodologies
Chainalysis	- Largest coverage - Strong government contracts (FBI, IRS) - Reactor tool for deep tracing - Direct integration with agencies	- Address clustering - Heuristic tagging (darknet, scams) - Flow analysis
Elliptic	- Focus on compliance (banks, exchanges) - Strong FATF Travel Rule solutions - Works with regulators and the private sector	- Behavioural activities - Risk scoring (0 -100) - Entity mapping
BitRank	- Real-time risk scoring - Affordable for SMEs - Covers 200+ coins - Used by crypto businesses	- Machine learning models - Address reputation scoring - Taint analysis
CipherTrace (Mastercard)	- Strong FATF Travel Rule compliance - Used by traditional financial institutions - Monero tracing: Limited but pioneering - 100+ supported chains	- Attribution database - VASP discovery - Proprietary Monero tracking
Fireblocks	- Real-time alerts for hacks/exploits - Multi-party computation - 1,500 tokens and 45+ blockchains supported	- Transaction policy engine - API[26] based threat detection - Anomaly monitoring (sudden large withdrawals)

7.5 International cooperation, information sharing, and regulatory framework

Effective collaboration among the Central Bank of Nigeria (CBN), the Economic and Financial Crimes Commission (EFCC), anti-money laundering agencies within Nigeria, and international anti-money laundering organizations like the Financial Action Task Force (FATF) is essential for combating illicit financial flows (IFFs) facilitated by cryptocurrency. Sharing information and intelligence about suspicious on-chain transactions (usually exceeding daily limits, and transacted using privacy coins and covert services), money laundering techniques, and emerging threats can significantly contribute to addressing the challenges posed by the anonymity and decentralization of blockchain technology.

Furthermore, given the elusive nature of cryptocurrencies, actors may exploit regulatory arbitrage opportunities presented by Nigeria's inconsistent cryptocurrency laws. Therefore, it is essential to ensure adherence to established international standards, particularly those promulgated by the Financial Action Task Force (FATF) on AML/Counter-Terrorist Financing (CTF) and the Financial Stability Board (FSB). Compliances like mandatory VASPs registration, identifying users' accounts with transactions above daily limits (Travel Rule) are crucial for mitigating illicit financial flows facilitated through the blockchain to maintain economic stability. The implementation of robust regulatory measures aligned with global best practices is essential to address the unique challenges posed by cryptocurrency transactions in the context of Nigeria's financial ecosystem.

7.6 Strong political will

Everything thrives or fails on leadership. Political will remains the underlying factor to every other recommendation. The political leaders, ranging from the presidency and members of the

[26] Application Programming Interface (API) is a set of rules and protocols that allow different software applications to communicate with each other
[27] Monovm (2025) https://monovm.com/blog/blockchain-security-tools/

parliament, both at the state and federal levels in Nigeria, should be ingenious and pragmatic in their approaches to regulating cryptocurrency and ensuring factors (like the recommendations here) that make for a good virtual financial ecosystem. This will not only reduce crime such as tax evasion, trade mispricing, terrorism financing and money laundering associated with cryptocurrency, but will also allow for a full realization of the benefits of the ecosystem in the nation.

8. Conclusion

This study aimed to identify the factors driving the use of cryptocurrency for illicit financial flows, its impact and workable solutions in Nigeria. By employing several extant literature, reports and Davis' Technology Acceptance Model (TAM) for empirical analysis, it revealed the inherent factors facilitating the use of cryptocurrency for illicit financial flows in Nigeria. The decentralized nature of blockchain and the anonymity orchestrated by mixers, tumblers, and private cryptocurrencies (privacy coins) are identified as primary enabling factors. These intricate aspects of the blockchain provide individuals and networks engaged in illicit activities such as tax evasion, trade mispricing and invoicing, cyber fraud, and terrorism financing with covert advantages for their illegal transactions. The recent trends of on-chain IFFs (Table 2) substantiate cryptocurrency's opportunity for such activities. While there are no concrete details on the sources of the illicit funds being linked to terrorism financing, trade mispricing and misinvoicing, the submission here is that illegal funds for/from such activities can be transacted through the blockchain, given the established possibility. These advantages, looking through the prism of the Technological Acceptance Model of this research, are categorized as "perceived usefulness"—connoting the technological benefits of cryptocurrencies—that drive its adoption and use for Illicit financial flow in Nigeria.

Furthermore, this study analyses the ease of cross-border transactions between the blockchain and commercial banks in Nigeria, postulating a costless, swifter, and more reliable channel for cross-border transactions using the blockchain as opposed to banks in Nigeria. A key informant interview with a staff member of an indigenous bank in Nigeria empirically demonstrates the comparatively higher costs and delays associated with initiating international transactions using Nigerian banks. The research findings highlight the limitations within commercial banks in Nigeria, where access to customer funds and the initiation of international transfers are constrained. Customers are unable to initiate foreign transfers even while using the mobile applications of these banks, especially as the Foreign Currency (FCY) form Q or A at the bank remains the sole viable means for international transfers. While these challenges align with the profit motives and regulatory compliance measures of commercial banks, the study shows they inadvertently lead criminal entities to seek alternative channels with greater ‘‘ease of use’’ such as the blockchain and its concomitant cryptocurrencies like Bitcoin (BTC), Ethereum (ETH), and Tether (USDT).

Additionally, based on the assembled academic literature, it is a given in this research that the legal framework regulating the use of cryptocurrency in Nigeria is ill-conceived thus, demonstrating a lack of comprehensiveness on cryptocurrency and the blockchain. In an attempt to address the challenges of decentralization and anonymity posed by cryptocurrency, the implicit ban on cryptocurrency in 2021 led to the launch of the Central Bank Digital Currency (CBDC). However, the first African CBDC, e-Naira, fell short of achieving this objective, as many Nigerians, particularly the youth, continue to rely on cryptocurrency for their covert and overt transactions (Oladipupo and Amodu, 2022, p. 113). More tenuous is that a reversal of the policy surrounding the ban on cryptocurrency was enacted in December 2023 following the emergence of a new political administration. Which was a showcase of the ill-conceived policy. The empirical deduction here remains steadfast: the fragile regulatory framework continues to pave the way for the ongoing illicit financial flows involving

cryptocurrency in Nigeria. While the study highlights the correlation between on-chain illicit financial flows and their detrimental impact on development and poverty eradication in Nigeria, it is important to acknowledge that cryptocurrencies and the blockchain are deemed amoral—capable of being used for positive or negative purposes—as highlighted in this study (reviewed literature) by Schär (2021, p. 153-134). Despite challenges such as money laundering and investment scams leading to substantial revenue losses or IFF in Nigeria, cryptocurrency and its morphing ecosystem can pave the way for financial inclusivity and prosperity in the country. According to this, it behooves the leadership of Nigeria to recognize this potential and not discard the benefits because of its drawbacks (decentralization and anonymity).

References

ANEEJ. (2018). *Impact of Illicit Financial Flow in Nigeria*. Africa Network for Environment and Economic Justice. https://www.aneej.org/wp-content/uploads/2021/08/IFFs-Research-Report_OSB-Final.pdf

Balaskas, A., & Franqueira, V. N. L. (2018). Analytical Tools for Blockchain: Review, Taxonomy and Open Challenges. *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, 1–8. https://doi.org/10.1109/CyberSecPODS.2018.8560672

Bancroft, A. (2020). Secrecy and Anonymity Online. In A. Bancroft (Ed.), *The Darknet and Smarter Crime. Palgrave Studies in Cybercrime and Cybersecurity* (pp. 175-196). Palgrave Macmillan. https://doi.org/10.1007/978-3-030-26512-0_10

Bear, K., Ruud, D.M., Shafik, H. & Micheal, K. (2023). *Taxing Cryptocurrencies* (IMF Working Paper 144). International Monetary Fund. https://doi.org/10.5089/9798400246586.001

Central Bank of Nigeria. (2023). *Circular to all Banks and other Financial Institutions. Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers VASPSA* (FPRIDIRIPUBICIRIOO2IOO3). Financial Policy & Regulation Department. https://www.cbn.gov.ng/out/2024/fprd/guidelines%20on%20operations%20of%20bank%20accounts%20for%20virtual%20asset%20providers.pdf

Chainalysis. (2023). *Geography of Cryptocurrency Report.* The 2023 Global Crypto Adoption Index. 2023, 1-95. https://go.chainalysis.com/geography-of-cryptocurrency-2023.html

Chainalysis. (2024). *The Latest Trends In Ransomware, Scams, Hacking, and more*. The 2024 Global Crypto Crime Report. Chainalysis. 1-112. https://go.chainalysis.com/crypto-crime-2024.html

Chen, Y., & Bellavitis, C. (2019). Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models Scholarly Paper. *Journal of Business Venturing Insights, Forthcoming, Stevens Institute of Technology School of Business Research Paper.* (SSRN 3483608). 1-22 https://doi.org/10.2139/ssrn.3483608

Chen, Y., Pereira, Igor, & Patel, Pankaj C. (2020). Platform Governance: A Mechanism Design Perspective. *Forthcoming, Stevens Institute of Technology School of Business Research Paper,* 1-58. https://ssrn.com/abstract=3553382

Chitimira, H., & Animashaun, O. (2023). The Adequacy of the Legal Framework for Combating Money Laundering and Terrorist Financing in Nigeria. *Journal of Money Laundering Control*, *26*(7), 110–126. https://doi.org/10.1108/JMLC-12-2022-0171

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *Management Information Systems Quarterly*, 13(3), 319-340. https://doi.org/10.2307/249008

Financial Services Agency. (2022). Anti-Money Laundering, Counter Financing of Terrorism, and Counter-Proliferation Financing. Current Status and Challenges. *Mutual Evaluation Report of Japan by the Financial Action Task Force (FATF), and FSA's initiatives,* FSA, 1-117. https://www.fsa.go.jp/en/news/2022/20221007/20221007.pdf

Folkinshteyn, D., & Lennon, M. (2016). Braving Bitcoin: A Technology Acceptance Model (TAM) Analysis. *Journal of Information Technology Case and Application Research*, *18*(4), 220–249. https://doi.org/10.1080/15228053.2016.1275242

Fuje, H., Quayyum, S., & Molosiwa, T. M. (2022). *Digital Currency Innovations in Sub-Saharan Africa* (The IMF Regional Economic Outlook Analytical Note). International Monetary Fund. 1-5 https://www.scribd.com/document/841837815/Digital-Currency-Note

GIABA. (2020). Virtual Assets and Virtual Assets Service Providers (VASPs) – AML/CFT Implications for GIABA Member States. *Policy Advisory,* 1-8 Legal Framework. Virtual Policy by FATF.pdf

Gopi, C., Kumar, S., Basha, S., Bandi, R., & Reshma, P. (2024). Cryptographic Innovations for Securing Transactions in Privacy Preserving Cryptocurrencies. *Journal Emerging Technologies and Innovative Research* 11(1), 520 -526. doi:10.1729/37563 https://doi.org/10.1729/Journal.37563

Greenfield, R. (2020). The State of Cryptocurrency Regulation: Nigeria. *Social Science Research Network*, 1-9 https://ssrn.com/abstract=4531980

Griffin, C. (2025). Gold, Bitcoin, and Central Banks in the 21st Century: The New Dynamic. *International Journal of Finance*, 10(2), 29–41. https://doi.org/10.47941/ijf.2569

Grover, P., Kar, A. K., Janssen, M., & Ilavarasan, P. V. (2019). Perceived Usefulness, Ease of use and User Acceptance of Blockchain Technology for Digital Transactions – Insights from User-generated Content on Twitter. *Enterprise Information Systems*, 13(6), 771–800. https://doi.org/10.1080/17517575.2019.1599446

Harvey, J., & Branco-Illodo, I. (2019). Why Cryptocurrencies Want Privacy: A Review of Political Motivations and Branding Expressed in 'Privacy Coin' Whitepapers. *Journal of Political Marketing*, 19. 1-29. https://doi.org/10.1080/15377857.2019.1652223

Houben, D. R., & Snyers, A. (2018). Cryptocurrencies and blockchain: Legal Context and Implications for Financial Crime, Money Laundering and Tax Evasion. *Document of the European Parliament*, 1-86. https://www.europarl.europa.eu/cmsdata/150761/TAX3%20Study%20on%20cryptocurrencies%20and%20blockchain.pdf

International Monetary Fund. (2021). *Regional Economic Outlook, October 2021, Sub-Saharan Africa* (LCC HC800.R445 2021). International Monetary Fund e-Library, 1-39 https://doi.org/10.5089/9781513591933.086

Jejelola, F. (2021). The Effect of Cryptocurrency on Transnational Crime in Nigeria: The Need for a Legal Framework to Regulate Digital Currency. *ResearchGate*, 1-51. doi:10.13140/RG.2.2.21737.16487

Jokić, S., Cvetković, A. S., Adamović, S., Ristić, N., & Spalević, P. (2019). Comparative Analysis of Cryptocurrency and Traditional Wallets. *Економика Journal* (Vol. 65). 65-75 https://doi.org/10.5937/ekonomika1903065J

Joseph, O. D. (2019). Illicit Financial Flows and Economic Development in Nigeria. *Journal of Public Administration*, *1*(2), 6–12. https://doi.org/10.22259/2642-8318.0102002

Kama, U. (2005). *The Economic Effects of Money Laundering on the Nigerian Economy: Some Emerging Issues.* (The Centrak Bank of Nigeria Economic and Financial Review). The Central Bank of Nigeria, *43*(1). 23-50. https://dc.cbn.gov.ng/efr/vol43/iss1/2

Kim, S., Miksjuk, A., Suryakumar, N., Tuladhar, A., Velculescu, D., Wu, Y., Zuniga, J., & Hallmark, N. (2024). *Digital Money, Cross-Border Payments, International Reserves, and the Global Financial Safety Net: Preliminary Considerations*. International Monetary Fund (Note/2024/001), 1-22. https://doi.org/10.5089/9798400253478.068

Micah, M., Okpe, U., & Abu, S. (2022). Forensic Accounting Investigation Techniques and Financial Crimes Reduction in Nigerian Public Sector: A Case Study of Anti-Graft Agencies (EFCC, ICPC and CCB) in Nigeria. *Archives of Business Research*, 10(8), 186–206. https://journals.scholarpublishing.org/index.php/ABR/article/view/12660

Moslavac, B. (2019). Cryptocurrency tumbler: Legality, Legalization, Criminalization. *Revista Acadêmica Escola Superior Do Ministério Público Do Ceará*, 11(2), 205–226. https://doi.org/10.54275/raesmpce.v11i2.97

Mueller, B., & Urbach, N. (2017). Understanding the Why, What, and How of Theories in IS Research. *Communications of the Association for Information Systems*, 41, 349–388. https://doi.org/10.17705/1CAIS.04117

Ngwakwe, C. (2015). Trade Misinvoicing, External Debt and Sustainable Development: A Nigerian Example. *Risk Governance and Control: Financial Markets and Institutions*, 5(2-1), 120–134. https://doi.org/10.22495/rgcv5i2c1art6

Nigerian Financial Intelligence Unit. (2023). *Money Laundering Typologies Through Fraud in Nigeria*. NFIU Report 2023 Print. 1- 88. Money Laundering Typologies through Frauds in Nigeria.pdf

Nuryyev, G., Wang, Y.-P., Achyldurdyyeva, J., Jaw, B.-S., Yeh, Y.-S., Lin, H.-T., & Wu, L.-F. (2020). Blockchain Technology Adoption Behavior and Sustainability of the Business in Tourism and Hospitality SMEs: An Empirical Study. *Sustainable Business and Development*, *12*(3), 1256. 1-21. https://doi.org/10.3390/su12031256

Ogege, P. (2024). Emerging Issues in Cryptocurrency Regulation in Nigeria. *Research Gate ,* 1-21, https://www.researchgate.net/publication/381111805_emerging_issues_in_cryptocurrency_regulation_in_nigeria

Ogunode, O. A., Iwala, A. T., Awoniyi, O. A., Amusa, B. O., Omosebi, T. R., Kassim, S. K., & Akintoye, R. I. (2022). Cryptocurrency and Global Practices: Lessons for Nigeria. *South Asian Journal of Social Studies and Economics,* 15 (1), 7–28. https://doi.org/10.9734/sajsse/2022/v15i130396

Okojie, C. (2018). *Illicit Transfers and Tax Reforms In Nigeria: Mapping of the Literature and Synthesis of the Evidence*. Partnership for African Social and Governance Research,1-37. https://www.pasgr.org/wp-content/uploads/2018/09/Nigeria-Illicit-Financial-Flows-Report.pdf

Oladipupo, A. O., & Amodu, A. A. (2022). Impact of Cryptocurrency Ban on the Development of Digital Currency in Nigeria. *Renaissance University Journal of Management and Social Sciences,* 8(2), 113-125. https://www.researchgate.net/publication/383703292_Impact_of_Cryptocurrency_Ban_on_the_Development_of_Digital_Currency_in_Nigeria

Olorundare, J., Fagboyo, R., Onyijen, O., Oni, M., & Adebunmi, A. (2023). Economic Prospect of Cryptocurrency: Nigeria as a Case Study. *International Journal of Research Publication and Reviews*, *4(3)*. pp 4444-4450. https://doi.org/10.55248/gengpi.2023.4.33777

Oni, S., & Oyedokun, G. (2023). Adopting Cryptocurrency in Nigeria: Tax, Legal and Financial Implications. Journal of Taxation and Fiscal Policy, 2(1),75-87. https://zenodo.org/records/17155126/files/JTFP%202%20Issue%201%20and%202%202025v2_84-end.pdf?download=1

Oyeyemi, O., Kess-Momoh, A., Omotoye, G., Bello, B., Tula, S., & Daraojimba, A. (2024). Entrepreneurship in the digital age: A comprehensive review of start-up success factors and technological impact. *International Journal of Science and Research Archive*, 11(1), 182–191. https://doi.org/10.30574/ijsra.2024.11.1.0030

Padalkar, N. R. (2023). Unveiling the Digital Shadows: Exploring the Role of Technology in Illicit Financial Flows. In *Measuring Money in the Digital Age. 11th IMF Statistical Forum*. 1- 17. https://www.imf.org/-/media/files/news/seminars/2023/11th-stats-forum/session-iii-nakul-r-padalkar.pdf

Ree, J. (2023). *Nigeria's eNaira, One Year After.* International Monetary Fund Working Papers (2023/104*),* 1- 46. https://doi.org/10.5089/9798400241642.001

Ruth, M., & Ismail, A. (2024, June 11). Nigeria Confronts Its Worst Economic Crisis in a Generation. *The New York Times* https://www.nytimes.com/2024/06/11/world/africa/nigeria-economy-strike.html

Sanusi, D. J. O. (2003, June 3). *Joseph O Sanusi: Central Bank of Nigeria's Standpoint of Anti-money Laundering Compliance.* [Conference Presentation]. ECOWAS Anti-Money Laundering Convention*,* Lagos, Nigeria. https://www.bis.org/review/r030606c.pdf

Schär, F. (2021). Decentralized Finance: On Blockchain- and Smart Contract-Based Financial Markets. *Economic Research Journal 103(2*). pp. 153-174. https://doi.org/10.20955/r.103.153-74

Securities and Exchange Commission, Nigeria. (2022). New Rules on Issuance, Offering Platforms and Custody of Digital Assets. *SEC Circular*, 1-54. https://sec.gov.ng/documents/8/Rules-on-Issuance-Offering-and-Custody-of-Digital-Assets.pdf

Scharnowski, S. (2024). Dark Web Traffic, Privacy Coins, and Cryptocurrency Trading Activity. *Finance Research Letters*, 67 Part B, 1-7. https://doi.org/10.1016/j.frl.2024.105875

Shahzad, M. F., Xu, S., Lim, W. M., Hasnain, M. F., & Nusrat, S. (2024). Cryptocurrency Awareness, Acceptance, and Adoption: The Role of Trust as a Cornerstone. *Humanities and Social Sciences Communications*, *11*(1), 4. 1-15. https://doi.org/10.1057/s41599-023-02528-7

UNCTAD. (2020). *Tackling illicit financial flows for sustainable development in Africa*. United Nations Conference on Trade and Economic Development of Africa Report 2020. 1-223. https://unctad.org/system/files/official-document/aldcafrica2020_en.pdf

UNCTAD. (2023). *Crypto Assets and Central Bank Digital Currencies: Potential Implications for Developing Countries*. Nations Conference on Trade and Economic Development ILibrary Publication. 1-52. https://doi.org/10.18356/9789210026178

Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized Finance. *Journal of Financial Regulation*, *6*(2), 172–203. https://doi.org/10.1093/jfr/fjaa010

World Bank Group. (2024). Nigeria by the Numbers, Overview and the latest. https://www.worldbank.org/en/country/nigeria/overview#1

Appendix

Appendix 1: **INTERVIEW QUESTIONS AND ANSWERS**

1. What is your name?
   Eze Obiajulu Collins
2. Where do you work and what is your job position?
   United Bank for Africa, Relationship Officer.
3. How can one make an international transfer at UBA?
   It can be done through FCY, i.e the customer is sourcing for their dollars, or through Government Provision of the FCY i.e Form Q or Form A.
4. How many days does an international transfer take to reach the receiver?
   Within 24 to 48 hrs.
5. How much is an international transfer charge and at what percentage?
   There is a $50 flat charge. Plus 0.05% of the amount plus 0.075% VAT charges.
6. What is the highest international transferable amount in a day or month at the UBA?
   $10,000.00
7. Can one initiate an international transfer from the UBA mobile application?
   No, you would have to come over to the bank to initiate an international transfer.
8. How much is the transfer charge for a $10,000 foreign transfer at the UBA?
   $103.75
9. Where can I get the breakdown of these charges?
   It is system-generated.
10. Okay, can I get a copy of this?
    No
11. What amount of international transfer flags one up for money laundering? $10,000.00
12. Is there a charge at the receiver's foreign bank after a successful transfer?
    Yes, it is called offshore charges.
13. Do you know about the blockchain and its international transfers?
    No, I don't.
14. If yes, do you think international transfers on the blockchain are cheaper than those of the UBA? I have no idea.

Okay, thank you.

10/08/2024
Signature and date
Eze Obiajulu Collins

10/08/2024
Signature and date
Author