1ALVAN JOURNAL OF SOCIAL SCIENCES (AJSS)
FACULTY OF SOCIAL AND MANAGEMENT SCIENCES
ALVAN IKOKU FEDERAL UNIVERSITY OF EDUCATION, OWERRI

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

RESEARCH ARTICLE

CRYPTO CURRENCY: A RENEWABLE ENERGY FOR FINANCING TERRORISM AND ARMED CONFLICT IN THE SAHEL AFRICA

SUNNY NNABUIHE NWACHUKWU, AMBROSE OLUCHUKWU ABANEME

Department of Political Science Alvan Ikoku Federal University of Education,
Owerri, Imo State.

ABSTRACT

This paper investigates the alarming trend of cryptocurrency usage in financing terrorism and armed conflict within the Sahel region of Africa. While the lack of publicly available data presents a significant challenge to comprehensive analysis, existing evidence suggests that terrorist organizations are increasingly exploiting the decentralized and pseudonymous nature of crypto currencies to circumvent traditional financial regulations and raise funds. This paper examines the various methods employed by terrorist groups to utilize crypto currencies, analyzing the challenges in tracking and mitigating this activity. Furthermore, the paper proposes potential strategies to combat the use of crypto currencies in fueling instability in the Sahel region, highlighting the need for international cooperation, enhanced regulatory frameworks and innovative technological solutions. The paper concludes by emphasizing the urgent need for a multi-faceted approach to address this emerging threat and prevent the further destabilization of the Sahel through crypto-currency enabled financing of terrorism

Keywords: Currency, renewable energy, finance, armed conflict, terrorism.

Corresponding Author

Sunny Nnabuihe Nwachukwu

E-mail Address: sunnynwachukwunna@gmail.com , Telephone: +2348060626448

Received: 15/12/2024; **Accepted:** 20:01/2025; **Published:** 15/03/2025

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

1. INTRODUCTION

The Sahel region of Africa, spanning across the vast land south of the Sahara Desert, is a complex and fragile region grappling with a multitude of challenges. Persistent poverty, climate change and political instability have created fertile ground for the proliferation of terrorist groups and armed conflict. These conflicts, fueled by a desire for political power, control of resources and ideological agendas, have devastating consequences for the region's population, displacing millions and hindering development (Christano and Prenio, 2020). Traditional methods of financing these activities, such as drug trafficking, arms smuggling, extortion and kidnapping for ransom, have long been prevalent in the Sahel. However, the emergence of crypto-currencies, particularly Bitcoin, has introduced a new and increasingly significant dimension to the financing of terrorism and armed conflict (Marriam and Kotler, 2020). This shift towards crypto-currency financing presents a unique set of challenges for law enforcement and international efforts to combat terrorism and promote peace and security in the Sahel (Tompihe, 2003). Crypto-currencies with their decentralized nature, pseudonymous transactions and relative anonymity, offer a level of financial opacity that is difficult to penetrate using traditional methods of financial tracking and regulation (Akartuna, et al, 2022).

This paper delves into the ways in which crypto-currencies, particularly Bitcoin, are being utilized to finance illicit activities in the Sahel. It examines the methods employed by terrorist organizations to leverage these digital assets, analyzes the challenges in tracking and mitigating this activity and explores the implications for regional stability. Furthermore, the paper will propose potential strategies to combat the use of crypto-currencies in fueling instability in the Sahel region, highlighting the need for international cooperation, enhanced regulatory framework, and innovative technological solutions. Ultimately this paper emphasizes the urgent need and approach to address this emerging threat and prevent the further destabilization of the Sahel through crypto-currency enabled financing of crimes.

2.0. CONCEPTUAL CLARIFICATIONS AND THEORITICAL FRAMEWORK

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

2.1. Conceptual Clarifications;

Cryptocurrency: A Revolution in Digital Money

Crypto-currency is a digital form of money that uses cryptography for security and operates independently of central banks or governments (Akartuna, et al., 2022). Unlike traditional currencies, crypto-currencies are decentralized, meaning they are not controlled by a single entity, instead, they rely on a distributed ledger technology called block chain to record transactions and maintain a secure and transparent system (Marron, 2008).

The key Features of Cryptocurrency are:

- **Decentralization:** Crypto-currencies are not issued or controlled by any central authority like governments or banks. This means that they are not subject to the same regulations and risks associated with traditional fiat currencies (Wang, 2021). This decentralized nature makes them attractive to these seeking to operate outside traditional financial systems and avoid government oversight.
- **Blockchain Technology:** Crypto-currencies utilize blockchain technology, a distributed ledger system that records all transactions in a secure and transparent manner. This ledger is shared across a network of computers, making it extremely difficult to tamper with or alter (Weinberg, 2008). Each transaction is added to a black, which is then linked to the previous block, creating a chain of information that is constantly growing and publicly verifiable.
- **Pseudonymity:** While not entirely anonymous, cryptocurrency transactions are often pseudonymous, meaning they are conducted under aliases or unique digital identities (Pasztor, 2024). This can make it challenging to trace the origin of funds and identify the individuals or entities involved. However, it's important to note that transactions can be linked back to specific wallents and with sufficient investigation, identities can often be revealed (Kettle and Mumford, 2017).
- **Encryption:** Cryptocurrencies utilize advanced cryptography to secure transactions and protect user information. This encryption makes it extremely

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

difficult for unauthorized individuals to intercept or alter data, ensuring the integrity security of the system.

2.2. Theoretical Framework: Greed and Grievance: The greed and grievance theory was popularized by Paul Collier and Anke Hoefler. Their model suggests that both greed and grievance contribute to conflict, and that these factors can interact in a feedback loop. The greed and grievance theory is a model that explains civil war as a result of both economic and social factors. Collier and Hoeffler's model suggests that what actually happens is that opportunities for predation (controlling primary commodity exports) cause conflict and the grievances this generates induce diasporas to finance further conflict. The point of policy intervention here is to reduce the absolute and relative attraction of primary commodity predation and to reduce the ability of diasporas to fund rebel movement.

Collier and Hoffler compared two contrasting motivations for rebellion: Greed and grievance. Most rebellions are ostensibly in pursuit of a cause, supported by a narrative of grievance. But since grievance assuagement through rebellion is a public good that a government will not supply, economists predict such rebellions would be rare. Empirically, many rebellions appear to be linked to the capture of resources (such as diamonds in Angola and Sierra Leone, drugs in Colombia, and timber in Cambodia). Collier and Hoffler set up a simple rational choice model of greed-rebellion and contrast its predictions with those of simple grievance model.

Greed is the idea that people rebel to improve their economic situations which includes factors like access to natural resources, government defense spending, and recruitment costs. While grievance is the idea that people rebel over social and political issues which includes factors like inequality, discrimination, and authoritarianism.

Policy implications of the theory include; the ability of rebel groups to finance themselves, reducing the attraction of primary commodity predation, increasing the costs of war through education programs and reducing dominance by one ethnic group in areas with ethnic diversity.

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

3.0. METHODOLOGY

Historical design was adopted in the study. The study anchored on documentary method of data collection which relied majorly on secondary sources of data such as collection of periodicals, books, survey data and internet materials. Previous reports of the cryptocurrency and financing terrorism were examined and designate crises where cryptocurrency were used to finance crises and terrorism were x-rayed**.** Greed and grievance theory was adopted as the theoretical framework of analysis. Qualitative content analysis was employed in the discourses and conclusion drawn through inferences

4. 0 DISCOURSES

4.1. The Evolving Trend of Cryptocurrency Financing of Crimes in the Sahel Region: 2010-2023

The Sahel region of Africa has experienced a concerning rise in cryptocurrency financing for criminal activities. While the precise extent and scope of this phenomenon remain difficult to quantify due to the decentralized nature of cryptocurrencies and limited publicly available data, the trend has become alarmingly apparent and concerning since the early 2010s.

Early Signs and Emerging Concerns (2010-2015)

- **Bitcoin's Emergence:** Bitcoin, the first and most prominent cryptocurrency, was introduced in 2009. Its decentralized nature, potential for anonymity and resistance to traditional financial regulations attracted early adopters seeking to operate outside traditional banking systems (Pasztor, 2024).
- **Initial Use Cases:** Early use cases of cryptocurrencies in the Sahel region primarily focused on remittances, particularly for sending funds between diaspora communities and families in the region (Pasztor, 2024). However, the potential for illicit financial activities started to emerge as criminal networks recognized the benefits of this emerging technology.

Growth and Diversification (2016-2020)

ALVAN JOURNAL OF SOCIAL SCIENCES (AJSS)
FACULTY OF SOCIAL AND MANAGEMENT SCIENCES
ALVAN IKOKU FEDERAL UNIVERSITY OF EDUCATION, OWERRI
https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

- **Increased Accessibility:** The growth of cryptocurrency exchanges and the rise of mobile wallets made accessing and using cryptocurrencies more accessible, facilitating adopting by a wider range of individuals and groups (Akartuna, et al, 2022).
- **Sophistication of Criminal Networks:** Criminal networks, including terrorist organizations, became increasingly sophisticated in their use of cryptocurrencies, employing money laundering schemes, leveraging decentralized exchanges and utilizing dark web platforms to move funds and evade detection (Akartuna, et al, 2022).
- **Ransomware Attacks:** The use of ransomware attacks, where victims pay a ransom in cryptocurrency to regain access to their data, became more prevalent, particularly in the Sahel region where digital infrastructure is vulnerable (Akartuna, et al., 2022).

Escalating Concerns and Targeting Action (2021-2023)

- **Increased Evidence:** Reports of cryptocurrency financing for terrorist activities in the Sahel, particularly by groups such as Boko Haram, Al-Qaeda in the Islamic Maghreb (AQIM) and the Islamic State in the Greater Sahara (ISGS), began to surface with increasing frequency (Pasztor, 2024).
- **Regulatory Efforts:** Governments and international organizations started focusing on regulating cryptocurrencies to combat illicit activities (Pasztor, 2024).
- **Counter**-Terrorism Initiatives: International counter-terrorism efforts began focusing on disrupting cryptocurrency-enabled financing networks through intelligence sharing, asset seizures and targeted sanctions (Pasztor, 2024).

4.2. Challenges in Tracking and Mitigation

Tracking and mitigating the use of cryptocurrencies in terrorism financing presents a formidable set of challenges:

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

- **Lack of Transparency:** The pseudonymous nature of cryptocurrency transactions often conducted under aliases or using complex cryptographic techniques, makes it incredibly difficult to trace the flow of funds and identify the individuals and organizations involved. This lack of transparency allows terrorist organizations to move funds with relative anonymity, hindering the ability of authorities to track their activities and disrupt their financial networks (Moghadam, 2013).
- **Technology Complexity:** Monitoring cryptocurrency transactions requires specialized expertise and advanced technology, which may not be readily available to all law enforcement agencies. Understanding the intricate workings of blockchain technology analyzing complex transaction patterns, and deciphering cryptographic protocols are essential for effective tracking and mitigation (Moghadam, 2013). The rapid evolution of cryptocurrencies and the emergence of new technologies further exacerbate this challenge, demanding continuous investment in training and technological infrastructure.
- **International Cooperation:** Effective countermeasures against cryptocurrency-enabled terrorism financing require robust international cooperation, involving the sharing of intelligence, coordination of efforts, and the development of joint strategies across borders. Terrorist organizations often operate across national boundaries, requiring a collective effort to track their financial networks and disrupt their activities (Wang, 2021).
- **Regulatory Gaps:** The rapidly evolving nature of cryptocurrencies often outpaces the development of effective regulatory frameworks. The decentralized and borderless nature of these digital assets challenges traditional regulatory approaches, requiring international collaboration a dynamic approach to crafting effective regulations (Tompihe, 2003).
- **Lack of Public Data:** The lack of publicly available data related to cryptocurrency transactions further hampers tracking efforts. While some cryptocurrency exchanges and wallets provide limited data, the decentralized nature of the technology often limits access to comprehensive transaction information (Cristano and Prenio, 2020).

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

4.3. Methods of Cryptocurrency use in the Sahel

Terrorist organizations in the Sahel region are leveraging the unique characteristics of cryptocurrencies to engage in a variety of fundraising activities, evolving their financial strategies beyond traditional methods. The following are some key methods employed:

1. **Crowdfunding and Online Donations:** Similar to legitimate crowdfunding platforms, terrorist groups are increasingly utilizing online channels to solicit donations from supporters. They often leverage encrypted messaging apps, social media platforms, and dark web forums to reach potential donors, promoting their ideology and soliciting contributions in cryptocurrencies (Marron, 2005). These platforms provide a degree of anonymity and accessibility, making it easier for individuals to donate without fear of detection (Kettle and Mumford, 2017).
2. **Exchange of Goods and Services:** Cryptocurrencies can be used to launder illicit funds obtained through other criminal activities such as drug trafficking, human trafficking and extortion. The decentralized and pseudonymous nature of cryptocurrencies makes it more difficult to trace the origin of the money, allowing terrorist groups to obfuscate the trait of funds and make it challenging to seize assets (Wang, 2021).
3. **Ransom Payments:** Cryptocurrencies are increasingly used as a payment method for ransom demands, particularly in cases of kidnapping. The anonymity and speed of cryptocurrency transactions make it easier for perpetrators to collect payments and avoid detection by law enforcement (Wang, 2021).
4. **Recruitment and Training:** Cryptocurrencies can facilitate payments for recruitment and training activities, allowing terrorist groups to compensate individuals for joining their ranks or for participating in training programs. This anonymity reduces the risk of detection and makes it easier for individuals to engage in these activities without fear of reprisal (Pasztor, 2024).
5. **Purchasing Supplies and Equipment:** Cryptocurrencies can be used to purchase supplies and equipment, including weapons, ammunition, vehicles and communication devices for terrorist activities. The decentralized nature of

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

cryptocurrencies allows for transactions to occur outside traditional financial systems, making it difficult for authorities to monitor and disrupt these purchases (Pasztor, 2024).

4.4. Potential Strategies and Solutions

Combating the use of cryptocurrencies in terrorism financing demands a multi-faceted and collaborative approach, encompassing enhanced regulatory frameworks, strengthened international cooperation, technological advancements and public awareness initiatives.

- **Enhanced Regulatory Frameworks:** Developing robust regulatory frameworks that specifically address the challenges posed by cryptocurrencies is crucial to mitigating the risks of terrorism financing. This involves:
    1. **Know Your Customer (KYC) and Anti-Money Laundering (AML) Measures:** Implementing stringent KYC and AML measures for cryptocurrency exchanges and platforms is essential to verifying the identifies of users and tracking the flow of funds (Akartuna, et al, 2022). This requires close collaboration between governments and cryptocurrency businesses to develop and enforce effective regulatory standards.
    2. **Transparency Requirements:** Requiring cryptocurrency exchanges and platforms to provide greater transparency in their operations, including transaction data and user information, can aid in tracking suspicious activities and tracing funds.
    3. **Licensing and Oversight: Establishing licensing requirements for** cryptocurrency business and implementing robust oversight mechanisms can help ensure compliance with regulatory standards and prevent the misuse of cryptocurrencies for illicit activities.
- **International Cooperation:** Strengthening international cooperation is essential to effectively combat cryptocurrency enable terrorism financing. This involves:
    1. **Information Sharing:** Establishing robust mechanisms for sharing intelligence and data between law enforcement agencies and financial

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

authorities across borders is crucial to tracking cryptocurrency transactions, identifying suspicious patterns and disrupting terrorist financing networks (Pasztor, 2024).

2. **Joint Operations:** Collaborative investigations and joint operations between law enforcement agencies in different countries can help dismantle cryptocurrency-based terrorist financing networks and bring perpetrators to justice.
3. **Harmonized Regulations:** Developing harmonizing regulatory frameworks for cryptocurrencies across international jurisdictions can help create a more consistent and effective approach to combating terrorism financing.

- **Technology Advancements:** Investing in advanced technologies and expertise is crucial to enhance the ability to track cryptocurrency transactions and identify suspicious activities. This includes:
    1. **Blockchain Analytics Tools:** Developing and utilizing sophisticated blockchain analytics tools that can analyze transaction data, identify patterns, and trace funds can significantly improve the effectiveness of counter terrorism efforts (Akartuna, et al, 2022).
    2. **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML can be used to analyze large data sets of cryptocurrency transactions, identify anomalies and predict potential threats (Pasztor, 2024).
    3. **Cybersecurity Measures:** Strengthening cybersecurity measures and investing in research and development of technologies to combat cybercrime and prevent the misuse of cryptocurrencies are crucial (Pasztor, 2024).
- **Public Awareness Campaigns:** Educating the public about the risks associated with cryptocurrency-based scams and the importance of reporting suspicious contributing to terrorist financing (Wang, 2021).
- **Collaboration with Cryptocurrency Exchanges**: Working closely with cryptocurrency exchanges to identify and flag suspicious transactions can help disrupt the flow of funds to terrorist organizations. This requires building trust and

ALVAN JOURNAL OF SOCIAL SCIENCES (AJSS)
FACULTY OF SOCIAL AND MANAGEMENT SCIENCES
ALVAN IKOKU FEDERAL UNIVERSITY OF EDUCATION, OWERRI

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 E-ISSN: 3043-5463

open communication channels between regulatory authorities and the cryptocurrency industry (Wang, 2021).

5.0. CONCLUSION

The use of cryptocurrencies like Bitcoin poses a significant threat to regional stability in the Sahel. The decentralized and pseudonymous nature of these digital currencies allows terrorist organizations to circumvent traditional financial systems and raise funds with relative ease. Addressing this challenge requires a concerted global effort involving enhanced regulation, international cooperation, technological advancements and public awareness campaigns. Failure to effectively combat this emerging threat could have severe consequences for peace and security in the Sahel and beyond.

Competing Interest

The authors had declared that no conflicting interest exist in this paper.

REFERENCES

Akartuna, E., Johnson, S. & Thomton, A. (2022). The money laundering and terrorist financing risks of new and disruptive technologies: a future-oriented scoping review. *Security Journal, the money laundering and terrorist financing risks of new and disruptive technologies* (Springer.com). p.9

Cristano, J. & Prenio, J. (2020). Financial crime in times of Covid-19- AML and Cyber resilience measures. Bank of International Settlements, https://pesquisa.busalud.org/global-literature-on-novel-coronavirus-2019-ncov/resource/pt/gre-740074.

Kettle, L. and Mumford (2017). Terrorist learning: a new analytical framework, studies in conflict and terrorism. 40(7) p. 523

https://ajsspub.org/publications VOLUME 2, ISSUE 1, 2025
ISSN: 1595-5842 **E-ISSN:** 3043-5463

Marron, D. (2008). Money talks, money walks: The war on terrorism financing in the West, policing. *A Journal of Policy and Practice.* 2(4): 441-451.

Merriam, L. & Kotler, M. (2020). Weaponized marketing: Defeating Islamic Jihad with marketing that built the world's top brands. Rowman & Littlefield, Lanham, MD, 2020

Moghadam, A. (2013). How Al-Qaeda innovates, security studies. 22(3): 446.

Pasztor, S. (2024). Terrorist financing from North Africa to the Sahel region: Exhaustible or inexhaustible stream? In terrorism and political contention: New perspectives on North Africa and the Sahel region (pp. 43-61).

Tompihe, J.G. (2003). Financing terrorism with fin techs in West Africa: In exploring the dark side of fin Tech and implications of monetary policy (pp. 118-143).

Wang, S. (2021). Evaluation of potential cryptocurrency development: Ability in terrorist financing, policing. *A Journal of Policy and Practice.* 15(4): 18