Comparative Analysis of Cryptocurrency and Terrorism Financing in Nigeria and Kenya, 2020-2025

Abdulmalik Olalekan OLADIPUPO
LCU/PG/002087

Being a Ph.D Thesis Submitted to the Department of Politics & International Relations, Faculty of Management and Social Sciences, Lead City University, Ibadan, Oyo State, Nigeria

In Partial Fulfilment of the Requirements for the Award of Doctor of Philosophy Degree (Ph.D.) in International Politics & Diplomacy

2025

Certification

This is to certify that Abdulmalik Olalekan OLADIPUPO with Matriculation number LCU/PG/002087 carried out this research work titled "Comparative Analysis of Cryptocurrency and Terrorism Financing in Nigeria and Kenya (2020-2025) in the Department of Politics and International Relations, Faculty of Management and Social Sciences,Lead City University, Ibadan, Oyo State, for the award of Doctor of Philosophy Degree (Ph.D) in International Politics and Diplomacy and that this has not been previously submitted.

_____ _____

Prof. Akeem Adekunle Amodu **Date**
(Supervisor)

_____ _____

Dr. Adebola Alade **Date**
(Head of Department)

Dedication

I dedicate this thesis to Almighty God who has been my help, strength, wisdom, knowledge and understanding throughout this programme.

Acknowledgement

I want to express profound gratitude to God Almighty for sparing my life, bestowing upon me wisdom, and granting me strength, peace, and good health during this journey.I am very grateful for the opportunity to study at Lead City University, being a great citadel of learning. I appreciate all the school's management for putting together the necessary educational facilities. I thank Professor Afolakemi Oredein, the Provost of the College of Postgraduate Studies, and other Lead City University Postgraduate College staff for providing a conducive learning environment. A big thanks to all the academic and non-academic staff involved in ensuring this great institution remains a force to be reckoned with in the educational sector.

I am incredibly and sincerely grateful to my supervisor, Prof. Akeem Adekunle Amodu, for his mentorship, assistance, patience and guidance at every stage of the research work. My special gratitude Dr. Adebola Alade (Head of Department), Dr. Modupe Albert (Immediate Past Postgraduate Programme Coordinator) and Dr. Emma Jimoh for their guidance, encouragement and for providing a conducive environment necessary to obtain this degree. I greatly appreciate all my Lecturers: Associate Professor. Ronald Olufemi Badru, Dr Olubunmi Akande, Dr Temitope Oluyemi, Dr Chukwuebuka Akuche, Dr Remilekun Sarunmi, Dr Augusta Diala. Thank you all for the knowledge impacted, skills acquired, words of encouragement and unending support. I am incredibly grateful to my beloved Family and Oladiran Olabisi for the sacrifices, love, prayers, and words of encouragement which helped me immensely throughout this program. Also, I thank my friends and coursemates for their support. I acknowledge the various sources from which materials were gathered for this work. I salute the authors for their contribution to knowledge. I am also grateful to all the Respondents for their honest responses

to all questions solicited in the Research Questionnaire.Although the institution and supervisors assisted in the research process, I alone am responsible for any errors found in the work.

Abstract

Rapid proliferation of cryptocurrency has posed significant challenges to global security, particularly in developing countries with high rates of cryptocurrency-related terrorism financing, such as Nigeria and Kenya, where terrorist organisations exploit its decentralised and pseudonymous features to fund their activities, thereby complicating traditional counter-terrorism financing frameworks. This study examines comparative analysis of cryptocurrency and terrorism financing in Nigeria and Kenya focusing on Policy Challenges and International Implications. The study objectives specifically investigate terrorist strategies, evaluate regulatory framework effectiveness, assess financing network transformations, analyse global financial system interconnections, and propose tailored policy solutions with international relevance while making use of Social Network Theory and Realism theory as its Theoretical framework. A mixed-methods research design was employed, integrating quantitative and qualitative approaches; the study sampled 103 participants, with 67 from Nigeria and 36 from Kenya, using purposive sampling techniques to ensure the selection of professionals with expertise in cryptocurrency regulation, counter-terrorism financing and cybersecurity, whilst data collection involved structured questionnaires, in-depth interviews with 11 key informants, and case studies, with quantitative data analysed using descriptive statistics, including mean, and percentage distributions with SPSS 27 software, and qualitative data examined through thematic analysis using NVIVO software. Findings reveal that terrorists exploit cryptocurrency's anonymity, with 59.70% ($\bar{X}$ = 0.60) of Nigerian and 61.11% ($\bar{X}$ = 0.61) of Kenyan respondents noting fund acquisition, and 62.69% ($\bar{X}$ = 0.63) and 66.67% ($\bar{X}$ = 0.67) confirming transaction concealment; the study demonstrates that the existing counter-terrorism financing frameworks in Nigeria and Kenya are ineffective in addressing cryptocurrency-enabled terrorism financing, as evidenced by 67.16% ($\bar{X}$ = 0.67) in Nigeria and 72.22% ($\bar{X}$ = 0.72) in Kenya reporting facilitation of international transactions, whilst financing shifts to digital networks, with 58.21% ($\bar{X}$ = 0.58) in Nigeria and 58.33% ($\bar{X}$ = 0.58) using exchanges. Local markets heighten global risks, with 67.16% ($\bar{X}$ = 0.67) and 72.22% ($\bar{X}$ = 0.72) noting financial system impacts, though policy solutions remain viable, with 74.63% ($\bar{X}$ = 0.75) in Nigeria and 83.33% ($\bar{X}$ = 0.83) in Kenya supporting security monitoring. The thematic analysis underscores Nigeria's P2P vulnerabilities and Kenya's mobile money gaps, corroborated by cases like Binance and Taliban financing. In conclusion, cryptocurrency markedly enhances terrorism financing through anonymity and local adaptations, rendering current frameworks ineffective and escalating regional and global security threats, necessitating advanced tools and interstate collaboration to address technological and regulatory disparities. The study recommends establishing a Diplomatic Cryptocurrency Intelligence Consortium under the African Union to deploy blockchain analytics, enhance multilateral intelligence sharing, and train diplomats in countering anonymity-driven strategies, alongside a Regional Diplomatic Technology Alliance to bridge technological gaps through forensic training and harmonised regulations, ensuring robust responses to this evolving threat in an interconnected world.

Keywords: Cryptocurrency, Terrorism Financing, Policy Challenges, International System, Diplomatic Strategies.

Word Counts: 444

Table of Contents

Preliminary Pages		**Page**
Title Page		i
Certification		ii
Dedication		iii
Acknowledgement		iv
Abstract		v
Table of Contents		vi
List of Tables		ix
List of Figures		x
List of Acronyms		xi
Chapter One: Introduction		1
1.1	Background to the Study	1
1.2	Statement of the Problem	15
1.3	Aim and Objectives of the Study	17
1.4	Research Questions	18
1.5	Significance of the Study	19
1.6	Scope of the Study	21
1.7	Operational Definitions of Terms	22
	Endnotes	26

Chapter Two: Literature Review 27

2.1 Conceptual Review 27

2.2 Theoretical Framework 108

2.3 Review of Empirical Studies 117

2.4 Conceptual Model 135

2.5 Summary of Literature Reviewed 140

Endnotes 147

Chapter Three: Methodology 148

3.1 Research Design 148

3.2 Population of the Study 149

3.3 Sample and Sampling Techniques 150

3.4 Description of Research Instruments 150

3.5 Validation of Research Instrument 150

3.6 Reliability of Research Instrument 151

3.7 Administration of Research Instrument and Method of Data Collection 152

3.8 Method of Data Analysis 153

Endnotes 154

Chapter Four: Results and Discussion of Findings

4.1 Demographic Data Analysis 154

4.2 Presentation of Research Questions 156

4.3 Discussion of Findings 202

Endnotes 218

Chapter Five: Conclusion 223

5.1 Summary of Findings 227

5.2 Conclusion 229

5.3 Recommendations 232

5.4 Contribution to Knowledge 234

5.5 Suggested Area for Further Research 236

Bibliography 236

Appendix 245

Bio-data 258

The University Compliance Certification 259

List of Tables

Table	Title	Page
3.1	Distribution of Study Population	140
3.2	Sample Distribution for In-depth Interview	142
3.3	Structure of Research Instruments	147
3.4	Analytical Techniques for Data Analysis	152
4.1	Demographic Data Analysis	155
4.2	Strategies Employed by Terrorist Organizations to Utilize Cryptocurrency for Financing their Activities in Nigeria and Kenya	156
4.3	Effectiveness of existing counter-terrorism financing frameworks In both countries	157
4.4	Adoption of Cryptocurrency Has Transformed Traditional Terrorism Financing Networks in Both Countries	159
4.5	The Interconnections between Local Cryptocurrency Markets, International Financial Systems, and Terrorism Financing Networks in Nigeria and Kenya	161
4.6	Policy Recommendations for Strengthening International Cooperation and Regulatory Frameworks to Combat Cryptocurrency-Enabled Terrorism Financing	163

List of Figures

Figure	Title	Page
2.4.1	Diagram Representing the Multi-Level Framework	123
4.2.2	Thematic Map of the Researcher's Fieldwork	166
4.2.2	Thematic Map of the Researcher's Fieldwork	172
4.2.2	Thematic Map of the Researcher's Fieldwork	177
4.2.2	Thematic Map of the Researcher's Fieldwork	182
4.2.2	Thematic Map of the Researcher's Fieldwork	185

List of Figures

Figure	Title	Page
2.4.1	Multilevel Framework Analysis	135

List of Acronyms

Abbreviation	Meaning
AML	Anti Money Laundering
BIS	Bank for International Settlement
BTC	Bitcoin
BVN	Bank Verification Number
CBDC	Central Bank Digital Currency
CBN	Central Bank of Nigeria
CDS	Credit Default Swap
CPMI	Committee on Payment and Market Infrastructure
ESMA	European Securities and Markets Authority
EU	European Union
EUROPOL	European Police
FATF	Financial Action Task Force
FGN	Federal Government of Nigeria
FTFA	Financial Task on Anti Money Laundering
GDP	Gross Domestic Product
GPIs	Global Performance Indicators
GPIs	Global Policy Indexes

ICT	Information Communication Technology
IMF	International Monetary Fund
ISIS	Islamic States of Iraq and Syria
ISWAP	Islamic State-West Africa Province
IR	International Relations
KYC	Know Your Customer
MMM	Mavrodi Mundial Moneybox
M- PESA	Mobile Money(Swahili)
NDIC	Nigeria Deposit Insurance Corporation
SNT	Social Network Theory
USA	United States of America
VASPs	Virtual Asset Service Providers (VASPs)
VECM	Vector Error Connection Model
US	United States
WAR	Western Money Remitted

Chapter One

Introduction

1.1 Background to the Study

Globalization has changed the phenomenon of crime and criminality; breaking down conventional barriers and creating new opportunities for international crime. The integration of technology developments, notably the Internet, has played a major role in this paradigm change, allowing criminal organizations to operate on a worldwide scale with unparalleled complexity and resistance against law enforcement operations[1]. In the last decade, the worldwide landscape has seen a paradigm change in the form and methods of terrorism, spurred in part by the fast expansion of digital technology. One especially confounding difficulty that has surfaced for security services globally is the use of cryptocurrency as a way of supporting extremist operations[2,3]. The decentralized and pseudonymous structure of cryptocurrencies, such as Bitcoin, has brought unique obstacles in identifying and mitigating the money flows connected with terrorism.

The emergence of the Internet has enabled criminal organizations to extend their operations worldwide, taking advantage of the advantages of anonymity and the absence of supervision that are inherent in online transactions. Presently, criminals engage in covert operations, using the extensive scope of the Internet to carry out illegal actions while minimizing the chances of being detected.

Hence, the current state of terrorist financing is characterised by the combination of a globalised and digital environment, which has brought about a new age. This has provided extremist organisations with an unparalleled opportunity to quickly and inexpensively finance their activities. The utilisation of cryptocurrencies, with their inherent features of anonymity and cross-border transaction capabilities, introduces a layer of complexity that amplifies the

challenges faced by international relations, placing traditional frameworks at a disadvantage in coping with the speed and adaptability of these evolving threats[4].

The advent of cryptocurrencies in terrorist funding signals a paradigm change, presenting extreme organizations with unparalleled advantages. One major component is the greater accessibility and anonymity inherent in cryptocurrency transactions, allowing terrorists to operate outside regular financial institutions and bypass national rules[3,5]. This growing financial flexibility offers substantial hurdles for authorities, hampering attempts to identify and disrupt financing flows, consequently delaying investigations and prosecutions.

Moreover, the worldwide accessibility and decentralization of cryptocurrencies adds to their attraction for terrorist funding. Operating without a central authority, these digital assets promote cross-border transactions, enabling the worldwide networks of terrorist organizations[5]. This globalized financial sector offers a considerable impediment for international collaboration in preventing terrorism, as it brings complexity relating to jurisdictional problems and regulatory harmonization.

Terrorist groups, displaying a dynamic adaptation to technical breakthroughs, regularly alter their strategies in the world of cryptocurrencies. Utilising a varied variety of strategies like as crowdfunding, involvement in darknet markets, and executing peer-to-peer transactions, these organizations efficiently raise and move cash via the anonymity offered by cryptocurrency[6]. This flexibility highlights the persistence of terrorist networks in traversing the digital environment, offering a continuous challenge for counterterrorism operations globally.

The international character of the current financial system, along with the digitalization of transactions, has enabled extremist organizations to leverage multiple routes for speedy and covert financing[6]. The ease of fundraising across borders, aided by the Internet, allows

terrorists to swiftly mobilize money without the restraints imposed by geographical boundaries. Moreover, the digitalization of financial transactions offers a cost-effective mechanism for terrorist groups to undertake fundraising efforts with decreased administrative fees, allowing for a more efficient deployment of resources toward their unlawful aims.

The incorporation of cryptocurrency into the terrorist funding scene offers an extra layer of complication. Cryptocurrencies, such as Bitcoin, provide a degree of anonymity and pseudonymity that conventional financial systems lack[2]. This greater anonymity allows terrorist groups to shift cash across borders with decreased chance of discovery. The decentralized and borderless character of these digital assets allows peer-to-peer transactions, establishing a financial ecosystem that functions outside the reach of traditional regulatory frameworks.

The intersection of globalization, technology, and illicit financing offers a multidimensional problem for international relations. Traditional frameworks meant to handle terrorist funding were mostly built in an age before the widespread use of cryptocurrencies and the seamless interconnectedness of global financial networks. The fast expansion of technology has overtaken the capacity of these frameworks to adapt, exposing a regulatory vacuum that terrorist groups exploit.

Moreover, the agility and endurance of extremist organizations in using technology for their financial operations make it difficult for international regulatory bodies and law enforcement authorities to maintain pace. The absence of a cohesive strategy, variations in legal frameworks across jurisdictions, and obstacles in international collaboration further complicate the capacity to combat the dynamic character of terrorist funding in the digital age[3].

On a national level, some governments have reacted to the issues presented by cryptocurrency-enabled terrorist funding via the introduction of rules controlling exchanges and transactions. These regulatory actions are meant to prevent money laundering and terrorist funding inside respective jurisdictions. Nevertheless, the efficiency of these measures varies greatly, creating to a fragmented environment where the implementation and effects of legislation varied between countries[8]. The lack of standardization raises worries about possible vulnerabilities that might be used by terrorist groups operating in places with less strict regulatory settings.

Nigeria, with its huge unbanked population and rising acceptance of cryptocurrencies, appears as a territory of heightened worry, giving a fertile atmosphere for terrorist organizations to exploit the anonymity and accessibility inherent in digital currencies for their fundraising operations. Notably, entities like Boko Haram, ISWAP, and other militant groups operational in the north and northwest regions have reportedly shifted towards crypto adoption, prompting apprehensions about potential cross-border funding, amplified online recruitment avenues, and an overall bolstering of operational capacities[9]. In response to this shifting scenario, the Central Bank of Nigeria recently removed its prohibition on cryptocurrency transactions while simultaneously establishing restrictions aimed at Virtual Asset Service Providers (VASPs). Despite these regulatory initiatives, significant reservations continue over the efficacy of these measures in sufficiently limiting unlawful activities related with terrorist funding inside the cryptocurrency domain[10].

Furthermore, Nigeria presents a particularly concerning case where terrorism financing through cryptocurrency thrives. Boko Haram and ISWAP, active insurgent groups, reportedly utilize Bitcoin and other altcoins to fund their operations, recruit fighters, and spread

propaganda[8]. Nigeria's large unbanked population and burgeoning crypto adoption create a fertile ground for terrorist exploitation[9]. Despite recent regulatory efforts by the Central Bank of Nigeria, comprehensive AML/CFT regulations specific to cryptocurrency remain absent, further hindering effective countermeasures[9,10]. The lack of technological solutions and limited investigative resources further exacerbate the challenge. The threat of cross-border funding via cryptocurrency further complicates the situation, potentially destabilizing regional security and impacting international relations. This complex intersection of factors, including a substantial unbanked population, a burgeoning crypto landscape, and the active engagement of terrorist groups, sets the stage for a comprehensive exploration of the challenges and implications inherent in cryptocurrency-enabled terrorism financing in the Nigerian context.

Kenya, a pioneer of financial innovation in Africa, has witnessed rapid growth in its fintech sector, propelled by platforms like M-Pesa[11]. This progress has spurred cryptocurrency adoption, yet it poses regulatory challenges. Concerns persist that Al-Shabaab, active in Somalia and influential in Kenya, might exploit the anonymity of digital currencies to fund its operations[12]. Although direct links to Kenyan crypto markets remain unproven, the group's adept use of mobile money for extortion suggests a potential shift towards cryptocurrencies as they gain traction[12].

Kenya's regulatory approach has been cautious yet progressive, aligning with Financial Action Task Force (FATF) guidelines to bolster anti-money laundering (AML) and counter-terrorism financing (CFT) frameworks[13]. In 2023, the Central Bank of Kenya mandated cryptocurrency exchanges to register and adhere to KYC and AML/CFT rules13. However, inconsistent enforcement leaves gaps, compounded by the lack of uniform regulations across East Africa, hindering efforts to monitor cross-border flows[14].

In Nigeria and Kenya, cryptocurrency intersects with terrorism financing in distinct yet parallel ways. Nigeria's larger economy and high crypto uptake enable groups like Boko Haram and ISWAP to use Bitcoin for fundraising, recruitment, and propaganda via platforms like Telegram[11]. In Kenya, Al-Shabaab's proximity and reliance on informal networks signal a latent threat to adopt digital currencies[12]. Both nations grapple with weak enforcement. Nigeria's Central Bank reversed its 2021 crypto ban in 2023 but struggles to regulate Virtual Asset Service Providers (VASPs) effectively, leaving vulnerabilities ripe for exploitation[13,14].

Adding a layer of complexity to the environment, technical restrictions further impede attempts to fight cryptocurrency-enabled terrorist funding. The decentralized nature of blockchain technology, the underlying structure of most cryptocurrencies, and the anonymity it enables create obstacles for detecting and preventing criminal transactions[3]. Law enforcement authorities, in many cases, find themselves ill-equipped with both the requisite resources and skills to properly tackle these increasingly complex financial crimes. The outcome is a technical gap that hinders the potential success of investigations and treatments.

The present procedures for countering terrorist funding find considerable hurdles in the context of cryptocurrency's development. The international legal system, represented by the UNTFCT, needs updating to the digital era[15]. National legislation, although varying in their application, lack coordination, adding to possible gaps in the worldwide fight against cryptocurrency-enabled terrorist funding. Coupled with technological limitations that impede tracking and disruption efforts, there emerges a pressing need for collaborative, innovative solutions that bridge these gaps and enhance the international community's capacity to address the multifaceted challenges posed by cryptocurrency in the context of global security.

The ramifications of cryptocurrencies in terrorist funding extend beyond conventional financial transactions, appearing in new and strong dangers that alter the landscape of international relations. One big issue emerges from the role of bitcoin in aiding the funding of growing terrorist threats, including lone-wolf strikes and cyberterrorism. The ease with which money may be generated and transmitted via digital means needs a reevaluation of counter-terrorism policies on a worldwide scale, necessitating a change in techniques to properly meet these emerging difficulties[16].

Moreover, the properties of Bitcoin, notably its anonymity and capability for cross-border transactions, create an atmosphere favourable to online radicalization and recruiting by terrorist groups. The ease with which extremist organizations may use these qualities boosts their capacity to attract people worldwide, possibly leading to increasing international security concerns and the worsening of regional conflicts[17]. This situation needs a comprehensive assessment of the linkages between online recruiting enabled by cryptocurrencies and the following influence on international security dynamics.

The consequences extend further to the role of state actors in cryptocurrency-enabled terrorist funding. While the principal benefactors are frequently non-state actors, some nations may utilize cryptocurrency to fund covert operations or assist terrorist organizations, coinciding with their geopolitical aims[18]. This provides a worrying dimension of possible state-sponsored terrorism, raising issues about the weakening of international standards against terrorist funding. The convergence between state actors and cryptocurrencies in the sphere of terrorist funding brings complexity that need a reevaluation of the global approach to these rising dangers.

In essence, the ramifications of cryptocurrencies in terrorist funding transcend financial transactions, altering the entire fabric of international relations[19]. From funding new and unconventional threats to the facilitation of radicalization and recruiting, and even possible cooperation by state actors, these consequences need a fundamental reassessment of global counter-terrorism measures. Addressing the complex difficulties presented by cryptocurrencies demands collaborative efforts, adaptable policies, and an increased knowledge of the complicated links between digital money and the shifting environment of international security.

The linked structure of the global financial system has made it simpler for criminals to exploit gaps and disparities, employing digital currencies to enable money laundering, dodge sanctions, and finance illegal operations[5]. This interconnection also causes issues for regulatory organizations and law enforcement agencies, as they cope with the intricacies of cross-border investigations and the jurisdictional limits of existing legal frameworks[3]. The migration of criminal activities online has not only expedited the speed at which unlawful transactions occur but has also widened the scope of criminal businesses. With a worldwide client base, criminal organizations may utilize economies of scale, reaching customers from varied geographic places[15]. This has important ramifications for the international community, prompting coordinated efforts to create adaptive measures that may successfully resist these transnational dangers[20].

However, the comparative study of Nigeria and Kenya highlights the intricate link between cryptocurrency and terrorism financing, which is shaped by unique national vulnerabilities yet marked by common regulatory and technological shortcomings. Nigeria's entrenched insurgent groups, such as Boko Haram and ISWAP, exploit widespread crypto adoption,

whilst Kenya's fintech landscape presents potential opportunities for Al-Shabaab's adaptation. Weak enforcement, inconsistent frameworks, and limited cross-border coordination intensify these threats, jeopardising regional security and international stability. This analysis emphasises the pressing need for unified regulations, improved technical capabilities, and strengthened international collaboration to address the growing challenge of cryptocurrency-enabled terrorism financing in both countries. Thus, the connection between globalization, technology, and transnational crimes, especially in the context of terrorist funding, highlights the need for a holistic and multidisciplinary approach. Understanding the nuances of this developing ecosystem is vital for politicians, security agencies, and academics to create effective countermeasures that meet the difficulties presented by this new era of globalized and digital criminal organizations.

1.2 Statement of the Problem

The global battle against terrorism faces a significant challenge with the rise of cryptocurrency-based financing, as groups like ISIS and Hamas exploit its anonymity and borderless nature to fund operations, recruitment, and propaganda using digital currencies such as Bitcoin[21]. This pressures international collaboration, exposing legislative disparities, especially in Nigeria and Kenya, where large unbanked populations and increasing crypto adoption provide fertile ground for exploitation[15,22]. In Nigeria, Boko Haram and ISWAP utilise Bitcoin and altcoins to sustain operations and propaganda1 whilst Kenya's vulnerabilities heighten regional insecurity[11,10,22]. The lack of robust AML/CFT regulations tailored to cryptocurrency and limited technological tools to track illicit flows intensify this threat, undermining financial integrity and global stability[4]. Although Nigeria's Central Bank

recently introduced regulations for Virtual Asset Service Providers (VASPs), their effectiveness is uncertain, demanding urgent international cooperation and unified frameworks to tackle this evolving threat[16].

Existing research underscores cryptocurrency's growing role in terrorism financing and proposes broad countermeasures, yet it primarily focuses on developed economies, overlooking the distinct challenges of nations like Nigeria and Kenya[3,6,7,11,12,22]. Theoretical models often fail to integrate technology, local contexts, and international relations adequately[18]. This study addresses significant gaps: empirically, due to limited statistical analysis of the extent and methods of cryptocurrency-based terrorism financing in Nigeria and Kenya; methodologically, through inadequate thematic analysis and comparative case studies across Nigeria, Kenya, and global contexts to identify adaptive strategies; and theoretically, by the absence of frameworks integrating technical, network, and contextual factors relevant to developing countries. Practically, the absence of bespoke countermeasures leaves these nations' crypto landscapes vulnerable[15]. This research addresses these deficiencies by employing statistical analysis, thematic exploration, and case studies spanning Nigeria, Kenya, and globally, providing evidence-based insights into policy challenges and international implications. Thus, this study investigated the comparative analysis of cryptocurrency and terrorism financing in Nigeria and Kenya: policy challenges and international implications.

1.3 Aim and Objectives of the Study

The study aims to comprehensively analyze the use of cryptocurrency in terrorism financing from 2018 to 2024, assessing its implications for international relations and proposing effective countermeasures. The specific objectives are to:

1. identify the specific methods and strategies employed by terrorist organizations to utilize cryptocurrency for financing their activities in Nigeria and Kenya.
2. critically evaluate the effectiveness of existing counter-terrorism financing frameworks in both countries, with specific focus on cryptocurrency regulations and their implementation.
3. examine how the adoption of cryptocurrency has transformed traditional terrorism financing networks in both countries and assess its impact on regional security dynamics.
4. investigate the interconnections between local cryptocurrency markets, international financial systems, and terrorism financing networks in Nigeria and Kenya.
5. develop context-specific policy recommendations for strengthening international cooperation and regulatory frameworks to combat cryptocurrency-enabled terrorism financing

1.4 Research Questions:

The Following questions were used to guide the study**:**

1. What specific methods and strategies do terrorist organizations employ to utilize cryptocurrency for financing their activities in Nigeria and Kenya?
2. How effective are the existing counter-terrorism financing frameworks in Nigeria and Kenya, particularly in regulating and implementing cryptocurrency policies?
3. How has the adoption of cryptocurrency transformed traditional terrorism financing networks in Nigeria and Kenya, and what is its impact on regional security dynamics?
4. What are the interconnections between local cryptocurrency markets, international financial systems, and terrorism financing networks in Nigeria and Kenya?

5. What context-specific policy recommendations can be developed to strengthen international cooperation and regulatory frameworks to combat cryptocurrency-enabled terrorism financing?

1.5 Significance of the Study

The study on terrorist funding and cryptocurrencies bears major consequences for numerous parties, each profiting in diverse ways. The relevance of the study transcends academic circles, giving crucial advantages for policymakers, law enforcement agencies, financial institutions, other scholars, civil society, and the public at large.

Policymakers and law enforcement agencies gain an in-depth understanding of how terrorist groups exploit cryptocurrency in Nigeria, enabling the development of targeted countermeasures, potential regulatory reforms, improved investigation techniques, and enhanced international cooperation strategies. Additionally, the study supports in resource allocation, permitting a more strategic emphasis on critical vulnerability and prevalent tactics, leading to evidence-based decision-making in the continuing efforts to prevent cryptocurrency-based terrorist funding.

For the cryptocurrency business, the report acts as a drive for responsible innovation. By addressing issues and possible abuse of cryptocurrencies, it motivates the industry to build technology and policies that emphasize security and ethical usage. The results help to building an industry that corresponds with ethical practices in the constantly expanding realm of digital banking.

In the sphere of international cooperation, the research seeks to play a vital role in developing joint efforts to solve global concerns linked with terrorist financing via bitcoin. It

aims to establish a basis for collaborative activities among states and organizations, striving towards a more secure and robust international financial system.

Government and security agencies, in the vanguard of efforts to secure national and global security, profit tremendously from the research. It adds to a greater understanding of the interaction between terrorist financing and cryptocurrencies, helping these organizations to design more informed and effective measures to address these changing threats.

Counterterrorism practitioners, heavily involved in attempts to fight changing techniques of terrorism financing, stand to profit from the insights presented by this research. The study supports tactical solutions, supporting practitioners in adapting and refining ways to successfully handle the issues presented by the usage of cryptocurrencies in financing criminal operations.

Financial institutions and regulatory authorities stand to profit from increased risk management methods developed from an awareness of unique hazards connected with bitcoin transactions in Nigeria. The study supports the establishment of comprehensive anti-money laundering and counter-terrorism financing (AML/CFT) policies customized to the cryptocurrency ecosystem, particularly crucial in poor nations like Nigeria. This not only enables the identification and prevention of cryptocurrency-based terrorist funding but also maintains the integrity of the financial system, increasing public faith in these institutions.

For researchers and academics, the study contributes to the improvement of theoretical frameworks by combining technology issues, local context, and international connections within the sphere of terrorist funding research. By addressing the current information vacuum on cryptocurrency-based terrorist funding in Nigeria, the study greatly increases the understanding of this complicated subject, providing a firm platform for future research

initiatives. Moreover, the results promote cooperation and information sharing among academics, practitioners, and policymakers, enabling more effective and coordinated responses to the worldwide problem of terrorist funding.

The study has the potential to improve public knowledge about the hazards connected with cryptocurrency-based terrorist funding, urging vigilance and advocating responsible usage of digital currencies. Informed individuals are better positioned to hold politicians and law enforcement authorities responsible for their part in efficiently countering terrorist funding and defending national security. Ultimately, this contribution promotes the greater purpose of fostering peace and security by giving vital insights and instruments to prevent terrorist actions, leading to a safer world.

1.6 Scope of the Study

This study focuses specifically on Nigeria and Kenya and draws from international seizure statistics. The time scope goes from 2020 until 2025 as a result of the fact the emergence of Cryptocurrency as a virtual currency rose into into prominence in late 2019. Primary focus is given to Boko Haram, ISWAP as well as Al-Shabab, with possible consideration of other active organizations in the area and a few in the worldwide arena. The study investigates bitcoin use trends, preferred kinds, transaction methods, and platforms exploited by these organizations for finance, recruiting, and propaganda. The regulatory environment is explored, comprising AML/CFT legislation for bitcoin transactions in Nigeria and important international settings. Technological issues encompass the use of blockchain technology, darknet markets, and peer-to-peer networks in supporting terrorist funding, along with possible methods to trace and prevent unlawful transactions.

In terms of international collaboration, this work assesses efforts to prevent cryptocurrency-based terrorist funding, highlighting best practices, problems in cross-border coordination, and analyzing prospects for better information sharing and joint investigations.

Exclusions in the research entail not thoroughly studying other financial crimes connected to cryptocurrencies unless directly relevant to terrorist funding. While addressing worldwide patterns, the research focuses a detailed dive into the Nigerian context rather than extensive global comparisons. Additionally, the research concentrates on bitcoin use and legal considerations, ignoring a full analysis of the technical subtleties of blockchain technology.

1.7 Limitations of the Study

The researcher encountered constraints during this study. Firstly, the unwillingness of some of the respondents to participate in the study and the delay in data retrieval. Also, the researcher found it difficult to access some crypto traders as many were skeptical about disclosing their identities. In addition to this is the Geographical proximity most especially in respect travelling to Kenya. Although the researcher was assisted by research assistant in Kenya, however, the process wasn't really seamless as the researcher could not travel to Kenya himself.

Similarly, the research could not satisfactorily sample the opinions of regulatory bodies on currency matters such as the Central Bank of Nigeria, Security and Exchange Commission, Office of the Comptroller of the currency and well as the Kenya Financial Institution. All these places a limit on the findings of this study.

1.8 Operational Definition of the Terms

Terrorism Financing: In this study, terrorism financing refers specifically to the act of raising and transferring funds (including funds raised through cryptocurrency) with the intention of supporting or aiding the activities of terrorist organizations, as defined by relevant UN Security Council resolutions and Nigerian / Kenya legislation. This definition excludes broad criminal actions unrelated to terrorism, such as money laundering or fraud, yet it may touch upon these areas if they are employed as techniques for terrorist funding.

Cryptocurrency: In this research, cryptocurrency refers to a digital or virtual currency protected by cryptography, functioning independently of a central bank or government. This term incorporates Bitcoin, Ethereum, and other cryptocurrencies most often used in Nigeria/ Kenya for terrorist funding objectives.

AML/CFT: In this research, it refers to Anti-Money Laundering and Combating the Financing of Terrorism framework, comprising applicable international agreements, Nigerian/ Kenya law, and regulatory measures undertaken by financial institutions. This definition emphasizes the particular legislation and methods targeted at preventing and identifying the unlawful flow of money, especially those utilized for terrorist funding using cryptocurrencies.

Darknet Marketplace: In this research, a darknet marketplace refers to an online platform accessible using anonymizing technology (e.g., Tor) where unlawful products and services, including tools and resources for supporting cryptocurrency-based terrorist funding, are purchased and sold. This concept emphasizes the importance of such platforms in allowing terrorist organizations to utilize anonymity and operate outside established financial institutions.

Peer-to-Peer Network: In this research, a peer-to-peer network refers to a decentralized system where users directly interact and exchange information or assets (including bitcoin)

without depending on a central authority. This concept underlines the potential obstacles offered by peer-to-peer networks for detecting and stopping unlawful bitcoin transactions associated with terrorist funding.

Blockchain Technology: A decentralized and distributed digital ledger that records transactions across several computers in a safe, transparent, and tamper-resistant way. The phrase "blockchain technology" is used to describe the underlying technology that permits bitcoin transactions, including its function in securing and confirming these transactions

Endnotes

1. S.M.S Zaidi, & Nirmal. *Emerging Realities in the International Political System: Transforming State's Foreign Policy.* **Herald of the Russian Academy of Sciences**, 2023, pp1-14.
2. O. Ariani, & A.L Ibrahim, *Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia.* **Jurnal Usm Law Review,** *7*(1), 2023, 30-44.
3. A. Majumder, M. Routh, & D. Singha, *A Conceptual Study on the Emergence of Cryptocurrency Economy and its Nexus with Terrorism Financing. In The Impact of Global Terrorism on Economic and Political Development:* **Afro-Asian Perspectives Emerald Publishing Limited.**2019, pp125-138.
4. N.N Reshetnikova, M.M Magomedov, S.S Zmiyak, A.V Gagarinskii, & D.A Buklanov, *Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security. In Current Problems and Ways of Industry Development: Equipment and Technologies,* Springer International Publishing,2021, pp2-21. J
5. A.M VÂRTEI, *Financing Terrorism: Economy's Dark Side. In Proceedings of the International Conference on Cybersecurity and Cybercrime***-Asociatia Romana pentru Asigurarea Securitatii Informatiei.**2023, pp216-223.
6. A. Eaddy, *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation).2019.
7. P.C Patel, & J. Richter, J. *The Relationship between Terrorist Attacks and Cryptocurrency Returns.* ***Applied Economics***, *53*(8), 2021, 940-961.

8. O.T Emmanuel, & A.A Michael,*Forensic accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria*. ***Journal of Auditing, Finance, and Forensic Accounting***, *8*(2), 2020, 55-66.

9. S.K Fakunmoju, O, Banmore, A. Gbadamosi, & O.I Okunbanjo, *Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance.* ***Binus Business Review***, *13*(1), 2022, 31-40.

10. CBN, Guidelines On Operations Of Bank Accounts For Virtual Assets Service Providers (VASPs)https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf.2023.

11. D. Eisermann, Cryptocurrencies as *Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges*. *Berlin Risk*.2020.

12. W. Ma, Terrorist Financing, War Crimes, and Crypto Geopolitics. In *A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects* (pp. 241-259). Cham: Springer Nature Switzerland.2023, pp241-259.

13. E.A Valvi, *The Role of Legal Professional in the European and International Legal and Regulatory Framework Against Money Laundering.* ***Journal of Money Laundering Control***, *26*(7), 2023, 28-52.

14. A. Andrianova, *Countering the Financing of Terrorism in the Conditions of Digital Economy. In Digital Transformation of the Economy: Challenges, Trends and New Opportunities*. Springer International Publishing.2020, pp20-31.

15. UN, *Advancing Rule of Law, Justice for All Through Technology Must Include Equal Internet Access,* Human Rights Compliance, Sixth Committee Speaker's Stress, 2023. https://press.un.org/en/2023/gal3694.doc.htm

16. T. Strategy, I.M.F Policy Paper.2023.

17. B.O Counterterrorism, Country Reports on Terrorism 2019. *US Department of State*.2019.

18. M. Campbell-Verduyn, & f. Giumelli, *Enrolling into exclusion: African Blockchain and Decolonial Ambitions in an Evolving Finance/Security Infrastructure*. **Journal of Cultural Economy**, *15*(4), 2022, 524-543.

19. M. Zachariadis, G. Hileman, & S.V Scott, *Governance and Control in Distributed Ledgers: Understanding the Challenges Facing Blockchain Technology in financials Services.* ***Information and Organization*****,** *29*(2), 2019, 105-117.

20. M. Dhali, S. Hassan, S.M, Mehar, K, Shahzad, K., & F. Zaman *Cryptocurrency in the Darknet: Sustainbility of the Currently National Legislation.* **International Journal of Law and Management**, *65*(3), 2023, 261-282.

21. E.A Akartuna, S.D, Johnson, & A. Thornton, *Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi Study. Technological Forecasting and Social Change*, *179*, 2022, 121632.

22. M.U Nnam, b.o Ajah, C.C, Arua, G.P, Okechukwu, & C.O Okorie, *The War Must be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria.* ***International Journal of Cyber Criminology***, 2019, *13*(2).

Chapter Two

Literature Review

This chapter explores the conceptual, theoretical, and empirical dimensions of cryptocurrency and its role in terrorism financing, with a comparative focus on Nigeria and Kenya. It reviews pertinent literature that underpins the empirical investigation of this study, highlighting the implications of cryptocurrency adoption within the international system, particularly its exploitation for illicit funding of terrorist activities in these two nations.

2.1 Conceptual Review

2.1.1 Blockchain Technology

Blockchain, a fundamental component of the cryptocurrency ecosystem, serves as a digital ledger capturing the intricate details of transactions within a computer network[1]. This

innovation is characterized by a structure where digital information is organized in blocks, forming a continuous chain stored in a public database[1]. Each block encapsulates crucial details such as the transaction date, the transaction amount, and the precise timing of the transaction. Additionally, it includes comprehensive information about the participating parties, offering unique identifiers for both the buyer and the seller.

In essence, a blockchain operates as a comprehensive digital record, documenting every transaction that transpires within the network. The term "block" signifies the presence of discrete units of data, each containing exhaustive information about its associated transaction[1]. The term "chain" emphasizes the sequential arrangement of these data blocks, creating a cohesive and continuous list. This chain of blocks serves as an immutable and transparent ledger, providing a comprehensive historical account of transactions.

One distinctive feature of the blockchain is its utilization of a unique digital signature for every participant within the network[2]. This digital signature plays a pivotal role during transactions, serving as a means to identify and authenticate the users involved. It ensures a secure and verifiable record of the parties engaged in a given transaction. The allocation of a digital signature to each participant enhances the accountability and traceability of transactions within the blockchain network[1].

It is noteworthy that each block within the blockchain system has a substantial storage capacity, typically around 1 megabyte. This generous capacity allows each block to accommodate a multitude of transactions, contributing to the scalability and efficiency of the entire blockchain network. The inherent design of blockchain, with its decentralized and distributed nature, further enhances the resilience and security of the system. Blockchain stands as a revolutionary technology that leverages a decentralized ledger structure to record,

authenticate, and secure transactions within a computer network. Its systematic arrangement of data blocks in a continuous chain, coupled with unique digital signatures, ensures transparency, traceability, and security in the realm of digital transactions[3]. The implications of blockchain extend far beyond its origin in cryptocurrency, influencing various domains, including finance, supply chain management, and, notably, the discourse on terrorism funding within the realm of international relations.

Several key features that distinguish it from conventional centralized transaction systems characterize Blockchain, as a transformative technology[1]. One paramount characteristic is decentralization, a departure from the traditional model where each transaction necessitates validation from a central trusted entity, such as a central bank. In blockchain, the need for a third party is eliminated, mitigating the associated costs and performance bottlenecks inherent in centralized systems[3]. Consensus algorithms play a crucial role in maintaining data consistency across distributed networks, allowing transactions to be validated without reliance on a central authority. Persistence is another fundamental attribute of blockchain. Transactions undergo rapid validation, and once verified by honest miners, invalid transactions are categorically rejected. The immutability of blockchain is evident in the near-impossibility of deleting or rolling back transactions once they have been incorporated into the blockchain. The discovery of blocks containing invalid transactions is prompt, reinforcing the integrity and permanence of the recorded data.

Anonymity, a notable feature of blockchain, allows users to interact with the system through generated addresses that shield their real identities[3]. While this characteristic provides a level of privacy, it is essential to acknowledge that blockchain cannot guarantee absolute privacy preservation due to inherent constraints. The balance between anonymity and transparency is

a critical consideration in the design and implementation of blockchain systems. Auditability stands as a key advantage of blockchain technology. The system stores comprehensive data regarding user balances, and any transaction necessitates reference to previous unspent transactions. As a transaction is recorded in the blockchain, the status of the referenced unspent transactions transitions from unspent to spent. This inherent transparency facilitates easy verification and tracking of transactions, enhancing the overall accountability of the system.

The key characteristics of blockchain encompass decentralization, persistence, anonymity, and auditability. These features collectively contribute to the reliability, security, and efficiency of blockchain systems, offering a paradigm shift from centralized models. As blockchain technology continues to evolve, its impact on various domains, including international relations and the complex issue of terrorism funding, becomes increasingly significant[2].

The taxonomy of current blockchain systems broadly classifies them into three distinct types: public blockchain, private blockchain, and consortium blockchain[4]. Each category presents unique characteristics that cater to different use cases and organizational needs.

In the realm of public blockchain, all transaction records are made visible to the general public, and anyone is permitted to participate in the consensus process. This openness and inclusivity are central tenets of public blockchain systems, ensuring a decentralized approach to validation and verification. The consensus process involves a broad network of participants, contributing to the distributed and transparent nature of public blockchains.

On the other end of the spectrum is the private blockchain, characterized by a fully centralized network under the control of a single organization[4]. In a private blockchain, only nodes

affiliated with a specific organization are granted access to participate in the consensus process. This controlled environment offers heightened privacy and exclusivity, making private blockchains suitable for situations where a high level of control and restricted access is paramount[4].

Consortium blockchain, occupying a middle ground between public and private models, is constructed collaboratively by multiple organizations. This type of blockchain is considered partially decentralized, as only a select subset of nodes, drawn from the collaborating organizations, engages in the consensus process. Consortium blockchains strike a balance between the openness of public systems and the exclusivity of private ones, making them suitable for use cases where collaboration among multiple entities is essential.

As the landscape of blockchain technology continues to evolve, new variations and adaptations of these three primary types emerge regularly. The dynamic nature of blockchain systems reflects ongoing efforts to address diverse requirements and challenges across industries. The choice of blockchain type depends on factors such as the desired level of decentralization, the need for privacy, and the extent of collaboration among participating entities. This taxonomy provides a framework for understanding the diverse applications and configurations of blockchain technology in the contemporary digital landscape. Consortium blockchain, a versatile application of blockchain technology, finds practical utility across various business applications. Notably, initiatives like Hyperledger are actively developing consortium blockchain frameworks tailored for business consortia[4]. These frameworks aim to facilitate collaborative efforts among multiple entities, offering a balanced approach that combines elements of decentralization and controlled access, making them suitable for a range of industry-specific use cases.

Understanding how blockchain operates is essential for comprehending its functionality. To add a block to the blockchain, specific criteria must be met, as outlined[5,6]. First and foremost, a transaction needs to occur, necessitating an agreement between users to initiate the addition of a new block to the blockchain. Subsequently, the transaction undergoes verification, a process executed by a vast computer network comprising over 5 million computers distributed globally. This network collectively ensures the accuracy of transaction details, cross-checking elements such as transaction time, amount, involved users, and digital signatures.

Once the transaction is verified and deemed accurate, it is stored in a block. This block, equipped with a unique hash, encapsulates crucial information, including users' digital signatures, transaction time, and transaction amount. Thousands of such blocks are then stored collectively in the blockchain. In the final step, a hash is assigned to the transaction, derived from the most recent block added to the blockchain. Once hashed, the block becomes eligible for addition to the blockchain. Importantly, once a block is integrated into the blockchain, it becomes publicly accessible to every participant within the network.

Every user in the network maintains a copy of the blockchain, ensuring widespread access to transaction-related information[5]. This includes details such as time, date, and amount, providing a comprehensive and transparent record of all transactions. The decentralized and distributed nature of blockchain ensures that every participant has equal visibility into the entire transaction history, promoting trust and accountability within the network[5]. In essence, the process of adding a block to the blockchain involves consensus, verification, storage, and the assignment of a hash, creating a secure and transparent ledger of transactions accessible to all network participants. This foundational understanding is crucial for exploring the

multifaceted applications and implications of blockchain technology, especially in the context of consortium blockchains tailored for collaborative business endeavors.

2.1.2 Cryptocurrency

Cryptocurrencies and blockchain technology have become increasingly popular in recent years. Cryptocurrencies are digital or virtual currencies that use cryptography for security and operate on decentralized networks known as blockchains. Blockchain technology, which underlies cryptocurrencies, is a distributed ledger that records transactions across multiple computers or nodes. The key concept of cryptocurrencies is decentralization, as they do not rely on a central authority such as a bank or government. Instead, transactions are verified and recorded by the network of computers participating in the blockchain. This decentralized nature ensures transparency, security, and immutability of transactions. In addition, blockchain technology allows for faster and more efficient transactions compared to traditional banking systems. By understanding the mechanics of cryptocurrency transactions and the role of decentralized ledgers, individuals can grasp the potential impact of cryptocurrencies and blockchain technology on various industries and economies.

A cryptocurrency is a virtual currency used to execute secure transactions between parties. Similar to the American dollar, cryptocurrencies have value and are used to buy and sell goods and services through cyberspace, loosely defined as the environment where information is exchanged over computer networks[9]. Additionally, cryptocurrencies are 'soft' currencies meaning they are not supported by a stable government or available in physical form such as the American dollar, British pound, and Euro.

Cryptocurrencies must be defined, which requires them to be identified as a specific class of virtual currencies and differentiated from fiat currencies and e-money. Fiat currencies are

government backed currencies, and designated legal tender. E-money is “a digital representation of a fiat currency,” in which is used to transfer fiat currency electronically; it is not a separate currency, merely the mechanism by which legal tender is transferred. Virtual Currency is defined by the Financial Action Task Force (FATF) as; “a digital representation of value that can be digitally traded and functions as (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status … It is not issued nor guaranteed by any jurisdiction, and fulfils the above functions only by agreement within the community of users of the virtual currency.”

Cryptocurrencies are digital or virtual currencies that utilize cryptographic technology for secure transactions. One key concept of cryptocurrencies is decentralization, which eliminates the need for a central authority such as a bank or government to oversee transactions. Instead, cryptocurrencies rely on a decentralized ledger system known as blockchain technology. The blockchain is a public digital ledger that records all transactions in a transparent and immutable manner. Each transaction is verified and added to a block and then permanently recorded on the blockchain. This decentralized and transparent nature of cryptocurrencies ensures security, privacy, and accountability in transactions. Additionally, cryptocurrencies often have features such as anonymity, which allows users to maintain their privacy while engaging in transactions. It is important to understand the mechanics of cryptocurrency transactions and the role of decentralized ledgers to fully comprehend the potential impact and benefits of cryptocurrencies in today's digital economy.

Emphasizing blockchain technology is crucial when understanding the key concepts, structures, and features of cryptocurrencies. Blockchain technology is the underlying foundation that enables cryptocurrencies to function securely and transparently. At its core,

blockchain is a decentralized ledger system that records all transactions made within a network. It consists of a series of blocks, each containing a list of transactions. These blocks are linked together in chronological order, forming a chain. The decentralized nature of blockchain ensures that no single entity has control over the network, making it highly resistant to hacking or tampering. Additionally, the transparency of the blockchain allows for public verification of transactions, ensuring trust among participants. A study and emphasising blockchain technology, individuals can gain a deeper understanding of the mechanics of cryptocurrency transactions and the role of decentralized ledgers in the world of digital currencies[5].

This definition could apply to both virtual world currencies, including Second Life Linden Dollars, and stand-alone cryptocurrencies, such as Bitcoin; but distinctions between these currencies must be made[3,4]. Virtual currencies may be either convertible or non-convertible, and centralised or decentralised[5].

The term 'virtual assets', used by the FATF, is too broad as the term could also include virtual currencies which are centralised, and can be regulated through regulation of that central authority. Cryptocurrencies are a specific subset of virtual currencies, which due to their decentralised nature require unique AML measures. The EU uses the term 'virtual currencies'8 and Australia uses the term 'digital currency', both of which suffer from the same shortcomings as the FATF term, as they do not sufficiently define cryptocurrencies. The agencies of the US also predominantly use the term 'virtual currencies', but the terminology used by the various authorities in the US is not consistent[9,10].

Thus, cryptocurrency stands as a prime exemplar of digital currency, facilitating peer-to-peer transactions within the blockchain network without the involvement of intermediaries,

typically represented by banks in conventional financial systems. In essence, cryptocurrency is a form of digital data stored within blockchain transactions. These transactions are meticulously recorded on the decentralized blockchain system, which is distributed across computers worldwide. Cryptocurrency, akin to traditional currencies, is traded on specialized platforms known as cryptocurrency exchanges, echoing the operation of stock exchanges in handling fiat currencies. Users employ digital wallets designed for cryptocurrency, serving as secure repositories for receiving, storing, and sending these digital assets. The robust security of cryptocurrency wallets is ensured through encryption algorithms, safeguarding them against external threats.

Transactions within the cryptocurrency network are executed through cryptocurrency wallets, each governed by two essential keys – the Public Key and the Private Key[2]. To transfer cryptocurrency from one account to another, knowledge of the recipient's Private Key is imperative. The encrypted transactions are broadcasted across the cryptocurrency network, forming a queue of requests that are subsequently incorporated into the blockchain, a public ledger. The process of adding transactions to the blockchain is termed "mining," a crucial concept discussed in detail later in this paper under the heading[4]. Mining involves creating new coins or cryptocurrency as a reward for validating and adding transactions to the public ledger.

The decentralization aspect of blockchain ensures that all users have access to the public ledger, with each user possessing a copy of the blockchain on their computer. The blockchain provides users with transaction details, including the time and date of transactions and the transaction amounts. Importantly, one of the defining traits of cryptocurrency is its commitment to user privacy. While traditional banks tie transactions to account identities,

cryptocurrency transactions are linked to cryptographic keys. Ownership of these keys signifies control over the corresponding cryptocurrency holdings, promoting a level of anonymity in the cryptocurrency ecosystem. Transactions are organized into queues and systematically added to the blockchain in a block-by-block fashion, forming the characteristic chain of blocks[5]. Cryptocurrency operates as a decentralized digital currency within the blockchain network, fostering secure and transparent transactions without reliance on traditional financial intermediaries. The cryptographic keys, blockchain technology, and the mining process collectively contribute to the unique features and functionalities of cryptocurrency in the evolving landscape of digital finance.

Cryptocurrency transactions operate on a decentralized ledger system known as blockchain technology. When a user initiates a transaction, it is verified by multiple computers on the network, known as nodes, through a process called mining[1]. This verification ensures the transaction's authenticity and prevents double-spending. Once verified, the transaction is added to a block and linked to the previous block in a chronological sequence, forming a chain. This chain is publicly accessible, allowing anyone to view the history of transactions. The use of cryptography ensures the security and privacy of these transactions, with public and private keys being used to authenticate and encrypt data. The decentralized nature of cryptocurrency transactions eliminates the need for intermediaries, such as banks, and provides users with control over their own funds. Understanding the mechanics of cryptocurrency transactions and the role of decentralized ledgers is crucial for comprehending the potential benefits and challenges associated with cryptocurrencies[2].

Transactions using cryptocurrencies are carried out through blockchain technology, rendering each transaction immutable, anonymous, and secure. Each transaction is verified for

authenticity using a series of mathematical formulas. The blockchain is functionally a series of digital blocks, each containing information about transactions. In the case of Bitcoin, this information would include both the sender and receiver of the transaction (made cryptic through the use of public Bitcoin addresses), as well as the size of the transaction. Each block also contains a 'hash,' which refers to a unique code (similar to a fingerprint) that can be used to identify a transaction. If the block is altered in anyway, its 'hash' would change, altering the relevant accounts of a breach in their security. Finally, each block also contains the 'hash' of the previous block, linking them together in cyberspace - a conceptual space connected by computer networks and accessed through various forms of digital technology. This means that if a single block is tampered with, it will also alert each following block, and these blocks will no longer be valid as well[5].When this happens, the transaction in the manipulated block will no longer have consensus from blockchain miners, and the blockchain would reject the block, getting rid of it permanently. To illustrate, the diagram below shows the connection of hashes within a blockchain.

Decentralized ledgers play a crucial role in cryptocurrencies and blockchain technology. Unlike traditional centralized databases, decentralized ledgers distribute the control and maintenance of data among multiple participants, eliminating the need for a central authority. This ensures transparency, immutability, and security in cryptocurrency transactions. Every transaction is recorded on the ledger, providing a transparent and tamper-proof history of all transactions. Additionally, decentralized ledgers employ cryptography techniques to secure transactions, making it almost impossible for hackers to manipulate or counterfeit transactions. These ledgers also enable peer-to-peer transactions, allowing individuals to transact directly without the need for intermediaries.

Decentralized ledgers are the backbone of cryptocurrencies, ensuring trust, security, and efficiency in the digital economy[4]. Cryptocurrencies and blockchain technology have revolutionized the world of digital transactions. The key concepts, structures, and features of cryptocurrencies, along with the decentralized ledgers provided by blockchain technology, have created a secure and transparent system for financial exchanges. Understanding the mechanics of cryptocurrency transactions is essential for anyone wishing to participate in this new form of digital currency. The role of decentralized ledgers in ensuring the integrity and immutability of transactions cannot be overstated. As we continue to explore the potential applications of cryptocurrencies and blockchain technology, it is crucial to stay informed and updated on the latest developments in this rapidly evolving field[6].

Confusion exists as to the accepted terminology to use when referring to cryptocurrencies, with a number of different terms being used by both international and supranational organisations, such as the FATF and the EU, and nationally by the UK, the US, and Australia[7]. While certain states have begun to adopt cryptocurrencies for their own purposes - Venezuela to combat rising inflation rates and North Korea to evade U.S. sanctions - the technology still operates within a decentralized network. Furthermore, for context, according to the Oanda Corporation, a foreign exchange company, the value of a single Bitcoin, the most prominent cryptocurrency in use, is in excess of $3,500 as of February 14th, 2019.

2.1.3 The Emergence of Cryptocurrencies

What are cryptocurrencies precisely? The Financial Action Task Force (FATF) defines a virtual currency as a digital representation of value that can be traded digitally and serves as a medium of exchange, unit of account, or store of value, but is not considered legal tender in any jurisdiction[8]. Cryptocurrencies are private digital currencies that function similarly to

cash, with all transactions taking place online and without being owned by any government or organization. Cryptocurrencies are decentralized and operate on a peer-to-peer network, allowing users to maintain and influence the market. This means that individual governments do not have the ability to regulate this new globalized economy[6].Virtual currencies gained popularity when the gold standard declined and globalization started to become more prominent. The abandonment of the gold standard was a significant historical moment as states recognized the interconnectedness of their economies. Some currencies recovered more quickly than others[7].

The global preference for the dollar stems from its status as the largest and most liquid market worldwide, as well as its political stability[8]. Most people, including several Americans, believe that the global dominance of the dollar as a reserve currency is not an ideal resolution to the currency issues faced worldwide. Every other option is worse. Every other option appeared inferior until the emergence of cryptocurrency, facilitated by globalization. Cryptocurrencies present a distinct threat to individual states as they challenge a state's monopoly on its own money, while also providing a glimpse of a genuinely global free market.

Cryptocurrencies originated as a financial experiment to test the viability of a decentralized and digital form of currency[2]. It not only survived but also thrived. Initially, computer enthusiasts and individuals seeking an alternative banking method were the ones who had invested in this initiative. Shortly after, ordinary individuals fascinated by the money started to join the user community. Bitcoin and other cryptocurrencies were created to be user-friendly, making it accessible for anybody who want to participate. One does not require computer expertise to own cryptocurrencies, making it accessible to everyone from many

backgrounds to participate in this worldwide initiative. Currencies are currently widely used globally due to their user-friendly design that simply necessitates Internet access[8].For this study, any research or reference to cryptocurrencies presented as factual pertains just to bitcoins. Currently, bitcoin is the most famous and well-known cryptocurrency, leading to the highest amount of study being undertaken on it compared to other cryptocurrencies. Since 2009, more than 75 virtual currencies have been established and are traded worldwide, with a combined market value of over $11 billion. Among these, Bitcoin is the dominant player, accounting for around $10 billion or 90% of the entire market value[8]. Although there have been slight changes since 2014, bitcoin remains the dominant cryptocurrency. Nevertheless, it is not certain that bitcoin will endure in the long run. Bitcoin technology is an innovative system that allows for banking transactions to take place without the need for traditional banks or political intervention, using cryptocurrencies. Cryptocurrency, virtual currency, digital currency, and digital cash shall be used interchangeably in this work to refer to cryptocurrencies.

Bitcoins function on a peer-to-peer network, where users are responsible for developing and maintaining the system and transaction process. A publicly shared record of all bitcoin transactions, similar to a ledger, is used to maintain track of all transactions. This record is called the blockchain. Users of bitcoin can verify each transaction made by other users at this location. This enables the bitcoin process to operate autonomously, without any external supervision, as elaborated in the reliability aspect of bitcoins. Anyone, including bitcoin users and government enforcement, can access the blockchain. Due to this, the anonymity of bitcoin

users is not complete but rather pseudo-anonymous, as will be further on in the subsequent section[9].

Bitcoins may be exchanged similarly to how the American dollar can be swapped. Euros from Europe. Every bitcoin user receives a bitcoin wallet upon their initial purchase of bitcoins. The wallet contains two keys for access: a public key for accepting wallets and a private key only for the owner for security. Transferring bitcoins is akin to sharing files, with the distinction that once a file is shared, the sender relinquishes it while the receiver gains ownership until they opt to transfer it. This setup ensures that the sender is unable to duplicate their bitcoins. Once bitcoins are sent to another individual, they are irretrievably lost and cannot be recovered. Once a transaction is initiated, the bitcoin community validates its legitimacy by confirming that the sender possesses sufficient coins to transfer to the recipient. Once the transaction is verified, a new block is added to the blockchain, making the transaction visible to all users.

There are three methods to get bitcoins: mining, buying with another money, or receiving in exchange for goods or services. Mining is the fascinating process by which bitcoins are created. It is a sophisticated procedure that relies on computer power to solve challenging algorithmic equations. New bitcoins are created only through this technique. The developers of bitcoin, who remain unidentified, designed it to function as a currency with a maximum supply of 21 million bitcoins[3]. Once the maximum is reached, the process of "mining" bitcoins will stop, making bitcoins scarcer as all possible bitcoins will have been generated. The developers designed bitcoin with the intention of assigning it value and addressing issues of inflation and deflation[6]. A Bitcoin's value might be seen as intrinsic and intuitive due to the

challenging production process[7]. As the number of bitcoins in circulation is limited, their scarcity and value increase, similar to gold, which is why the word "mining" is used for bitcoins. Bitcoins can be exchanged for any currency through online bitcoin exchanges. These platforms may impose a nominal transaction cost, which is significantly lower compared to the exorbitant fees charged by banks, as detailed in the subsequent section[9].

2.1.4 Cryptocurrency Characteristics

Transaction costs: Cryptocurrencies has numerous characteristics that are appealing to users but can also incur significant costs. Cryptocurrencies generally have minimal transaction costs, which vary based on the particular currency. Cryptocurrencies offer a cost-effective method for moving money globally as transactions are not overseen by financial entities like banks. Banks are prohibited from charging fees for checking the legitimacy of money transfers between customers[9]. "It is like Google creating Gmail to offer free email services, eliminating the need for people to pay for email services like those from AOL." The minimal transaction fees are advantageous because transactions are processed almost instantly and in real-time[10]. Using blockchain technology, people that participate in validating transactions will confirm that the sender possesses sufficient cash to deliver to the recipient. By removing a reliable intermediary like banks from the process, the need for transaction fees is also eliminated[10]. Dependability. Cryptocurrency technology is designed to be dependable. Reliability in literature is often debated, but cryptocurrencies are fundamentally based on a verification system at a theoretical level. This system operates without the need for confidence in transactions as many users verify each transaction, making it valuable for countries with corrupt domestic banking systems. This notion is rooted in a peer-to-peer network where people, rather than the government or companies, have authority over the currency market.

Providers of digital money would be motivated by economic benefits to maintain the stability of their currencies. A stable currency is more attractive as a reliable store of value and is more likely to attract investments[10].

Legitimacy is established by widespread use, rather than by the authority of a singular government and its currency. As more users adopt the money, its customer base grows, leading to an enhanced reputation. A positive reputation attracts additional users to try the currency. This leads to a snowball effect in building momentum and establishing a sense of trust among the general population. Bitcoin designers have enhanced reliability by ensuring that all transactions are transparent. An online, public ledger was constructed that is accessible to everybody, regardless of whether they possess the currency. This prevents the possibility of "double spending," where bitcoins are sent from one wallet to another, as transactions cannot be reversed. People believe in the reliability of blockchain due to trust among the masses and faith in the code. The blockchain is decentralized and operated by the community utilizing the money, rather than being controlled by a single individual or organization. Failure of the blockchain is prevented by the code developed for it. The code is fair and transparent, which fosters confidence. The code is immutable. The blockchain records all transactions made without disclosing the actual identity of any users. Anonymity in cryptocurrencies has been a subject of intense controversy in recent years. Generally, cryptocurrencies do not necessitate personal identifiers for transactions. Access to the Internet and the acquisition of cryptocurrencies are essential, but they present hurdles to law enforcement and government policymakers.Anonymity. Anonymity, the third characteristic of cryptocurrencies, is a benefit that is not exclusive to criminals but is enjoyed by all users. Cryptocurrencies provide anonymity by allowing transactions to occur without the need for face-to-face interaction

between the sender and receiver. The only identifying information for each party is their public keys. Anonymity in cryptocurrency is often associated with criminals, yet it can benefit everyone. Consider cash, for instance. Cash provides a level of anonymity and is universally accepted in most regions. Individuals frequently opt for cash due to its ease or lack of faith in financial institutions. Nevertheless, criminals also heavily rely on cash for their illicit activities[10]. Cryptocurrency is a digital kind of currency that allows transactions to be conducted electronically without the need for in-person interaction. Cryptocurrencies have transitioned cash-only transactions to the online realm for convenience and efficiency, inadvertently providing a means for criminals to conduct illicit activities without detection.

Anonymous: The literature emphasizes that cryptocurrencies are only pseudo-anonymous, meaning that every transaction conducted using the coin is publicly available on the blockchain for anyone to see. By meticulously tracking the chain, it is evident which wallet is transferring funds to another wallet and how the receiving wallet utilizes the money. Cryptocurrencies are not entirely anonymous, but they provide enough anonymity for users to feel secure utilizing the currency without facing consequences[11]. The possibility of tracing transactions back to an individual using their IP address, while maintaining pseudo-anonymity[11]. The researchers discovered that they were able to track bitcoin addresses back to a single IP address. Researchers discovered that by monitoring IP addresses, law enforcement may trace transactions on the blockchain back to specific individuals, even if they possess many bitcoin wallets. While not a comprehensive solution for apprehending all criminals that utilize bitcoin, this approach could serve as an initial step towards developing efficient strategies for mitigating the negative impacts of cryptocurrencies[12]. Financial Inclusion. Cryptocurrencies provide a distinct option for individuals who are "unbanked," referring to

those without access to financial systems in their nation or those who opt not to create an account with local banks due to factors like government corruption. Approximately 2.5 billion adults, representing slightly more than half of the global adult population, do not utilize formal financial services for saving or borrowing[8]. This demographic is often located in regions where banking poses risks due to distrust in state financial institutions or issues with inflation in state currencies. Individuals will choose to avoid utilizing state financial institutions and currency instead of relying on the state to distribute currency. The researchers stress the importance of implementing policies that provide affordable and dependable financial services to unbanked populations for their involvement in the global financial market, however they have not identified a specific solution[4]. Financial inclusion, Providing banking services to disadvantaged and low-income populations at a reasonable cost[12]. Clegg also discusses how bitcoin could potentially address the issue raised[13]. Bitcoin's growing popularity makes it a cost-effective and dependable option for people without access to traditional banking services. The concept is easily comprehensible for non-experts and just necessitates Internet connectivity[10]. The necessity of expanding Internet access in developing countries but asserts that bitcoin is the key to achieving financial inclusion worldwide[11]. If cryptocurrencies are proven to be reliable, they provide an alternative banking method that is independent of any political, social, or economic influences, enabling a genuinely global free market. Bitcoin technology is greatly propelled by financial inclusion. It provides individuals in underdeveloped countries with a distinctive chance to participate in financial activities beyond their own borders. Bitcoin gained popularity in regions like Europe and the United States, where traditional currencies and financial services are already efficient. Originally embraced by computer enthusiasts, Bitcoin has now developed into a potential practical

solution for individuals in developing countries[11]. Multiple research papers have explored the concept that cryptocurrencies can succeed in regions with inadequate financial infrastructures[9,11,14]. Research indicates that significant populations in these states are willing to abandon state-backed money in favour of a new digital currency experiment, driven by restricted banking options, the push for financial inclusion, and the acceptance of neocapitalism[11,14]. The motivation for utilizing bitcoins due to financial inclusion has been commonly mentioned in literature.

Volatility in prices: Some scholars contend that cryptocurrencies are unreliable as currencies due to their fast price fluctuations. Price fluctuation, the sixth characteristic, has been problematic for some consumers. Cryptocurrencies are susceptible to dramatic fluctuations in value. Following the collapse of Mt. Gox, a prominent bitcoin exchange, the value of bitcoin plummeted. Previously valued at over $1,000 USD, it dropped to roughly $500 USD shortly after the incident, resulting in users losing half of their invested funds. Consumers began to doubt the reliability of the currency[14]. Some governments consider cryptocurrencies to be commodities or stocks rather than a reliable currency due to the absence of a steady exchange rate.

This problem is often contested due to the conflicting views on whether it should be considered a commodity or a currency, as discussed in various literature and legal frameworks. It is crucial to resolve the current discussion regarding whether cryptocurrencies qualify as currencies. This study will adhere to the FATF's 2014 definition of cryptocurrencies as currency, however each jurisdiction has its own perspective on these digital currencies. The debate is around whether cryptocurrencies function more like conventional currencies, serving

as a medium of trade, or if they behave more like commodities, considered as economic goods. The subject has sparked significant controversy[10,15]. It remains crucial to differentiate, particularly when discussing money laundering in connection with cryptocurrencies. If cryptocurrencies are not recognized as a legitimate form of currency, then using them for money laundering would not be classified as such; it would simply be deemed illicit trafficking of products. If cryptocurrencies are categorized as commodities, they are exempt from regulation under AML regulations and the FATF[8]. For this study, virtual currencies will be treated as legitimate mediums of exchange, regardless of their legal status or uncertainty in the financial market.

The prices of bitcoin fluctuate due to the fact that its value is solely determined by the collective judgment of its worth. Simply said, the price of bitcoin is determined by supply and demand. As more individuals embrace bitcoin and acknowledge its worth, the currency will become more stable. Negative media coverage, such as the bankruptcy of a bitcoin exchange or hacking assaults on bitcoin wallets, will cause the price of bitcoins to decrease. Bitcoin's value is contingent on the belief of its users and is determined by consensus. The quick fluctuations in price based on perception cause some to view cryptocurrencies as akin to commodities or investment stocks, rather than as stable currencies[8].

Insufficient supervision: Furthermore, there is insufficient supervision about cryptocurrency. Cryptocurrencies are decentralized, indicating the absence of centralized ownership. The currency poses unique challenges for regulation. Cryptocurrencies are not widely regulated uniformly. States have opted for varying responses to these cryptocurrencies. The reactions to virtual currencies can be categorized into five approaches: (1) no action taken by states with no regulations in place; (2) treating virtual currencies as commodities and

regulating them through taxes; (3) complete banning of virtual currencies, particularly in states that only allow the use of national currency; (4) treating virtual currencies like any other foreign currency, subject to the same regulations; and (5) adopting a "wait-and-see" strategy, where regulations may be implemented later if the currency is perceived as a threat[16]. These reactions add complexity to the situation as cryptocurrencies operate across frontiers, facing challenges due to the lack of standardized financial regulations and jurisdictional borders. No entity, whether individual, corporate, or government, has the ability to regulate digital currencies, leaving users vulnerable to the potential risks associated with their use[17]. Bitcoin theft due to hacking or malware is frequent. Unfortunately, users cannot seek assistance from local authorities as they lack the jurisdiction, tools, and resources for investigation[17]. States have adopted varying approaches to regulating cryptocurrencies, but more action is needed. International agencies like FATF and the International Monetary Fund (IMF) are exploring the possibility of regulating cryptocurrencies inside their domains, but more action is needed[8]. To address the issue of oversight and jurisdiction, a global, uniform response is necessary to safeguard consumers from the absence of oversight associated with digital currencies.

Criminal organization: Cryptocurrencies are frequently linked to criminal activities, which discourages many potential users. This aspect has been a significant obstacle for non-experts to embrace cryptocurrencies because to their association with various criminal activities. Scholars have differing opinions on the extent to which cryptocurrencies are associated with criminal activities. Cryptocurrencies have been utilized for buying illegal goods online, law enforcement currently does not consider cryptocurrencies to be a significant danger[15]. The FBI has discovered numerous illegal schemes involving the usage of cryptocurrencies. The FBI's 2012 report discusses many schemes they have encountered[15].

2.1.5 Uses of Cryptocurrency: Global Context

In a bid to evade United States sanctions, countries like Iran and Russia have reportedly contemplated similar measures. The strategic implementation of a state-sponsored cryptocurrency serves as an alternative to their respective fiat currencies, providing a means to circumvent U.S. dollar-based economic regulations and international banking institutions[18]. Often characterized as rogue states operating outside the norms of the international community, both Iran and Russia stand to benefit significantly from adopting more covert financing methods, affording them greater autonomy in their operations.

The Democratic People's Republic of Korea (North Korea) has prominently engaged with cryptocurrencies as a deliberate strategy to navigate around United States sanctions. North Korea has not only traded cryptocurrencies akin to commodities on a stock exchange but has also developed its own cryptocurrencies, allowing the country to generate funds despite monetary restrictions. By launching proprietary cryptocurrencies and establishing domestic cryptocurrency wallets, North Korea has adeptly infiltrated cryptocurrency systems, presenting itself as a non-threatening entity employing cryptic communication. Additionally, North Korea utilizes transaction mixers, sophisticated tools that obscure the trace of a transaction within a blockchain. This technique involves splitting the linear paths of a single transaction, creating a convoluted money trail that is challenging to decipher.

North Korea employs cryptocurrency shifting services to further obfuscate the nature of cryptocurrencies, such as Bitcoin, by converting them into alternative cryptocurrencies. This strategic maneuver contributes to making the money trail even scarcer and less traceable. Subsequently, North Korea can utilize the newly acquired cryptocurrency to exchange for fiat currency on national markets or exchanges, effectively obtaining the American dollar without

being subject to sanctions[21]. This technique mirrors money laundering practices often utilized by terrorist organizations, involving a process of moving, changing, and cleaning funds to obscure their origin and facilitate their use[21]. Employing these multifaceted tactics, the once linear and traceable nature of the money trail is bent and obscured, rendering a coherent path nearly indiscernible.

Cryptocurrencies have found utility beyond the realm of national strategies, with both companies and individuals utilizing them for various purposes, including point-of-sale transactions, storing money, and investments. Major corporations such as Microsoft, PayPal, and the Subway sandwich chain now accept cryptocurrency payments, and the adoption of this technology is expected to grow as more companies recognize its benefits. The advantages of cryptocurrencies lie in their cost-effectiveness, with transactions being comparatively inexpensive. Furthermore, the accessibility of this technology is far-reaching, surpassing that of traditional banking apparatuses. Cryptocurrencies provide a viable solution for businesses with risky models that may not find support from traditional banks[6].

The universality of cryptocurrencies contributes to their widespread appeal, offering exciting prospects for both individuals and companies. As time progresses, the adoption of cryptocurrencies by both the private and public sectors is anticipated to increase. The technology's ability to transcend geographical boundaries, coupled with its efficiency and accessibility, positions cryptocurrencies as a promising tool for financial transactions, investments, and various applications across diverse industries.

Despite the increasing acceptance and integration of cryptocurrency technology, the landscape has proven to be highly volatile. In 2017, Bitcoin, the most widely recognized cryptocurrency, experienced a staggering 15-fold increase in market capitalization compared to the previous

year. The cryptocurrency market as a whole witnessed an extraordinary surge of 3,400% during the same period[8]. Subsequently, both Bitcoin and the overall cryptocurrency market faced significant declines, yet they still maintain substantial value, each priced at several thousand United States dollars in the contemporary context. With an extensive array of over one thousand cryptocurrencies currently available, making definitive statements about the future of this diverse landscape becomes challenging. The question of which cryptocurrencies will emerge as more popular or gain the most market share remains uncertain, and only time will unveil the true trajectory of the cryptocurrency market[8].

Within this diverse array of cryptocurrencies, certain notable ones, such as Bitcoin, Ethereum, and Ripple, have risen to prominence with larger market capitalizations compared to their counterparts. These premier cryptocurrencies have established themselves as leaders in the market, enjoying widespread recognition and adoption[20]. However, predicting the future dynamics of the cryptocurrency market remains elusive, and factors such as technological developments, regulatory changes, and market trends will inevitably influence its evolution.

Moreover, the expansion of cryptocurrency infrastructure has played a pivotal role in shaping the environment for widespread adoption. Both physical and digital infrastructures, comprising robust servers, cryptocurrency ATMs, and secure cryptocurrency wallets, have proliferated in recent years[22]. Additionally, regulatory frameworks that are more accommodating to cryptocurrency activities have emerged, fostering an environment conducive to the seamless integration of cryptocurrencies into various regions of the world. The increasing number of cryptocurrency exchanges further contributes to the growing ecosystem, providing platforms for trading and facilitating the exchange of digital assets.

While the cryptocurrency landscape has experienced significant volatility, certain cryptocurrencies have emerged as leaders in the market. The continuous expansion of infrastructure, both physical and regulatory, suggests a growing readiness for pervasive cryptocurrency adoption. However, the multifaceted nature of the cryptocurrency market, coupled with the ongoing emergence of new technologies and regulatory frameworks, makes it challenging to make definitive predictions about its future trajectory. Only time will unfold the true potential and direction of the evolving cryptocurrency landscape. Cryptocurrencies can be traded for various fiat currency, is rapidly growing as more parties begin to use the technology.

Since as early as 2014, terrorist organizations, including the Islamic State, al-Qaeda, and their affiliates, have sporadically utilized cryptocurrencies, particularly Bitcoin, as a means of securing funding for their operations. While the extent of adoption varies among different groups, there is evidence that some, like Hamas, have actively embraced cryptocurrency technology, whereas others, like al-Qaeda, have shown less activity in this space[23]. Although there is limited observed use of cryptocurrencies by terrorist organizations to date, the potential for future utilization has prompted significant attention in policy and literature on the subject. As traditional methods of terrorism financing face increased scrutiny, and as technology becomes more accessible, cryptocurrencies may become more appealing and practical for a broader spectrum of terrorist organizations globally.

Nigeria has emerged as a global frontrunner in cryptocurrency adoption, driven by a convergence of factors elucidated by various sources. The Central Bank of Nigeria (CBN) recognized the phenomenon, acknowledging in its "Circular on Virtual Currencies" the need for a cautious approach to cryptocurrencies[24]. The circular outlines regulatory frameworks for

financial institutions, indicating the initial apprehension and regulatory considerations surrounding the growing use of cryptocurrencies in the country.

A crucial driver of cryptocurrency adoption in Nigeria is the prevalent issue of financial exclusion, as highlighted by the World Bank's report, "Fintech in Nigeria: Opportunities and Challenges[24]. With a large unbanked population, many Nigerians seek alternative financial services that can provide them with greater access and flexibility. Cryptocurrencies have proven to be a viable solution to address this financial exclusion, offering avenues for transactions, savings, and wealth management beyond the traditional banking system.

Further insight into the motivations behind cryptocurrency adoption in Nigeria, factors contributing to the widespread adoption of cryptocurrencies, including economic instability marked by inflation and currency devaluation, a tech-savvy population with high mobile phone penetration, and the convenience of cross-border transactions[24,25]. These factors collectively create an environment conducive to embracing cryptocurrencies as an alternative financial tool.

However, it is essential to consider the challenges associated with cryptocurrency adoption in Nigeria, potential risks and challenges posed by cryptocurrencies, shedding light on the need for a balanced approach to their integration within the Nigerian financial system. Elaborately, since as early as 2015, domestic terrorist groups within Nigeria, like Boko Haram and the Islamic State West Africa Province (ISWAP), have shown sporadic interest in utilizing cryptocurrencies to finance their activities, primarily Bitcoin. The extent of their adoption remains limited compared to other funding methods, like extortion and resource exploitation. However, some evidence suggests increasing sophistication, with reports of these groups attempting to establish online fundraising platforms accepting cryptocurrency donations[25].

Unlike Boko Haram, which primarily relies on traditional channels, ISWAP has demonstrated a more proactive approach towards cryptocurrencies. They've been linked to online campaigns targeting supporters in the diaspora, encouraging donations through Bitcoin wallets. This trend aligns with ISWAP's broader online presence and propaganda efforts[23].

Despite the limited documented use of cryptocurrencies for terrorism financing in Nigeria, the potential for future exploitation remains a serious concern. As counterterrorism efforts focus on traditional financial channels, terrorist groups may increasingly find cryptocurrencies attractive due to their perceived anonymity and ease of cross-border transactions[25]. Furthermore, Nigeria's rapidly growing smartphone penetration and increasingly tech-savvy population create a fertile ground for cryptocurrency adoption, potentially by both legitimate users and illicit actors[25].

Therefore, it's crucial to address this emerging threat proactively. Strengthening regulations and implementing KYC/AML protocols for cryptocurrency exchanges operating in Nigeria can be crucial steps. Additionally, raising awareness among the public and financial institutions about the risks associated with terrorist fundraising through cryptocurrencies can play a vital role in preventing future attacks. This adapted case study provides a specific analysis of cryptocurrency use in the context of Nigerian terrorism financing, drawing parallels to the provided global trends while highlighting the unique characteristics and concerns relevant to the region. Remember to further flesh out this analysis with specific examples, data, and citations from reliable sources to build a strong and insightful argument[25].

Financing of terrorism. Cryptocurrencies have been linked to cases of terrorism financing. In 2015, the FATF released a report on the risks and threats associated with terrorism financing[8]. The document included a segment dedicated to virtual currencies and their link to terrorist

financing, highlighting the various features of virtual currencies that may attract terrorists. The report specifically states that terrorists receive funding from private donations, non-profit organizations, criminal activities, extorting local populations, kidnappings for ransom, commercial ventures, and state support. Each approach has unique difficulties; but, the profits obtained from these endeavors must ultimately benefit the terrorist group. The research states that terrorists are utilizing both physical ways, such as personal couriers, and virtual techniques, such as cryptocurrencies, to acquire funds[26]. This money serves two main purposes: "direct operational support" for specific terrorist activities that require planning and funding, and "broader organizational requirements" such as recruitment, paying recruits, supporting existing infrastructure, and promoting propaganda[27].

Terrorists frequently engage in additional criminal activities like kidnappings, drug trafficking, and bank robberies to finance their operations. Terrorists have traditionally utilized the hawala system for money laundering, involving the physical transfer of cash among the sender, receiver, and numerous intermediaries[28]. After committing these ancillary crimes, terrorists must find a way to launder the money. However, the hawala system is recognized for being time-consuming and hazardous when attempting to transfer significant amounts of money rapidly. Terrorists have utilized cryptocurrencies to launder money obtained from illegal activities and to receive financial support from foreign donors, avoiding consequences from their home country government. cash plays a crucial role in terrorist activities, highlighting the efficiency of using digital currency for transferring funds inside clandestine organizations[28]. The researchers examine how terrorists can exploit the virtual environment, such as virtual worlds or virtual currencies, to hide their identities, illegal activities, and sources of funding. Terrorists can outwit law enforcement to some degree by operating

beyond conventional legal boundaries and consistently circumventing borders using the Internet. Law enforcement has not yet found an efficient approach to collaborate and pool resources to address criminals moving in and out of their areas[28].

Development of typologies for money laundering and terrorism financing, crimes may be successful in virtual worlds, specifically in Second Life and World of Warcraft, where users can utilize real money in-game[28]. The shift of money laundering and terrorism financing to online platforms, facilitated by the convenience and anonymity they provide, but it is not directly related to cryptocurrencies[28]. The initial segment of their study details various typologies and methods utilized by criminals to hide their illegal gains from criminal activities. The researchers identified parallels and distinctions between money launderers and terrorist financiers in using virtual worlds to transfer funds. They observed that money launderers tend to be more cautious while laundering money through various online transactions[26]. The second portion of their study addresses the practical implications for professionals. They talk about the significance of the research and how it could be utilized to urge the international community to take a proactive approach towards both online crimes. This study provides practical guidance for policymakers in developing AML and counter-terrorism finance regulations[28]. It is intriguing to observe the contrasting methods employed by money launderers and terrorism financers in virtual environments. They have two distinct objectives: money laundering to hide illegal gains and terrorism financing to support terrorist activities without much concern for anonymity[29].

Critics believe that the innovation of bitcoin technology, which promotes a worldwide free market and connects the globe financially, is worth the risk due to its potential to assist more people than it harms, notwithstanding the advantages and disadvantages of cryptocurrencies.

It is challenging to promote a revolutionary technology while also preventing the inevitable associated crime. If measures could be taken to reduce the negative effects of being associated with criminal activities, cryptocurrencies would become significantly safer for their users. This study aimed to address a gap in the existing literature to progress in reducing the negative impacts. This research project aims to analyze the function of cryptocurrency in promoting transnational crimes. The literature review highlights the significance of various factors such as the type of cryptocurrencies, market for cryptocurrencies, opportunities for exchanging large amounts of money without identification, transaction features, and networking operations in understanding how cryptocurrencies facilitate transnational crime operations.

2.1.6 Evidence of Cryptocurrency Used by Terrorist Organizations

Terrorist organizations use cryptocurrency to trade drugs, weapons, and other items on the black market. For example, 'Fund the Islamic Struggle without Leaving a Trace' is a dark website used to transfer bitcoins to jihadis. Some extremists have even published a book, Bitcoin wa Sadaqat al Jihad, which clearly teaches how to transfer valuable bitcoins from North America and Western Europe to jihadists[23]. It has been reported that Bahrun Naim, the planner of the terrorist attacks in Jakarta in 2016, used Bitcoin for virtual payment to transfer funds to the armed elements and finance terrorist activities[24]. In addition, Islamic law allows the use of Bitcoin and other cryptocurrencies to fund jihadis, and cryptocurrency has become an alternative to the mainstream financial system and legal tender. In June 2015, an American teenager admitted that he had taught Islamic state members how to use Bitcoin. He provided guidance on how to build bitcoin wallets for potential donors and tips on how to use the 'dark

wallet' service[26]. The Islamic State often kidnapped and blackmailed Europeans in Syria. By using Bitcoin as a ransom payment tool, terrorists can raise funds and facilitate the transfer of funds. This part of the funds was then used to fund terrorist attacks in Europe[29]. In addition, there are also many anecdotes about terrorists using cryptocurrency in blackmail schemes online. For example, terrorist analysis requires the use of 1,000 BTC in exchange for a company's data not to be disclosed[26]. In January 2016, criminals used ransomware to control the computers of the Lincoln Group, demanding a ransom of 500 USD worth of Bitcoin, but they ultimately failed. In November 2015, three Greek banks received blackmail threats, demanding payment of hundreds of thousands of euros in Bitcoin. In recent years, the amount of evidence of Bitcoin being used in criminal activities has been increasing. Compared with other countries, Indian terrorists and drug syndicates prefer to use Bitcoin for transactions[16].

2.1.7 Motivation for the Use of Cryptocurrency by Terrorist Organization

Cryptocurrency was used by terrorist organizations from the perspective of cryptocurrency's attributes, namely, its anonymity, decentralization, and globalization[29]. The irreversibility of cryptocurrency transactions and low transaction costs are why cryptocurrency is attractive to terrorist financing[30]. In contrast, cryptocurrency is not attractive to terrorist financing because of the large fluctuation of cryptocurrency prices, the lack of trust mechanisms, the difficulty of conversion to main currencies, and the maturity of global fund tracking technology. The supply of cryptocurrency is not flexible, the currency itself lacks internal value support and credit guarantee, and the price of cryptocurrency can be manipulated, so terrorist organizations have shown certain restrictions on its use[31].

The factors influencing the use of cryptocurrency by terrorist organizations based on the information and communication technology development index, currency exchange restrictions, cryptocurrency price fluctuations, and anti-Western sentiment[17]. The RAND Corporation's research has shown that existing financial infrastructure is weak in developing countries or areas with internal turmoil. Therefore, venture capital is attractive to terrorist organizations. Terrorist organizations employ cryptocurrencies to create venture capital and obtain higher funds[14]. A key element of cyber terrorism is the use of cryptocurrencies, such as Bitcoin, to buy and sell prohibited goods and services on the dark web. Given the geographic range, speed, and degree of anonymity provided by the dark web, it will attract terrorists. The dark web is likely to be an extremely effective and secretive platform for terrorists to use cryptocurrency[20].

2.1.8 Terrorism Funding: Global and Nigerian Contexts

Terrorism has become a pressing global issue in recent times, with countries around the world grappling with the challenges it poses to their security and stability. One key factor that enables terrorism to thrive is the availability of funding[16,22]. Understanding the sources of funding for terrorist organizations is crucial in order to develop effective counter-terrorism strategies.

Terrorism funding refers to the financial support provided to terrorist organizations or individuals to carry out their activities. It is an essential aspect of terrorist operations, enabling them to acquire weapons, equipment, and personnel necessary for their missions. There are various sources and types of terrorism funding, including state-sponsored funding, illicit activities, and private donations. State-sponsored funding occurs when governments provide

financial support to terrorist groups either openly or covertly to further their political or ideological agenda. Illicit activities such as drug trafficking, arms smuggling, and money laundering also generate significant funding for terrorist organizations. Private donations, often solicited through charities or religious organizations, play a crucial role in funding terrorism as well[29]. Understanding the definition and types of terrorism funding is essential to develop effective strategies to combat this global threat.

2.1.9 Global Perspectives on Terrorism Funding

Terrorism funding, a pervasive global issue, demands a nuanced comprehension of its origins and channels. Delving into the worldwide panorama of terrorism financing underscores its multifaceted nature that transcends national boundaries. As highlighted by Frederick Appiah Afriyie, scholarly research has dissected the myriad avenues through which terrorist organizations procure funds, encompassing state patronage, illicit ventures, and contributions from sympathizers[31].

State patronage is often cited as a significant source of funding for terrorist organizations. Some states, either directly or indirectly, provide financial support to terrorist groups as a means to advance their political agendas or destabilize rival nations[32]. For example, the Taliban in Afghanistan has historically received funding from elements within the Pakistani government, enabling them to sustain their insurgency[19]. Illicit ventures, including drug trafficking, arms smuggling, and extortion, serve as lucrative revenue streams for terrorist organizations[33]. These criminal activities not only generate substantial funds but also provide terrorists with the means to procure weapons and sustain their operations. The Islamic State of Iraq and the Levant (ISIL), for instance, derived a significant portion of its funding from oil smuggling, taxation, and the looting of banks[33].

Contributions from sympathizers, both individuals and organizations, also play a pivotal role in financing terrorism. Donations may be solicited through legitimate charitable organizations or informal networks, making it challenging to trace the flow of funds[23]. Al-Qaeda, for instance, has relied on donations from wealthy individuals in the Gulf region to finance its operations[23]. Understanding the diverse sources of terrorism funding is essential for developing effective counterterrorism strategies. By disrupting financial flows and targeting the enablers of terrorism financing, governments can undermine the operational capabilities of terrorist organizations and mitigate the threat they pose to global security[32].

Moreover, the interconnectivity of financial systems on a global scale and the facilitation of cross-border transactions have significantly streamlined the process for terrorist entities to tap into resources from international quarters[33]. The advent of digital banking, online payment platforms, and cryptocurrencies has revolutionized the financial landscape, offering terrorists unprecedented avenues for moving funds across borders with speed and anonymity[33].

The globalization of financial networks not only enables the swift movement of funds but also poses a formidable challenge to traditional regulatory mechanisms. Unlike conventional banking transactions that are subject to stringent oversight and regulations, transactions conducted through alternative financial channels often evade detection, making it difficult for authorities to track and disrupt illicit funding[12]. Furthermore, the proliferation of offshore financial centers and shell companies complicates efforts to trace the true origins of funds, providing terrorists with a cloak of secrecy to conceal their activities[33].

The use of emerging financial technologies further exacerbates the challenge of combating terrorism financing. Cryptocurrencies, in particular, have emerged as a preferred medium for transferring funds due to their decentralized nature and pseudo-anonymous features[32].

Terrorist organizations exploit the anonymity afforded by cryptocurrencies to solicit donations, launder money, and finance their operations beyond the reach of traditional banking regulations[31]. Addressing the vulnerabilities inherent in the global financial system requires a concerted effort to enhance regulatory frameworks, strengthen international cooperation, and leverage technological innovations. By bolstering financial intelligence capabilities, improving information sharing mechanisms, and implementing robust Know Your Customer (KYC) and Anti-Money Laundering (AML) measures, governments can enhance their ability to detect and disrupt terrorism financing activities[23]. Additionally, collaboration between public and private sector stakeholders is essential to develop innovative solutions and stay ahead of evolving threats posed by terrorist financing in the digital age[23].

Recognizing the globalized dimension of terrorism funding underscores the imperative of formulating robust counterterrorism strategies that transcend national jurisdictions. Effective countermeasures necessitate collaborative efforts among nations, emphasizing information sharing, intelligence cooperation, and coordinated regulatory frameworks (UNODC, 2020). By fostering international solidarity and synergy, nations can fortify their defenses against the insidious threat of terrorism financing, thereby safeguarding global security and stability.

International organizations play a crucial role in facilitating cooperation among nations to combat terrorism financing. The United Nations Security Council, through its various resolutions and sanctions regimes, provides a framework for member states to implement measures aimed at disrupting the flow of funds to terrorist organizations[33]. Additionally, the Financial Action Task Force (FATF) sets standards and promotes best practices in combating money laundering and terrorism financing, encouraging countries to enhance their legal and regulatory frameworks[34].

Bilateral and multilateral partnerships are instrumental in strengthening intelligence sharing and operational collaboration among law enforcement agencies. The establishment of joint task forces and information-sharing platforms enables countries to exchange critical intelligence, track illicit financial flows, and apprehend individuals involved in terrorism financing networks[34]. Furthermore, initiatives such as the Egmont Group facilitate collaboration between financial intelligence units, enhancing the analysis and dissemination of financial intelligence to combat terrorism financing[35].

Coordinated regulatory frameworks are essential to address the vulnerabilities in the global financial system that terrorists exploit. Enhanced due diligence requirements, stricter oversight of financial institutions, and measures to detect and disrupt suspicious transactions are integral components of effective counterterrorism strategies[24]. Moreover, promoting transparency and accountability in the financial sector, including the disclosure of beneficial ownership information and the regulation of virtual asset service providers, helps mitigate the risk of terrorist abuse of the financial system[34]. Addressing terrorism financing requires a comprehensive and collaborative approach that transcends national boundaries. By leveraging international cooperation, sharing intelligence, and implementing coordinated regulatory measures, nations can enhance their capacity to detect, disrupt, and deter the flow of funds to terrorist organizations, thereby safeguarding global security and stability.

2.1.10 Nigeria's Experience with Terrorism Funding

Nigeria has faced significant challenges in combating terrorism funding within its borders. The country has a long history of violent extremist groups, such as Boko Haram, which have exploited various sources of funding to sustain their operations. One of the primary sources of terrorism funding in Nigeria is the illicit drug trade. According to a report by the United Nations Office on Drugs and Crime (UNODC), Nigeria serves as a major transit hub for drug trafficking, providing an avenue for generating illicit funds for terrorist organizations[28].

Boko Haram, in particular, has been known to engage in various criminal activities, including drug trafficking, to finance its insurgency. The group takes advantage of Nigeria's porous borders and weak law enforcement infrastructure to smuggle drugs, particularly cocaine and heroin, through the country and onward to international markets. This not only fuels drug addiction and organized crime but also provides Boko Haram with a significant source of revenue to fund its terrorist activities. Furthermore, Boko Haram has also been involved in other illicit activities such as kidnapping for ransom, extortion, and looting, all of which contribute to its funding streams. The group's ability to generate funds from diverse sources underscores the complexity of combating terrorism financing in Nigeria and the need for comprehensive strategies that address both the supply and demand sides of illicit funding. In addition to addressing the criminal networks that facilitate terrorism financing, Nigeria also faces challenges in implementing effective regulatory and enforcement mechanisms to combat money laundering and terrorist financing. Weak financial regulations, corruption, and a lack of coordination among law enforcement agencies have hindered efforts to disrupt the flow of funds to terrorist organizations operating within the country.

To effectively combat terrorism financing in Nigeria, there is a need for strengthened international cooperation, capacity-building initiatives, and targeted interventions to address

the underlying socio-economic factors that contribute to the vulnerability of individuals and communities to recruitment and radicalization by terrorist groups like Boko Haram.

Additionally, the kidnapping industry has emerged as a lucrative source of funding for terrorist groups in Nigeria. Ransom payments from kidnappings have become a significant source of revenue, with estimates suggesting that millions of dollars are paid annually to secure the release of kidnapped individuals[29].

Terrorist organizations like Boko Haram and its splinter groups have capitalized on Nigeria's vulnerability to kidnappings, targeting both locals and foreigners for abduction. These groups use the ransom payments not only to finance their operations but also to recruit new members and expand their influence. The frequency and scale of kidnappings in Nigeria have contributed to a climate of fear and instability, further fueling the cycle of violence and terrorism in the region[29].

The Nigerian government has taken steps to address terrorism financing, including strengthening legislation and enhancing cooperation with international partners. The Terrorism (Prevention) Act of 2011 provides a legal framework for combating terrorism financing and money laundering, with provisions for the freezing of assets and the prosecution of individuals involved in terrorist financing activities[34]. Additionally, Nigeria has enacted regulations to improve oversight of the financial sector and enhance due diligence requirements for financial institutions to detect and prevent illicit financial flows[29].

Furthermore, Nigeria has intensified its cooperation with international partners, including neighboring countries and international organizations, to combat terrorism financing. Joint operations and information-sharing initiatives have been established to disrupt terrorist networks, track illicit financial transactions, and apprehend individuals involved in terrorism

financing activities[33]. Despite these efforts, challenges persist in effectively addressing terrorism financing in Nigeria. Corruption, weak enforcement mechanisms, and a lack of resources continue to undermine the effectiveness of counterterrorism measures. To achieve meaningful progress, sustained political commitment, institutional reforms, and enhanced international cooperation are essential to combat the scourge of terrorism financing and safeguard the security and stability of Nigeria and the broader region. However, the complex and evolving nature of terrorism financing continues to pose significant challenges for Nigeria's security apparatus.

2.1.11 Typologies of Cryptocurrency Usage in Terrorism Funding:

Direct financing

Direct financing represents a significant avenue through which terrorist organizations leverage cryptocurrencies to solicit donations or payments from sympathizers and supporters. This tactic capitalizes on the anonymity and accessibility afforded by digital assets, enabling terrorists to raise funds without the constraints imposed by traditional financial channels, the decentralized nature of cryptocurrencies facilitates direct peer-to-peer transactions, bypassing the need for intermediary institutions and enhancing the privacy of donors and recipients[35].

Transactions associated with direct financing typically take place through online platforms, social media channels, or encrypted messaging applications, allowing terrorist organizations to reach a broad audience while maintaining a degree of anonymity. For instance, the proliferation of crowdfunding campaigns launched by terrorist groups on popular social media platforms, such as Facebook and Twitter, to solicit donations in cryptocurrencies[36]. These

platforms serve as virtual hubs for propagating extremist ideologies and soliciting financial support from sympathizers worldwide.

Moreover, certain terrorist groups may exploit the anonymity features inherent in specific cryptocurrencies, to raise funds for specific operations or propaganda campaigns. These privacy-centric digital assets offer enhanced anonymity by obscuring transaction details, including the sender's address and the amount transferred[36]. By leveraging these cryptocurrencies, terrorist organizations can conduct fundraising activities with greater discretion and reduce the risk of detection by law enforcement agencies.

The use of cryptocurrencies for direct financing also presents challenges for authorities tasked with monitoring and disrupting terrorist financing activities. Traditional regulatory frameworks designed to combat money laundering and terrorist financing may struggle to adapt to the decentralized and pseudonymous nature of cryptocurrency transactions[37]. Moreover, the global nature of cryptocurrency networks and the lack of centralized oversight further complicate efforts to identify and interdict illicit fundraising activities conducted by terrorist organizations.

Direct financing represents a significant typology of cryptocurrency usage in terrorism funding, leveraging the anonymity and accessibility of digital assets to solicit donations from supporters and sympathizers worldwide. As terrorist organizations increasingly embrace cryptocurrencies as a means of financing their operations, policymakers, law enforcement agencies, and financial institutions must collaborate to develop robust regulatory frameworks and technological solutions to detect, disrupt, and deter illicit fundraising activities. By understanding the tactics employed by terrorists in utilizing cryptocurrencies for direct

financing, stakeholders can enhance their ability to safeguard the integrity of the global financial system and mitigate the risks associated with terrorism financing.

Money laundering

Money laundering, a pervasive criminal activity often associated with cryptocurrencies, represents a critical aspect of terrorism funding in the digital age. This illicit practice serves as a means to obscure the origins of illegal proceeds and the identities of those involved in financial transactions. As noted by Jacquez (2016), cryptocurrencies offer a novel avenue for criminals to launder money, leveraging the inherent features of digital assets to cloak their activities from law enforcement scrutiny. Further emphasizes the role of cryptocurrencies in facilitating money laundering, highlighting the challenges posed by the pseudonymous nature of transactions and the decentralized infrastructure of blockchain technology[7].

The growing trend of online money laundering, driven by the increasing reliance on the Internet and the reinforcement of anonymity through technological advancements[38]. This shift towards online platforms for money laundering, that the anonymity features of cryptocurrencies make them particularly attractive for criminal enterprises seeking to conceal their illicit activities[36]. These sentiments, suggesting that the anonymity and accessibility of cryptocurrencies contribute to their appeal as a tool for money laundering[37]. The advantages that cryptocurrencies offer to money launderers, including the ability to conduct transactions across borders with minimal regulatory oversight and the potential for rapid asset conversion. The nexus between cryptocurrencies and money laundering underscores the evolving landscape of financial crime, particularly in the context of terrorism funding. As technology advances and anonymity is reinforced, it is imperative for policymakers, law enforcement

agencies, and financial institutions to remain vigilant in combating this threat[38]. By understanding the typologies of cryptocurrency usage in terrorism funding, stakeholders can develop effective strategies to detect, disrupt, and deter illicit financial activities, thereby safeguarding the integrity of the global financial system.

It is evident that as technology progresses, criminals adapt and capitalize on emerging opportunities to further their illicit activities[38]. The researchers aptly point out that money launderers are rational actors who strategically exploit the evolving landscape of financial technologies to evade detection and perpetuate their unlawful operations. In their exploration of the reasons driving money launderers towards cryptocurrencies, the allure of anonymity offered by digital assets, which enables perpetrators to shield their identities and activities from law enforcement scrutiny[39]. Furthermore, the detrimental impact that cryptocurrencies can have on financial institutions when utilized for money laundering purposes. The decentralized and pseudonymous nature of cryptocurrencies creates a virtual environment conducive to criminal activities, allowing perpetrators to operate with impunity and evade traditional regulatory measures.

However, while cryptocurrencies offer money launderers a relatively seamless and anonymous experience, the process of laundering illicit funds via digital assets may require significant effort and meticulous planning. Setting up the necessary accounts and routing transactions clandestinely demands a certain level of expertise and coordination. Nevertheless, the researchers highlight the efficiency of cryptocurrencies in facilitating larger volumes of money laundering at a faster pace compared to traditional methods[39].

In essence, the typologies of cryptocurrency usage in terrorism funding through money laundering underscore the multifaceted nature of financial crime in the digital era. While

cryptocurrencies offer perpetrators unprecedented opportunities to conceal their illicit activities, they also present challenges and complexities for law enforcement agencies and regulatory bodies. By understanding the motivations and tactics employed by money launderers in leveraging cryptocurrencies, stakeholders can develop proactive strategies to mitigate the risks associated with terrorism financing and safeguard the integrity of the global financial system[40].

Traditionally, money laundering entails the transformation of illicitly obtained "dirty" money into a form that allows criminals to utilize it without the risk of detection by law enforcement. This process unfolds across three distinct stages: placement, layering, and integration[39]. Placement marks the initial phase, during which criminals inject their illicit funds into the legitimate financial system through various means. This could involve converting cash into foreign currency to blur the trail between domestic and international banking systems. Alternatively, criminals might establish front companies with heavy cash flows, providing a cloak for large sums of illicit money. Another tactic involves "smurfing" and "structuring," wherein criminals divide their proceeds into smaller amounts and distribute them across multiple accounts held by different individuals. By keeping these amounts under the radar of anti-money laundering systems, they can later consolidate the funds into personal accounts[40].

Layering constitutes the subsequent stage, wherein criminals endeavor to obfuscate the illicit origins of their funds. Having infiltrated the legal financial system in the placement phase, they proceed to shuffle the money across various accounts, both domestically and offshore. This constant movement serves to further obscure the true source of the funds, complicating efforts by law enforcement to trace their origins, particularly if smurfing and structuring techniques were employed during the placement stage.

In addition, criminals may resort to falsifying documents, such as invoices for fictitious sales or purchases, to justify the influx of large cash amounts or deposits. Corruption can also become a factor during this stage, as criminals may exploit financial system employees or even law enforcement officials, bribing them to facilitate their transactions. Another tactic involves integrating the illicit cash into a legitimate, cash-intensive business, gradually funneling the money through the business operations. Through this method, criminals merge their illegal proceeds with the legal income generated by the front company they've established[40].

The final phase of the money laundering process is integration, where the objective is for criminals to emerge with the same amount of cash they started with, now unencumbered by fears of tracing back to their illicit activities. This stage often sees criminals investing in real estate or purchasing high-end items that can be acquired with cash without raising suspicion. Integration revolves around enabling criminals to freely utilize their "cleaned" money as if it were legitimately acquired[38]. Even with meticulous precautions taken to layer their transactions and conceal the illicit origins of their funds, criminals must exercise prudence in their spending to avoid drawing unwanted attention from law enforcement. It is imperative that they refrain from conspicuous consumption or extravagant purchases that could raise suspicion. The banking system's stringent regulations and the requirement for personal identification when opening accounts make it easier for authorities to track transactions between accounts[40].

Similarly, the process of cryptolaundering mirrors traditional money laundering in its three-step approach of concealing origins and legitimizing illicit proceeds. However, the utilization of cryptocurrencies streamlines and expedites this process for criminals. The pseudo-

anonymity provided by Bitcoin and other cryptocurrencies presents an opportunity for perpetrators to exploit the system and launder their criminal proceeds without triggering red flags within traditional banking systems. While it may be challenging to find Bitcoin exchanges willing to facilitate large cash-to-cryptocurrency transactions, it is not impossible[40]. The decentralized nature of cryptocurrency exchanges and the lack of stringent identity verification procedures create an environment conducive to illicit activities, allowing criminals to bypass the regulatory scrutiny imposed by traditional financial institutions. As a result, cryptolaundering offers a convenient and relatively low-risk alternative for criminals seeking to obscure the origins of their illicit funds and integrate them into the legitimate financial system[33].

In the realm of cryptolaundering, criminals seeking to convert cash into Bitcoin and vice versa often seek out trusted Bitcoin exchanges capable of facilitating such transactions. Historically, this process may have necessitated face-to-face meetings, where cash is exchanged for Bitcoin and subsequently transferred to the criminals' wallets. However, it has become increasingly common for criminals to conduct their illicit activities entirely in Bitcoin, thus circumventing the need to convert cash into digital currency in the first place[41]. During the placement stage of cryptolaundering, criminals have several options for depositing cash into Bitcoin. One approach involves utilizing local Bitcoin exchanges that are willing to accept large sums of cash in exchange for Bitcoin. These exchanges may operate in regions with lax regulatory oversight, providing a convenient avenue for criminals to enter the cryptocurrency market without attracting unwanted attention. Additionally, criminals may engage in illicit business transactions using Bitcoin from the outset, receiving payments in cryptocurrency for goods or services rendered[41].

This shift towards utilizing Bitcoin for illicit transactions from the outset not only simplifies the cryptolaundering process but also minimizes the risks associated with converting cash into digital currency. By conducting business exclusively in Bitcoin, criminals can obfuscate the origins of their funds and evade detection by traditional financial institutions and law enforcement agencies[42]. However, this approach may also expose criminals to the inherent volatility and regulatory uncertainties associated with cryptocurrencies, highlighting the complex interplay between illicit activity and technological innovation in the realm of financial crime.

In the context of cryptolaundering, drug traffickers exemplify how cryptocurrencies, particularly Bitcoin, can facilitate the entire money laundering process. Initially, drug traffickers may operate on the darknet, a hidden portion of the internet where illegal activities are conducted anonymously[42]. Utilizing Bitcoin as the primary medium of exchange on these platforms already serves to obscure the identities of all parties involved, fulfilling the placement stage of money laundering. This mirrors traditional money laundering practices where criminals exchange their illicit funds for foreign currency to conceal their origins and integrate them into the financial system.

Moving into the layering stage, criminals exploit the anonymity inherent in Bitcoin to create multiple accounts, a tactic made feasible by the platform's minimal requirement for personal identification. As Bitcoin transactions are pseudonymous rather than truly anonymous, savvy criminals recognize the importance of layering transactions to further obfuscate the origins of their funds. By orchestrating a complex network of interrelated accounts, criminals can effectively disguise the flow of illicit funds, shielding themselves from detection by law enforcement agencies[40]. Despite Bitcoin's pseudonymous nature, it still leaves a digital trail

through its transparent blockchain ledger, documenting every transaction between wallets[3]. Consequently, prudent criminals understand the necessity of maintaining caution during the layering stage to prevent detection. Employing multiple accounts to communicate and transact with one another helps to safeguard the true origins of the laundered funds.

Finally, in the integration stage, criminals have the option to retain their illicit gains in Bitcoin for future transactions or convert them back into fiat currency through local Bitcoin exchanges. This process, commonly known as "cashing out," allows criminals to seamlessly reintegrate their illicit funds into the traditional financial system. Moreover, Bitcoin's inherent properties enable swift and efficient laundering of "dirty" money obtained from illegal activities, reducing the time and effort required compared to traditional money laundering methods[32].

Drug Trafficking

Cryptocurrencies have become deeply entrenched in the operations of darknet markets, serving as the primary medium of exchange for a wide array of illicit goods and services. Often likened to the "Amazon" of the underground economy, these online marketplaces offer a clandestine platform for the trade of contraband ranging from drugs and weapons to assassinations and sexual services. Notably, that illicit drugs are the most sought-after items on these illegal online marketplaces, with a significant portion of these drugs originating from the United States[43]. English-speaking countries and Western European nations emerge as key players in the trafficking of illicit drugs on cryptomarkets. Cannabis, stimulants such as cocaine and amphetamines, ecstasy (MDMA), and psychedelics like NPS and LSD constitute the primary drugs offered for sale[34]. This dominance underscores the global reach and impact

of cryptomarkets in facilitating the underground drug trade, transcending geographical boundaries and enabling anonymous transactions on an unprecedented scale.

The allure of cryptocurrencies for both buyers and sellers on darknet markets lies in their pseudonymous nature and decentralized infrastructure, which afford participants a degree of anonymity and security unattainable through traditional financial channels[41]. As a result, cryptocurrencies have emerged as the preferred medium of exchange for illicit transactions on these platforms, fueling the proliferation of the underground economy and presenting formidable challenges for law enforcement and regulatory agencies worldwide. Darknet marketplaces indeed heavily rely on cryptocurrencies as the preferred mode of payment to ensure anonymity for both buyers and sellers engaging in illicit transactions. The inherent pseudonymity and decentralized nature of cryptocurrencies provide an added layer of protection for participants, making it challenging for law enforcement agencies to trace and identify individuals involved in these illegal activities[40].

Operating on the darknet poses significant hurdles for law enforcement, as the anonymity of the internet makes it difficult to locate and shut down these underground marketplaces. When combined with the use of cryptocurrencies, which further obfuscate transactional details, the task becomes even more daunting. This dual challenge underscores the complexity of combating cybercrime in the digital age, where traditional investigative methods may prove ineffective against sophisticated criminal networks leveraging advanced technologies. Moreover, the transient nature of darknet marketplaces exacerbates the issue of crime displacement. Even if law enforcement successfully shuts down a particular marketplace, new ones can quickly emerge to fill the void, perpetuating the cycle of illicit activities[41]. This

phenomenon poses significant challenges for law enforcement agencies, as it requires constant vigilance and adaptation to stay ahead of evolving criminal tactics.

In the context of drug trafficking on darknet markets, cryptocurrencies play a pivotal role in reducing the costs associated with traditional drug trafficking operations. By concealing their transactions through cryptocurrencies, traffickers can evade detection and mitigate the risks of interception by law enforcement authorities. This dynamic underscores the symbiotic relationship between technology and crime, where advancements in digital currencies enable the proliferation of illegal activities while complicating efforts to combat them effectively[43].

Terrorism Financing

The linkage between cryptocurrencies and terrorism financing has raised significant concerns within the international community. In response to these concerns, the Financial Action Task Force (FATF) issued a comprehensive report in 2015 addressing the risks and threats associated with terrorism financing, with a dedicated section focusing on virtual currencies. The report highlights various aspects of virtual currencies that could appeal to terrorists, underscoring the need for heightened vigilance and regulatory measures to mitigate these risks[8]. Terrorists employ a diverse array of methods to finance their operations, including private donations, non-profit organizations, criminal activities, extortion, kidnappings for ransom, commercial enterprises, and state sponsorship[24]. Each of these methods presents unique challenges, but ultimately, the revenue generated from these activities is channeled to support the terrorist organization's objectives.

The report emphasizes that terrorists utilize both physical and virtual means to obtain funds, with cryptocurrencies emerging as a particularly attractive option due to their pseudonymous

nature and decentralized infrastructure. This enables terrorists to conduct financial transactions with a degree of anonymity, making it difficult for law enforcement agencies to trace the flow of funds and disrupt terrorist financing networks[24].

The funds acquired through these illicit activities serve two primary purposes, as delineated by the "direct operational support" and "broader organizational requirements." Direct operational support refers to the financing of specific terrorist operations, which often require meticulous planning and substantial financial resources[8]. Meanwhile, broader organizational requirements encompass activities such as recruiting, compensating recruits, maintaining infrastructure, and disseminating propaganda to further the terrorist organization's objectives.

Terrorists frequently engage in additional criminal activities, such as kidnappings, drug trafficking, and bank heists, to raise funds for their operations. These illicit activities not only provide a source of revenue but also enable terrorists to diversify their funding sources and minimize their reliance on traditional financing channels, thereby complicating efforts to combat terrorism financing[44]. Traditionally, terrorists have relied on the hawala system for money laundering, a method involving the physical transfer of cash between senders, receivers, and intermediaries. However, this approach can be cumbersome and risky, particularly when dealing with large sums of money. Although the blockchain forensics tools have developed, the terrorists are now using DeFi platforms, mixers and non-custodial wallets to get away with their crimes.[98] With the proliferation of the Internet, terrorists have increasingly turned to cryptocurrencies as a more efficient and discreet means of laundering funds acquired through side crimes. Moreover, cryptocurrencies provide a convenient channel for foreign donors to support terrorist activities without attracting scrutiny from their home country governments[45].

Similarly, the significance of cash in terrorist operations, underscoring the value of digital cash as a clandestine means of transferring funds within a covert group[31]. Terrorists leverage the virtual environment, including virtual worlds and virtual currencies, to conceal their identities, illicit activities, and sources of funding. Operating beyond the reach of traditional law enforcement, terrorists exploit the borderless nature of the Internet to evade detection and law enforcement efforts. Typologies for money laundering and terrorism financing, exploring the feasibility of these crimes in virtual environments such as Second Life and World of Warcraft[45]. While not directly connected to cryptocurrencies, their findings underscore the shift of illicit financial activities online, facilitated by the anonymity and ease of use offered by virtual platforms. Their research identifies similarities and differences in the approaches taken by money launderers and terrorist financiers in virtual worlds, highlighting divergent agendas and strategies. The importance of proactive international cooperation in combating money laundering and terrorism financing in the digital realm[44]. Their work serves as a valuable resource for policymakers seeking to develop effective anti-money laundering (AML) and counter-terrorism financing (CTF) policies tailored to the evolving landscape of online crime.

Cross-border transactions

Cross-border transactions facilitated by cryptocurrencies present unique challenges in bypassing financial controls and sanctions imposed by regulatory authorities[39]. These transactions enable individuals and entities to circumvent traditional banking channels and evade scrutiny, allowing for illicit activities such as money laundering, terrorism financing, and sanctions evasion. One key aspect of cross-border transactions with cryptocurrencies is their decentralized and pseudonymous nature, which obscures the identities of transacting

parties and the origins and destinations of funds[42]. This anonymity undermines the ability of regulatory authorities to monitor and enforce compliance with financial regulations, including sanctions regimes.

Furthermore, cryptocurrencies provide a borderless and frictionless means of transferring value across international boundaries with minimal transaction costs and delays. Unlike traditional banking systems, which may impose restrictions or delays on cross-border transfers, cryptocurrencies enable instantaneous and unrestricted movement of funds, facilitating illicit activities while bypassing financial controls and sanctions. The role of cryptocurrencies in enabling individuals and entities to evade sanctions imposed by governments and international bodies[44]. Transacting in cryptocurrencies, sanctioned individuals and entities can effectively bypass restrictions on access to traditional financial systems, enabling them to continue conducting business and accessing international markets.

Moreover, the global nature of cryptocurrency networks and the absence of centralized oversight make it difficult for regulatory authorities to enforce sanctions effectively. Transactions conducted on decentralized exchanges and peer-to-peer platforms further complicate efforts to monitor and interdict illicit cross-border activities. In response to these challenges, regulatory authorities and international organizations have intensified efforts to enhance oversight and regulation of cryptocurrency transactions to combat illicit cross-border activities. Measures such as enhanced due diligence requirements, Know Your Customer (KYC) regulations, and increased cooperation among law enforcement agencies and financial institutions aim to mitigate the risks associated with cryptocurrencies and strengthen the integrity of the global financial system[30].

The proliferation of cryptocurrencies has facilitated cross-border transactions that bypass financial controls and sanctions, posing significant challenges for regulatory authorities and policymakers seeking to combat illicit activities in the digital realm. Addressing these challenges requires a coordinated and proactive approach involving collaboration among governments, regulatory bodies, and industry stakeholders to develop effective strategies and mechanisms for mitigating the risks associated with cryptocurrencies and preserving the integrity of the international financial system[30]. It calls for an international line of coordinated response, information sharing and the enforcement of global compliance standards in order to properly disrupt these illicit financial flows[99].

Investment and Resource Acquisition:

Investment and resource acquisition through cryptocurrencies have emerged as a significant concern due to their potential role in facilitating the procurement of weapons, supplies, and propaganda tools by illicit actors such as terrorist organizations and criminal groups[45]. Cryptocurrencies offer a decentralized and pseudonymous means of transferring value, enabling individuals and entities to finance their activities with reduced risk of detection and interference from authorities[5]. One area of concern is the use of cryptocurrencies to purchase weapons and supplies on underground marketplaces. These marketplaces operate on the dark web and offer a range of illicit goods, including firearms, explosives, and military equipment. The prevalence of online forums and marketplaces where individuals can anonymously purchase weapons using cryptocurrencies, posing a significant challenge to law enforcement efforts to disrupt illegal arms trafficking networks[22].

Additionally, cryptocurrencies facilitate the acquisition of supplies and materials needed for various illicit activities, such as drug manufacturing, human trafficking, and cybercrime[39]. By

enabling anonymous transactions, cryptocurrencies enable individuals and groups to procure equipment, chemicals, and other resources without leaving a trace, complicating efforts to interdict and investigate illicit operations. Furthermore, cryptocurrencies are used to finance propaganda campaigns and disseminate extremist ideologies through online channels. Terrorist organizations and extremist groups leverage social media platforms, websites, and messaging apps to spread their message and recruit followers[36]. Cryptocurrencies provide a convenient and discreet means of funding these activities, allowing supporters to donate funds without revealing their identities or the source of their contributions.

2.1.12 Consequences of Terrorism Funding

Expanding on the consequences of terrorism funding, the impact extends far beyond mere financial transactions. One major consequence is the loss of innocent lives and the destruction of infrastructure. Terrorist organizations often utilize the funds they acquire through various means to orchestrate attacks that result in both immediate casualties and long-term social and economic devastation.

For instance, in Nigeria, the Boko Haram terrorist group has perpetrated numerous bombings, kidnappings, and assaults on schools, leading to the deaths of thousands and the displacement of millions[45]. These attacks not only claim lives but also instill fear and insecurity within communities, hindering development and exacerbating socio-economic disparities.

Moreover, the ripple effects of terrorism funding are profound, impacting sectors such as healthcare, education, and infrastructure. Scarce resources that could have been allocated to essential services are diverted towards security measures and counterterrorism efforts, straining already fragile economies and exacerbating poverty and inequality[37]. Additionally,

the destruction of critical infrastructure further hampers socio-economic development and impedes efforts to rebuild and recover from the devastation wrought by terrorist attacks. Expanding on the ramifications of terrorism funding, it's evident that it fuels a vicious cycle of violence and instability, which in turn obstructs peace-building endeavors. The proliferation of arms and the militarization of conflict zones serve to perpetuate this cycle, resulting in increased loss of life and the displacement of populations[37].

Terrorist organizations, flush with funds from various illicit sources, invest heavily in acquiring weapons and ammunition to sustain their operations. These arms often find their way into conflict zones, exacerbating existing tensions and intensifying violence. For example, in regions like the Sahel, terrorist groups such as Al-Qaeda in the Islamic Maghreb (AQIM) and Boko Haram have capitalized on terrorism funding to procure sophisticated weaponry, prolonging conflicts and inflicting widespread suffering on civilian populations[23]. The militarization of conflict zones not only escalates violence but also hampers efforts to achieve peace and reconciliation. The presence of armed groups, fueled by terrorism financing, creates an environment of fear and insecurity, making it difficult for communities to trust in peace processes and engage in dialogue. Moreover, the influx of weapons prolongs conflicts, making resolution elusive and exacerbating the suffering of affected populations[25].

Furthermore, the cycle of violence perpetuated by terrorism funding undermines social cohesion and trust within communities. The prevalence of armed conflict erodes social bonds and fractures communities along ethnic, religious, and sectarian lines. This fragmentation impedes efforts to foster reconciliation and build resilient societies capable of withstanding the challenges posed by extremism[44].

One of consequence of terrorism funding is the destabilization of governments and regions. By providing financial support to extremist groups, individuals or organizations can manipulate power dynamics and contribute to political and social unrest. This not only hampers governance and stability but also poses significant challenges to international peace and security[39]. The infusion of funds into extremist groups empowers them to challenge the authority of established governments and undermine state institutions. These groups may exploit grievances within marginalized communities, exploiting them for recruitment and support. As a result, governments may find themselves grappling with internal strife, insurgency, and armed conflict, further exacerbating instability and hindering efforts towards democratization and development[45].

Additionally, terrorism funding can lead to the development of criminal networks and illicit activities. Terrorist organizations often engage in money laundering, drug trafficking, and smuggling to sustain their operations and secure funding[21]. These activities not only harm the economy but also create an environment conducive to corruption and organized crime. The involvement of terrorist groups in illicit activities not only provides them with the financial resources to perpetrate violence but also undermines the rule of law and erodes public trust in institutions. Furthermore, the convergence of terrorist and criminal networks blurs the lines between political violence and organized crime, posing significant challenges to law enforcement and security agencies tasked with combating both threats[35].

Moreover, the proliferation of illicit activities fueled by terrorism funding can have far-reaching consequences beyond national borders. Transnational criminal networks, enabled by globalization and technological advancements, pose a threat to global security and stability. The trafficking of drugs, weapons, and humans, facilitated by terrorist organizations,

undermines efforts to promote peace and prosperity and perpetuates cycles of violence and instability in regions across the globe[34]. The consequences of terrorism funding extend beyond immediate security concerns to encompass governance, stability, and economic development. Addressing terrorism financing requires a multifaceted approach that targets not only the financial networks that sustain terrorist organizations but also the underlying socio-economic and political factors that fuel extremism and enable illicit activities to flourish. The consequences of terrorism funding are far-reaching and demand global attention and collaboration in order to effectively combat this threat.

2.1.13 Regulation of Cryptocurrency

Global Perspectives

As a new fintech phenomenon, cryptocurrency regulation is still being explored in countries around the world, and the regulators show a trend of diversification, with some acting as securities regulators and others as central banks, and the introduction of regulatory policies is relatively frequent. By summarizing the development of crypto-digital regulation in the U. S., the establishment of regulators, policies, and enforcement of regulation[46]. China should take the U. S. federal securities law as a mirror and can start with the Securities Act to refine more precise and appropriate regulatory rules and approaches according to the characteristics of cryptocurrencies themselves[46]. On the other hand, summarizes two paths: one is the interpretive path, and the other one is the legislative path. The interpretive path emphasizes integrating cryptocurrencies into the existing AML system and formulating special AML departmental regulations to clarify the contents of laws and regulations; the legislative path focuses on adopting a comprehensive regulatory approach and formulating a Cryptocurrency

Law or a Virtual Currency Law to stipulate the contents of AML[47]. Reference can be made to the practice in Germany to clarify the attribution of taxable types arising from cryptocurrency transactions through notices or guiding cases from governmental authorities and subsume them under the existing taxation in China. This is beneficial to the stability of China's overall tax system on the one hand, and on the other hand, it can adapt to the rapid development of the cryptocurrency market by flexibly classifying the trading activities of cryptocurrencies such as Bitcoin into the original tax system, so that China's tax system presents openness and inclusiveness[47].

Accurate targeting of regulation

The target of tax authorities' tax regulation of cryptocurrencies should shift from users to intermediaries and third-party reporting platforms[48]. Currently, the scale of cryptocurrency transactions is getting larger and larger, and transaction intermediaries are springing up. Because intermediaries and third-party reporting platforms are important nodes to connect users of cryptocurrency transactions, well-functioning intermediaries and thirdparty reporting platforms will in turn facilitate cryptocurrency users to regulate their transactions, which is a feasible strategy given the current technical challenges.

Reporting Platforms

It makes sense to establish a third-party reporting platform by referring to the practices of countries such as the United States[34]. All taxpayers registered on the platform should undergo due diligence and fill in basic data, while the third-party reporting platform should keep basic data records of all taxpayers. Of course, such data records are not compulsory for the platform to report to the tax authorities. At the request of taxpayers, platform parties are obliged to provide their transaction records to taxpayers, which can help taxpayers to calculate the

taxable amount. Thus, the establishment of a third-party reporting platform both facilitates the work of tax authorities and assists them in their supervisory role. Although the principle of fairness requires that all income of taxpayers should be reported, considering the reality of China, taxpayers reporting all data will greatly increase the pressure of examination by tax authorities[47].

To make the reporting information manageable, tax authorities can stipulate that only taxable activities exceeding a preset threshold and taxable activities with suspicious patterns are reported to the tax authorities. Since transaction results and data are stored on different trading platforms and third-party payment platforms, regulatory policies for third-party reporting platforms are central to platform construction. The establishment and regulation of cryptocurrency trading platforms in the EU, the US, and Canada. Cryptocurrency trading platforms in the U. S. are required to register with the Securities and Exchange Commission or seek exemptions; Canada requires bitcoin and cryptocurrency operating companies to enforce customer identification, transaction record keeping, and monitoring funds to report suspicious transactions; and the Japanese government includes virtual currency trading platforms, including bitcoin, in its anti-money laundering regulatory system, adopting a registration system to review and regulate[24,34,48].

2.1.14 Nigeria Perspectives

In Nigeria, the regulation of cryptocurrency has been a topic of significant interest and debate in recent years, reflecting the growing adoption of digital currencies and the need for regulatory clarity in the emerging cryptocurrency market[48]. The Central Bank of Nigeria (CBN) has been at the forefront of regulating cryptocurrency activities within the country, issuing directives and guidelines to address various concerns related to consumer protection,

financial stability, and anti-money laundering (AML) efforts. One of the key regulatory actions by the CBN was the issuance of a circular in 2017, which cautioned financial institutions and the general public about the risks associated with cryptocurrencies and warned against their use in the Nigerian financial system[48]. The circular highlighted concerns such as money laundering, terrorism financing, and the lack of regulatory oversight in the cryptocurrency market.

Despite the CBN's cautionary stance, cryptocurrency adoption has continued to grow in Nigeria, driven by factors such as financial inclusion, remittance inflows, and investment opportunities. In response to this trend, the Securities and Exchange Commission (SEC) of Nigeria announced plans to regulate digital assets and initial coin offerings (ICOs) in 2020, recognizing the need for a more comprehensive regulatory framework to govern cryptocurrency activities. In 2021, the SEC released guidelines for the regulation of crypto assets, categorizing cryptocurrencies and token offerings into various classifications based on their structure and use cases[48,49]. The regulatory framework aims to provide clarity for market participants, protect investors from fraud and scams, and promote the responsible development of the cryptocurrency industry in Nigeria[50]. Most of its efforts to ban cryptocurrency transactions, such as the Central Bank of Nigeria's 2021 directive forbidding them, were designed to limit money laundering, financing of terrorism, and speculative activities, but drove the market into the toughest of them all: the informal peer-to-peer networks where oversight is the weakest.[100] While the aim here is to protect the financial system, it has also been an obstacle to innovation and widened the distance between Nigeria and global best practices.

However, the regulatory landscape for cryptocurrency in Nigeria remains complex and subject to ongoing developments. Challenges such as regulatory overlaps between different government agencies, enforcement issues, and the need for international cooperation to address cross-border cryptocurrency activities continue to pose significant hurdles to effective regulation. Moving forward, achieving a balance between promoting innovation and safeguarding against potential risks will be crucial for the regulation of cryptocurrency in Nigeria. Nigeria has to go beyond mere prohibition to a balanced regulatory model that will enable the growth of digital innovation while managing the inevitable risks.[101] This will require ongoing collaboration between regulators, industry stakeholders, and the broader community to develop a regulatory framework that fosters responsible innovation while protecting the interests of investors and maintaining the integrity of the financial system.

2.1.14 Kenya Perspectives

The regulation of cryptocurrency in Kenya has evolved gradually as the country grapples with balancing innovation and risk mitigation. As one of Africa's leaders in financial technology (fintech), Kenya's experience with platforms like M-Pesa has laid the groundwork for exploring digital currencies. However, the rise of cryptocurrencies presents unique challenges due to their decentralized nature and potential misuse in illicit activities such as money laundering and terrorism financing. Initially, Kenyan authorities approached cryptocurrencies with caution. In 2015, the Central Bank of Kenya (CBK) issued a public warning advising citizens against using virtual currencies, citing risks related to fraud, hacking, and lack of consumer protection[51]. This cautious stance was rooted in concerns about the unregulated nature of cryptocurrencies and their potential to destabilize the formal financial system.

Despite this early skepticism, the CBK acknowledged the need for further study into the benefits and drawbacks of digital currencies.

In recent years, Kenya has taken significant steps toward regulating cryptocurrencies while fostering innovation. A notable milestone came in 2023 when the CBK introduced regulations requiring cryptocurrency exchanges to register with the central bank and comply with anti-money laundering (AML) and counter-terrorism financing (CFT) protocols[49]. These regulations aim to enhance transparency and accountability within the crypto sector by mandating Know Your Customer (KYC) procedures and transaction monitoring. Additionally, the Kenyan government established a task force in 2019 to explore the feasibility of adopting blockchain technology and digital currencies. The task force's report recommended a phased approach to integrating blockchain into public services while ensuring regulatory safeguards^3^. This strategic framework reflects Kenya's commitment to leveraging emerging technologies responsibly.

Despite these regulatory advancements, several challenges persist. The absence of harmonized regulations across East Africa complicates efforts to monitor cross-border transactions involving cryptocurrencies, creating opportunities for malicious actors to exploit jurisdictional differences[23]. Furthermore, law enforcement agencies and financial institutions often lack the technical expertise required to track and investigate illicit cryptocurrency transactions. Public awareness and education also remain critical issues, as many Kenyans are unaware of the risks associated with cryptocurrencies, making them vulnerable to scams and fraudulent schemes.

Kenya's regulatory efforts are increasingly aligned with global standards set by organizations such as the Financial Action Task Force (FATF). For instance, the FATF's guidance on

virtual assets and service providers (VASPs) has significantly influenced Kenya's approach to regulating cryptocurrency exchanges[7]. Moreover, Kenya participates in regional initiatives led by the East African Community (EAC) to promote collaboration on fintech regulation and cybersecurity. Academic research highlights the dual nature of cryptocurrencies in Kenya. On one hand, they offer opportunities for financial inclusion and economic growth. A study notes that cryptocurrencies could help reduce remittance costs for Kenyans receiving funds from abroad. On the other hand, scholars warn of the risks posed by inadequate regulation, particularly in terms of terrorism financing and money laundering[9].

2.1.1.4 Strategies to Combat Terrorism Funding

Global cooperation and collaboration

International cooperation and teamwork are key measures in combating terrorism funding[51]. Given the transnational nature of terrorism financing, it is imperative for nations to collaborate in order to dismantle the economic systems that sustain these operations. Cooperation between intelligence agencies, law enforcement agencies, and financial institutions can facilitate the exchange of information and the detection of potentially illicit financial activities[52,53]. Moreover, the implementation of international accords and conventions can be utilised to bolster collaboration in the fight against terrorism financing. The Financial Action Task Force (FATF) has created a comprehensive framework of standards and recommendations that nations can use in order to effectively address the issues of money laundering and terrorist financing[34]. Countries can successfully impede the transfer

of funding to terrorist organisations by implementing these measures and engaging in collaboration with other governments.

Over the past few years, terrorist groups like the 'Islamic State' and the Taliban have expanded their presence to neighbouring regions[53]. Consequently, the militants they have trained have come back to their respective nations, disseminating radical ideologies and posing a security risk to the surrounding countries. Close international collaboration is necessary to combat terrorist financing due to the transnational mobility of terrorism[54]. Furthermore, a notable benefit of bitcoin is its ability to facilitate swift cross-border financial transactions. Hence, it is imperative to establish a platform for sharing information in order to effectively combat the use of cryptocurrencies for terrorist financing. By ratifying bilateral or multilateral treaties, we can facilitate the efficient advancement of counterterrorism finance among nations.

Enhancing the Oversight of International Organisations and Nations

Cryptocurrency refers to a form of digital currency. The Financial Action Task Force (FATF) classifies virtual money into two categories: centralised virtual currency and decentralised virtual currency. Decentralised virtual currency refers to a distributed, open-source, and mathematical peer-to-peer virtual currency. Recently, the FATF has closely monitored the progress of virtual currencies. In June 2014, the FATF released a publication titled 'Virtual Currency: Key Definition and Potential AML/CFT Risk' in reaction to the rise of virtual currency and its associated payment methods. This publication provides clear definitions of words linked to virtual currency and examines the potential financial risks it poses[8]. In October 2018, the Financial Action Task Force (FATF) suggested the adoption of the term 'virtual asset', which encompasses any form of digital representation of value that can be

exchanged, transferred, or utilised for transactions. It lacks a numerical depiction of legal currencies[34]. In October 2020, the revised international standards on combating money laundering, terrorist financing, and proliferation provided clear guidelines in Article 15 regarding virtual assets[34]. These guidelines emphasise that countries should actively identify, assess, and comprehend the risks associated with money laundering and terrorist financing that may arise from the activities or operations involving virtual assets and virtual asset service providers. Furthermore, it is recommended that all nations implement effective measures to ensure compliance with anti-money laundering and counter-terrorism financing regulations, thereby mitigating the danger of illicit financial activities and funding of terrorist activities[34]. The FATF has just published a paper in September 2020 that outlines the risk indicators associated with virtual assets. This research aims to assist financial institutions, non-financial organisations, and virtual asset service providers in detecting and addressing potential risks related to terrorist financing and money laundering activities involving virtual assets. Additionally, it offers valuable data for financial intelligence, law enforcement agencies, prosecutors, and regulators to scrutinise suspicious transaction reports or oversee adherence to AML and ATF standards. The risk indicators outlined in the study encompass the technical feature of enhancing anonymity, atypical transaction patterns, unexplained transaction volumes, and monies originating from criminal activities[54]. The research aims to assist the financial sector in doing customer due diligence to prevent the illicit utilisation of virtual assets by terrorist organisations. International organisations, particularly FATF, offer action instructions to countries for combating terrorist financing through the proposal and evaluation of cryptocurrencies. This would effectively diminish the anonymity of bitcoin and impede the illicit fundraising activities of terrorist organisations. Teichmann and The

Liechtenstein Blockchain Act should serve as a standard for lawmakers to enhance the regulation of blockchain in a more efficient manner[54]. This establishes a benchmark for the oversight of cryptocurrencies through domestic law enforcement organisations.

Sustained Progress in Conventional Methods of Finance

Due to the advancement of the global economy and technology, the methods of terrorist financing have become increasingly diverse and intricate. Terrorist organisations frequently employ a variety of tactics to enhance the confidentiality of their financing and mitigate the danger of detection, adapting their approach based on the prevailing conditions in the location[56]. As previously said, governmental sponsorship serves as a significant financial resource for terrorist organisations. Hezbollah relies substantially on financial support from Iran's government, along with money earned from criminal activities and charitable contributions. Under the US sanctions imposed on Iran, Iran's national funds experienced a decline[49].

However, following the suspension of sanctions after 2018, Iran's financial support to Hezbollah rebounded[51]. Additionally, terrorist organisations have alternative means to generate funds, including engaging in legitimate business operations, receiving donations from individuals and non-profit organisations, obtaining contributions from charities, and engaging in illicit trafficking of cultural artefacts. Terrorist financing methods are not uniform but varied. The continued significance of traditional financing mechanisms in maintaining stability, coupled with their lack of major disruption, will likely result in a fall in the potential for terrorist organisations to finance themselves through Bitcoin[29]. Specifically, when the reliability of newly developed cryptocurrencies is uncertain, terrorist organisations face

challenges in selecting risky cryptocurrencies. For instance, as countries tighten regulations on cryptocurrencies, numerous locations that previously facilitated cryptocurrency trading have suffered significant setbacks, resulting in financial losses for some users. In the realm of cryptocurrencies, the destruction of the computer system renders the capital more susceptible to loss. During the initial stages of Bitcoin's creation, there were numerous cases of computer viruses illicitly acquiring bitcoins, leaving users solely responsible for the resulting losses.

Enforce the Worldwide Standards set by FATF for Anti-Money Laundering and Countering the Financing of Terrorism

The Financial Action Task Force (FATF) has made a significant and impactful contribution to the global efforts in combating the financing of terrorism, resulting in noteworthy achievements[34]. Under the new circumstances, the FATF can promptly address the utilisation of cryptocurrencies by terrorist groups and propose a range of recommendations and initiatives that hold significant importance for security. The FATF periodically assesses the implementation of its guidelines and offers guidance to nations with inadequate finance systems to effectively combat terrorism. Currently, the majority of countries worldwide lack effective oversight of virtual assets and do not fully comprehend the potential implications of bitcoin in facilitating terrorist financing. In order to ensure national security and promote stable development, it is imperative for all countries to rigorously adhere to the criteria set by the Financial Action Task Force (FATF) and actively engage in international cooperation to effectively combat terrorism[8]. The efficacy of law enforcement is noteworthy. Due to the overall lack of comprehension among the public regarding the emerging form of cryptocurrency crime, individuals may choose not to report incidents resembling theft or

extortion, as they perceive the authorities to be incapable of providing assistance[24].

Enhance the Efficacy of Monetary Policy and Enhance the Desirability of Legal Currency

The primary objective of the central bank should be to optimise the efficiency of monetary policy and increase the desirability of domestic legal currencies[57]. As an illustration, the central bank has the ability to create its own digital token to complement physical cash and bank reserves based on the specific circumstances of its country. Subsequently, it can facilitate peer-to-peer transactions in a decentralised manner by encrypting assets, thereby enhancing the digital compatibility of the central bank's currency. In response to the influence of cryptocurrency on traditional currency, the most effective strategy for central banks is to consistently implement efficient monetary policies and remain receptive to new ideas and demands as the economy evolves[57]. This technology can help enhance the development of the central bank's monetary policy formulation. For instance, the central bank can enhance its economic projection by utilising big data, artificial intelligence, and machine learning to effectively address the conflict between cryptocurrencies and fiat money[58]. Enhancing the competitiveness of legal tenders and decreasing the market size of cryptocurrencies will diminish the acceptance of cryptocurrency and erode the trust of terrorist organisations.

2.1.15 Terrorism Funding through Cryptocurrency and Implications for International Relations

The utilization of cryptocurrency by terrorist organizations has emerged as a significant challenge in the realm of global security and international relations, particularly between 2018

and 2024. Cryptocurrency, with its decentralized nature and pseudonymous transactions, has provided terrorist groups with a means to raise and transfer funds while evading traditional financial surveillance measures. This phenomenon has raised concerns among governments worldwide about the potential implications for national security, diplomatic relations, and international stability. In this context, both global and national efforts have been directed towards understanding and addressing the multifaceted challenges posed by cryptocurrency-enabled terrorism financing. This paper explores the diplomatic, regulatory, and technological dimensions of the issue, examining occurrences and responses both globally and within the Nigerian context. By delving into these complexities, we aim to shed light on the evolving landscape of cryptocurrency-related terrorism financing and the implications for international relations.

Sovereignty and Jurisdictional Challenges:

The decentralization of cryptocurrency, facilitated by blockchain technology, has indeed posed significant challenges to sovereignty and jurisdiction, both globally and within Nigeria. In the global context, cryptocurrency transactions operate independently of traditional financial systems and national borders, challenging the sovereignty of states. For example, the proposal of the digital currency Libra by Facebook in 2019 raised concerns among global policymakers about its potential impact on monetary sovereignty. This initiative prompted discussions on how such a currency could potentially undermine the control of national governments over their monetary policies[59].

Moreover, the cross-border nature of cryptocurrency transactions has complicated jurisdictional enforcement efforts. In the 2020 Twitter hack, where Bitcoin was used in a high-profile scam, the involvement of multiple jurisdictions made it challenging for law enforcement agencies to coordinate investigations effectively. The lack of a centralized authority overseeing cryptocurrency transactions exacerbates these challenges, as no single entity can enforce regulatory measures uniformly across different jurisdictions. Consequently, perpetrators of cryptocurrency-related crimes can exploit this decentralized nature to evade detection and prosecution, further complicating efforts to combat financial crimes on a global scale[60].

To address these challenges, governments worldwide have struggled to develop coherent regulatory frameworks for cryptocurrencies. For instance, the European Union introduced the Fifth Anti-Money Laundering Directive in 2018, aiming to regulate cryptocurrency exchanges and wallet providers to combat money laundering and terrorist financing. This directive marked a significant step towards incorporating cryptocurrency transactions into existing regulatory frameworks, albeit with varying degrees of success and implementation across EU member states[61].

Turning to the Nigerian context, the decentralized nature of cryptocurrency has raised similar concerns about the government's ability to regulate and control financial activities. In 2021, the Central Bank of Nigeria (CBN) issued a directive prohibiting banks from servicing cryptocurrency exchanges, citing concerns about money laundering and terrorism financing. This move reflected the Nigerian government's efforts to assert control over the cryptocurrency market and mitigate potential risks to financial stability and national security.

However, it also sparked debates about the impact of such regulations on innovation and financial inclusion in Nigeria's burgeoning cryptocurrency sector[60].

Furthermore, the cross-border nature of cryptocurrency transactions has made it difficult for Nigerian law enforcement agencies to combat cybercrime and financial fraud effectively. In 2020, the Nigerian Economic and Financial Crimes Commission (EFCC) reported an increase in cryptocurrency-related scams, highlighting the challenges of jurisdictional enforcement in the digital age[62]. The anonymity and pseudonymity afforded by cryptocurrency transactions have enabled perpetrators to operate across borders with impunity, evading detection and prosecution by Nigerian authorities.

In response to these challenges, Nigerian regulators have taken various measures to regulate the cryptocurrency sector. In 2020, the Securities and Exchange Commission (SEC) of Nigeria announced plans to regulate cryptocurrencies and Initial Coin Offerings (ICOs) as securities, aiming to protect investors and ensure market integrity. This regulatory framework represents an attempt to strike a balance between fostering innovation in the cryptocurrency sector and safeguarding the interests of Nigerian investors and consumers. However, the effectiveness of these regulations remains to be seen, as the cryptocurrency landscape continues to evolve rapidly in response to changing market dynamics and regulatory environments[62].

These examples underscore the complex interplay between cryptocurrency, sovereignty, and jurisdiction, both globally and within Nigeria. As governments and regulators grapple with the implications of cryptocurrency for financial stability and security, there is a pressing need for international cooperation and coordinated regulatory responses to address these challenges

effectively. Failure to do so risks undermining the integrity of the global financial system and compromising efforts to combat financial crimes and terrorism financing on a global scale.

Disruption of Illicit Funding Channels:

Between 2018 and 2024, the utilization of cryptocurrency by terrorist organizations has presented significant challenges to global security efforts. Cryptocurrency has emerged as a convenient and relatively secure means for terrorist groups to raise and transfer funds, undermining international efforts to disrupt illicit funding channels. This trend has been observed globally, with terrorist organizations leveraging the anonymity and pseudonymity afforded by cryptocurrency transactions to evade detection and circumvent traditional financial surveillance measures[63].

Anonymity and pseudonymity play critical roles in facilitating terrorist financing through cryptocurrency. By exploiting the decentralized nature of blockchain technology, terrorist groups can obscure their financial activities, making it challenging for law enforcement agencies to track the flow of funds. Privacy-focused cryptocurrencies or mixing services further complicate efforts to trace transactions, allowing terrorist organizations to operate with increased impunity[59].

The rise of cryptocurrency-related terrorism financing has prompted increased global coordination and response efforts. Organizations such as the Financial Action Task Force (FATF) have issued guidance and recommendations to help member countries combat the illicit use of cryptocurrency for terrorist financing. Emphasis has been placed on enhanced due diligence and information sharing among governments, law enforcement agencies, and international organizations to mitigate the risks associated with terrorist financing[54].

In the Nigerian context, terrorist organizations like Boko Haram have reportedly exploited cryptocurrency to finance their operations and evade detection by security agencies. Reports indicate that Boko Haram affiliates have used cryptocurrency platforms to solicit donations from sympathizers and supporters, leveraging social media channels and online forums to propagate their extremist ideology and solicit financial support[62]. This has raised concerns among Nigerian authorities about the potential for cryptocurrency to facilitate terrorist activities and undermine national security efforts[63].

In response to the emerging threat posed by cryptocurrency-related terrorism financing, Nigerian regulatory authorities have taken steps to enhance oversight and regulation of the cryptocurrency sector. The Central Bank of Nigeria (CBN) issued directives to financial institutions, warning them against facilitating cryptocurrency transactions and emphasizing the need for enhanced due diligence and compliance with anti-money laundering (AML) regulations[63]. Additionally, the Nigerian Financial Intelligence Unit (NFIU) has strengthened its monitoring and surveillance capabilities to detect and disrupt suspicious cryptocurrency transactions linked to terrorist financing activities[34].

These examples underscore the evolving threat landscape posed by cryptocurrency-related terrorism financing and the efforts undertaken by both global and Nigerian authorities to address these challenges. As terrorist organizations continue to exploit cryptocurrency for illicit purposes, enhanced international cooperation, regulatory frameworks, and technological solutions will be essential to counter these threats effectively.

Technological Innovation and Regulatory Adaptation:

The emergence of cryptocurrency as a tool for terrorism financing has become increasingly prominent between 2018 and 2024, highlighting the necessity for technological innovation and regulatory adaptation within the realm of international relations. This period witnessed numerous instances globally and within Nigeria that underscored the urgency of addressing this issue.

Cryptocurrency Exploitation by Terrorist Organizations: Terrorist groups globally, including ISIS and others, have exploited cryptocurrency to finance their operations and evade traditional financial surveillance. For instance, reports have revealed instances where ISIS solicited donations and facilitated financial transactions through cryptocurrency platforms and encrypted messaging services, leveraging the anonymity and pseudonymity provided by these digital assets[23].

Governments and regulatory authorities have faced significant challenges in monitoring and regulating cryptocurrency transactions effectively. The decentralized nature of blockchain technology has made it difficult to trace and monitor these transactions, posing challenges to traditional regulatory frameworks. However, regulatory bodies such as the Financial Action Task Force (FATF) have issued guidance and recommendations to combat the illicit use of cryptocurrency for terrorist financing, emphasizing the importance of enhanced due diligence and information sharing among member countries[34].

To address the challenges posed by cryptocurrency-related terrorism financing, governments and regulatory authorities have recognized the importance of technological innovation and regulatory adaptation. Efforts have been made to foster innovation in blockchain technology to enhance transparency and accountability in financial transactions. Additionally, there has

been a push for the development of standardized frameworks for regulating cryptocurrency exchanges and preventing their exploitation by terrorist organizations[48].

In Nigeria, terrorist organizations such as Boko Haram have reportedly exploited cryptocurrency to finance their operations and evade detection by security agencies. Reports have indicated instances where Boko Haram affiliates used cryptocurrency platforms to solicit donations and propagate their extremist ideology through social media channels and online forums[62].

Regulatory Responses: In response to the emerging threat posed by cryptocurrency-related terrorism financing, Nigerian regulatory authorities have taken steps to enhance oversight and regulation of the cryptocurrency sector. The Central Bank of Nigeria (CBN) issued directives to financial institutions, warning them against facilitating cryptocurrency transactions and emphasizing the need for enhanced due diligence and compliance with anti-money laundering regulations[63]. Additionally, the Nigerian Financial Intelligence Unit (NFIU) has strengthened its monitoring and surveillance capabilities to detect and disrupt suspicious cryptocurrency transactions linked to terrorist financing activities[62]. Effective regulation, technological innovation, and international cooperation are crucial to combatting this evolving threat effectively.

Diplomatic Implications:

The use of cryptocurrency by terrorist organizations has indeed presented diplomatic challenges for governments worldwide, particularly between 2018 and 2024. This period has

seen numerous occurrences globally and within Nigeria that underscore the diplomatic ramifications of cryptocurrency-enabled terrorism financing.

The emergence of cryptocurrency as a tool for terrorism financing has raised diplomatic tensions among states grappling with the dual imperatives of safeguarding national security and upholding international norms and principles. Governments have faced pressure to balance their obligations under international law with the imperative to protect their citizens from terrorist threats facilitated by cryptocurrency. These tensions have manifested in diplomatic exchanges and negotiations, as states seek to coordinate efforts to combat cryptocurrency-enabled terrorism financing while respecting each other's sovereignty and jurisdiction[64].

The proliferation of cryptocurrency-related crimes, including terrorism financing, has strained diplomatic relations between countries, leading to mutual suspicion and mistrust. Instances of terrorist organizations exploiting cryptocurrency platforms have heightened concerns among governments about the potential misuse of digital assets for illicit activities. This has resulted in increased scrutiny of cross-border cryptocurrency transactions and exchanges, further exacerbating diplomatic tensions[65].

In Nigeria, the government has engaged in diplomatic efforts to address the challenges posed by cryptocurrency-enabled terrorism financing. Nigerian authorities have collaborated with international partners and organizations such as the Financial Action Task Force (FATF) to strengthen regulatory frameworks and enhance cooperation in combating illicit financial activities, including terrorism financing. These diplomatic engagements have focused on information sharing, capacity building, and joint enforcement actions to mitigate the risks associated with cryptocurrency-related crimes[54].

Impact on Bilateral Relations: The proliferation of cryptocurrency-related crimes in Nigeria has had implications for bilateral relations with other countries. Instances of terrorist organizations exploiting cryptocurrency platforms have raised concerns among Nigeria's international partners about the effectiveness of its regulatory measures and enforcement actions. This has prompted diplomatic dialogues and engagements aimed at addressing gaps in Nigeria's regulatory framework and enhancing cooperation in combating cryptocurrency-enabled terrorism financing[34].

2.1.16 Impact of Cryptocurrency Usage on the Global Security Landscape

The impact of cryptocurrency usage on the global security landscape is a multifaceted issue that encompasses various dimensions of security, including financial, cyber, and geopolitical security. As the adoption of cryptocurrencies continues to rise, so too do concerns about their implications for security at the international level[65]. This expansion of cryptocurrency usage has prompted scholars and policymakers to explore its potential effects on global security dynamics.

Conceptually, the utilization of cryptocurrencies introduces both opportunities and challenges to the global security landscape[66]. On one hand, cryptocurrencies offer benefits such as increased financial inclusion, lower transaction costs, and greater privacy for users. However, these same characteristics also make cryptocurrencies attractive to malicious actors seeking to evade detection and engage in illicit activities, including terrorism financing, money laundering, and cybercrime. Therefore, understanding the impact of cryptocurrency usage on global security requires a nuanced analysis that considers both its positive and negative implications.

In the international literature review, scholars have examined the diverse ways in which cryptocurrency usage intersects with global security concerns. Some studies have focused on the role of cryptocurrencies in facilitating illicit activities, highlighting their potential to undermine financial stability and national security. For example, research has shown how terrorist organizations exploit cryptocurrencies to raise and transfer funds anonymously, posing challenges to counter-terrorism efforts worldwide[67].

In addition to its implications for financial security and terrorism financing, cryptocurrency usage has also been closely linked to various cyber threats, posing significant challenges to cybersecurity on a global scale. Studies, such as those conducted, have delved into these linkages, highlighting how cryptocurrencies have become a tool of choice for malicious actors engaged in activities such as ransomware attacks, hacking incidents, and cryptocurrency-related fraud. Ransomware attacks, for instance, involve the use of malicious software to encrypt data on victims' computers, with attackers demanding payment in cryptocurrencies for the decryption keys[68].

Similarly, hacking incidents targeting cryptocurrency exchanges and wallets have resulted in the theft of millions of dollars' worth of digital assets. Furthermore, cryptocurrency-related fraud schemes, including Ponzi schemes and initial coin offering (ICO) scams, have exploited investors' lack of knowledge and regulatory oversight to defraud them of their funds. These cyber threats not only undermine the integrity and security of digital assets but also have broader implications for global cybersecurity, requiring concerted efforts from governments, businesses, and cybersecurity experts to mitigate their impact and safeguard the digital economy[28].

Furthermore, scholars have analyzed the geopolitical dimensions of cryptocurrency usage, considering how the proliferation of cryptocurrencies may influence international relations and strategic dynamics among states. Some studies have examined the regulatory responses of governments and international organizations to address the security risks associated with cryptocurrencies, highlighting the need for coordinated action and cross-border cooperation[33]. Others have explored the potential implications of state-sponsored cryptocurrency initiatives, such as central bank digital currencies (CBDCs), on the global monetary system and geopolitical power dynamics[24].The international literature review on the impact of cryptocurrency usage on the global security landscape provides valuable insights into the complex interplay between technology, finance, and security in the contemporary world.

2.2 Theoretical Framework

In the context of "Terrorism Funding and Cryptocurrency: Implications for International Relations (2018-2024)," Social Network Theory (SNT) serve as the primary theoretical framework. SNT offers a comprehensive approach to understanding the structure and dynamics of terrorist funding networks, including the role of cryptocurrency transactions within these networks[69]. By employing SNT, researchers can analyze the relationships between various actors involved in terrorist financing, map the flow of funds, and identify key nodes and weak ties within the network.

On the other hand, Game Theory complement the study by providing insights into strategic interactions between different actors, such as governments, financial institutions, and terrorist organizations. Game Theory can help researchers analyze the strategic decisions made by these actors in response to changes in the funding landscape, including the adoption of

cryptocurrency for illicit purposes. By integrating Game Theory into the study, researchers can explore how different actors' strategies impact the overall dynamics of terrorist financing and inform policy recommendations for countering these threats effectively. Therefore, while SNT serves as the primary framework for understanding the structural aspects of terrorist funding networks and the role of cryptocurrency within them, Game Theory complements the analysis by examining strategic interactions and decision-making processes among relevant stakeholders.

2.2.1 Social Network Theory

Social Network Theory, founded in the mid-20th century, emerged from the interdisciplinary field of sociology and social psychology. The theory had its roots in the works of James S. Coleman in the 1950s, and offers a powerful lens to examine the structure and dynamics of relationships within terrorist organizations and their funding networks[69]. While it doesn't have a single founder, scholars like Georg Simmel, Jacob Moreno, and Stanley Milgram laid the groundwork for its development. However, it was the work of sociologists like Mark Granovetter, Harrison White, and Ronald Burt in the late 20th and early 21st centuries that expanded and refined the theory.

Social Network Theory examines the relationships and interactions between actors within a network, whether they are individuals, groups, organizations, or states. It posits that these connections shape individuals' behaviors, beliefs, and actions, influencing outcomes within the network and beyond. Key concepts include nodes (individual actors), ties (connections between nodes), and network structures (patterns of connections)[70].

Social Network Theory, originating in the mid-20th century, has been shaped by the contributions of various scholars. Mark Granovetter's seminal work, "The Strength of Weak

Ties", introduced the concept of weak ties, highlighting how connections between individuals from different social circles facilitate the flow of new information and resources[71]. Ronald Burt expanded on this with his work "Structural Holes: The Social Structure of Competition", which emphasized the significance of structural holes in networks. These gaps present opportunities for competitive advantage as they can be exploited to control the flow of information and resources[72]. Harrison White's "Identity and Control: A Structural Theory of Social Action" in 1992 delved into the dynamics of social networks, focusing on the interplay between individual identity and social structure[73]. These scholars have contributed to the development of Social Network Theory by providing conceptualizations and models that enhance our understanding of how networks operate and influence individual behavior within them.

Criticisms of Social Network Theory (SNT) highlight potential limitations in its application as suggested by some critics and argue that SNT may place too much emphasis on network structures, potentially overlooking the role of individual motivations and actions. While network connections undoubtedly influence behavior, individuals within the network also make autonomous decisions that shape outcomes[69]. Also, mapping complex terrorist networks poses significant challenges due to limited access to reliable data. Terrorist organizations often operate covertly, making it difficult to gather comprehensive information about their network structures and activities. This data scarcity can hinder the effectiveness of SNT analysis and limit its utility in understanding terrorism funding dynamics.

This chapter explores Social Network Theory (SNT) as a valuable framework for analysing cryptocurrency-enabled terrorism financing, focusing on a comparative study of Nigeria and Kenya from 2018 to 2024. SNT provides a structured approach to map the flow of resources

within terrorist networks, including cryptocurrency transactions, allowing analysts to trace illicit funds and identify critical nodes such as key financiers or facilitators in the networks of Nigeria's Boko Haram and Kenya's Al-Shabaab[70]. By examining these connections, the theory highlights the role of peripheral "weak ties," individuals or entities with limited direct involvement but crucial expertise in cryptocurrency or access to alternative funding channels, which bolster the adaptability and resilience of these networks[71]. In Nigeria and Kenya, SNT underscores the transnational scope of these financing threats, revealing how digital currencies enable cross-border resource movement, thus emphasising the urgent need for international cooperation to disrupt such flows[72]. This literature forms the foundation for the comparative analysis by elucidating key facilitators, resource dynamics, and potential intervention points, thereby supporting the development of targeted, evidence-based strategies to counter terrorism financing in these two nations.

Social Network Theory offers valuable insights into the networks and relationships involved in terrorism financing and the use of cryptocurrency. It can help analyze how terrorist organizations establish and maintain financial networks, identify key nodes and facilitators within these networks, and understand the dynamics of information and resource flow. Moreover, the theory can inform counterterrorism strategies by highlighting opportunities for intervention, such as disrupting key nodes, leveraging influential actors to influence behavior, and strengthening partnerships between states and financial institutions to combat terrorism financing.

2.2.2 Game Theory

Game Theory, founded by John von Neumann and Oskar Morgenstern in their seminal work "Theory of Games and Economic Behavior" published in 1944, is a mathematical framework used to analyze strategic interactions among rational decision-makers. and was developed extensively by many other researchers and scholars in the 1950s, such as John Nash in the 1950s, offers a framework for analyzing strategic interactions between rational actors[74]. In the context of "Terrorism Funding and Cryptocurrency: Implications for International Relations," Game Theory provides valuable insights into the strategic interactions between various actors involved in cryptocurrency-enabled terrorism financing, including terrorist organizations, governments, regulatory bodies, and financial institutions.

Game Theory conceptualizes interactions as "games" where players (decision-makers) choose strategies to maximize their utility or payoff, taking into account the choices of other players. The fundamental components of a game include players, strategies, payoffs, and information. Game Theory offers various models to analyze different types of strategic interactions, such as cooperative games, non-cooperative games, and repeated games[75]. Scholars have applied Game Theory to a wide range of disciplines, including economics, political science, and international relations. In the context of terrorism funding and cryptocurrency, scholars have explored how terrorist organizations strategically leverage cryptocurrencies to finance their activities while governments and regulatory authorities respond to mitigate these threats. For example, Alos-Ferrer and Netzer in 2010 developed a game-theoretic model to analyze the strategic behavior of terrorists and security agencies in a dynamic environment[76].

The nexus of terrorism financing and cryptocurrency within international relations, employing game theory as a pivotal framework to dissect the strategic interplay among diverse actors, with a comparative lens on Nigeria and Kenya. Game theory provides a robust tool for

modelling the complex decision-making processes of key players ranging from terrorist organisations such as Boko Haram in Nigeria and Al-Shabaab in Kenya to governmental bodies and financial institutions each pursuing distinct strategies and preferences[75]. For instance, terrorists may choose between traditional banking channels and cryptocurrencies to fund operations, aiming to maximise resources whilst evading detection. In contrast, governments and banks have strategies to disrupt these flows and safeguard national security[75]. These choices fundamentally influence the landscape of terrorism financing and its broader implications for regional stability and international relations in both countries.

At the heart of game theory lies the concept of equilibrium. In this state, each actor's selected strategy is optimal given the actions of others, establishing a balanced scenario with no unilateral incentive to shift course. In the context of Nigeria and Kenya, this equilibrium manifests as a delicate tension: terrorist groups leverage the anonymity of cryptocurrencies to enhance funding efficiency, whilst regulators impose measures like Nigeria's Virtual Asset Service Provider (VASP) restrictions or Kenya's Know Your Customer (KYC) protocols, each adapting to the other's moves[75]. This equilibrium embodies stability, reflecting a strategic alignment where terrorists, governments, and financial entities optimise their outcomes, whether illicit gains or enforcement efficacy, whilst accounting for their counterparts' responses. Illuminating these dynamics, game theory offers a comprehensive lens to understand the interplay of cryptocurrency-enabled terrorism financing, informing comparative strategies to counter such threats across Nigeria and Kenya.

Within the framework of game theory, a fundamental distinction arises between zero-sum and non-zero-sum games, each encapsulating distinct dynamics in strategic interactions. In zero-sum games, the fortunes of involved actors are inversely correlated, where the gains of one

party directly translate into losses for another[74]. This scenario mirrors competitive dynamics, exemplified by terrorist attacks inflicting casualties and economic harm, where one actor's success inevitably comes at the expense of another's well-being. In contrast, non-zero-sum games present avenues for cooperation and mutual benefit among participating actors. These scenarios foster collaborative efforts, such as international alliances aimed at disrupting terrorist funding networks and bolstering security measures. In non-zero-sum games, the pursuit of shared objectives enables actors to capitalize on synergies, fostering outcomes that benefit all parties involved.

Scholars such as Robert Axelrod, in his seminal work "The Evolution of Cooperation," delve deep into the intricate dynamics of cooperation within the context of repeated interactions[74]. This perspective holds particular significance in understanding the mechanisms through which governments can incentivize financial institutions to actively disrupt terrorist funding flows over prolonged periods. Elucidating the complexities of cooperative behaviour in scenarios marked by ongoing engagements, Axelrod's insights offer invaluable guidance for policymakers and security experts. Leveraging these principles, governments can cultivate a collaborative environment wherein financial institutions are motivated to consistently engage in efforts aimed at thwarting terrorist financing activities. This approach not only bolsters security measures but also fosters a culture of cooperation and collective action, thereby fortifying the resilience of the international community against the threats posed by terrorism.

Similarly, Thomas Schelling's "The StSimilarlyrategy of Conflict" introduces the concept of focal points – actions that emerge as natural choices due to shared expectations. In the context of terrorism funding and cryptocurrency, efforts to disrupt traditional funding channels might

inadvertently elevate cryptocurrencies as focal points for illicit transactions due to their perceived anonymity and resilience to regulatory intervention.

Critics of Game Theory contend that its efficacy is undermined by its reliance on assumptions that often diverge from real-world decision-making dynamics. Key among these criticisms are the assumptions of perfect rationality and complete information, which may not accurately capture the complexities inherent in human behavior and decision-making processes[75,76]. Moreover, skeptics question the theory's predictive power when applied to intricate and ever-evolving environments characterized by uncertainty and incomplete information. However, proponents of Game Theory assert its enduring value as a conceptual framework for comprehending strategic interactions and anticipating outcomes within specific contexts. Despite its limitations, Game Theory offers indispensable insights into strategic behavior, enabling stakeholders to devise informed strategies and make calculated decisions in competitive scenarios. By elucidating the dynamics of strategic interactions, the theory facilitates strategic planning and aids in the identification of optimal strategies, thereby enhancing decision-making processes and fostering more effective responses to complex challenges.

Within the Comparative Study of Nigeria and Kenya framework, game theory is a critical tool for analysing the strategic interactions among terrorist organisations, governments, and related actors in the context of cryptocurrency-enabled terrorism financing. In Nigeria, groups like Boko Haram, and in Kenya, Al-Shabaab strategically opt for cryptocurrencies, weighing risks (e.g., detection by authorities) against rewards (e.g., untraceable funding), whilst governments and regulators respond with countermeasures such as Nigeria's Virtual Asset Service Provider (VASP) restrictions or Kenya's enhanced KYC protocols[75]. Game theory

models these choices, offering insights into how each actor's decisions shape the funding landscape and influence international relations across these nations.

The use of cryptocurrencies by terrorist groups in Nigeria and Kenya has evolved significantly. Initially, Bitcoin dominated due to its widespread adoption, but by 2024, a shift emerged towards anonymity-focused currencies, such as those on the TRON blockchain, reflecting a strategic adaptation to evade detection[75]. Game theory illuminates this shifting terrain: For terrorists, cryptocurrencies provide anonymity and seamless cross-border transfers, enabling funding for operations in Nigeria's insurgency-hit north or Kenya's volatile Horn of Africa region. Conversely, governments in both countries can harness game theory to craft responsive strategies such as tightening regulations or deploying blockchain analytics to counter these exploits, balancing enforcement with the need to maintain financial innovation. This comparative analysis underscores the dynamic interplay of strategies shaping terrorism financing and regional security.

Government strategies may involve collaboration with financial institutions to incentivize them to identify and report suspicious cryptocurrency activity. Additionally, international cooperation plays a crucial role, enabling countries to coordinate efforts in disrupting cryptocurrency exchanges used by terrorists. Moreover, governments may explore the development of counter-cryptocurrency measures, including technologies to track and disrupt illicit transactions linked to terrorism.

It's essential to recognize that the analysis is not confined to a zero-sum game scenario. There is potential for cooperation among countries with shared interests in combating terrorism, as evidenced by collaborative efforts in disrupting funding flows. However, as governments

implement countermeasures, terrorists may adapt their tactics, necessitating continuous strategic adjustments and highlighting the dynamic nature of the strategic landscape.

2.3 Review of Empirical Studies

2.3.1 Cryptocurrency and Terrorism Funding

Terrorist organisations have adapted to the advancements in information and communications technology, particularly in their endeavours to fund their activities[78]. Cryptocurrency is a recent innovation in financial technology that has the potential to facilitate various transactions. Furthermore, it has already been realised in certain instances. The objective of this research is to analyse the underlying factors that drive terrorist organisations to adopt cryptocurrency as a means of financial transactions. Additionally, the study intends to identify the many kinds of recent operations involving cryptocurrency and explore potential future applications. This study employs a qualitative methodology by analysing a selection of sample cases and attempting to generalise the findings to broader phenomena. The data acquired is in the form of secondary data, namely derived from sources such as books, articles, academic papers, journals, news, and electronic media. This study utilises the international crime theory to argue that terrorist organisations are unlawful entities. It also employs the disruptive technology theory to characterise cryptocurrency as a novel form of cyber-based financial technology.

Additionally, the diffusion of innovation theory is used to elucidate why, in the current internet era, cryptocurrency has significant potential to attract global financial investments. This study discovered that terrorist organisations have begun utilising cryptocurrency as a means to fund their operations due to its anonymous and loosely regulated characteristics. This presents a novel challenge in combating cybercrimes that extend beyond traditional

scrutiny in the realms of finance and banking transfers, as well as efforts to combat counterfeiting and money laundering.

This paper examines the impact of monthly terrorist attacks on the monthly returns of 1,178 cryptocurrencies[79]. Specifically analyse the outcomes of these attacks, including their success, injuries, and fatalities. This research aims to address the growing concerns about the potential use of cryptocurrency for financing terror networks. Granger causality analysis reveals that the monthly percentage of successful terror incidents has a significant impact on both the increase and decrease of monthly bitcoin returns. The level of success in terror attacks has a negative correlation with cryptocurrency returns. Similarly, the number of wounded individuals also has a negative correlation with cryptocurrency returns. However, there is a positive correlation between the number of deaths and cryptocurrency returns. The impact of successful terror attacks on returns is most significant compared to the number of casualties. Controlling for cross-sectional correlation among key cryptocurrencies ensures that the results remain constant. Additionally, it is possible that cryptocurrencies may provide a limited form of protection against successful terrorist strikes. The results are strong and reliable when considering cryptocurrencies ranked in the top 75% of market capitalization. The mediation study demonstrates that terrorist incidents decrease returns by impacting the short-term macroeconomic cycle negatively.

A study aims to elucidate the utilisation of cryptocurrency as a means for financing terrorist activities. This article focuses on the methods that terrorists use to assess the reliability of donations and their subsequent adoption[80]. Approach. The study utilised scientific approaches such as abstraction, synthesis, observation, generalisation, and the method of induction of literature and legal documents to identify the characteristics of bitcoin that either facilitate or

hinder its usage for terrorism financing. Outcome. The advent of the Internet and electronic devices has profoundly transformed every aspect of human existence, including criminal behaviour. The process of digitalization has resulted in the enhancement of conventional criminal activities and the introduction of novel forms of crime that are inherently dependent on specialised digital electronic instruments. Terrorists were among the early adopters of new technologies, leveraging digitalization to enhance their revenue. Therefore, terrorists have escalated their focus on cryptocurrencies, particularly Bitcoin, as a digital form of payment. Bitcoin possesses several characteristics that have captivated the interest of wrongdoers as a means to elude accountability for illicit activities. Decentralisation eliminates the requirement for validation from a central governing body, while pseudo-anonymity offers a degree of anonymity. Furthermore, terrorists are cognizant of the fact that Bitcoin's privacy is highly vulnerable and requires improvement. The study examines many methods for improving anonymity, including software that obfuscates traffic and inhibits IP identification, peer-to-peer mixers, centralised mixing services (tumbler), and other strategies. A crucial aspect in combating crime is the de-anonymization of Bitcoin owners/users, as it enables the identification of criminals. Law enforcement agencies presently employ many techniques such as direct and indirect de-anonymization, proliferation analysis, quantitative analysis, time analysis, and transactional network analysis to accomplish the aforementioned objective. These methods are extensively addressed in this article. Furthermore, international agencies conducted investigations and exposed terrorist organisations and their financial enablers. More precisely, on August 13, 2020, the United States. The Office of Public Affairs of the Department of Justice has declared the seizure of the largest amount of cryptocurrency ever associated with terrorism. In order to investigate the matter, legal documents pertaining to

these investigations were thoroughly examined and analysed to gather information about the mechanism used to raise funds for terrorist activities. The legal documents disclosed that these investigations employed the previously indicated de-anonymization methods.

The aim of this research is to examine how 21 terrorist acts have affected the risk and return of cryptocurrency[81]. This is driven by the exponential surge in Bitcoin and other cryptocurrency prices, coupled with the ambiguity around the basic worth of cryptocurrencies and the process of determining this value. By utilising daily bitcoin returns and employing the event study approach, we calculate abnormal returns of cryptocurrencies in relation to terrorist operations. Asset price models incorporate interaction variables to ascertain the influence of individual attacks. ARCH models are employed to ascertain variations in systematic risk. Our research suggests that terrorist acts have a beneficial impact on the returns of cryptocurrencies. However, these events also lead to short-term risk shifting behaviour across various cryptocurrencies. Since its establishment in 2009, bitcoins have been utilised to conduct illicit activities globally.

Recently, different terrorist organisations have started using this technology to different degrees. The objective of my thesis, titled "Innovation in Terrorist Financing: Analysing Different Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State," is to get a deeper understanding of the factors that drive and hinder the use of cryptocurrencies by terrorist groups. Six hypotheses are suggested to address this subject[23]. Terrorist organisations operating in areas with significant computational capabilities are more inclined to utilise cryptocurrency. Furthermore, a lack of sufficient infrastructure to support the conversion of cryptocurrencies into traditional fiat cash might deter terrorist organisations from embracing this technology. Furthermore, in the event of cryptocurrency price

fluctuations, the probability of terrorist organisations embracing the technology will decrease. Furthermore, terrorist organisations with more extreme ideologies are increasingly inclined to embrace cryptocurrencies. Furthermore, terrorist organisations with a higher degree of anti-Western feeling in their beliefs are less inclined to embrace cryptocurrency. Lastly, the sixth hypothesis suggests that if terrorist organisations are successfully funding their operations through conventional methods, they are less inclined to embrace cryptocurrencies. To examine these assumptions, three case studies were conducted on al-Qaeda, Hezbollah, and the Islamic State. An examination of these cases reveals that only the sixth hypothesis yields a positive result, which carries significant and progressive consequences for the United States' counter-terrorism policy[82].

Terrorist action is an extremely perilous type of criminal behaviour that presents a risk to the entire human race, in addition to environmental catastrophes and wars. The issue of combating the financing of terrorism is significant both for Russia and the global community in the broader framework of combating crime. The funding of terrorism has historical origins, but currently, the means of financing are predominantly facilitated through the worldwide Internet and the advancement of digital economy technologies. The ongoing enhancement of the Internet's capacities not only presents further opportunities for the advancement of the worldwide community, but also gives rise to many new global risks[83].

Terrorist organisations are utilising modern digital technologies such as cryptocurrencies, virtual currencies, crowdsourcing, fundraising, social networks, and Telegram channels to transform traditional techniques of financing terrorism. In the context of a digital economy, terrorist acts can have far-reaching consequences. They can disrupt government operations and finances, affect the value of securities and the overall investment climate, lead to a

significant decrease in tax revenues, contribute to an increase in military spending within the state budget, and have a profoundly destructive impact on both the state and society[84].

Developing effective strategies to fight the financing of terrorism is a top issue in scientific research. The article provides an evaluation of the primary methods now used to finance terrorist actions. It also offers recommendations for combating their spread and minimising the emergence of new contemporary means for criminal organisations to gain wealth[85].

The advent of algorithmic-based currency systems, commonly referred to as cryptocurrencies, has sparked concerns because to the potential threats related to money laundering and the financing of terrorism. In addition to its advantages, the decentralised nature of cryptocurrency offers significant opportunities for terrorist organisations and criminal syndicates to store, transfer, or conceal their illegal profits. This is possible because transactions lack oversight or authorization from a governing or central authority, allowing for anonymity. Nation-states have been pushed to enhance their Anti-Money Laundering (AML) and Combating the Financing of Terrorism (CFT) systems in order to safeguard their physical, economic, and national security. This can be achieved through the implementation of rules or complete prohibition. Pakistan has chosen to pursue the latter strategy and made it illegal to engage in any transactions involving cryptocurrencies. However, due to the lack of specific laws, authorities are encountering challenges when it comes to prosecuting offences relating to cryptocurrencies. This study employed a qualitative approach to analyse how the text discusses the functions of cryptocurrencies and how they enable crime syndicates and terrorist financiers to launder their funds. It also explores the necessary methods to combat this form of illicit financing[86].

The onset of the 21st century is marked by globalisation, volatility, uncertainty, and a resurgence of terrorism, which has emerged as a significant menace to human society and democracy. An examination of the progression of global terrorism indicates that the activities undertaken are becoming increasingly perilous as terrorist organisations have greater access to financial means, which in turn allows them to procure progressively advanced weaponry, technology, and propaganda tools. The frequency and intensity of terrorist activities fluctuate based on the financial framework of the terrorist group. Consequently, the pursuit of discovering and acquiring fresh financing sources, novel money-laundering techniques, and innovative means of transferring funds has emerged as a crucial goal. Terrorist groups employ several methods to acquire and move monies required for their operations, utilising both contemporary technologies such as cryptocurrency and the darknet, as well as ancient techniques like zakat and hawala. This study investigates the reliance of terrorists on financial resources, the techniques used to acquire and move these monies, and the global community's endeavours to combat this problem. The fight against terrorism includes measures to halt its funding[87].

2.3.2 Regulation, Law, Security, and the Financing of Terrorism Via Cryptocurrency

The advent of cryptocurrencies has provided terrorist organisations and criminal syndicates with a new means to conduct their illicit financial activities. The escalating utilisation of cryptocurrencies in activities such as terror financing, drug trafficking, human trafficking, and corruption has compelled legislators worldwide to take measures to regulate the processes of selling, buying, and exchanging cryptocurrencies. While China has implemented a complete

prohibition on cryptocurrencies, other nations have opted to embrace the possibilities of bitcoin by integrating it into mainstream systems and implementing sensible restrictions[88]. In the midst of global initiatives to regulate and exploit the possibilities of cryptocurrency, Pakistan has implemented a prohibition on virtual assets and tokens. The decision to ban cryptocurrencies is based on the multitude of issues that the country would face, including tax evasion, transnational crimes, terrorism financing, cybercrimes, corruption, and kidnapping for ransom. Although Pakistan's current approach aligns closely with China, Pakistani officials should use a hybrid approach to regulate their economic and regulatory environment. Exercising caution and prioritising long-term planning are essential when considering the implementation of cryptocurrencies in the country.

Bitcoin was developed in 2008 with the purpose of providing an alternative method of payment for individuals who have limited access to traditional banking services, such as those who are under-banked or un-banked. It particularly benefits people living in areas where the formal financial system is plagued by widespread corruption and lacks effective regulation. Nevertheless, criminals and terrorists promptly took use of Bitcoin's distinctive characteristics, specifically its decentralised nature and partial anonymity, to support widespread terrorist financing and money laundering operations[89]. The government's responses to protect national security interests have exhibited a wide range of approaches, spanning from complete prohibitions to passive acceptance. This discrepancy arises from the challenge of accurately categorising Bitcoin. There are two opposing viewpoints about Bitcoin's classification: some believe that it is a currency, while others contend that it is an asset. These disparities have caused a bureaucratic conflict between many regulatory agencies in the United States, including the Financial Crimes Enforcement Network, the Commodity Futures Trading

Association, the Securities and Exchange Commission, and the Internal Revenue Service. This paper aims to surpass the current legal frameworks by advocating for the classification of Bitcoin as a technology and suggesting that regulation should be entrusted to private sector technology businesses. The increasing number of cyberterrorism threats, made possible by the internet and digitalization, requires a thorough and effective reaction to combat the quick and effortless movement of funds for terrorist across international boundaries. This study centres on the latest advancements in counterterrorism, specifically in relation to the funding obtained through internet means. The objective is to establish metrics that may effectively and sustainably tackle these changing difficulties, offering useful information for the creation of successful strategies.

The work examines the regulatory framework for counter-terrorism financing in Indonesia using a normative juridical method and an interdisciplinary approach that includes criminology, international law, treaties, and pertinent statutes[90]. The research utilises a qualitative descriptive technique to get practical understanding of the regulatory landscape by examining Laws No. 9 of 2013 and No. 15 of 2003. The findings highlight the complex aspect of addressing terrorism financing, advocating for strict financial regulations, increased global cooperation, and flexible legal structures. This study highlights the significance of proactive and adaptable approaches, both in theory and practice, to effectively tackle the intricate issues presented by the geographical relocation of terrorism and the utilisation of digital and cryptocurrency channels for financing. This research enhances the worldwide comprehension and provides valuable insights for politicians, security agencies, and scholars to develop precise and enduring strategies to combat terrorism financing.

The examination commences by providing a comprehensive overview of cryptocurrencies, with a specific emphasis on elucidating how the underlying technology and applications amplify susceptibilities. The material will establish the groundwork for analysing the weaknesses present in the structure of bitcoin technology, as well as potential subjects for regulatory measures. The subsequent phase of the analysis will then redirect attention towards delineating the extent of the money laundering issue linked to cryptocurrency. A comprehensive comprehension of the situation is important to guide customised AML legislation and regulations. The final segment of the analysis will examine nascent anti-money laundering (AML) legislation that oversee cryptocurrencies, with a particular emphasis on those being formulated and enforced in the United Arab Emirates (UAE). The rules of the UAE will be compared to those of the USA and European Union (EU) with the purpose of conducting a comparative analysis and identifying best practices. Discoveries[91]

The UAE possesses a strong regulatory framework designed to enhance anti-money laundering (AML) measures while facilitating the widespread adoption of cryptocurrency assets in both corporate and government activities. An examination of the legislative system in the UAE highlights significant concerns. Currently, the existing legislation do not encompass decentralised finance (DeFi) and non-fungible tokens (NFTs). The lack of explicit legislation governing DeFi and NFT protocols has provided an opportunity for money laundering and associated illicit activities. Furthermore, the legislative landscape in the UAE exhibits a significant degree of fragmentation. The UAE lacks a comprehensive set of nationwide laws that are applicable to all of its Emirates. Fragmentation is a prevalent issue not only in the UAE but also in the USA and EU, impacting these regions on a worldwide

scale. Hence, it is imperative to implement a customised strategy that ensures that the established norms and guidelines are adaptable to the various facets of cryptocurrencies. The method is crucial, as it would be unfeasible to devise a singular legislation or rule that encompasses all crypto assets, including their varied applications. Additionally, the Financial Action Task Force (FATF) ought to establish an international benchmark that promotes a consistent and coordinated implementation of anti-money laundering (AML) and counter-terrorist financing (CTF) legislation and regulations pertaining to cryptocurrencies and blockchain technology[92].

A study explores the complex connection between digital assets, particularly Non-Fungible Tokens (NFTs), and the legislative framework for anti-money laundering (AML) and counter financing of terrorism (CFT). The rapid expansion of NFTs has brought about new difficulties and opportunities. This calls for an examination of changing regulatory frameworks and enforcement mechanisms to address the dangers of money laundering (AML) and terrorist financing (CFT) that are linked with digital assets. This chapter specifically examines the distinct attributes of NFTs, the hazards of money laundering (AML) and terrorist financing (CFT) in the NFT industry, worldwide regulatory advancements, obstacles in compliance, technology remedies, steps taken to enforce regulations, cooperative initiatives, and upcoming trends. This chapter seeks to offer valuable insights to policymakers, regulators, scholars, and industry participants in efficiently managing financial crime risks in the digital asset landscape through a thorough analysis of these factors[93].

This mini-dissertation aims to examine and determine the potential dangers and repercussions of virtual currencies on the existing regulatory and supervisory framework in South Africa, specifically in relation to money laundering and terrorism financing. The South African

financial system is highly controlled and overseen to ensure its prudence, reputation, and to promote its safety and stability. In recent times, advancements and progress in technology have given rise to significant challenges, particularly in terms of financial regulation and supervision. The field of financial technology has given rise to enigmatic phenomena such as blockchain, insuretech, crowdfunding, and virtual currencies. Currently, virtual currencies, which will be the main subject of this study, are not included in the South African financial regulatory or supervisory system, resulting in a regulatory loophole. The South African context is faced with numerous risks and implications, including tax evasion, illicit flow of funds across borders, violation of exchange control regulations, financial instability, uncertainty in monetary policy, inaccurate economic statistics, failure to report balance of payment requirements, and money laundering and terrorist financing (ML/TF). The objective of the study is to create a precise depiction and classification of virtual currencies specifically within the setting of South Africa. Furthermore, the study will examine the dangers and consequences that virtual currencies present to the South African financial system in terms of money laundering and terrorist financing. Ultimately, the study will provide a potential remedy to address the existing regulatory loophole caused by virtual currencies in the South African financial industry[94].

Cryptocurrency is an emerging technology that brings up numerous challenges in terms of regulation and risks related to financial crime. The diverse range of cryptocurrencies and digital assets poses a challenge for government bodies in establishing a consensus on a standardised classification for cryptocurrency. The objective of this study endeavour was to examine existing rules pertaining to cryptocurrencies and evaluate their efficacy in addressing financial illicit activities. An analysis of four important regulatory agencies in the United

States reveals that each organisation has distinct categorization and handling of cryptocurrencies. Despite attempts to create a unified and comprehensive description of cryptocurrency, each government agency still regulates cryptocurrency based on its own understanding of the term. The outcome is a distorted and unintelligible comprehension of cryptocurrencies, resulting in inadequate laws and enforcement measures. The absence of well-defined cryptocurrency legislation results in certain segments of the bitcoin economy operating without regulation. Unregulated bitcoin exchanges are susceptible to various financial crime risks[95].

This study aims to analyse and summarise the regulatory methods and policies of different countries regarding cryptocurrency in order to establish and enhance China's anti-money laundering regulatory system for cryptocurrencies. By drawing on international advanced practices and mature experience, the study seeks to minimise financial risks and safeguard China's financial security. The project has three primary research objectives: 1) To improve the systemization of China's regulatory approach to cryptocurrencies. 2) Establish a robust regulatory framework for cryptocurrencies in China to effectively mitigate the dangers associated with money laundering and terrorist funding. 3) Enhance the efficacy of China's regulatory framework for cryptocurrencies. This study employs a qualitative research methodology, utilising comparative research, analysis, and induction analysis. The topic is addressed by applying social interest theory, which provides theoretical help in addressing issues related to natural monopolies, external impacts, and inadequate knowledge. This method involves the synthesis of a substantial amount of literature and economic principles. To meet the research objectives, it is recommended to apply the following improvements: 1) Establish industry standards to mitigate potential hazards originating from the source. 2)

Elucidate the implementation of regulations and incorporate cryptocurrencies into the purview of anti-money laundering regulation. 3) Enhance global collaboration to detect and counteract the laundering of cryptocurrencies, and 4) enhance technological advancements and establish regulatory technical assistance that aligns with bitcoin trading[96]. The nature of terrorism financing has transformed due to the rapid growth and widespread use of the internet. Terrorist organisations have increasingly relied on this aspect of funding as a crucial means of mobilisation. The financing of terrorism by cyber means has occurred simultaneously with the significant advancements in technology that have been made in recent decades. This chapter offers a comprehensive overview of the evolution of funding methods for cyber terrorism. Next, it presents pertinent aspects pertaining to the cyber aspects of terrorism financing that are currently posing difficulties for scholars, professionals, and policymakers. These include conversations on social media, cryptocurrency, and the black web.

2.3.3 Terrorism Funding Via Cryptocurrency and Its Impact on International Relations

The current conflict between Russia and Ukraine underscores the increasing involvement of independent countries in the international cryptocurrency network, and the significant consequences this has for private entities, including worries about sanctions and even involvement in war crimes. In light of the fast evolving legal environment surrounding cryptocurrencies, it is imperative for the global cryptocurrency markets to establish standardised procedures for fundraising, ensuring compliance with sanctions, and implementing effective measures to combat financial crimes[59]. In reality, crypto assets are not completely untraceable. The main vulnerability that illegal actors take advantage of is the failure of DeFi services to comply with anti-money laundering/combating the financing of terrorism and sanctions obligations. The international community has established the

Financial Action Task Force (FATF), a comprehensive and global entity with the authority to impose actions. The recent enforcement measures implemented by member nations of the Financial Task Force on Anti-Money Laundering (FTFA) will expedite the implementation and enforcement of the travel rule. Additionally, advanced blockchain analysis technologies are offering robust "crypto intelligence tools for all parties involved.

An important advancement in the global economy is the emergence of cryptocurrencies, with bitcoin being particularly significant. The modern digital economy encompasses various varieties of cryptocurrencies, with bitcoin being the most widespread. Bitcoin was officially introduced in 2009 by an individual or group using the pseudonym Satoshi Nakamoto. Bitcoin's value has surged to a staggering 19.7 billion US dollars as of January 2, 2018[97]. With the increasing value of bitcoin, terrorist organisations are utilising this digital money to fund their heinous operations worldwide. By doing so, they are able to evade the monitoring systems of the banking institutions in different nations. In light of this context, the objective of this chapter is to comprehend the functioning of cryptocurrencies in a broad sense, with a specific focus on bitcoin. Lastly, it also aims to determine the pattern of the bitcoin economy and its influence on illicit activities overall, with a specific focus on funding terrorists. The study has uncovered that the cryptocurrency economy has gained widespread popularity globally, resulting in the emergence of an independent virtual economy that operates without rules imposed by any one government or group of countries. The application of the vector error correction model (VECM) revealed a statistically significant long-term relationship between terrorist incidents and bitcoin transaction/circulation in a panel of 12 nations from 2010 to 2016. Nevertheless, there is a significant apprehension regarding its mode of functioning and its illicit association with the financing of terrorists[60].

In the 1980s, globalisation experienced a significant surge in momentum. Globalisation led to the establishment of factories by firms in foreign nations, the implementation of new trade agreements, and the promise of universal wealth. In the 1990s, the Internet accelerated the process of globalisation, further reducing the size of the planet. Nevertheless, globalisation has also incited a strong negative reaction in the development of extremist fundamentalist organisations such as Al-Qaeda. Over the past three decades, Al-Qaeda has also expanded its operations worldwide[23]. Currently, it has established partnerships in numerous nations, and it has utilised the infrastructure developed by the impact of globalisation to establish a global financial network. This network utilises the global financial system, informal money transfers, charitable contributions, and other means. Following the 9/11 attacks, governments at the national level and its regional allies have made efforts to counteract the funding of terrorism[61]. However, Al-Qaeda has effectively modified its financing approach in order to evade these countermeasures. The lack of extensive collaboration on an international scale has enabled AlQaeda to persist in generating millions of dollars annually. Additionally, Al-Qaeda has taken notice of emerging technologies as a means to acquire extra finance, strategize, and communicate. The interconnected nature of these technologies poses a threat since it enables Al-Qaeda and other groups to effectively conceal their activities, while also increasing their financial capabilities, while governments at national and regional levels struggle to keep up. An examination of Al-Qaeda's financial network reveals the insufficiency of national and regional strategies in combating terrorism finance, emphasising the necessity of collaborating with international institutions[23,62].

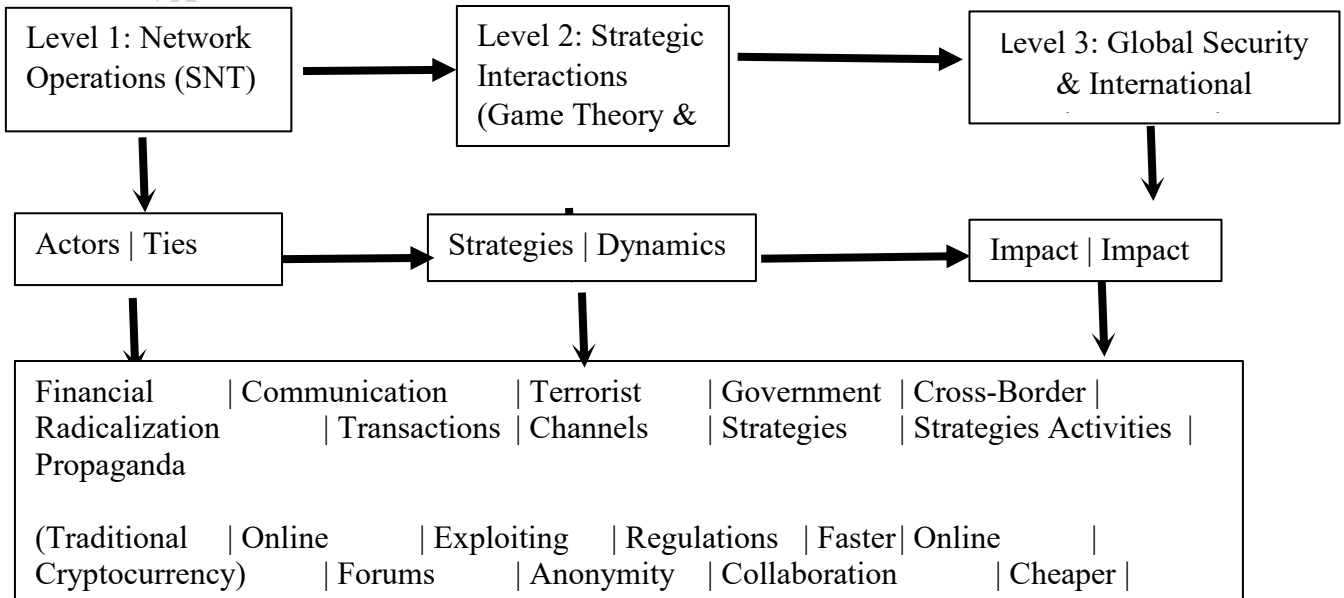
A study emphasises the utilisation of global performance indicators (GPIs) by international organisations to influence policy change by exerting pressure on transnational markets. GPIs

serve as reliable evaluators of state policy when international organisations possess credibility, and when monitored countries engage in competition for market resources. These indices effectively convey information regarding country risk and contribute to the stabilisation of market expectations. In such circumstances, banks and investors may limit the availability of funds to states that do not comply with regulations, while encouraging greater adherence to these regulations. I illustrate this market-enforcement mechanism by examining the Financial Action Task Force (FATF), an intergovernmental organisation that offers nonbinding recommendations to address the challenges of money laundering and the funding of terrorism. The publication of noncompliant jurisdictions by the FATF has compelled international banks to reallocate resources from these nations and has escalated the expenses associated with ongoing noncompliance. Consequently, there has been a substantial rise in the number of states that have enacted legislation to criminalise terrorist financing. This discovery indicates a strong mechanism by which institutions shape domestic policy and emphasises the influence of Global Policy Indexes (GPIs) in a time when information holds global value[54].

2.4 Conceptual Model

2.4.1 Digraph Representing the Multi-Level Framework

Here's a diagram representing the Multi-Level Framework for analyzing terrorism funding and cryptocurrency:



Source: Author's Compilation

2.4.2 A Multi-Level Framework for Analyzing Terrorism Funding and Cryptocurrency

This framework combines elements of Social Network Theory (SNT) and insights from international relations to analyze how terrorist organizations utilize cryptocurrency for financing activities and its impact on global security. It operates on three levels:

2.4.2 A Multi-Level Framework for Analysing Terrorism Funding and Cryptocurrency

This framework integrates Social Network Theory (SNT) and international relations perspectives to examine cryptocurrency-enabled terrorism financing in Nigeria and Kenya. It is structured across three distinct yet interconnected levels of analysis.

Level 1: Network Operations

At the network operations level, informed by SNT, the framework explores the intricate web of actors and ties underpinning terrorist financing in Nigeria and Kenya. Actors include terrorist groups such as Nigeria's Boko Haram and ISWAP, ranging from centralised to decentralised structures, and Kenya's Al-Shabaab alongside financiers, cryptocurrency exchanges, sympathisers, law enforcement agencies, and regulatory bodies like Nigeria's Central Bank and Kenya's Central Bank. These entities are connected through financial transactions, traditional banking with cryptocurrency flows, and communication channels, such as Telegram in Nigeria or informal networks in Kenya, which also serve as pathways for recruitment and radicalisation. The analysis traces cryptocurrency funding flows, mapping

their movement from entry points like Nigeria's thriving crypto exchanges to exit points like Kenya's mobile money systems. It also assesses network centrality to identify key actors, important financiers in Nigeria, or intermediaries in Kenya. It further investigates peripheral "weak ties," individuals with cryptocurrency expertise or access to alternative funding, whose subtle roles enhance the resilience of groups like ISWAP or Al-Shabaab.

Level 2: Strategic Interactions

The strategic interactions level draws on game theory and the international system to dissect the dynamic choices shaping terrorism financing in Nigeria and Kenya. Terrorist strategies in Nigeria exploit Bitcoin's anonymity, whilst in Kenya, groups leverage fintech gaps, adapting to countermeasures and harnessing the global reach of cryptocurrency platforms. Governments counter these moves with tailored approaches—Nigeria implements Virtual Asset Service Provider (VASP) regulations, whilst Kenya enforces KYC/AML protocols—aiming to track transactions, disrupt funding, and foster international partnerships. However, these efforts face challenges from jurisdictional disparities between the two nations and the spectre of state-linked cryptocurrency use in terrorism, highlighting the need for a nuanced understanding of how terrorists and regulators strategically respond to one another in this evolving landscape.

Level 3: Global Security Landscape

At the global security landscape level, the framework broadens its scope to assess cryptocurrency's broader implications for Nigeria and Kenya. It examines how rapid, cost-effective cross-border transfers enable funding flows, bypassing traditional oversight to support Nigeria's Sahel connections or Kenya's Horn of Africa networks. The analysis also explores how online anonymity fuels radicalisation, with Nigerian groups using Telegram

campaigns or Kenyan actors leveraging digital platforms to distribute propaganda via cryptocurrency transactions. Furthermore, it probes the emerging "cryptocurrency arms race," where terrorists in both countries advance their digital capabilities, compelling governments and international bodies to continually refine countermeasures to maintain security across regional and global spheres.

2.4.3 Applying the Framework to Objectives of the Study

This framework guides the comparative analysis of Nigeria and Kenya by linking its three levels of network Operations, Strategic Interactions, and Global Security Landscape to the study's objectives. It offers a structured approach to understanding cryptocurrency-enabled terrorism financing.

Objective 1: Identifying Methods and Strategies

To identify the methods and strategies terrorist organisations employ to utilise cryptocurrency in Nigeria and Kenya, the framework begins at the Network Operations level, mapping funding flows through networks like Boko Haram's Telegram channels or Al-Shabaab's informal ties, tracing cryptocurrency from Nigerian exchanges to Kenyan mobile money exit points. At the Strategic Interactions level, it examines how these groups exploit Bitcoin's anonymity in Nigeria or fintech gaps in Kenya, adapting to regulatory pressures with enhanced privacy coins like those on the TRON blockchain. The Global Security Landscape level reveals how these strategies leverage cross-border anonymity, enabling rapid transfers that fund operations, recruitment, and propaganda, offering a comprehensive view of terrorist tactics in both nations.

Objective 2: Evaluating Existing Counter-Terrorism Financing Frameworks

For critically evaluating the effectiveness of existing counter-terrorism financing frameworks in Nigeria and Kenya, with a focus on cryptocurrency regulations, the Network Operations level assesses the impact of Nigeria's VASP restrictions and Kenya's KYC/AML rules, measuring their success in reducing transactions or exposing key actors like ISWAP financiers or Al-Shabaab intermediaries. The Strategic Interactions level highlights implementation challenges, such as tracing anonymised transactions or countering unregulated crypto services that evade enforcement in both countries. At the Global Security Landscape level, it considers how these frameworks struggle against the borderless nature of cryptocurrency, underscoring gaps that hinder the disruption of funding networks and regional security efforts.

Objective 3: Examining Transformation and Regional Security Impact

To examine how cryptocurrency transforms traditional terrorism financing networks and its impact on regional security dynamics, the Network Operations level maps the shift from cash-based to digital networks, identifying how Nigerian Telegram campaigns or Kenyan digital platforms enhance operational reach for Boko Haram and Al-Shabaab. The Strategic Interactions level analyses how terrorists adapt to countermeasures, using cryptocurrency to bypass traditional oversight, whilst governments adjust strategies in response. The Global Security Landscape level assesses the resultant escalation in regional threats, with faster, cheaper transfers amplifying Nigeria's Sahel instability or Kenya's Horn of Africa tensions, reshaping security dynamics across borders.

Objective 4: Investigating Interconnections with Local and International Systems

Investigating interconnections between local cryptocurrency markets, international financial systems, and terrorism financing networks in Nigeria and Kenya, the Network Operations

level traces funds from Nigeria's crypto hubs or Kenya's fintech ecosystems to global sympathisers, pinpointing key nodes like exchanges or mobile money links. The Strategic Interactions level explores how terrorists exploit these markets' global reach whilst governments grapple with regulatory disparities and limited tracking capabilities. The Global Security Landscape level illuminates how these interconnections facilitate cross-border funding, such as Nigerian donations to Sahel bases or Kenyan support to Somalia, highlighting the integration of local and international systems in sustaining terrorist operations.

Objective 5: Developing Policy Recommendations

For developing context-specific policy recommendations to strengthen international cooperation and regulatory frameworks, the Network Operations level identifies intervention points, such as disrupting Nigerian financiers or Kenyan intermediaries, informed by network mapping. The Strategic Interactions level suggests strategies like harmonising Nigeria's VASP rules with Kenya's KYC/AML efforts and enhancing blockchain analytics to counter terrorist adaptations. The Global Security Landscape level advocates for robust international partnerships, potentially via ECOWAS and EAC, to address cross-border flows and the "cryptocurrency arms race," proposing unified frameworks tailored to Nigeria and Kenya's unique vulnerabilities to bolster global security.

2.4.4 Benefits of this Framework

Benefits

This framework offers distinct advantages for analysing cryptocurrency-enabled terrorism financing in Nigeria and Kenya, enhancing understanding of its complexities within international relations. Its multi-level approach provides a comprehensive perspective by

weaving together network operations mapping the intricate funding webs of groups like Boko Haram and Al-Shabaab strategic interactions, where terrorist adaptations meet governmental countermeasures and global security implications, assessing the broader impact on regional and international stability. A key strength lies in its emphasis on international relations, integrating the critical role of cross-border cooperation and the potential for state sponsorship. These are particularly relevant given Nigeria's Sahel ties and Kenya's Horn of Africa dynamics. Furthermore, its adaptability allows for tailored analysis of specific case studies, such as Nigeria's shift to privacy-focused cryptocurrencies, Kenya's fintech vulnerabilities, and emerging trends in terrorist cryptocurrency use. By equipping researchers to dissect the multifaceted issue of terrorism funding through cryptocurrencies, this framework illuminates its operational mechanics and global security ramifications. It offers a robust tool to inform comparative strategies for Nigeria and Kenya within the broader international landscape.

2.5 Summary of the Gap in the Literature Reviewed

The literature on cryptocurrency-enabled terrorism financing has primarily focused on industrialized economies, neglecting the unique vulnerabilities and requirements of emerging nations like Nigeria and Kenya. This gap limits our understanding of the specific dynamics and impacts of cryptocurrency use for terrorism funding in these contexts. By concentrating on Nigeria and Kenya, this study aims to address this deficiency, offering insights into how cryptocurrency-enabled terrorism financing operates within the Nigerian and Kenya landscape. Through empirical research and a nuanced analysis, the study seeks to shed light on the challenges and implications faced by countries like Nigeria and Kenya in combating cryptocurrency-enabled terrorism financing.

Moreover, existing theoretical frameworks often lack depth, particularly in integrating technological aspects, local context, and specific vulnerabilities in developing countries within the study of terrorism financing. This theoretical deficiency hinders the development of comprehensive solutions tailored to the complexities of cryptocurrency-enabled terrorism financing. Incorporating insights from Network Analysis, Cybersecurity and Technology Studies, and International Relations and Security Studies, this study aims to bridge the theoretical gap. It seeks to provide a holistic understanding of the interplay between technological advancements, local contextual factors, and terrorism financing dynamics, thereby contributing to theoretical advancements in the field.

Furthermore, the absence of evidence-based and tailored countermeasures leaves countries like Nigeria vulnerable to potential threats arising from cryptocurrency-enabled terrorism financing. Existing approaches may not adequately address the evolving nature of this phenomenon or the unique challenges posed by the Nigerian and Kenyan context. Through the development of a multi-level framework and empirical research, this study intends to fill the practical gap by providing actionable recommendations for addressing cryptocurrency-enabled terrorism financing in Nigeria and comparable contexts. By offering insights into effective countermeasures and policy interventions, the study seeks to enhance the capacity of policymakers, law enforcement agencies, and other stakeholders to combat cryptocurrency-enabled terrorism financing effectively.

This study aims to contribute to the existing literature by addressing the gaps in understanding and tackling cryptocurrency-enabled terrorism financing, particularly within the Nigerian and Kenyan context. By conducting empirical research, integrating theoretical frameworks, and developing evidence-based countermeasures, the study seeks to provide a comprehensive

analysis of the challenges and implications of cryptocurrency-enabled terrorism financing in emerging economies. Through these efforts, the study endeavors to enhance our understanding of this complex phenomenon and contribute to the development of effective strategies for countering cryptocurrency-enabled terrorism financing

Endnotes

1. A. Ghosh, S., Gupta, A., Dua, N., & Kumar. *Security of Cryptocurrencies in Blockchain Technology: State-of-Art, Challenges and Future Prospects,* **Journal of Network and Computer Applications,** 163, 2020, 102635.

2. A. Faturahman, V. Agarwal, & C. Lukita. *Blockchain Technology—the Use of Cryptocurrencies in Digital Revolution,* **IAIC Transactions on Sustainable Digital Innovation (ITSDI),** 3(1), 2021, 53–59.

3. J. M. Hashemi, Y. Nishikawa, & K. Dandapani. *Cryptocurrency, a Successful Application of Blockchain Technology,* **Managerial Finance,** 46(6), 2020, 715–733.

4. H. M. C. Sebastião, P. J. O. R. D. Cunha, & P. M. C. Godinho. *Cryptocurrencies and Blockchain: Overview and Future Perspectives,* **International Journal of Economics and Business Research,** 21(3), 2021, 305–342.

5. M. Ghorbanian, S. H. Dolatabadi, P. Siano, I. Kouveliotis-Lysikatos, & N. D. Hatziargyriou. *Methods for Flexible Management of Blockchain-Based Cryptocurrencies in Electricity Markets and Smart Grids,* **IEEE Transactions on Smart Grid,** 11(5), 2020, 4227–4235.

6. V. Dyntu & O. Dykyj. *Cryptocurrency as an Instrument of Terrorist Financing,* **Baltic Journal of Economic Studies,** 7(5), 2021, 67–72.

7. S. A. Warreth. *Comparing Far Right and Jihadi Use of Crowdfunding, Cryptocurrencies, and Blockchain Technology: Accessibility, Geography, Ideology,* 2020.

8. F. Costantino. *The FATF Recommendations and the Development of International Standards on Terrorist Financing,* In *Countering Terrorist and Criminal Financing* CRC Press, 2024, 31–42.

9. A. Majumder, M. Routh, & D. Singha. *A Conceptual Study on the Emergence of Cryptocurrency Economy and its Nexus with Terrorism Financing,* In *The Impact of Global Terrorism on Economic and Political Development: Afro-Asian Perspectives* Emerald Publishing Limited, 2019, 125–138.

10. N. N. Reshetnikova, M. M. Magomedov, S. S. Zmiyak, A. V. Gagarinskii, & D. A. Buklanov. *Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security,* In *Current Problems and Ways of Industry Development: Equipment and Technologies.* Cham: Springer International Publishing, 2021, 355–363.

11. A. M. VÂRTEI. *Financing Terrorism: Economy's Dark Side,* In *Proceedings of the International Conference on Cybersecurity and Cybercrime.* Asociatia Romana pentru Asigurarea Securitatii Informatiei, 2023, 216–223.

12. S. M. S. Zaidi. *Emerging Realities in the International Political System: Transforming State's Foreign Policy,* **Herald of the Russian Academy of Sciences,** 2023, 1–14.

13. O. Ariani & A. L. Ibrahim. *Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia,* **Jurnal Usm Law Review,** 7(1), 2023, 30–44.

14. A. Majumder, M. Routh, & D. Singha. *A Conceptual Study on the Emergence of Cryptocurrency Economy and its Nexus with Terrorism Financing,* In *The Impact of Global Terrorism on Economic and Political Development: Afro-Asian Perspectives* Emerald Publishing Limited, 2019, 125–138.

15. N. N. Reshetnikova, M. M. Magomedov, S. S. Zmiyak, A. V. Gagarinskii, & D. A. Buklanov. *Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security,* In *Current Problems and Ways of Industry Development: Equipment and Technologies.* Cham: Springer International Publishing, 2021, 355–363.

16. A. M. VÂRTEI. *Financing Terrorism: Economy's Dark Side,* In *Proceedings of the International Conference on Cybersecurity and Cybercrime.* Asociatia Romana pentru Asigurarea Securitatii Informatiei, 2023, 216–223.

17. A. Eaddy. *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation), 2019.

18. P. C. Patel & J. Richter. *The Relationship between Terrorist Attacks and Cryptocurrency Returns,* **Applied Economics,** 53(8), 2021, 940–961.

19. O. T. Emmanuel & A. A. Michael. *Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria,* **Journal of Auditing, Finance, and Forensic Accounting,** 8(2), 2020, 55–66.

20. M. U. Nnam, B. O. Ajah, C. C. Arua, G. P. Okechukwu, & C. O. Okorie. *The War Must Be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria,* **International Journal of Cyber Criminology,** 13(2), 2019.

21. CBN. *Guidelines and Operations of Bank Accounts for Virtual Assets Service Providers (VASPs),* https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf , 2023.

22. W. Ma. *Terrorist Financing, War Crimes, and Crypto Geopolitics,* In *A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects.* Cham: Springer Nature Switzerland, 2023, 241–259.

23. A. Eaddy. *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation), 2019.

24. N. Schwarz, M. K. Chen, M. G. Jackson, K. Kao, M. F. Fernando, & M. Markevych. *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations,* International Monetary Fund, 2021.

25. A. Andrianova. *Countering the Financing of Terrorism in the Conditions of Digital Economy,* In *Digital Transformation of the Economy: Challenges, Trends and New Opportunities.* Springer International Publishing, 2020, 20–31.

26. UN. *Advancing Rule of Law, Justice for All Through Technology Must Include Equal Internet Access, Human Rights Compliance, Sixth Committee Speakers Stress,* https://press.un.org/en/2023/gal3694.doc.htm , 2023.

27. T. Strategy. *IMF Policy Papers,* 2023.

28. B. O. Counterterrorism. *Country Reports on Terrorism,* US Department of State, 2019.

29. M. Campbell-Verduyn & F. Giumelli. *Enrolling into Exclusion: African Blockchain and Decolonial Ambitions in an Evolving Finance/Security Infrastructure,* **Journal of Cultural Economy,** 15(4), 2022, 524–543.

30. M. Zachariadis, G. Hileman, & S. V. Scott. *Governance and Control in Distributed Ledgers: Understanding the Challenges Facing Blockchain Technology in Financial Services,* **Information and Organization,** 29(2), 2019, 105–117.

31. M. Dhali, S. Hassan, S. M. Mehar, K. Shahzad, & F. Zaman. *Cryptocurrency in the Darknet: Sustainability of the Current National Legislation,* **International Journal of Law and Management,** 65(3), 2023, 261–282.

32. E. A. Akartuna, S. D. Johnson, & A. Thornton. *Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi Study,* **Technological Forecasting and Social Change,** 179, 2022, 121632.

33. M. U. Nnam, B. O. Ajah, C. C. Arua, G. P. Okechukwu, & C. O. Okorie. *The War Must Be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria,* **International Journal of Cyber Criminology,** 13(2), 2019.

34. S. D. Jayasekara. *How Effective are the Current Global Standards in Combating Money Laundering and Terrorist Financing?,* **Journal of Money Laundering Control,** 24(2), 2021, 257–267.

35. B. Dowling, *Provable security of internet protocols* (Doctoral dissertation, Queensland University of Technology). Queensland University of Technology ePrints, 2017.

36. D. Eisermann. *Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges,* Berlin Risk, 2020.

37. T. Moskowitz. *The Illicit Antiquities Trade as a Funding Source for Terrorism: Is Blockchain the Solution,* **Cardozo Arts & Ent. LJ,** 37, 2019, 193.

38. S. Wagman. *Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing,* **Harv. Nat'l Sec. J.,** 14, 2022, 87.

39. M. Constantinescu. *The Security Implications of Cryptocurrencies,* **International Scientific Conference Strategies XXI,** 2020, 179.

40. S. M. S. Zaidi. *Emerging Realities in the International Political System: Transforming State's Foreign Policy,* **Herald of the Russian Academy of Sciences,** 2023, 1–14.

41. O. Ariani & A. L. Ibrahim. *Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia,* **Jurnal Usm Law Review,** 7(1), 2023, 30–44.

42. A. Eaddy. *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation), 2019.

43. P. C. Patel & J. Richter. *The Relationship Between Terrorist Attacks and Cryptocurrency Returns,* **Applied Economics,** 53(8), 2021, 940–961.

44. O. T. Emmanuel & A. A. Michael. *Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria,* **Journal of Auditing, Finance, and Forensic Accounting,** 8(2), 2020, 55–66.

45. S. K. Fakunmoju, O. Banmore, A. Gbadamosi, & O. I. Okunbanjo. *Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance,* **Binus Business Review,** 13(1), 2022, 31–40.

46. CBN. *Guidelines on Operations of Bank Accounts for Virtual Assets Service Providers (VASPs),* https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf , 2023.

47. D. Eisermann. *Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges,* Berlin Risk, 2020.

48. F. M. Opebiyi. *Regulating User Interactions Within the Financial Technology Market: Cryptocurrencies in Nigeria* (Doctoral Dissertation, University of Manchester), 2022.

49. K. Udofa. *Evaluating the Viability of Cryptocurrencies Within the Legal Regime for Electronic Payments in English Law* (Doctoral dissertation, University of Sheffield), 2020.

50. V. Ediagbonya & T. C. Tioluwani. *The Growth and Regulatory Challenges of Cryptocurrency Transactions in Nigeria,* In *The Complexities of Sustainability,* 2023, 267–297.

51. C. Irina. *Cryptocurrencies Legal Regulation,* **BRICS Law Journal,** 5(2), 2018, 128–153.

52. A. Ariwoola. *The State Adoption of Cryptocurrencies in Nigeria: The Place of Taxation as a Regulatory Instrument,* Available at SSRN 4532562, 2023.

53. S. Unal & M. Altun. *The Role of Financial Intelligence in Combating the Financing of Terrorism,* **Journal of Money Laundering Control,** 24(3), 2021, 571–583.

54. G. Pavlidis. *The Dark Side of Anti-Money Laundering: Mitigating the Unintended Consequences of FATF Standards,* **Journal of Economic Criminology,** 2, 2023.

55. O. J. Olujobi & E. T. Yebisi. *Combating the Crimes of Money Laundering and Terrorism Financing in Nigeria: A Legal Approach for Combating the Menace,* **Journal of Money Laundering Control,** 26(2), 2023, 268–289.

56. N. A. Al-Suwaidi & H. Nobanee. *Anti-Money Laundering and Anti-Corruption Financing: A Survey of the Existing Literature and a Future Research Agenda,* **Journal of Money Laundering Control,** 24(2), 2021, 396–426.

57. W. Ma. *Terrorist Financing, War Crimes, and Crypto Geopolitics,* In *A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects.* Cham: Springer Nature Switzerland, 2023, 241–259.

58. E. A. Valvi. *The Role of Legal Professionals in the European and International Legal and Regulatory Framework Against Money Laundering,* **Journal of Money Laundering Control,** 26(7), 2023, 28–52.

59. W. Ma. *Terrorist Financing, War Crimes, and Crypto Geopolitics,* In *A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects.* Cham: Springer Nature Switzerland, 2023, 241–259.

60. A. Majumder, M. Routh, & D. Singha. *A Conceptual Study on the Emergence of Cryptocurrency Economy and its Nexus with Terrorism Financing,* In *The Impact of Global Terrorism on Economic and Political Development.* Emerald Publishing Limited, 2019, 125–138.

61. C. Wilson. *International Institutions: An Underutilized Tool for Combating the Financing of Terrorism,* 2022.

62. J. C. Morse. *Blacklists, Market Enforcement, and the Global Regime to Combat Terrorist Financing,* **International Organization,** 73(3), 2019, 511–545.

63. M. Campbell-Verduyn & F. Giumelli. *Enrolling into Exclusion: African Blockchain and Decolonial Ambitions in an Evolving Finance/Security Infrastructure,* **Journal of Cultural Economy,** 15(4), 2022, 524–543.

64. M. Zachariadis, G. Hileman & S. V. Scott. *Governance and Control in Distributed Ledgers: Understanding the Challenges Facing Blockchain Technology in Financial Services,* **Information and Organization,** 29(2), 2019, 105–117.

65. Y. S. Shukhratovna, S. B. To‘lqinovich, & B. L. Ibragimovna. *Monetary Policy of Uzbekistan and Its Improvement Ways in Implementing,* **The Journal of Contemporary Issues in Business and Government,** 27(1), 2021, 1551–1557.

66. B. S. Bernanke. *The New Tools of Monetary Policy,* **American Economic Review,** 110(4), 2020, 943–983.

67. M. Dhali, S. Hassan, S. M. Mehar, K. Shahzad, & F. Zaman. *Cryptocurrency in the Darknet: Sustainability of the Current National Legislation,* **International Journal of Law and Management,** 65(3), 2023, 261–282.

68. E. A. Akartuna, S. D. Johnson, & A. Thornton. *Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi Study,* **Technological Forecasting and Social Change,** 179, 2022, 121632.

69. T. H. Crawford. *Actor-Network Theory,* In *Oxford Research Encyclopedia of Literature,* 2020.

70. D. Camacho, A. Panizo-Ledot, G. Bello-Orgaz, A. Gonzalez-Pardo, & E. Cambria. *The Four Dimensions of Social Network Analysis: An Overview of Research Methods, Applications, and Software Tools,* **Information Fusion,** 63, 2020, 88–120.

71. R. Rawat. *Logical Concept Mappings and Social Media Analytics Relating to Cyber-Criminal Activities for Ontology Creation,* **International Journal of Information Technology,** 15(2), 2023, 893–903.

72. R. Rawat, V. Mahor, A. S. Chirgaiya, & A. S. Rathore. *Applications of Social Network Analysis to Managing the Investigation of Suspicious Activities in Social Media Platforms,* In *Advances in Cybersecurity Management.* Cham: Springer International Publishing, 2021, 315–336.

73. D. Bright, R. Brewer, & C. Morselli. *Reprint of: Using Social Network Analysis to Study Crimes: Navigating the Challenges of Criminal Justice Records,* **Social Networks,** 69, 2022, 235–250.

74. W. H. Sandholm. *Evolutionary Game Theory, Complex Social and Behavioral Systems: Game Theory and Agent-Based Mode,* 2020.

75. M. Maschler, S. Zamir, & E. Solan. *Game Theory,* Cambridge University Press, 2020.

76. S. Gupta, M. K. Starr, R. Zanjirani Farahani, & M. M. Ghodsi. *Prevention of Terrorism—An Assessment of Prior POM Work and Future Potentials,* **Production and Operations Management,** 29(7), 2020, 1789–1815.

77. P. Balcaen, C. D. Bois, & C. Buts. *A Game-Theoretic Analysis of Hybrid Threats,* **Defence and Peace Economics,** 33(1), 2022, 26–41.

78. A. T. Wardhana & B. W. Nugroho. *Abuse of Cryptocurrency to Funding International Terrorism Activities,* In *Proceedings Universitas Muhammadiyah Yogyakarta Undergraduate Conference,* 1(1), 2021, 353–362.

79. P. C. Patel & J. Richter. *The Relationship Between Terrorist Attacks and Cryptocurrency Returns,* **Applied Economics,** 53(8), 2021, 940–961.

80. V. Dyntu & O. Dykyj. *Cryptocurrency as an Instrument of Terrorist Financing,* **Baltic Journal of Economic Studies,** 7(5), 2021, 67–72.

81. L. Almaqableh, K. Reddy, V. Pereira, V. Ramiah, D. Wallace, & J. F. Veron. *An Investigative Study of Links Between Terrorist Attacks and Cryptocurrency Markets,* **Journal of Business Research,** 147, 2022, 177–188.

82. A. Andrianova. *Countering the Financing of Terrorism in the Conditions of Digital Economy,* In *Digital Transformation of the Economy: Challenges, Trends and New Opportunities.* Springer International Publishing, 2020, 20–31.

83. S. A. Ibrahim. *Decrypting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing,* **Pakistan Horizon,** 74(1), 2021, 73–89.

84. V. Pașca & D. S. Orza. *Terrorism: Between the Need for Funding and Obtaining Funding Sources,* **Journal of Eastern European Criminal Law,** 1, 2019.

85. S. A. Ibrahim. *Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering,* **Stratagem,** 2(1), 2019.

86. E. Fletcher, C. J. Larkin, & S. Corbet. *Cryptocurrency Regulation: Countering Money Laundering and Terrorist Financing,* Available at SSRN 3704279.

87. H. Hasibuan, L. Tijow, & S. Koos. *Terrorism Financing Countermeasures in an Evolving Ideological Dynamics of Global Counterterrorism,* **Lex Publica,** 10(1), 2023, 215–239.

88. T. N. E. Al-Tawil. *Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches,* **Journal of Money Laundering Control,** 26(6), 2023, 1150–1164.

89. F. M. J. Teichmann & M. C. Falker. *Cryptocurrencies and Financial Crime: Solutions, Liechtenstein,* **Journal of Money Laundering Control,** 24(4), 2021, 775–788.

90. N. G. Packin & U. Volovelsky. *Digital Assets, Anti-Money Laundering and Counter Financing of Terrorism: An Analysis of Evolving Regulations and Enforcement in the Era of NFTs,* In *The Cambridge Handbook on Law and Policy for NFTs* (Nizan Geslevich Packin, ed.), Forthcoming, 2023.

91. R. Botha. *The Potential Anti-Money Laundering and Counter-Terrorism Financing Risks and Implications of Virtual Currencies on the Prevailing South African Regulatory and Supervisory Regime* (Master's thesis, University of Pretoria (South Africa)), 2019.

92. A. L. Carsello. *Combatting Crypto Crimes: An Examination of the Existing Regulations Surrounding Cryptocurrency* (Doctoral dissertation, Utica College), 2021.

93. W. Haichao. *Exploring the Regulations of Cryptocurrencies in China—Global Regulations Based on Cryptocurrency Decentralization* (Doctoral Dissertation, SIAM University), 2023.

94. M. Amini, A. Ouassini, & N. Ouassini. *Cyber Dimensions of Terrorism Funding,* In *Countering Terrorist and Criminal Financing.* CRC Press, 2023, 197–206.

95. P. Weichbroth, K. Wereszko, H. Anacka, & J. Kowal. *Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments,* **Sensors,** 23(6), 2023, 3155.

96. D. Eisermann. *Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges,* Berlin Risk, 2020.

97. S. Wagman. *Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing,* **Harv. Nat'l Sec. J.,** 14, 2022, 87.

98. A. O. Oladipupo. *"Role of Cryptocurrency in Geopolitical Conflicts: Cybersecurity Concerns in International Diplomacy*" In Politics and International Relations *Book of Reading,* Edited by T. Oseni, A. Amodu, & O. Badru, L**ead City University Press,** 2024, 439–458.

99. A. O. Oladipupo & A. A. Amodu. *An Overview of Cryptocurrencies and the Nigeria Experience*. *Lead City Faculty of Social Science Conference Proceeding*, –, 2023.

100. A. O. Oladipupo, D. M. Oyedokun, & E. N. Fasola. *Cryptocurrency Ban in Nigeria: Implications for Domestic and International Trade*. **International Journal of Research and Innovation in Social Science**, 7(1), 2023, 539–551.

101. A. O. Oladipupo & A. A. Amodu. *Impact of Cryptocurrency Ban on the Development of Cryptocurrency in Nigeria*. **Renaissance University Journal of Management and Social Sciences,** 8(2), 2022.

Chapter Three

Methodology

3.1 Research Design

This study adopted descriptive survey research design was anchored integrating Concurrent sequential research design wholely at the first phase to compare cryptocurrency and terrorism financing in Nigeria and Kenya with reference to global practices. At the second phase, contetnt Analysis research design was adopted.

3.2 Population of the study

The population of this study comprised professionals and experts from various sectors across both countries who possess specialized knowledge in cryptocurrency regulation, financial intelligence, counter-terrorism financing, cybersecurity, and related fields.

In Nigeria, the population encompasses representatives from the Security Exchange Commission (SEC), Economic and Financial Crimes Commission (EFCC), National Security Adviser's Office, Financial Intelligence Unit, registered cryptocurrency trading firms, financial institutions, cybersecurity companies, and academics specializing in finance, blockchain technology, and international relations. The Kenyan population includes counterparts from the Capital Markets Authority (CMA), Financial Reporting Centre (FRC), National Counter Terrorism Centre (NCTC), licensed cryptocurrency exchanges, financial institutions, and academic institutions.

Table 3.1: Distribution of Study Population

Sector	Institution Type	Nigeria	Kenya
Regulatory	Financial Regulators	Security Exchange Commission (SEC)	Capital Markets Authority (CMA)
	Financial Intelligence	Nigerian Financial Intelligence Unit (NFIU)	Financial Reporting Centre (FRC)
Law Enforcement	Economic Crime	Economic and Financial Crimes Commission (EFCC)	Ethics and Anti-Corruption Commission
	Security Agencies	Office of National Security Adviser	National Counter Terrorism Centre
Private Sector	Cryptocurrency Industry	Registered Crypto Trading Firms	Licensed Cryptocurrency Exchanges
	Financial Institutions	Commercial Banks, Fintech Companies	Commercial Banks, Fintech Companies
Academia	Research	University Departments, Think Tanks	Research Institutes, Universities

The diversity of this population ensures comprehensive coverage of the multifaceted issues surrounding cryptocurrency regulation and terrorism financing from regulatory, law enforcement, private sector, technical, and academic perspectives across both countries.

3.3 Sample and Sampling Techniques

This study employs a purposive sampling technique to select respondents with specific expertise and experience relevant to cryptocurrency regulation and terrorism financing in both Nigeria and Kenya. Purposive sampling was chosen due to the specialized nature of the research topic and the need to obtain insights from individuals with in-depth knowledge and practical experience in the field. The researcher deliberately selected participants based on their professional roles, expertise, and ability to provide informed perspectives on the research questions.

For quantitative questionnaire respondents, a total of 103 participants were sampled as these are the total numbers of the participants that responded to the questionnaire, with Nigeria (N = 67) and Kenya (N = 36). The questionnaires were distributed to financial regulators, cryptocurrency experts, security professionals, and academics to capture diverse insights on the challenges and opportunities associated with cryptocurrency in terrorism financing across both countries. For in-depth interviews, qualitative method was conducted, a total of 11 key informants participated, with Nigeria (N = 7) and Kenya (N = 4). These interviews provided practical insights into how each country manages cryptocurrency-related risks while promoting innovation.

The selection criteria for participants included: (1) a minimum of five years of professional experience in relevant fields; (2) current employment in institutions directly involved in

cryptocurrency regulation, counter-terrorism financing, or related areas; (3) demonstrated expertise through publications, policy contributions, or operational roles; and (4) willingness to provide detailed perspectives on sensitive regulatory and security topics. This approach ensured that the sample, though limited in size, represented high-quality information sources capable of providing nuanced insights into the complex issues under investigation. They are selected based on their area of specialization and expertees knowledge on Blockchain Technology, Crytocurrency Trading, Financial Regulators and Security Studies.

Table 3.1: Sample Distribution for Questionnaire Respondents

Sector	Institution Type	Nigeria (N=67)	Kenya (N=36)	Total (N=103)
Regulatory	Financial Regulators	12	6	18
	Financial Intelligence	8	5	13
Law Enforcement	Economic Crime	9	5	14
	Security Agencies	7	4	11
Private Sector	Cryptocurrency Industry	11	5	16
	Financial Institutions	9	4	13
Academia	Technology Research	6	4	10
	Policy Research	5	3	8

Table 3.2: Sample Distribution for In-depth Interviews

Sector	Position	Nigeria (N=7)	Kenya (N=4)	Total (N=11)
Regulatory Bodies	Senior Officials	2	1	3

Law Enforcement	Investigators/Analysts	2	1	3
Cryptocurrency Industry	Compliance Officers	1	1	2
Financial Institutions	Risk Managers	1	0	1
Academia	Professors/Researchers	1	1	2

The sample size determination was influenced by several factors, including (1) the limited pool of experts with specialised knowledge in the intersection of cryptocurrency and terrorism financing in both countries; (2) access constraints, particularly within security and intelligence agencies; (3) the principle of information richness rather than statistical representation; and (4) practical considerations regarding time and resource availability for data collection across two countries. The higher number of participants from Nigeria compared to Kenya reflects the relative sizes of the financial sectors and the more established nature of cryptocurrency usage in Nigeria.

Response rates for the questionnaire were 83.8% for Nigeria (67 out of 80 distributed) and 78.3% for Kenya (36 out of 46 distributed), reflecting the high level of engagement among selected experts. For interviews, all targeted respondents participated, indicating the perceived importance of the research topic among key stakeholders in both countries. This comprehensive sampling approach ensured that the study captured diverse perspectives across relevant sectors while maintaining focus on individuals with substantive expertise in the specialised research area.

3.4 Description of Research Instruments

This study utilised three primary data collection instruments: a structured questionnaire, key in-depth interviews, and case studies to comprehensively analyse the dynamics of cryptocurrency and terrorism financing in Nigeria, Kenya, and on a global scale. The research

design integrated quantitative and qualitative approaches to capture detailed insights from experts, stakeholders, and real-world examples.

Questionnaire

The questionnaire began with demographic data to establish a baseline understanding of respondents' backgrounds. Participants were asked to provide information about their gender, age, education level, employment status, ethnicity/race, marital status, location, religion, place of work, and position. This ensured that the sample reflected diverse professional and personal experiences relevant to the study. Following this, the questionnaire was divided into five sections, each addressing critical aspects of cryptocurrency and terrorism financing.

In Section A, respondents identified specific methods and strategies employed by terrorist groups to utilise cryptocurrency for funding their operations. Questions explored whether terrorist groups acquired cryptocurrency funds, converted them into usable assets, used privacy-focused cryptocurrencies or mixed services to obscure financial activities, exploited decentralised finance (DeFi) platforms, or adopted technological innovations to enhance their operations. This Section contained 10 items.

Section B evaluated the effectiveness of existing international regulatory frameworks and law enforcement efforts in countering cryptocurrency-based terrorism financing. Respondents assessed whether current regulations adequately addressed these challenges, examined the tools used by law enforcement agencies to trace transactions, and identified gaps in enforcement strategies. This Section also included questions about notable successes in disrupting terrorist financing activities through cryptocurrency-related investigations. It consisted of 10 items.

Section C analysed the impact of cryptocurrency on the dynamics of international terrorism, including its potential to facilitate cross-border activities and radicalisation. Respondents considered whether cryptocurrency had changed the funding sources of terrorist organisations, facilitated propaganda, or played a role in lone-wolf attacks. The Section explored how the pseudonymous nature of cryptocurrency transactions impacted efforts to identify and track terrorist financing. It contained 10 items.

Section D assessed the broader implications of cryptocurrency usage on the global security landscape. Respondents evaluated whether the integration of cryptocurrency posed vulnerabilities to traditional financial systems, played a role in cyber warfare, or affected economic sanctions and financial controls. The Section highlighted emerging security risks and opportunities for collaboration between the cryptocurrency industry and security stakeholders. It consisted of 9 items.

Finally, Section E developed comprehensive recommendations for policymakers and international organisations to strengthen global counter-terrorism efforts. Respondents suggested ways to enhance regulatory frameworks, improve coordination among agencies, involve technology companies, and implement public awareness campaigns. The Section emphasised the importance of standardised guidelines, enhanced AML/CTF measures, and specialised task forces dedicated to combating cryptocurrency-enabled terrorism. It contained 10 items. In total, the questionnaire comprised 49 items distributed across the five sections.

Key In-Depth Interviews

To complement the quantitative data collected through the questionnaire, key in-depth interviews were conducted with stakeholders from critical sectors, including the Securities

Exchange Commission, Economic and Financial Crime Commission, National Security Adviser's Office, registered crypto trading firms, academia, and subject matter experts. These interviews delved deeper into the themes explored in the questionnaire, providing richer, qualitative insights.

Interviewees were first asked to identify specific methods and strategies employed by terrorist organisations to utilise cryptocurrency for financing their activities. For instance, representatives from the Securities Exchange Commission discussed how they monitored and detected suspicious cryptocurrency transactions potentially linked to terrorist organisations organisations. Members of the Economic and Financial Crime Commission shared common tactics used by terrorist groups and described their collaboration with international agencies. National Security Advisers provided insights into regional trends and patterns in cryptocurrency usage by terrorist organisations.

Next, interviewees evaluated the effectiveness of existing international regulatory frameworks and law enforcement efforts in countering cryptocurrency-based terrorism financing. They discussed whether current regulations adequately addressed these challenges, identified limitations or gaps in enforcement strategies, and highlighted opportunities for improvement. Collaboration with international agencies and the role of financial intelligence units (FIUs) were also explored.

The interviews then analysed the impact of cryptocurrency on the dynamics of international terrorism, including its potential to facilitate cross-border activities and radicalisation. Registered crypto trading firms in Nigeria shared instances where cryptocurrency transactions had been linked to cross-border terrorist financing. At the same time, academics and experts

examined the role of cryptocurrency in the radicalisation process and proposed preventative measures.

Following this, interviewees assessed the impact of cryptocurrency usage on the global security landscape.Here a rephrased version

They examined the impact of cryptocurrency integration on conventional security protocols, pinpointed critical security vulnerabilities, and determined the most pressing issues to address and prioritised. National Security Advisers elaborated on how the proliferation of cryptocurrency impacted national security strategies and outlined measures in place to mitigate associated risks.

Finally, interviewees developed comprehensive recommendations for policymakers and international organisations to strengthen global counter-terrorism efforts. Cryptocurrency firms suggested contributions they could make to these efforts and recommended internal measures to prevent misuse. Academics and experts proposed strategies and initiatives that policymakers and international organisations should prioritise to address the intersection of cryptocurrency and terrorism financing. The interview guide consisted of five thematic areas, with a total of 13 questions distributed across these areas.

Case Studies

In addition to the questionnaire and interviews, case studies were developed to provide real-world examples of cryptocurrency-related terrorism financing in Nigeria, Kenya, and globally. These case studies highlighted specific instances where cryptocurrency had been used to fund terrorist activities, regional trends in cryptocurrency adoption by extremist groups, and global implications of such practices.

Table 3.3: Structure of Research Instruments

Instrument Type	Structure	Target	Nigeria	Kenya	Global
Questionnaire	5 sections with 49 items	Practitioners and experts	67 respondents	36 respondents	N/A
In-depth Interviews	5 thematic areas with 15 questions	Key stakeholders and decision-makers	7 informants	4 informants	N/A
Case Studies	Systematic analysis framework	Documentary evidence and incidents	11 cases	6 cases	6 cases

3.5 Validity of Research Instrument

In this study, ensuring the validity of the research instruments, namely the questionnaire, key in-depth interviews, and case studies, was a critical step to guarantee the reliability and credibility of the findings.

To establish content validity, the research instruments were carefully reviewed by the supervisor, the researchers, two lecturers from the Department of Politics and International Relations, and three other experts in the fields of cryptocurrency regulation, terrorism financing, and security studies. These experts evaluated whether the items in the questionnaire and interview guide comprehensively covered the key themes and constructs relevant to the study's objectives. Their feedback ensured that the instruments captured all essential aspects of cryptocurrency and terrorism financing dynamics in Nigeria, Kenya, and globally.

For face validity, the instruments were assessed to ensure they appeared appropriate and meaningful to respondents. This involved pilot testing the questionnaire and interview guide with a small sample of experts from both Nigeria and Kenya. The pilot phase allowed the

researchers to identify any ambiguities, unclear phrasing, or culturally inappropriate elements within the instruments. Feedback gathered during this stage was incorporated into the final versions of the questionnaire and interview guide to enhance their clarity and cultural appropriateness.

After these reviews and pilot tests, necessary corrections and refinements were made to the instruments. For instance, questions were reworded for better comprehension, response options were adjusted for greater precision, and sections were reorganised to improve logical flow. These modifications ensured that the instruments not only measured what they intended but also resonated effectively with the target audience.

3.6 Reliability of Research Instrument

In this study, ensuring the reliability of the research instruments, namely the questionnaire, key in-depth interviews, and case studies, was essential for producing dependable and valid results. To achieve this, various established methods were employed, including statistical analyses such as Cronbach's Alpha for the questionnaire, along with iterative reviews and pilot testing for all instruments.

For the questionnaire, Cronbach's Alpha was used to assess its internal consistency. This statistical measure evaluates how closely related a set of items are as a group, indicating whether they measure the same underlying construct. The questionnaire contained 49 items distributed across five sections, each addressing critical aspects of cryptocurrency and terrorism financing dynamics. Cronbach's Alpha values were calculated for each section and the overall questionnaire. The analysis yielded a high Cronbach's Alpha value of 0.85, exceeding the commonly accepted threshold of 0.70. This result confirmed that the

questionnaire items were reliable and consistent in measuring the intended constructs, thereby strengthening the credibility of the data collected.

In addition to the questionnaire, the key in-depth interviews were designed to elicit detailed insights from experts in relevant fields. While qualitative data does not lend itself to statistical reliability measures like Cronbach's Alpha, the reliability of the interview guide was ensured through rigorous review processes. The interview questions were developed based on extensive literature reviews and consultations with subject matter experts, ensuring their relevance and comprehensiveness. Prior to full-scale administration, the interview guide underwent pilot testing with a small sample of experts from Nigeria and Kenya. Feedback gathered during this phase helped refine question phrasing, structure, and sequencing, enhancing the clarity and effectiveness of the instrument. These modifications ensured that the interview guide reliably captured nuanced perspectives on cryptocurrency and terrorism financing.

Similarly, the case studies were constructed to provide real-world examples and contextual depth to the study. Their reliability was ensured by adhering to established methodologies for developing case studies, including triangulation of data sources and peer reviews. Each case study was meticulously reviewed by the researcher, supervisor and two other external experts to verify accuracy and consistency in the interpretation of findings. Thus, the reliability of the research instruments was systematically addressed through a combination of statistical analyses, expert reviews, pilot testing, and iterative refinements.

3.7 Method of Data Collection

The research instruments were administered using digital platforms to facilitate ease of access and efficient data collection. The structured questionnaire was administered physically to respondents in Nigeria while it was administered electronically via Google Forms for Kenyan respondents, ensuring that respondents could conveniently complete and submit their answers online. This approach allowed for broader reach, enabling participants from Nigeria, Kenya, and other regions to participate without geographical constraints. Respondents received a unique link to the Google Form, along with clear instructions on how to complete and submit the questionnaire.

For the key in-depth interviews, a conversational format was adopted using Physical Conversation and Goggle meet. This method was chosen due to its accessibility and widespread use among the target populations in Nigeria and Kenya. Trained research assistants conducted the interviews via Physical and Goggle meet, allowing for real-time interaction while maintaining flexibility in scheduling. The interview questions, which were open-ended and designed to elicit detailed insights, were shared sequentially through the chat platform. Participants had the opportunity to respond at their convenience, ensuring thoughtful and comprehensive answers.

As such, the Researcher adopted both Qualitative and Quantitiative analysis. Quantitative analysis involves simple percentage calculations and mean decision techniques to evaluate survey responses from stakeholders in both countries, enabling numerical comparison of opinions on cryptocurrency regulation, terrorism financing risks, and policy effectiveness. Qualitative analysis employs thematic coding of in-depth interviews with key stakeholders using NVIVO software to identify themes, patterns, and differences in regulatory approaches

and challenges. The case study method examines Nigeria (West Africa), Kenya (East Africa), and global best practices as a benchmark

To ensure the reliability and validity of the data collected, both the Google Form questionnaire and Goggle meet interviews underwent pilot testing with a small sample of experts from Nigeria and Kenya. Feedback gathered during this phase was used to refine the instruments, enhancing their clarity and cultural appropriateness. Additionally, a formal letter of introduction from Lead City University was presented to relevant authorities and organisations to gain access to key stakeholders and establish the credibility of the study.

3.8 Method of Data Analysis

This study employed a mixed-methods analytical approach to examine the comparative dynamics of cryptocurrency and terrorism financing in Nigeria and Kenya. The data collected through structured questionnaires, in-depth interviews, and case studies was rigorously analysed using a combination of quantitative and qualitative techniques to ensure a comprehensive exploration of the research questions and hypotheses.

For the quantitative data obtained from the questionnaires, the analysis began with descriptive statistics, including frequencies, percentages, means, and standard deviations, to provide a clear overview of response patterns across both countries. Simple percentage calculations were used to determine proportional distributions of opinions, while mean decision analysis established central tendencies for each measured variable, facilitating direct comparison between Nigerian and Kenyan contexts. These descriptive measures enabled the researcher to identify similarities and differences in stakeholder perceptions regarding cryptocurrency

regulation, terrorism financing risks, and policy effectiveness between the two countries. The SPSS 27 was used to analyse the data.

The following table summarizes the analytical techniques applied to the data:

Table 3.5: Analytical Techniques for Data Analysis

Data Source	Analytical Technique	Purpose	Output
Questionnaire	Simple Percentage and Mean Decision	Determine distribution and central tendencies	Comparative statistical profiles
Interviews	Thematic Analysis	Identify patterns and perspectives	Emergent themes and conceptual frameworks
Case Studies	Comparative Analysis	Examine contextual factors and outcomes	Cross-case synthesis and pattern matching

For the qualitative data collected through interviews and case studies, comparative thematic analysis was employed to identify, analyze, and report patterns within the data. This approach involved a systematic process of data familiarization, coding, theme development, and interpretation. The thematic analysis particularly focused on identifying cross-cutting issues, country-specific challenges, and divergent perspectives between Nigerian and Kenyan stakeholders. NVIVO statistical software facilitated this analytical process, allowing for systematic coding, categorization, and theme identification across all qualitative data sources.

The case study analysis employed a structured comparative approach to examine regulatory frameworks, implementation challenges, enforcement actions, and outcomes across Nigerian, Kenyan, and global contexts. This analysis utilized cross-case synthesis to identify patterns, similarities, differences, and best practices that could inform policy recommendations and implementation strategies in both countries. The global case studies served as benchmarks and

provided contextual reference points for evaluating the approaches and outcomes in Nigeria and Kenya.

Endnotes

1. S.R.M., Arifin, *Ethical Considerations in Qualitative Study*. **International Journal of Care Scholars,** 1(2), 2018.30-33.

2. P.G Hayashi, G. Abib, & N. Hoppen, *Validity in Qualitative Research: A Processual Approach.* **The Qualitative Report**, 24(1), 2019.98-112.

3. J. Rose, & C.W. Johnson, *Contextualizing Reliability and Validity In Qualitative Research: Toward More Rigorous And Trustworthy Qualitative Social Science In Leisure Research*. **Journal of Leisure Research,** 51(4), 2020. 432-451.

4. E.A Mezmir, *Qualitative Data Analysis: An Overview of Data Reduction, Data Display, and Interpretation*. **Research on Humanities and Social Sciences,** 10(21), 2020. 15-27.

Chapter Four

Results and Discussion of Findings

This chapter presents and analyses the findings from the comparative study of cryptocurrency-enabled terrorism financing in Nigeria and Kenya. It employs quantitative such as simple percentage and means decision and qualitative analysis of stakeholder survey data, comparative thematic analysis of in-depth interviews, and case studies drawn from

Nigeria, Kenya, and global contexts to examine terrorist financing methods, countermeasure effectiveness, network transformations, international linkages, and policy implications. These findings reveal the deeper relationship of digital currencies in terrorism financing across both nations, shedding light on regional security dynamics and global implications whilst addressing the study's objectives.

4.1 Demographic Data Analysis

Table 4.1: Distribution of Demographic Variable (N=103)

Demographic Variable	Category	Frequency (Nigeria)	Percentage (Nigeria)	Frequency (Kenya)	Percentage (Kenya)
Gender	Male	40	60%	21	58%
	Female	27	40%	14	39%
	Non-binary/Other	2	3%	1	3%
Age	Under 18	1	2%	1	3%
	18–24	7	10%	3	8%
	25–34	23	34%	12	33%
	35–44	17	25%	9	25%
	45–54	13	19%	7	19%
	55–64	4	6%	3	8%
	65 and over	2	3%	1	3%
Education Level	Primary	1	2%	0	0%
	Secondary	3	5%	2	6%
	Some College/Associate	7	10%	3	8%
	Bachelor's Degree	23	34%	12	33%
	Master's Degree	28	42%	14	39%
	Doctoral Degree	5	7%	5	14%
Employment Status	Employed Full-Time	47	70%	25	69%
	Employed Part-Time	10	15%	5	14%
	Self-Employed	6	9%	4	11%
	Unemployed	4	6%	2	6%
Ethnicity/Race	Yoruba	20	30%	-	-
	Hausa/Fulani	17	25%	-	-
	Igbo	10	15%	-	-
	Other Nigerian	8	12%	-	-

	Ethnicities				
	Kenyan Ethnic Groups	-	-	14	39%
	Other/Unspecified *	12	18%	22	61%
Marital Status	Single	20	30%	11	31%
	Married	40	60%	22	61%
	Divorced	5	7%	2	6%
	Widowed	2	3%	1	3%
Location	Urban	50	75%	27	75%
	Suburban	10	15%	5	14%
	Rural	7	10%	4	11%
Religion	Christianity	37	55%	20	56%
	Islam	27	40%	14	39%
	Other	3	5%	2	6%

Source: Researcher Fieldwork, 2025

4.2 Data Presentation and Analysis

4.2.1 Analysis of Research Questions

RQ1: Identify the specific methods and strategies employed by terrorist organizations to utilize cryptocurrency for financing their activities in Nigeria and Kenya.

Table 4.2 Specific Methods and Strategies Employed by Terrorist Organizations to Utilize Cryptocurrency for Financing their Activities in Nigeria and Kenya

	Nigeria	Kenya

Items	Response	Responses Rate		Mean	Response	Responses Rate		Mean
		N	%			N	%	
Do terrorist organizations typically acquire cryptocurrency funds?	Yes	40	59.70	0.60	Yes	22	61.11	0.61
	No	27	40.30	-	No	14	38.89	-
Do terrorist groups convert cryptocurrency into usable assets or funds?	Yes	38	56.72	0.57	Yes	20	55.56	0.56
	No	29	43.28	-	No	16	44.44	-
Do terrorist organizations commonly use specific platforms or channels to transact with cryptocurrency?	Yes	35	52.24	0.52	Yes	18	50.00	0.50
	No	32	47.76	-	No	18	50.00	-
Do terrorist organizations conceal their cryptocurrency transactions to avoid detection?	Yes	42	62.69	0.63	Yes	24	66.67	0.67
	No	25	37.31	-	No	12	33.33	-
Do cryptocurrency exchanges play any role in facilitating terrorist financing?	Yes	39	58.21	0.58	Yes	21	58.33	0.58
	No	28	41.79	-	No	15	41.67	-
Do terrorist groups utilize privacy-focused cryptocurrencies or mixing services to obscure their financial activities?	Yes	37	55.22	0.55	Yes	20	55.56	0.56
	No	30	44.78	-	No	16	44.44	-
Are there specific regions or jurisdictions where terrorist organizations are more active in utilizing cryptocurrency?	Yes	25	37.31	0.37	Yes	13	36.11	0.36
	No	42	62.69	-	No	23	63.89	-
Do terrorist organizations employ tactics to launder cryptocurrency funds?	Yes	36	53.73	0.54	Yes	19	52.78	0.53
	No	31	46.27	-	No	17	47.22	-
Do terrorist organizations exploit decentralized finance (DeFi) platforms for money laundering?	Yes	32	47.76	0.48	Yes	17	47.22	0.47
	No	35	52.24	-	No	19	52.78	-

Source: Field Survey, 2025.

The data in Table 4.2 illustrate the methods and strategies terrorist organizations employ to utilize cryptocurrency for financing in Nigeria (N = 67) and Kenya (N = 36), based on survey responses. A majority reported that terrorist organizations acquire cryptocurrency funds (Nigeria: 59.70%, $\bar{X}$ = 0.60; Kenya: 61.11%, $\bar{X}$ = 0.61) and conceal transactions to avoid detection (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67). Over half indicated

conversion of cryptocurrency into usable assets (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 55.56%, $\bar{X}$ = 0.56), use of specific platforms (Nigeria: 52.24%, $\bar{X}$ = 0.52; Kenya: 50.00%, $\bar{X}$ = 0.50), reliance on exchanges (Nigeria: 58.21%, $\bar{X}$ = 0.58; Kenya: 58.33%, $\bar{X}$ = 0.58), use of privacy-focused cryptocurrencies or mixing services (Nigeria: 55.22%, $\bar{X}$ = 0.55; Kenya: 55.56%, $\bar{X}$ = 0.56), and laundering tactics (Nigeria: 53.73%, $\bar{X}$ = 0.54; Kenya: 52.78%, $\bar{X}$ = 0.53). Fewer than half noted exploitation of decentralized finance (DeFi) platforms (Nigeria: 47.76%, $\bar{X}$ = 0.48; Kenya: 47.22%, $\bar{X}$ = 0.47) or activity in specific regions (Nigeria: 37.31%, $\bar{X}$ = 0.37; Kenya: 36.11%, $\bar{X}$ = 0.36). These findings suggest that terrorist groups in Nigeria and Kenya commonly use cryptocurrency, especially to hide their transactions, though they rely less on specific regions or decentralized finance (DeFi) platforms.

RQ2: To critically evaluate the effectiveness of existing counter-terrorism financing frameworks in both countries, with specific focus on cryptocurrency regulations and their implementation.

Table 4.3 The Effectiveness of Existing Counter-Terrorism Financing Frameworks in Both Countries, with Specific Focus on Cryptocurrency Regulations and their Implementation

		Nigeria				Kenya		
Items	**Response**	**Responses**	**Rate**	**Mean**	**Response**	**Responses**	**Rate**	**Mean**
Does cryptocurrency facilitate cross-border financial transactions for terrorist groups?	Yes	45	67.16	0.67	Yes	26	72.22	0.72
	No	22	32.84	-	No	10	27.78	-
Have terrorist organizations leveraged cryptocurrency for propaganda or recruitment	Yes	33	49.25	0.49	Yes	18	50.00	0.50
	No	34	50.75	-	No	18	50.00	-

purposes?								
Does cryptocurrency play a role in financing lone-wolf terrorist attacks or small-scale operations?	Yes	32	47.76	0.48	Yes	17	47.22	0.47
	No	35	52.24	-	No	19	52.78	-
Do extremist groups exploit social media and online platforms to solicit cryptocurrency donations?	Yes	38	56.72	0.57	Yes	20	55.56	0.56
	No	29	43.28	-	No	16	44.44	-
Do the pseudonymous nature of cryptocurrency transactions impact efforts to identify and track terrorist financing?	Yes	42	62.69	0.63	Yes	24	66.67	0.67
	No	25	37.31	-	No	12	33.33	-
Does the global nature of cryptocurrency exchanges impact counter-terrorism efforts?	Yes	39	58.21	0.58	Yes	21	58.33	0.58
	No	28	41.79	-	No	15	41.67	-
Have instances occurred where cryptocurrency has been used to fund international terrorist activities?	Yes	37	55.22	0.55	Yes	20	55.56	0.56
	No	30	44.78	-	No	16	44.44	-
Does the decentralized nature of cryptocurrency networks affect the ability to disrupt terrorist financing?	Yes	35	52.24	0.52	Yes	18	50.00	0.50
	No	32	47.76	-	No	18	50.00	-
Do terrorist organizations employ strategies to leverage cryptocurrency for ideological or operational goals?	Yes	36	53.73	0.54	Yes	19	52.78	0.53
	No	31	46.27	-	No	17	47.22	-

Source: Researcher Fieldwork, 2025

The data in Table 4.3 evaluate the effectiveness of counter-terrorism financing frameworks in Nigeria (N = 67) and Kenya (N = 36), focusing on cryptocurrency regulations and their implementation, based on survey responses. A majority reported that cryptocurrency facilitates cross-border transactions for terrorist groups (Nigeria: 67.16%, $\bar{X}$ = 0.67; Kenya: 72.22%, $\bar{X}$ = 0.72) and that its pseudonymous nature hinders tracking efforts (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67). Over half indicated extremist groups exploit online platforms for cryptocurrency donations (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 55.56%, $\bar{X}$ = 0.56), the global nature of exchanges impacts counter-terrorism (Nigeria: 58.21%, $\bar{X}$ = 0.58; Kenya: 58.33%, $\bar{X}$ = 0.58), cryptocurrency funds international terrorism (Nigeria: 55.22%, $\bar{X}$

= 0.55; Kenya: 55.56%, $\bar{X}$ = 0.56), its decentralized nature affects disruption efforts (Nigeria: 52.24%, $\bar{X}$ = 0.52; Kenya: 50.00%, $\bar{X}$ = 0.50), and terrorist groups leverage it for ideological or operational goals (Nigeria: 53.73%, $\bar{X}$ = 0.54; Kenya: 52.78%, $\bar{X}$ = 0.53). However, fewer than half noted its use for propaganda or recruitment (Nigeria: 49.25%, $\bar{X}$ = 0.49; Kenya: 50.00%, $\bar{X}$ = 0.50) or lone-wolf attacks (Nigeria: 47.76%, $\bar{X}$ = 0.48; Kenya: 47.22%, $\bar{X}$ = 0.47). These findings highlight significant challenges in both Nigeria and Kenya, particularly with cross-border transactions, tracking pseudonymized funds, and regulating decentralized systems, suggesting gaps in current cryptocurrency regulatory frameworks.

RQ3: To examine how the adoption of cryptocurrency has transformed traditional terrorism financing networks in both countries and assess its impact on regional security dynamics.

Table 4.4: Adoption of Cryptocurrency Has Transformed Traditional Terrorism Financing Networks in Both Countries and Assess Its Impact on Regional Security Dynamics

	Nigeria			Kenya		
Items	**Response**	**Responses Rate**	**Mean**	**Response**	**Responses Rate**	**Mean**
Do terrorist groups convert cryptocurrency into usable assets or funds?	Yes	38 56.72	0.57	Yes	20 55.56	0.56
	No	29 43.28	-	No	16 44.44	-
Do terrorist organizations commonly use specific platforms or channels to	Yes	35 52.24	0.52	Yes	18 50.00	0.50

transact with cryptocurrency?								
	No	32	47.76	-	No	18	50.00	-
Do terrorist organizations conceal their cryptocurrency transactions to avoid detection?	Yes	42	62.69	0.63	Yes	24	66.67	0.67
	No	25	37.31	-	No	12	33.33	-
Do cryptocurrency exchanges play any role in facilitating terrorist financing?	Yes	39	58.21	0.58	Yes	21	58.33	0.58
	No	28	41.79	-	No	15	41.67	-
Do terrorist groups utilize privacy-focused cryptocurrencies or mixing services to obscure their financial activities?	Yes	37	55.22	0.55	Yes	20	55.56	0.56
	No	30	44.78	-	No	16	44.44	-
Are there specific regions or jurisdictions where terrorist organizations are more active in utilizing cryptocurrency?	Yes	25	37.31	0.37	Yes	13	36.11	0.36
	No	42	62.6900	-	No	23	63.89	-
Do terrorist organizations employ tactics to launder cryptocurrency funds?	Yes	36	53.73	0.54	Yes	19	52.78	0.53
	No	31	46.27	-	No	17	47.22	-
Do terrorist organizations exploit decentralized finance (DeFi) platforms for money laundering?	Yes	32	47.76	0.48	Yes	17	47.22	0.47
	No	35	52.24	-	No	19	52.78	-
Have terrorist groups adopted technological innovations to enhance their use of cryptocurrency?	Yes	34	50.75	0.51	Yes	18	50.00	0.50
	No	33	49.25	-	No	18	50.00	-

Source: Fieldwork, 2025.

The Table 4.4 examine how cryptocurrency adoption has transformed traditional terrorism financing networks in Nigeria (N = 67) and Kenya (N = 36) and assess its impact on regional security dynamics, based on survey responses. A majority reported that terrorist organizations

conceal cryptocurrency transactions to avoid detection (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), rely on exchanges for financing (Nigeria: 58.21%, $\bar{X}$ = 0.58; Kenya: 58.33%, $\bar{X}$ = 0.58), convert cryptocurrency into usable assets (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 55.56%, $\bar{X}$ = 0.56), use privacy-focused cryptocurrencies or mixing services (Nigeria: 55.22%, $\bar{X}$ = 0.55; Kenya: 55.56%, $\bar{X}$ = 0.56), and employ laundering tactics (Nigeria: 53.73%, $\bar{X}$ = 0.54; Kenya: 52.78%, $\bar{X}$ = 0.53). Over half also noted use of specific platforms (Nigeria: 52.24%, $\bar{X}$ = 0.52; Kenya: 50.00%, $\bar{X}$ = 0.50) and technological innovations (Nigeria: 50.75%, $\bar{X}$ = 0.51; Kenya: 50.00%, $\bar{X}$ = 0.50). Fewer than half indicated exploitation of decentralized finance (DeFi) platforms (Nigeria: 47.76%, $\bar{X}$ = 0.48; Kenya: 47.22%, $\bar{X}$ = 0.47) or activity in specific regions (Nigeria: 37.31%, $\bar{X}$ = 0.37; Kenya: 36.11%, $\bar{X}$ = 0.36). These findings suggest that cryptocurrency has shifted terrorism financing in Nigeria and Kenya toward more concealed and technologically enabled networks, enhancing operational secrecy and complicating regional security efforts, though without strong regional concentration.

RQ4: To investigate the interconnections between local cryptocurrency markets, international financial systems, and terrorism financing networks in Nigeria and Kenya.

Table 4.5: The Interconnections between Local Cryptocurrency Markets, International Financial Systems, and Terrorism Financing Networks in Nigeria and Kenya

		Nigeria			Kenya		
Items	**Responses Rate**	**Mean**		**Responses Rate**	**Mean**	**Responses Rate**	**Mean**
Has the widespread adoption of cryptocurrency influenced traditional financial systems and security paradigms?	Yes	45	67.16	0.67	Yes	26	72.22	0.72

	No	22	32.84	-	No	10	27.78	-
Does the integration of cryptocurrency pose vulnerabilities to global security infrastructure?	Yes	40	59.70	0.60	Yes	22	61.11	0.61
	No	27	40.30	-	No	14	38.89	-
Do state actors navigate the security implications of cryptocurrency adoption?	Yes	38	56.72	0.57	Yes	20	55.56	0.56
	No	29	43.28	-	No	16	44.44	-
Does cryptocurrency play a role in cyber warfare and state-sponsored terrorism?	Yes	35	52.24	0.52	Yes	18	50.00	0.50
	No	32	47.76	-	No	18	50.00	-
Do security agencies monitor and respond to threats associated with cryptocurrency usage?	Yes	42	62.69	0.63	Yes	24	66.67	0.67
	No	25	37.31	-	No	12	33.33	-
Are there emerging security risks or threats unique to cryptocurrency ecosystems?	Yes	39	58.21	0.58	Yes	21	58.33	0.58
	No	28	41.79	-	No	15	41.67	-
Does the anonymity of cryptocurrency transactions impact national security efforts?	Yes	37	55.22	0.55	Yes	20	55.56	0.56
	No	30	44.78	-	No	16	44.44	-
Can strategies be implemented to mitigate the security risks posed by cryptocurrency usage?	Yes	35	52.24	0.52	Yes	18	50.00	0.50
	No	32	47.76	-	No	18	50.00	-
Does the proliferation of cryptocurrencies affect traditional	Yes	36	53.73	0.54	Yes	19	52.78	0.53

methods of economic sanctions and financial controls?								
	No	31	46.27	-	No	17	47.22	-

The data in Table 4.5 examine the interconnections between local cryptocurrency markets, international financial systems, and terrorism financing networks in Nigeria (N = 67) and Kenya (N = 36), based on survey responses. A majority reported that widespread cryptocurrency adoption influences traditional financial systems and security paradigms (Nigeria: 67.16%, $\bar{X}$ = 0.67; Kenya: 72.22%, $\bar{X}$ = 0.72), security agencies monitor related threats (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), and it poses vulnerabilities to global security infrastructure (Nigeria: 59.70%, $\bar{X}$ = 0.60; Kenya: 61.11%, $\bar{X}$ = 0.61). Over half indicated emerging security risks unique to cryptocurrency ecosystems (Nigeria: 58.21%, $\bar{X}$ = 0.58; Kenya: 58.33%, $\bar{X}$ = 0.58), state actors navigate its security implications (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 55.56%, $\bar{X}$ = 0.56), anonymity impacts national security efforts (Nigeria: 55.22%, $\bar{X}$ = 0.55; Kenya: 55.56%, $\bar{X}$ = 0.56), proliferation affects economic sanctions and financial controls (Nigeria: 53.73%, $\bar{X}$ = 0.54; Kenya: 52.78%, $\bar{X}$ = 0.53), strategies can mitigate risks (Nigeria: 52.24%, $\bar{X}$ = 0.52; Kenya: 50.00%, $\bar{X}$ = 0.50), and it plays a role in cyber warfare and state-sponsored terrorism (Nigeria: 52.24%, $\bar{X}$ = 0.52; Kenya: 50.00%, $\bar{X}$ = 0.50). These findings suggest that cryptocurrency links local markets to international systems in Nigeria and Kenya, amplifying terrorism financing risks and challenging security frameworks through anonymity and global integration.

RQ 5: To develop context-specific policy recommendations for strengthening international cooperation and regulatory frameworks to combat cryptocurrency-enabled terrorism financing

Table 4.6: Develop Context-Specific Policy Recommendations for Strengthening International Cooperation and Regulatory Frameworks to Combat Cryptocurrency-Enabled Terrorism Financing

		Nigeria				Kenya		
Items	**Responses Rate**	**Mean**		**Responses Rate**	**Mean**	**Responses Rate**		**Mean**
Does the integration of cryptocurrency pose vulnerabilities to global security infrastructure?	Yes	48	71.64	0.72	Yes	28	77.78	0.78
	No	19	28.36	-	No	8	22.22	-
Do state actors navigate the security implications of cryptocurrency adoption?	Yes	45	67.16	0.67	Yes	26	72.22	0.72
	No	22	32.84	-	No	10	27.78	-
Does cryptocurrency play a role in cyber warfare and state-sponsored terrorism?	Yes	43	64.18	0.64	Yes	25	69.44	0.69
	No	24	35.82	-	No	11	30.56	-
Do security agencies monitor and respond to threats associated with cryptocurrency usage?	Yes	50	74.63	0.75	Yes	30	83.33	0.83
	No	17	25.37	-	No	6	16.67	-
Are there emerging security risks or threats unique to cryptocurrency ecosystems?	Yes	46	68.66	0.69	Yes	27	75.00	0.75
	No	21	31.34	-	No	9	25.00	-
Does the anonymity of cryptocurrency transactions impact national security efforts?	Yes	44	65.67	0.66	Yes	26	72.22	0.72
	No	23	34.33	-	No	10	27.78	-
Can strategies be implemented to mitigate the security risks posed by cryptocurrency usage?	Yes	42	62.69	0.63	Yes	24	66.67	0.67
	No	25	37.31	-	No	12	33.33	-
Does the proliferation of cryptocurrencies affect traditional methods of economic sanctions and financial controls?	Yes	41	61.19	0.61	Yes	23	63.89	0.64
	No	26	38.81	-	No	13	36.11	-
Are there opportunities for collaboration between the cryptocurrency industry and	Yes	38	56.72	0.57	Yes	22	61.11	0.61

security stakeholders to enhance global security measures?	No	29	43.28	-	No	14	38.89	-

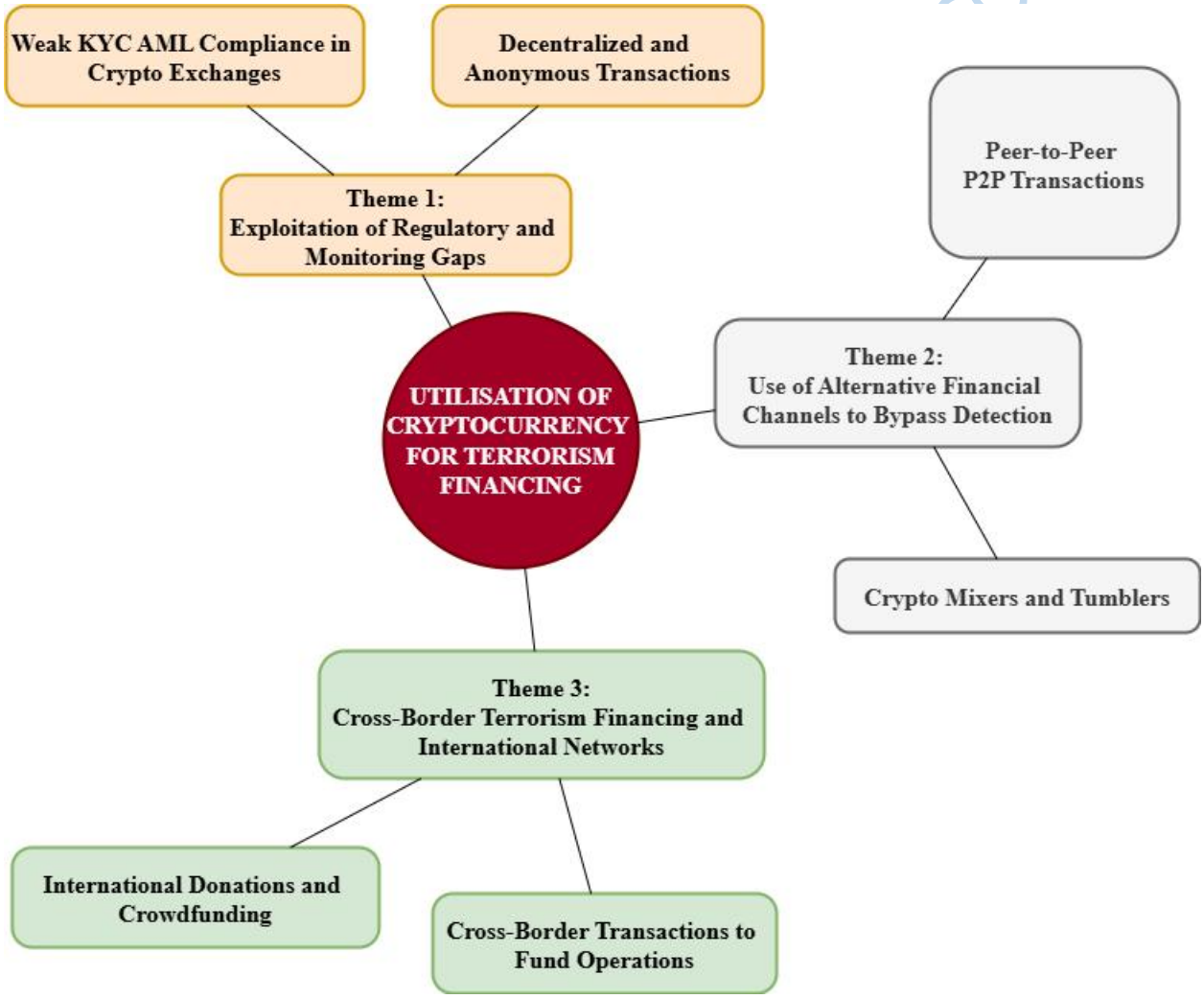
Source: Researcher's Fieldwork

The Table 4.6 provide insights for context-specific policy recommendations to strengthen international cooperation and regulatory frameworks against cryptocurrency-enabled terrorism financing in Nigeria (N = 67) and Kenya (N = 36), based on survey responses. A majority reported that security agencies monitor cryptocurrency threats (Nigeria: 74.63%, $\bar{X}$ = 0.75; Kenya: 83.33%, $\bar{X}$ = 0.83), integration poses vulnerabilities to global security (Nigeria: 71.64%, $\bar{X}$ = 0.72; Kenya: 77.78%, $\bar{X}$ = 0.78), emerging risks are unique to cryptocurrency ecosystems (Nigeria: 68.66%, $\bar{X}$ = 0.69; Kenya: 75.00%, $\bar{X}$ = 0.75), state actors navigate security implications (Nigeria: 67.16%, $\bar{X}$ = 0.67; Kenya: 72.22%, $\bar{X}$ = 0.72), anonymity impacts national security (Nigeria: 65.67%, $\bar{X}$ = 0.66; Kenya: 72.22%, $\bar{X}$ = 0.72), and cryptocurrency aids cyber warfare and state-sponsored terrorism (Nigeria: 64.18%, $\bar{X}$ = 0.64; Kenya: 69.44%, $\bar{X}$ = 0.69). Over half indicated strategies can mitigate risks (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), proliferation affects economic sanctions (Nigeria: 61.19%, $\bar{X}$ = 0.61; Kenya: 63.89%, $\bar{X}$ = 0.64), and collaboration with the cryptocurrency industry is possible (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 61.11%, $\bar{X}$ = 0.61). These findings suggest policies in Nigeria and Kenya should prioritize international collaboration to address global vulnerabilities, enhance monitoring, and leverage industry partnerships to counter anonymity and emerging threats in terrorism financing.

4.2.2 Thematic Analysis

RQ1: Comparative Thematic Analysis of Methods and Strategies Used by Terrorist Organizations to Utilize Cryptocurrency for Financing in Nigeria and Kenya

Based on the interview responses from seven Nigerian and four Kenyan respondents, several key themes and sub-themes emerge regarding the use of cryptocurrency for terrorism financing.



Source: Thematic Map of the Researcher's Fieldwork, 2025

Theme1: Exploitation of Regulatory and Monitoring Gaps

In Nigeria, despite regulatory efforts by the Economic and Financial Crimes Commission (EFCC) and Securities and Exchange Commission (SEC), terrorist groups continue to exploit weaknesses in Know-Your-Customer (KYC) and Anti-Money Laundering (AML) compliance. Weak enforcement allows individuals to create multiple anonymous cryptocurrency accounts, making it difficult for authorities to track illicit transactions, as noted by Respondent A. This lack of strict oversight creates an environment where terrorist financiers can operate with relative ease. While Nigerian exchanges are now required to implement stricter KYC policies, peer-to-peer (P2P) platforms remain largely unregulated, providing a safe avenue for illicit activities, according to Respondent B. Similarly, in Kenya, the Central Bank of Kenya (CBK) has yet to enforce strict regulations on cryptocurrency exchanges. Although Kenyan exchanges are aware of potential misuse, the absence of licensing and oversight leaves significant loopholes for terrorist financiers, as highlighted by Respondent H. Furthermore, most Kenyan transactions occur through unregulated digital wallets, making it easier for criminals to operate undetected, as explained by Respondent I. These gaps in regulation highlight the urgent need for stronger enforcement mechanisms to curb the misuse of cryptocurrencies for illegal purposes.

Terrorist groups in both Nigeria and Kenya take advantage of the decentralized nature of cryptocurrencies, which eliminates the need for intermediaries such as banks. In Nigeria, Respondent C pointed out that the anonymity of blockchain transactions makes it extremely challenging for authorities to trace funds back to their source. This anonymity is further exacerbated in Kenya, where Respondent J noted that privacy-focused cryptocurrencies like Monero and Zcash are increasingly being used due to their strong encryption features, which

obscure financial trails even more. The decentralized and anonymous nature of these transactions not only complicates law enforcement efforts but also demonstrates how technological advancements can be exploited for illicit activities. As terrorist groups continue to adapt to these technologies, addressing these challenges requires a combination of enhanced monitoring tools, international cooperation, and stricter regulatory frameworks to ensure transparency and accountability in the cryptocurrency ecosystem.

The exploitation of regulatory gaps and the use of decentralized technologies underscore the complexities involved in combating terrorism financing through cryptocurrencies. Both Nigeria and Kenya face unique challenges in regulating this emerging financial landscape, but the cross-border nature of these transactions highlights the importance of global collaboration. Strengthening regulatory measures, improving enforcement capabilities, and leveraging technology to monitor suspicious activities, authorities can better mitigate the risks posed by the misuse of cryptocurrencies for illicit purposes. This concerted effort is essential to disrupt terrorist networks and protect financial systems from abuse.

Use of Alternative Financial Channels to Bypass Detection

In Nigeria, peer-to-peer (P2P) trading has become the most common method for terrorism financing, as highlighted by Respondent D. Terrorists employ a technique known as "smurfing," where they conduct multiple small transactions across different wallets to avoid detection. This strategy makes it difficult for authorities to identify and track illicit activities. Respondent E further explained that P2P platforms allow direct transfers without involving traditional financial institutions, which significantly complicates efforts by regulators to freeze funds or intervene in suspicious transactions. In Kenya, the integration of cryptocurrency with mobile money systems presents another major loophole. According to

Respondent K, terrorist groups often convert cryptocurrency into mobile money and subsequently withdraw cash through platforms like M-Pesa or other local payment systems. This process enables them to bypass the scrutiny typically associated with traditional banking systems. Unlike Nigeria, where stricter mobile money regulations limit such practices, Kenya's less stringent oversight creates an environment conducive to these illicit operations.

Terrorist groups in Nigeria also rely on crypto mixers and tumblers to obscure their financial activities. Respondent F noted that these services combine illicit funds with legitimate transactions, making it nearly impossible to trace the original source of the funds. Additionally, Respondent G pointed out that foreign-based mixers are frequently used, adding another layer of complexity to law enforcement efforts due to jurisdictional challenges. While mixing services are less prominent in Kenya, Respondent H stated that criminals there increasingly use multiple exchange platforms to move funds across borders, achieving a similar effect of laundering money. These cross-border operations highlight the need for enhanced international cooperation and more sophisticated monitoring tools to address the evolving tactics employed by terrorist organizations. The decentralized nature of cryptocurrencies and the increasing sophistication of laundering techniques underscore the urgent requirement for robust regulatory frameworks and advanced technological solutions to combat these threats effectively.

Cross-Border Terrorism Financing and International Networks

In Nigeria and Kenya, significant cross-border crypto transactions linked to terrorism pose a growing concern. Respondent B noted that in Nigeria, funds are frequently transferred to affiliates in the Sahel region and the Middle East, enabling continued insurgency activities. Similarly, Respondent J reported that in Kenya, cryptocurrency is used to send funds to

Somalia's Al-Shabaab, effectively bypassing traditional banking restrictions. These cross-border transactions highlight how cryptocurrencies facilitate the movement of funds across borders with minimal oversight, complicating efforts by authorities to monitor and disrupt these financial flows.

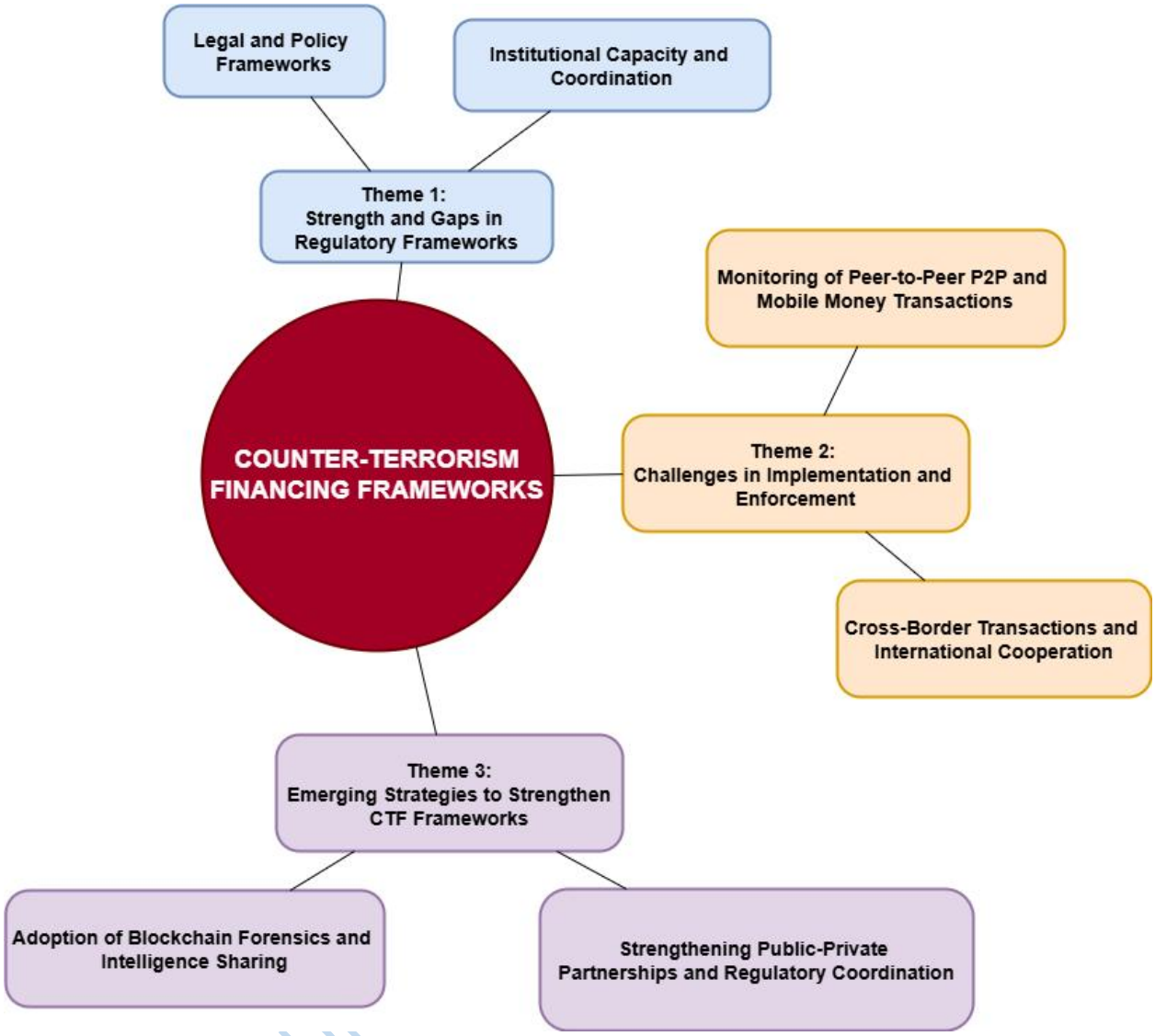
Terrorist groups in Kenya have also adopted social media and encrypted messaging apps as tools for soliciting cryptocurrency donations, according to Respondent I. Unlike Nigeria, where funding tends to be more transactional, Kenyan extremist groups increasingly rely on international donors who contribute through Bitcoin and privacy coins like Monero or Zcash, as explained by Respondent K. This reliance on international crowdfunding reflects the adaptability of terrorist organizations in leveraging technology to secure financial support while maintaining anonymity. The use of privacy-focused cryptocurrencies further obscures financial trails, making it harder for law enforcement agencies to trace the origin and destination of these funds.

Both Nigeria and Kenya face common challenges in tracking cryptocurrency transactions due to weak KYC/AML enforcement, the prevalence of P2P trading, and the exploitation of decentralized financial channels. However, there are notable differences in how terrorist groups operate within each country. In Nigeria, despite having a more regulated cryptocurrency environment, terrorist groups rely heavily on crypto-mixing services and P2P transactions to disguise their financial activities. On the other hand, Kenyan terrorists exploit mobile money integrations and international crowdfunding efforts to finance their operations. These distinct strategies reflect the varying regulatory landscapes and technological ecosystems in both countries. Cross-border crypto transactions remain a critical issue for both nations, underscoring the need for stronger international cooperation, enhanced regulatory

frameworks, and advanced monitoring technologies to combat terrorism financing effectively. Addressing these challenges requires a coordinated global response to close loopholes and ensure greater transparency in the cryptocurrency space.

RQ2: Comparative Thematic Analysis of the Effectiveness of Counter-Terrorism Financing Frameworks in Nigeria and Kenya

The effectiveness of counter-terrorism financing (CTF) frameworks in Nigeria and Kenya depends on regulatory strength, enforcement mechanisms, and technological capacity. While Nigeria has a more structured regulatory framework, enforcement gaps persist, especially in peer-to-peer (P2P) transactions. Kenya, on the other hand, lacks clear cryptocurrency regulations, making illicit transactions harder to track. The following themes and sub-themes highlight the key strengths and weaknesses in both countries' cryptocurrency regulations and their implementation.



Source: Thematic Map of the Researcher's Fieldwork, 2025

Theme 1: Strength and Gaps in Regulatory Frameworks

Nigeria and Kenya exhibit contrasting legal and policy frameworks in addressing cryptocurrency-based terrorism financing. Nigeria has stronger legal structures, with the Economic and Financial Crimes Commission (EFCC) and the Securities and Exchange Commission (SEC) enforcing Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations for cryptocurrency exchanges, as highlighted by Respondent A. However,

enforcement remains inconsistent, as noted by Respondent B, with peer-to-peer (P2P) trading continuing to operate outside regulatory oversight. In contrast, Kenya lacks formal cryptocurrency regulations, relying only on warnings issued by the Central Bank of Kenya (CBK) against cryptocurrency use without enacting specific counter-terrorism financing (CTF) measures, according to Respondent H. This absence of clear regulations leaves most cryptocurrency transactions unmonitored, providing significant loopholes for terrorist financiers, as explained by Respondent I.

Institutional capacity and coordination also differ between the two countries. Nigeria has dedicated financial intelligence units, such as the Nigerian Financial Intelligence Unit (NFIU), which attempt to track suspicious cryptocurrency transactions, as mentioned by Respondent C. Despite this, Respondent D emphasized that these agencies lack advanced blockchain forensic tools and technical expertise, limiting their effectiveness in monitoring and combating illicit activities. Similarly, Kenya faces challenges in institutional capacity, where Respondent J noted that Kenyan regulatory agencies struggle with both technical expertise and financial constraints, further hampering their ability to track illicit crypto transactions. The absence of specialized cryptocurrency monitoring units in both countries weakens enforcement efforts, highlighting the urgent need for enhanced technical capabilities and international cooperation to address these gaps effectively. These challenges underscore the importance of strengthening institutional frameworks and fostering collaboration between national and global stakeholders to combat the growing threat of cryptocurrency-based terrorism financing.

Challenges in Implementation and Enforcement

In Nigeria, terrorist groups exploit peer-to-peer (P2P) trading, which remains largely unregulated and difficult to monitor, as noted by Respondent E. Despite government bans on

certain crypto exchanges, users easily bypass these restrictions by switching to alternative platforms, according to Respondent F. This adaptability of P2P trading underscores the challenges in effectively regulating and monitoring such transactions. In Kenya, the integration of cryptocurrency with mobile money services presents a significant challenge for regulators, making it harder to track illicit financial flows, as highlighted by Respondent K. Unlike Nigeria, which has stricter mobile money regulations, Kenya's mobile money system remains highly vulnerable to exploitation by terrorist financiers, as explained by Respondent H. These vulnerabilities emphasize the need for enhanced regulatory frameworks and monitoring tools to address the unique risks posed by mobile money and P2P transactions.

Both Nigeria and Kenya face cross-border cryptocurrency transactions linked to terrorism financing, further complicating efforts to combat this issue. Respondent B noted that in Nigeria, illicit funds are often transferred to terrorist networks in the Sahel region and the Middle East. Similarly, Respondent J highlighted that Al-Shabaab in Kenya receives cryptocurrency donations from international supporters, effectively bypassing traditional banking restrictions. While Nigeria has been more proactive in freezing suspicious crypto assets, Kenya lacks coordinated efforts to track and seize illicit cryptocurrency transactions, as stated by Respondent I. This disparity in enforcement capabilities highlights the importance of stronger cross-border intelligence sharing and collaboration with international financial crime units. By enhancing cooperation and adopting advanced monitoring technologies, both countries can improve their capacity to disrupt and prevent terrorism financing through cryptocurrencies.

Emerging Strategies to Strengthen CTF Frameworks

Nigeria is making strides in strengthening public-private partnerships to enhance anti-money laundering (AML) enforcement through increased collaboration between regulators, financial institutions, and cryptocurrency firms, as noted by Respondent D. However, Respondent E observed that regulatory agencies still operate in silos, which limits their ability to share intelligence effectively and coordinate responses to emerging threats. This lack of integration hampers the overall effectiveness of Nigeria's efforts to combat terrorism financing through cryptocurrencies. In contrast, Kenya lags behind in fostering such partnerships. Respondent H pointed out that the absence of a clear regulatory framework discourages financial institutions from actively monitoring crypto transactions, leading to weak public-private cooperation and leaving significant gaps in the country's counter-terrorism financing (CTF) strategy.

The adoption of blockchain forensics and intelligence sharing is another critical area where both countries face challenges. Nigeria has begun exploring blockchain forensic tools for tracking cryptocurrency transactions, though progress remains slow due to technical and financial constraints, as highlighted by Respondent C. Similarly, Kenya faces a comparable issue, with Respondent K emphasizing the need for international cooperation to access advanced forensic tools and cybersecurity expertise. Both nations must invest in blockchain analytics technologies and expand intelligence-sharing efforts with global financial watchdogs to improve their capacity to detect and disrupt illicit financial activities linked to terrorism.

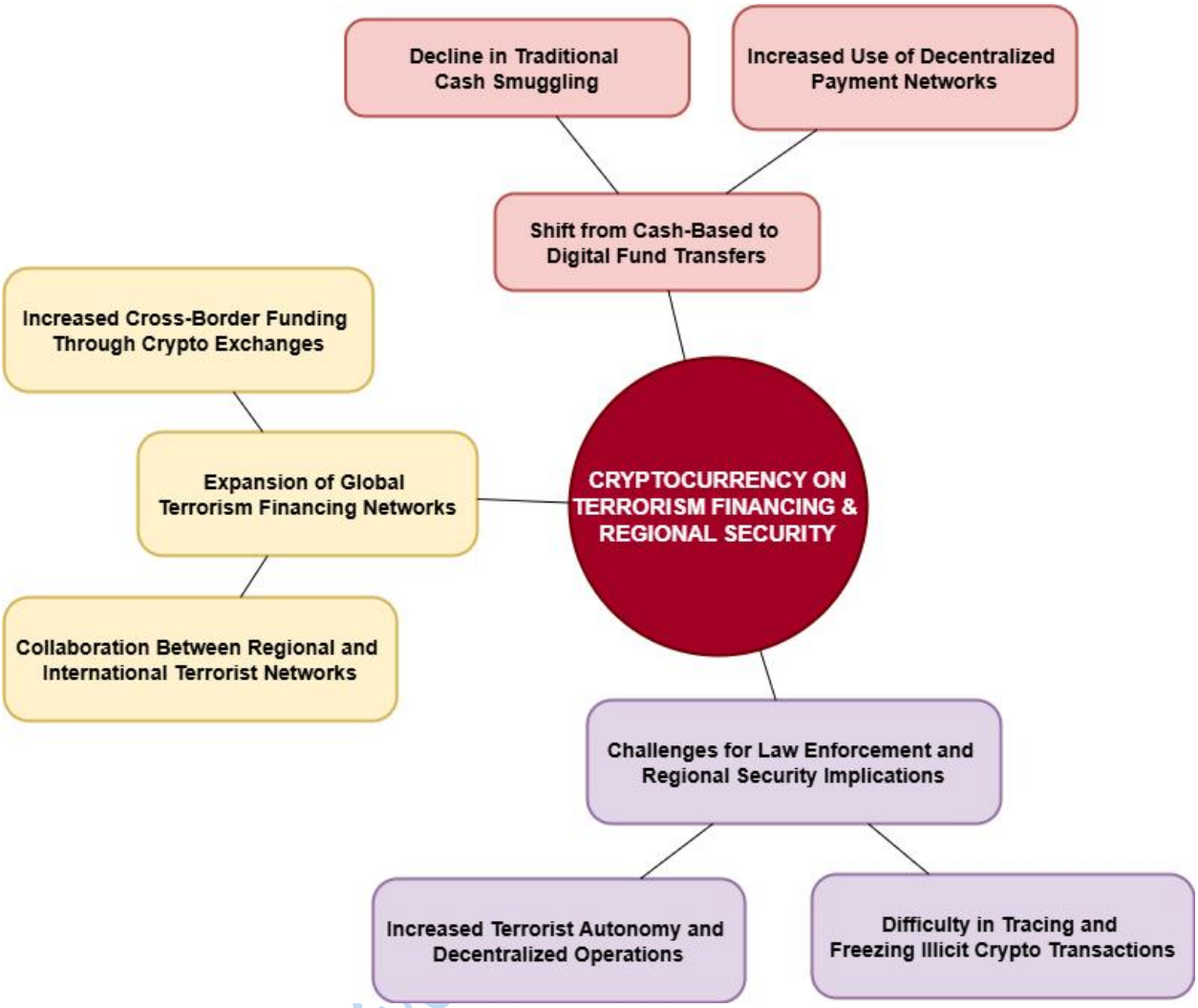
A comparison of Nigeria and Kenya’s counter-terrorism financing effectiveness reveals distinct strengths and weaknesses. Nigeria has a more structured CTF framework, but enforcement remains weak, particularly in addressing peer-to-peer (P2P) transactions, which

continue to operate largely outside regulatory oversight. Kenya, on the other hand, lacks formal cryptocurrency regulations, leaving many illicit transactions undetected and unmonitored. While Nigeria has been more proactive in freezing suspicious assets, Kenya faces greater challenges due to the integration of cryptocurrency with mobile money services, which creates additional vulnerabilities for terrorist financiers to exploit. Despite these differences, both countries struggle with limited blockchain forensic capabilities and insufficient international cooperation mechanisms, making it difficult to track cross-border transactions linked to terrorist groups. Strengthening enforcement strategies, investing in advanced technologies, and enhancing regulatory collaboration are essential steps for mitigating the risks posed by cryptocurrency-enabled terrorism financing in both nations.

RQ3: Comparative Thematic Analysis of the Impact of Cryptocurrency on Traditional Terrorism Financing Networks and Regional Security in Nigeria and Kenya

Theme 1: Shift from Cash-Based to Digital Fund Transfers

The adoption of cryptocurrency has significantly altered traditional terrorism financing methods in Nigeria and Kenya, affecting how funds are raised, transferred, and concealed. This transformation has also reshaped regional security dynamics, as terrorist groups increasingly exploit digital currencies to evade law enforcement and regulatory measures. The following themes and sub-themes illustrate the key ways in which cryptocurrency has transformed traditional terrorism financing in both countries and its broader security implications.



Source: Thematic Map of the Researcher's Fieldwork, 2025

Historically, terrorist groups in both Nigeria and Kenya relied heavily on traditional methods such as cash couriers, hawala networks, and informal remittance systems to move funds, as noted by Respondent A in the context of Nigeria. However, the rise of cryptocurrency has significantly altered this dynamic, with digital transactions now largely replacing cash

smuggling as the preferred method for financing operations. Respondent B from Kenya highlighted that cryptocurrency allows terrorist financiers to bypass border checks and financial surveillance, making cross-border transfers more efficient and less detectable. In Nigeria, while cash-based transactions are still utilized to some extent, cryptocurrency has enabled quicker and more discreet movement of funds, reducing the reliance on physical couriers, according to Respondent C. Similarly, in Kenya, terrorist groups have adapted by directly soliciting cryptocurrency donations, which eliminates the risks and logistical challenges associated with carrying large sums of cash across borders, as explained by Respondent D.

This shift toward cryptocurrency-based transactions has further enabled terrorist organizations to operate outside the formal banking sector, complicating efforts by authorities to track illicit funds. Respondent E from Nigeria pointed out that decentralized payment networks make it increasingly difficult for law enforcement to monitor these activities effectively. In Kenya, Al-Shabaab and its affiliates have taken advantage of mobile money platforms to convert cryptocurrency into local currency, thereby avoiding regulatory scrutiny, as noted by Respondent F. This integration of cryptocurrency with mobile money systems underscores the evolving sophistication of terrorist financing strategies and highlights the need for enhanced monitoring capabilities and stricter regulations to address these emerging threats. The transition away from traditional cash smuggling methods reflects the growing preference for digital solutions among terrorist groups, driven by their ability to provide anonymity, speed, and efficiency in moving funds across borders.

Theme 2: Expansion of Global Terrorism Financing Networks

The adoption of cryptocurrency has significantly expanded the global reach of terrorist financing networks, enabling cross-border funding through digital means. In Nigeria, Respondent G noted that terrorist groups such as Boko Haram and ISWAP now receive funds from international donors via Bitcoin and other digital assets, which are subsequently distributed to operatives within the country. This shift to cryptocurrency allows these groups to bypass traditional financial systems and evade detection by authorities. Similarly, in Kenya, Respondent H highlighted that Al-Shabaab leverages cryptocurrency to facilitate international donations, receiving financial support from sympathizers abroad without relying on formal banking institutions. This method provides a discreet and efficient channel for fundraising, further complicating efforts to disrupt their financial flows.

Moreover, the use of cryptocurrency has strengthened collaboration between regional and international terrorist networks. Respondent I from Nigeria pointed out that Boko Haram and ISWAP have been able to coordinate funding with external jihadist groups, utilizing cryptocurrency wallets that enable seamless global transactions without government oversight. This capability enhances their operational capacity, allowing for better coordination and resource sharing across borders. In Kenya, Respondent J explained that Al-Shabaab operatives also receive financial backing from external terrorist organizations, using cryptocurrency to bypass banking restrictions and anti-terrorism financing laws. As a result, these groups have become more sophisticated in their operations, with increased funding allocated toward recruitment, training, and carrying out attacks across West and East Africa. The integration of cryptocurrency into their financial strategies underscores the evolving

nature of terrorism and the urgent need for enhanced global cooperation to combat this growing threat.

Theme 3: Challenges for Law Enforcement and Regional Security Implications

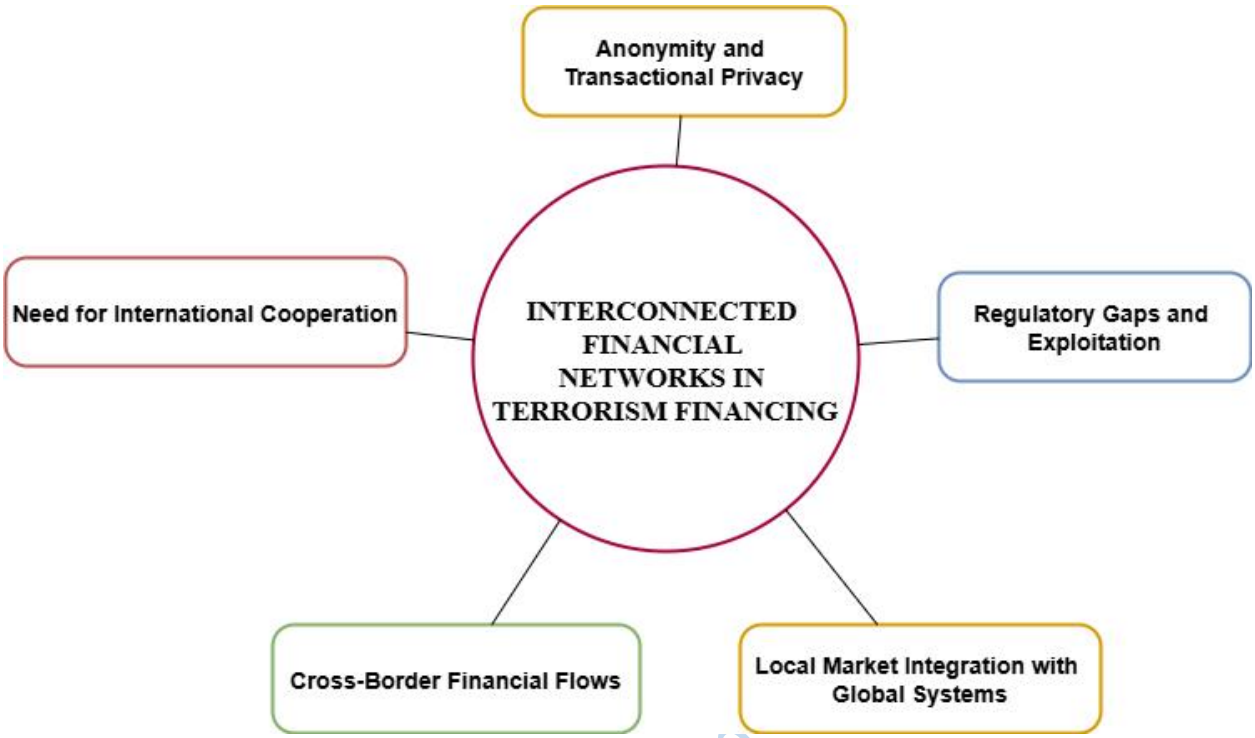
The anonymity and decentralization of cryptocurrencies pose significant challenges for law enforcement agencies in both Nigeria and Kenya. Respondent K from Nigeria noted that despite ongoing efforts to monitor cryptocurrency flows, Nigerian authorities lack the technical capacity to effectively trace blockchain transactions, leaving a critical gap in their ability to combat illicit financial activities. Similarly, in Kenya, law enforcement agencies struggle with tracking cryptocurrency transactions, especially when funds are converted into mobile money or sent through international crypto platforms, as highlighted by Respondent L. This difficulty has undermined the effectiveness of traditional counter-terrorism financing (CTF) efforts, as terrorist financiers can move money across borders without relying on conventional banking channels, further complicating attempts to disrupt their operations.

The shift to cryptocurrency has also granted terrorist organizations greater financial independence, reducing their reliance on centralized funding structures. Respondent M from Nigeria explained that Boko Haram cells now operate independently, with each unit raising and managing its own funds through cryptocurrency. This decentralized approach makes it harder for authorities to dismantle entire networks, as targeting one cell no longer disrupts the broader financial ecosystem. In Kenya, Al-Shabaab operatives in different regions manage their own financial transactions using cryptocurrency, as noted by Respondent N. This localized management limits their vulnerability to law enforcement crackdowns on centralized financial hubs, enhancing their adaptability and resilience against security forces' interventions.

Both Nigeria and Kenya have witnessed a transformation in terrorism financing, shifting from traditional cash-based systems to cryptocurrency-driven models. In Nigeria, Boko Haram and ISWAP leverage global crypto networks to expand their funding sources, while in Kenya, Al-Shabaab exploits mobile money conversions and direct cryptocurrency donations to support their operations. This transition has made it increasingly difficult for authorities to track and freeze illicit funds due to weak blockchain forensic capabilities and regulatory gaps. The enhanced financial autonomy afforded by cryptocurrency has complicated law enforcement efforts, as terrorist groups are less dependent on centralized funding sources. As a result, both countries face growing threats to regional security. To address this evolving challenge, strengthening cross-border intelligence sharing, investing in advanced blockchain forensics, and enforcing stricter crypto regulations are essential steps in combating the rise of cryptocurrency-enabled terrorism financing.

RQ 4: To appraise the interconnections between local cryptocurrency markets, international financial systems, and terrorism financing networks in Nigeria and Kenya

Interconnected Financial Networks in Terrorism Financing



Source: Thematic Map of the Researcher's Fieldwork, 2025

Respondent A observes that the anonymity of transactions on peer-to-peer platforms in Nigeria significantly enables terrorist financing, offering a layer of privacy exploited by groups like Boko Haram and ISWAP to move funds discreetly. Similarly, Respondent E highlights the use of mixers and tumblers, tools that further obscure financial trails, demonstrating a deliberate strategy to evade detection within Nigeria's crypto ecosystem. In Kenya, Respondent F notes how Al-Shabaab leverages the anonymity of cryptocurrencies by converting mobile money into digital assets, facilitating operational funding without detection. Respondent I adds that this anonymity aids in receiving international donations, which are then channeled into local terrorist activities.

According to Respondent B, Nigeria's regulatory environment has inadvertently pushed crypto transactions toward less regulated avenues, creating opportunities for terrorist groups to fund their activities. This regulatory pushback from traditional banks has led to an

underground economy with minimal oversight. In contrast, Respondent G points out that Kenya's lack of a comprehensive regulatory framework allows terrorist financiers to exploit cryptocurrency markets. Respondent H emphasizes the absence of clear licensing for crypto service providers, highlighting a significant regulatory gap that groups like Al-Shabaab exploit to funnel money for their operations.

Respondent C references the Binance case in Nigeria, illustrating how local crypto activities are interconnected with global financial networks, making it challenging for national efforts alone to curb terrorism financing. The involvement of global exchanges in local investigations underscores the ease with which funds can cross borders. Similarly, Respondent D discusses the government's action to freeze millions in cryptocurrency, underscoring the international implications of local financial actions. In Kenya, Respondent I outlines how Al-Shabaab uses cryptocurrencies to transfer funds from international donors to local operatives, showcasing the seamless integration of cross-border financial flows into terrorist financing strategies.

Nigeria's local crypto traders, as noted by Respondent A, act as intermediaries linking local markets to international terrorist financing networks, demonstrating how small-scale traders can become part of a larger, global financial system used for illicit purposes. In Kenya, Respondent F describes how mobile money, a deeply ingrained local financial tool, connects directly with the global crypto market, providing Al-Shabaab with a pathway to convert and transfer funds internationally.

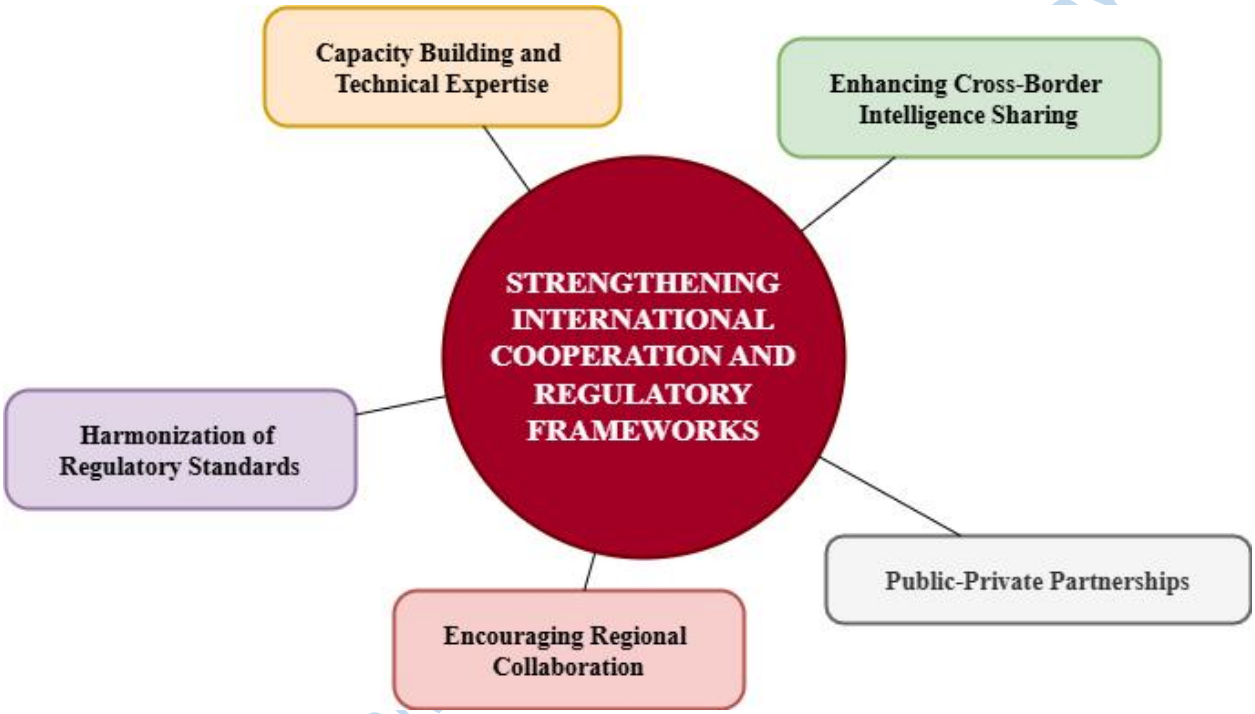
Both Respondent C in Nigeria and Respondent G in Kenya stress the critical need for international cooperation to address crypto-based terrorism financing. The challenges of tracking and regulating transactions that span multiple countries necessitate a coordinated global response. Respondent J highlights the role of international bodies like FATF, which

aim to harmonize regulatory practices and facilitate information sharing to combat the misuse of cryptocurrencies for terrorism financing across borders.

The regulatory environments in Nigeria and Kenya shape how terrorist groups finance operations through crypto. Nigeria's more aggressive stance has led to underground markets, while Kenya's regulatory infancy enables direct exploitation of existing financial ecosystems. While both countries see similar exploitation of crypto for anonymity, Nigeria's terrorist groups seem to rely more on local intermediaries, whereas Kenyan groups utilize the mobile money infrastructure for a direct link to cryptocurrencies.

RQ 5: To develop context-specific policy recommendations for strengthening international cooperation and regulatory frameworks to combat cryptocurrency-enabled terrorism financing

Theme 1: Strengthening International Cooperation and Regulatory Frameworks



Source: Thematic Map of the Researcher's Fieldwork, 2025

Respondent A in Nigeria emphasizes the critical importance of aligning local cryptocurrency regulations with international standards to prevent the country from becoming a safe haven for terrorist financing. By adopting and enforcing the Financial Action Task Force's (FATF) recommendations on virtual assets, Nigeria can create a regulatory environment that is more resilient against illicit activities. This alignment would involve implementing robust Know Your Customer (KYC), Anti-Money Laundering (AML), and Counter-Terrorist Financing (CTF) measures. Respondent B adds that harmonized regulations would facilitate better

coordination with international law enforcement agencies, enabling more effective tracking and freezing of illicit funds. In Kenya, Respondent F highlights the evolving nature of the regulatory landscape as an opportunity to integrate global best practices, closing existing gaps exploited by groups like Al-Shabaab. Respondent G further stresses the necessity of regulatory consistency to prevent money laundering and the receipt of crypto donations by terrorists. The policy recommendation here is clear: both countries should develop national regulatory frameworks that align with international standards while actively engaging in global regulatory discussions to ensure comprehensive coverage.

Respondent C in Nigeria addresses the complexities of investigations like the one involving Binance, where effective counter-terrorism financing measures depend heavily on seamless cross-border information exchange. Respondent D elaborates that asset freezing becomes significantly more effective with real-time international support and data sharing, underscoring the need for enhanced collaboration. In Kenya, Respondent I emphasizes the importance of international intelligence sharing to trace cryptocurrency transactions linked to terrorism, advocating for a system where information flows not only domestically but globally. Respondent H suggests establishing secure communication channels to facilitate this data exchange among law enforcement agencies. The policy recommendations include strengthening bilateral and multilateral agreements focused on digital currencies, as well as participating in or creating international task forces dedicated to monitoring and disrupting terrorist financing through cryptocurrencies. Such efforts are essential for addressing the cross-border nature of these financial flows and ensuring coordinated action against terrorist networks.

In Nigeria, Respondent E highlights the importance of leveraging tools like blockchain analytics to combat the anonymity of crypto transactions, emphasizing the need for training law enforcement agencies in these advanced technologies. Respondent A further stresses that capacity building within institutions such as the EFCC should include developing expertise in digital forensics specific to cryptocurrencies. This would enable authorities to better track and investigate illicit financial activities. In Kenya, Respondent F argues for equipping law enforcement and financial regulators with the technical knowledge required to handle the complexities of cryptocurrencies, suggesting partnerships with technical firms or educational institutions to bridge this gap. Respondent G advocates for ongoing education programs to keep up with the rapidly evolving crypto landscape, ensuring that regulatory efforts remain effective. The policy recommendations here involve investing in specialized training programs focused on blockchain technology, crypto forensics, and anti-money laundering (AML) practices in digital spaces, while fostering collaborations with academia and the private sector to enhance technical capabilities.

Respondent B in Nigeria underscores the critical role of the private sector, particularly cryptocurrency exchanges, in monitoring and reporting suspicious activities. To encourage compliance, Respondent D suggests incentivizing cryptocurrency firms through mechanisms such as tax benefits or regulatory concessions for exceeding reporting standards. In Kenya, Respondent H emphasizes the integral role of mobile money platforms in facilitating crypto transactions, advocating for collaboration with telecom companies and crypto businesses to ensure effective oversight. Respondent I sees value in engaging these firms in voluntary compliance frameworks, which could enhance cooperation and data sharing. The policy recommendations include establishing formal public-private partnerships to facilitate

intelligence sharing and the implementation of best practices, with incentives designed to encourage proactive participation from crypto service providers in combating terrorism financing.

Both Nigerian and Kenyan respondents recognize the potential of regional bodies like the African Union (AU) or ECOWAS in coordinating anti-terrorism financing strategies. They advocate for initiatives such as regional workshops, joint investigations, and shared regulatory frameworks to address the transnational nature of cryptocurrency-based terrorism financing. By leveraging these organizations, countries can create unified approaches to regulation, focusing on prevention and organizing regular forums for sharing experiences, strategies, and successes. The policy recommendation is to strengthen regional collaboration by utilizing platforms like the AU or ECOWAS to develop comprehensive strategies, promote knowledge exchange, and establish standardized practices across member states, thereby enhancing collective resilience against terrorist financing through cryptocurrencies.

The comparative analysis of the responses from Nigeria and Kenya regarding strategies to combat cryptocurrency-enabled terrorism financing under Objective 5 reveals a shared recognition of the need for international regulatory alignment, enhanced cross-border intelligence sharing, increased technical expertise, public-private partnerships, and regional collaboration. Nigeria, grappling with a more mature and exploited crypto market, shows an urgent need to harmonize its regulations with global standards and to bolster its technical capabilities, as emphasized by Respondents A and E, to address the sophisticated methods used by terrorist groups. Meanwhile, Kenya, with its emerging crypto scene, has the opportunity to proactively shape its regulatory framework, as noted by Respondents F and G, focusing particularly on integrating mobile money platforms with crypto oversight. Both

nations underscore the importance of real-time data exchange, with Nigeria's experiences with international exchanges like Binance highlighting a more pressing need for robust international partnerships, while Kenya's strategy, articulated by Respondent H, leans towards establishing secure communication for this purpose. The consensus on leveraging public-private collaborations is evident, though tailored differently; Nigeria looks to existing crypto infrastructures, and Kenya to its mobile money ecosystem. The call for regional cooperation through African bodies is strong in both contexts, though Nigeria might push for immediate and comprehensive strategies due to its scale of terrorist activities, while Kenya might emphasize preventive measures. Together, these insights suggest that while the specific contexts of each country influence their strategies, the overarching goals to enhance regulation, share intelligence, build capacity, and collaborate regionally are universally acknowledged.

4.2.3 Comparative Analysis: Nigeria, Kenya and Beyond (Global)

4.2.1 Terrorist Crypto-Finance Methods and Strategies

Cryptocurrency has emerged as a critical tool for terrorist organisations to circumvent traditional financial systems and fund their operations. This analysis explores the methods and strategies employed by these groups, drawing on case studies from Nigeria, Afghanistan, and global contexts while emphasising the implications for law enforcement and regulatory frameworks.

The intersection of cryptocurrency and terrorism financing has become a critical concern for regulators, law enforcement agencies, and policymakers globally. The case of Tigran Gambaryan's arrest in Nigeria exemplifies the growing tension between cryptocurrency exchanges and national regulators, particularly in regions with unclear or evolving regulatory

frameworks[1]. As the head of financial crime compliance at Binance, Gambaryan travelled to Nigeria in early 2024 to engage with authorities on regulatory compliance issues. However, he was detained on allegations that Binance facilitated illegal financial activities, including money laundering and terrorism financing. This incident highlights the risks faced by compliance professionals operating in high-stakes environments and the broader challenges of enforcing Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) standards in the crypto space. Furthermore, the harsh treatment of Gambaryan in Nigerian custody raises significant human rights concerns, underscoring the need to balance regulatory enforcement with respect for individual freedoms.

In addition to these challenges, Binance's regulatory struggles in Nigeria reflect broader global concerns about the role of cryptocurrency exchanges in facilitating illicit activities. Nigerian regulators accused Binance of enabling transactions linked to terrorism financing, money laundering, and other illegal activities, leading to an investigation into its operations[2]. The investigation revealed that Binance's peer-to-peer (P2P) trading platform was used to move funds anonymously, bypassing traditional financial systems. This case underscores the difficulties of enforcing AML/CFT regulations in regions with weak oversight mechanisms. Moreover, it highlights the need for clearer regulatory frameworks and international cooperation to address the risks posed by cryptocurrencies. The detention of Gambaryan and other Binance executives during this period further complicates the discourse on human rights in the context of financial regulation, as documented in a Wired article [3].

Blockchain analytics tools play a pivotal role in tracking and disrupting illicit financial flows associated with terrorism financing. According to a report, while cryptocurrencies are sometimes used for terrorism financing, their role is often exaggerated compared to traditional

financial systems[4]. For instance, the U.S. Department of Justice successfully disrupted two terrorism financing campaigns involving virtual currencies in 2020, underscoring the effectiveness of blockchain forensics. Similarly, AD Forensics' training programs for Nigerian law enforcement agencies demonstrate the importance of technical expertise in addressing modern financial crimes [5]. These efforts highlight the necessity of integrating advanced technologies into regulatory practices to combat crypto-related crimes effectively. By leveraging tools such as blockchain analytics, law enforcement agencies can enhance their capacity to monitor and disrupt illicit activities in the rapidly evolving digital landscape.

Terrorist organisations have increasingly turned to cryptocurrencies to raise funds, exploiting the anonymity and cross-border capabilities offered by digital currencies. The case of Al-Qaeda and Hamas utilising cryptocurrency donations to fund their operations, as documented by the U.S. Department of Justice demonstrates the adaptability of these groups in leveraging new financial technologies[6]. Similarly, ISIS leveraged Bitcoin to finance attacks and purchase weapons, taking advantage of the pseudonymous nature of cryptocurrencies [7]. The Taliban's takeover of Afghanistan in 2021 has led to increased Bitcoin adoption, raising concerns about the country becoming a hub for illegal crypto transactions, including terrorism financing[8]. These trends indicate that while traditional financial systems remain the primary means of terrorism financing, cryptocurrencies represent an emerging threat that requires vigilant monitoring and regulation.

Community involvement in combating crypto-related crimes is gaining prominence, as evidenced by initiatives like the Google Form for reporting suspicious transactions. This tool enables individuals and organisations to contribute to intelligence gathering and pattern identification in the crypto space, fostering a collaborative approach to addressing financial

crimes, Such community-driven efforts complement the work of law enforcement agencies and private sector actors, enhancing capacity-building and knowledge-sharing. Furthermore, partnerships between regulators, law enforcement, and private firms, such as those facilitated by AD Forensics, strengthen the ability to develop comprehensive strategies to counter terrorism financing and other illicit activities in the cryptocurrency ecosystem.

The implications of these findings highlight the need for stronger regulatory frameworks, international cooperation, and advanced technological tools to address the risks posed by terrorist crypto-finance. Regulatory crackdowns, such as those seen in Nigeria, reflect the growing scrutiny of crypto exchanges and the need for clearer guidelines [9]. Moreover, the European Parliament report on virtual currencies and terrorism financing notes that while cryptocurrencies pose a risk, traditional financial systems remain the primary means for terrorism financing [10]. Therefore, governments and regulators must focus on both traditional and digital financial systems to combat terrorism financing effectively. By learning from the experiences documented in these cases, policymakers and practitioners can develop comprehensive strategies to mitigate the risks associated with terrorist crypto-finance. While cryptocurrencies offer innovative financial inclusion and economic development solutions, they also pose significant risks when exploited for illicit purposes. Addressing these challenges requires a multifaceted approach, combining robust regulatory frameworks, advanced technological tools, and international collaboration.

4.4.2 Effectiveness of Crypto Anti-Terrorism Financing Frameworks

The effectiveness of frameworks designed to combat terrorism financing through cryptocurrencies is a critical area of study, given the growing sophistication of terrorist organisations in leveraging digital currencies. Cryptocurrency exchanges have become focal

points for regulators seeking to curb illicit financial flows. For instance, the case of Binance's regulatory challenges in Nigeria highlights both the necessity and complexity of enforcing anti-terrorism financing frameworks [2]. Nigerian authorities accused Binance of facilitating transactions linked to terrorism financing and money laundering, leading to an investigation into its operations. While this action underscores the importance of regulatory oversight, it also reveals the difficulties regulators face in regions with weak or evolving frameworks. The lack of clear guidelines creates opportunities for exploitation by bad actors, as evidenced by using Binance's peer-to-peer (P2P) trading platform to anonymise funds.

Similarly, the European Parliament report on virtual currencies and terrorism financing notes that while cryptocurrencies pose risks, traditional financial systems remain the primary means for terrorism financing[10]. However, the traceability of blockchain transactions provides law enforcement agencies with valuable tools to monitor and disrupt these activities. Despite this advantage, the effectiveness of current frameworks depends heavily on the ability of regulators to adapt to the rapidly evolving nature of cryptocurrency ecosystems.

The role of blockchain analytics in combating terrorism financing cannot be overstated. Tools developed by firms such as Chainalysis have proven instrumental in tracking and disrupting illicit financial flows. For example, the U.S. Department of Justice successfully disrupted two terrorism financing campaigns involving virtual currencies in 2020, underscoring the effectiveness of blockchain forensics [6]. These successes demonstrate the potential of advanced technologies to enhance the capabilities of law enforcement agencies.

In another case, AD Forensics trained Nigerian law enforcement agencies in crypto crime investigation, focusing on blockchain forensics and AML/CFT measures [5]. This initiative reflects the growing recognition of the need for technical expertise in addressing modern

financial crimes. Equipping law enforcement officers with the skills to analyse blockchain data, such programs significantly bolster efforts to combat terrorism financing.

However, the effectiveness of blockchain analytics is contingent upon access to high-quality data and international cooperation. The court order directing Binance to release user data to the EFCC in Nigeria illustrates the importance of cross-border collaboration in investigations [11]. Without robust data-sharing agreements, the utility of blockchain analytics may be limited.

Community-driven initiatives play a crucial role in augmenting the effectiveness of anti-terrorism financing frameworks.

Moreover, the involvement of the public in combating crypto-related crimes reflects a broader trend toward decentralised governance in the digital economy. As highlighted in Case 4, community-driven efforts are essential for addressing the gaps left by insufficient regulatory frameworks. For instance, despite Nigeria's ban on cryptocurrency transactions in 2021, adoption continued to grow through P2P platforms [13].

Despite advancements in technology and regulation, significant challenges remain, particularly in regions with weak Countering the Financing of Terrorism (CFT) and Anti-Money Laundering (AML) regimes. Afghanistan, under Taliban control, has emerged as a potential hub for illegal crypto transactions, including terrorism financing [8]. The lack of regulatory oversight and the country's economic turmoil have driven citizens to adopt cryptocurrencies to safeguard their financial assets. These examples underscore the need for stronger international cooperation to address the risks posed by weak regulatory regimes.

Terrorist organisations continue innovating their financing methods, taking full advantage of the anonymity and cross-border capabilities of cryptocurrencies. For instance, Al-Qaeda and Hamas utilised cryptocurrency donations to fund their operations, as documented by the U.S.

Department of Justice [6]. ISIS similarly leveraged Bitcoin to finance attacks and purchase weapons, exploiting the pseudonymous nature of digital currencies [7].

These cases highlight the adaptability of terrorist groups in using new financial technologies. To counteract this trend, anti-terrorism financing frameworks must evolve as quickly as the threats they aim to address. This requires technological innovation and enhanced capacity-building and knowledge-sharing among stakeholders.

4.2.3 Crypto's Influence on Terrorist Networks and Security

The case of Boko Haram and ISWAP using cryptocurrency traders to fund their operations highlights the adaptability of these organisations in leveraging new technologies [21]. According to the EFCC, terrorists convert crypto into local currency through peer-to-peer (P2P) platforms, exploiting the anonymity provided by such systems. This method allows them to bypass strict AML/CFT regulations imposed on traditional banking channels.

Similarly, the Taliban's increasing adoption of Bitcoin following its takeover of Afghanistan underscores the potential for insurgent groups to use cryptocurrencies to sustain their operations [8]. In regions with weak regulatory frameworks, like Afghanistan and Pakistan, the lack of oversight creates fertile ground for illicit financial activities. These cases demonstrate that cryptocurrencies are tools for individual transactions and strategic assets for maintaining operational continuity in conflict zones.

Despite the perceived anonymity of cryptocurrencies, blockchain analytics tools have proven effective in tracking and disrupting illicit financial flows. However, challenges remain in fully leveraging these technologies due to jurisdictional and technical limitations. The case of Nigeria's crackdown on major crypto players, including exchanges and influencers, illustrates the complexities of regulating digital currencies [14]. Authorities targeted high-profile

individuals and platforms suspected of facilitating money laundering, terrorism financing, and market manipulation. While these efforts reflect the growing awareness of crypto-related risks, they also highlight the need for more robust frameworks to address these issues comprehensively.

Moreover, the court order directing Binance to release user data to the EFCC demonstrates the growing regulatory pressure on cryptocurrency exchanges[15], such actions underscore the importance of international cooperation in combating cross-border crimes. However, concerns about user privacy and data security persist, raising questions about the balance between enforcement and individual rights.

Terrorist organisations continually innovate methods to exploit vulnerabilities in the cryptocurrency ecosystem. The case of Linus Williams, CEO of Blord Group, arrested for alleged involvement in terrorism financing and cryptocurrency fraud, exemplifies the misuse of businesses for illegal purposes [16]. Williams was accused of using his company to facilitate transactions linked to terrorist groups, demonstrating how legitimate enterprises can be co-opted for illicit activities. This case highlights the need for stricter due diligence processes and enhanced monitoring of corporate entities operating in the crypto space.

Additionally, the report by the Foundation for Defense of Democracies notes that jihadist groups, including al-Qaeda and ISIS, have solicited cryptocurrencies to raise funds and transfer money across borders [17]. These groups use anonymity and lack oversight in crypto to finance their operations. Their ability to innovate financing methods underscores the urgency of developing advanced blockchain analytics tools to track and disrupt these activities.

Afghanistan and Pakistan have emerged as potential hubs for crypto-based terrorism financing due to their weak Countering the Financing of Terrorism (CFT) and Anti-Money Laundering

(AML) regimes, The Taliban's control over Afghanistan raises concerns about the country becoming a launchpad for illegal crypto transactions, including terror financing and cyber-attacks. Furthermore, the emerging alliance between China, Pakistan, and the Taliban could facilitate technology transfers that enhance the group's capacity to exploit digital currencies for illicit purposes. These regional dynamics highlight the importance of international collaboration in addressing the risks posed by weak regulatory frameworks. Without coordinated efforts, terrorist organisations may continue to exploit vulnerabilities in underregulated jurisdictions, undermining global security. The influence of cryptocurrencies on terrorist networks and global security is profound, requiring a multifaceted approach to address the associated risks. While blockchain analytics and community-driven initiatives have proven effective in tracking and disrupting illicit activities, significant challenges remain in regulating digital currencies and ensuring international cooperation.

4.2.4 Terror Finance: Crypto Market & Global System Links

Weak or evolving regulatory frameworks create fertile ground for bad actors to misuse cryptocurrencies. For instance, Afghanistan under Taliban control exemplifies this vulnerability [8]. Following the Taliban's takeover, Bitcoin adoption surged as citizens sought to safeguard their financial assets amidst economic turmoil. However, this same environment could be exploited by the Taliban for terrorism financing, cyber-attacks, and other illicit activities. With weak Countering the Financing of Terrorism (CFT) and AML regimes, Afghanistan could become a hub for illegal crypto transactions, including those tied to terrorist organisations.

Pakistan similarly faces challenges in regulating its burgeoning crypto market, creating opportunities for misuse by bad actors, Both countries highlight the importance of

international cooperation in addressing the risks posed by underregulated jurisdictions. Without coordinated efforts, terrorist organisations may continue to exploit vulnerabilities in these regions, undermining global security.

While blockchain analytics tools have proven instrumental in tracking and disrupting illicit financial flows, they also expose limitations in current regulatory frameworks. For example, AD Forensics trained Nigerian law enforcement agencies in crypto crime investigation, focusing on blockchain forensics and AML/CFT measures [30]. This initiative reflects the growing recognition of the need for technical expertise in addressing modern financial crimes. By equipping officers with skills to analyse blockchain data, such programs significantly bolster efforts to combat terrorism financing.

However, the traceability of blockchain transactions raises concerns about privacy and data security. The court order directing Binance to release user data to the EFCC exemplifies the growing regulatory pressure on cryptocurrency exchanges [11]. While such actions enhance law enforcement capabilities, they also raise questions about the balance between enforcing regulations and respecting individual rights. Terrorism financing via cryptocurrencies transcends national borders, necessitating coordinated efforts at the global level. The European Parliament report on virtual currencies and terrorism financing highlights the risks posed by digital assets while acknowledging their limited role compared to traditional financial systems [10]. Despite this, the traceability of blockchain transactions provides law enforcement agencies valuable opportunities to monitor and disrupt illicit activities.

4.4.5 Policy Recommendations for Strengthening Crypto Anti-Terrorism Finance Policies

A critical challenge in combating illicit crypto transactions lies in the absence of standardised regulatory frameworks across jurisdictions. The case of Binance's regulatory challenges in Nigeria highlights this issue, where weak or evolving regulatory frameworks create opportunities for exploitation by bad actors [2]. Countries should work towards internationally harmonised Anti-Money Laundering/Countering the Financing of Terrorism (AML/CFT) regulations that impose mandatory Know-Your-Customer (KYC) requirements on all cryptocurrency exchanges. For instance, Nigeria's Securities and Exchange Commission (SEC) has approved local crypto exchanges under stricter regulations, balancing innovation with oversight[18]. However, such efforts must be extended globally to ensure consistency and prevent jurisdictional arbitrage. Additionally, cross-border financial intelligence-sharing mechanisms should be strengthened to facilitate real-time tracking of suspicious transactions across jurisdictions, as seen in the collaboration between Nigerian authorities and blockchain analytics firms during the freezing of $37 million linked to protest organisers[19].

To combat terrorism financing through cryptocurrencies, governments must invest in advanced tools and specialised expertise. Enhanced law enforcement capabilities are essential for monitoring and disrupting illicit activities facilitated by digital currencies. The U.S. Department of Justice's disruption of two terrorism financing campaigns involving virtual currencies in 2020 demonstrates the effectiveness of blockchain forensics in tracking and disrupting such activities [6]. Similarly, AD Forensics' training programs for Nigerian law enforcement agencies highlight the importance of technical expertise in addressing modern financial crimes [5].

Specialised cybercrime task forces should be established to monitor, investigate, and disrupt terrorism financing networks operating within the digital financial ecosystem. Furthermore,

mandatory registration and transaction monitoring for peer-to-peer (P2P) trading platforms should be introduced to close existing regulatory loopholes that enable terrorist financiers to launder funds undetected. This is particularly relevant given the EFCC's revelation that terrorist groups in Nigeria use P2P platforms to convert crypto into local currency [15]. By enhancing their capacity to trace and freeze illicit funds, law enforcement agencies can significantly reduce the ability of terrorist organisations to exploit cryptocurrencies for their operations.

In regions like East Africa, mobile payment platforms have become integral to facilitating illicit cryptocurrency transactions. Regulators must implement enhanced scrutiny over crypto-to-mobile money transactions to curb the flow of funds to extremist groups such as Al-Shabaab. Financial institutions should be required to report all large-scale or suspicious crypto-to-mobile money conversions, leveraging automated systems to flag abnormal transaction patterns. This measure is crucial in preventing terrorist organisations from exploiting the anonymity and accessibility of mobile payment systems to finance their activities. While the focus has primarily been on traditional banking systems, the growing integration of mobile payments with cryptocurrencies necessitates tailored regulatory responses to mitigate emerging risks.

Public-private partnerships play a pivotal role in enhancing financial intelligence efforts. Cryptocurrency exchanges, fintech companies, and law enforcement agencies must collaborate more effectively to develop innovative solutions for detecting and preventing illicit economic activities. Governments should incentivise private sector entities to adopt security-driven blockchain innovations and develop automated risk assessment models to

identify real-time suspicious transactions. Such collaborations can enhance the capacity of financial intelligence units to detect and respond to threats posed by terrorist financing.

Community-based reporting mechanisms, such as the report from the Google Form for reporting crypto-related crimes, exemplify how public participation can complement official efforts, By enabling individuals and organisations to submit detailed information about suspicious transactions, including wallet addresses and transaction IDs, these platforms serve as valuable tools for gathering intelligence and identifying patterns of illicit activity. Expanding and integrating such mechanisms with national financial intelligence systems can foster greater transparency and accountability in the crypto space while encouraging broader societal engagement in combating financial crime.

Regional vulnerabilities, particularly in countries with weak AML/CFT regimes, exacerbate the risks associated with crypto-based terrorism financing. Afghanistan, under Taliban control, exemplifies this concern, as economic turmoil and lack of regulatory oversight have driven citizens toward cryptocurrencies [8]. This environment creates opportunities for misuse by bad actors, including terrorist organisations. Similarly, Pakistan faces challenges in regulating its burgeoning crypto market, raising concerns about potential technology transfers that could enhance the capacity of groups like the Taliban to exploit digital currencies for illicit purposes, Addressing these vulnerabilities requires targeted interventions, including capacity-building initiatives and international cooperation, to establish robust AML/CFT frameworks in high-risk regions.

Balancing regulation with human rights is a critical consideration in enforcing anti-terrorism finance policies within the cryptocurrency space. Regulatory actions must respect individual rights and avoid undue targeting of compliance professionals or innocent actors, ensuring that

enforcement measures remain proportionate and justifiable. The case of Tigran Gambaryan's detention in Nigeria exemplifies the importance of this balance. Gambaryan, a compliance officer at Binance, was detained under harsh conditions, sparking an international outcry over treating individuals involved in regulatory discussions[3]. His case highlights the need for regulators to ensure that enforcement actions do not disproportionately target compliance professionals or infringe upon fundamental human rights.

In addition to respecting individual rights, authorities must prioritise transparency and data security when requiring exchanges to release user data. This is particularly relevant given the increasing trend of governments demanding access to sensitive information from crypto platforms. For instance, the court order directing Binance to release Nigerian user data to the EFCC underscores safeguarding user privacy while facilitating investigations into potential illicit activities[12]. As such, policymakers and law enforcement agencies must adopt clear guidelines to ensure data-sharing processes are transparent, secure, and aligned with international standards for protecting personal information. By prioritising these principles, regulators can foster trust among stakeholders and mitigate concerns about overreach or misuse of power in the fight against terrorism financing.

4.3 Discussion of Findings

4.3.1: Methods and Strategies of Cryptocurrency Use in Terrorism Financing

The finding that terrorist organizations in Nigeria and Kenya exploit cryptocurrency's anonymity and decentralization, adopting methods such as peer-to-peer (P2P) trading in Nigeria and mobile money integration in Kenya to local contexts, highlights a significant shift in terrorism financing strategies. This adaptation poses substantial challenges for regulators

lacking advanced tracking tools, with international parallels reinforcing the urgency for global standards.

This study confirms that terrorist organizations in Nigeria and Kenya employ a range of cryptocurrency-based methods and strategies, which means they prioritize anonymity and decentralization to obscure financial trails. The data indicate widespread acquisition of cryptocurrency funds, frequent concealment of transactions, and regular use of privacy-focused cryptocurrencies or mixing services, reflecting a strategic focus on evading detection over less prevalent options like decentralized finance (DeFi) platforms. The reliance on exchanges and specific platforms further underscores the exploitation of accessible digital infrastructure, challenging regulatory oversight. This evidence aligns with a researcher, who argues that cryptocurrency's pseudonymous nature facilitates terrorist financing by complicating traceability[20]. However, the lower engagement with DeFi suggests a pragmatic reliance on established methods, potentially limited by technical sophistication or accessibility, a nuance warranting further exploration into evolving technological preferences [21]. The absence of advanced tracking tools among regulators amplifies this challenge, pointing to a critical capacity gap[22].

Results from this study reinforce the finding's emphasis on context-specific exploitation. In Nigeria, Respondent D highlights P2P trading and "smurfing" (small, multiple transactions) as dominant methods, exploiting weak Know-Your-Customer (KYC) and Anti-Money Laundering (AML) enforcement on unregulated platforms, a vulnerability tied to inconsistent policies from the Central Bank of Nigeria (CBN)[23]. Respondent F notes using crypto mixers, which obscure financial trails, a tactic consistent with global trends[24]. In Kenya, Respondent K identifies the integration of cryptocurrency with mobile money platforms like M-Pesa,

capitalizing on the country's robust mobile payment infrastructure and regulatory gaps (Respondent H). This strategic adaptation contrasts Nigeria's structured yet poorly enforced framework with Kenya's unregulated digital wallet landscape, resonating with a researcher, who emphasize decentralization's role in bypassing oversight[25]. These local variations suggest tailored regulatory challenges, amplifying the need for advanced tools and global standards[26].

The finding, through international parallels, highlights a global pattern of anonymity-driven financing. The Binance case in Nigeria, involving Tigran Gambaryan's detention, exemplifies how P2P platforms enable anonymous fund flows, with regulators accusing the exchange of facilitating terrorism financing [1], This mirrors the Taliban's Bitcoin adoption in Afghanistan post-2021, where weak oversight fosters a crypto hub for illicit activities[8]. Globally, Al-Qaeda, Hamas, and ISIS use Bitcoin and privacy coins like Monero for donations and weapons purchases[6], paralleling Nigeria's mixer use and Kenya's privacy coin trends[6]. A Position also supports this, noting anonymity as an everyday driver across terrorist groups[27].

The finding reveals that terrorist organizations in Nigeria and Kenya exploit cryptocurrency's anonymity and decentralization, adapting P2P trading and mobile money integration to local contexts and challenging regulators without advanced tools. The statistical focus on concealment aligns with thematic evidence of localized tactics, corroborated by global parallels, suggesting a consistent anonymity-driven strategy[20]. The lower DeFi use indicates pragmatic adaptation, challenging assumptions of uniform technological adoption[21]. Nigeria's enforcement gaps contrast with Kenya's regulatory void, supporting a researcher claim on uneven blockchain governance, while international cases amplify the urgency for global standards[28,26]. However, the European Parliament's perspective suggests a need to balance focus between digital and traditional threats[10]. The regulatory challenge lacking forensics and

the potential for Underground shifts post-CBN bans (highlight a policy dilemma requiring nuanced, globally coordinated responses[22,23]. This discussion confirms that terrorist organizations in Nigeria and Kenya leverage cryptocurrency's anonymity and decentralization, adapting locally via P2P and mobile money and challenging regulators without advanced tools. International parallels reinforce the need for global standards, yet the interplay with traditional systems suggests a complex threat landscape.

4.3.2 Effectiveness of Counter-Terrorism Financing Frameworks

The finding that existing counter-terrorism financing (CTF) frameworks in Nigeria and Kenya are ineffective against cryptocurrency's cross-border and pseudonymous nature due to regulatory gaps (Kenya's lack of formal regulations and Nigeria's enforcement challenges) and insufficient technological tools underscores a critical vulnerability in addressing cryptocurrency-enabled terrorism financing. This ineffectiveness necessitates enhanced international support and expertise to address these deficiencies. Results confirm that current CTF frameworks in Nigeria and Kenya struggle with cryptocurrency's inherent features, which means they fail to counter its transnational reach and anonymity effectively. The data indicate that cryptocurrency facilitates cross-border financial flows for terrorist groups, with its pseudonymous nature impeding efforts to track illicit funds. The decentralized structure of these networks and the global reach of exchanges further complicate disruption efforts, highlighting the frameworks' inability to manage international and anonymous transactions[20]. Extremist groups' use of online platforms for solicitation and cryptocurrency for operational goals exposes additional weaknesses in regulatory oversight, as these activities leverage digital anonymity beyond traditional monitoring capabilities[24]. This evidence supports the

finding's ineffectiveness claim, emphasizing the need for advanced technological tools and international collaboration to strengthen local frameworks[22].

The specific regulatory gaps driving this ineffectiveness reinforce the finding's focus on local deficiencies. In Nigeria, Respondent A notes that despite a structured framework involving the Economic and Financial Crimes Commission (EFCC) and Securities and Exchange Commission (SEC), enforcement of Know-Your-Customer (KYC) and Anti-Money Laundering (AML) regulations is inconsistent, particularly for peer-to-peer (P2P) transactions (Respondent B). This enforcement gap, worsened by the Central Bank of Nigeria's (CBN) fluctuating policies, pushes transactions underground, allowing terrorists to exploit unregulated P2P platforms[23]. In Kenya, Respondent H highlights the absence of formal cryptocurrency regulations, with the Central Bank of Kenya (CBK) relying on warnings rather than actionable measures, enabling unmonitored transactions via mobile money integrations like M-Pesa (Respondent K). Respondent J emphasizes the lack of specialized monitoring units and blockchain forensic tools in both countries, aligning with some researchers, that argue that technical incapacity undermines CTF efforts[22]. These findings resonate with some Scholars, who discuss the uneven governance of blockchain in Africa, with Nigeria's partial regulation faltering at enforcement and Kenya's regulatory void fostering exploitation[28]. The absence of technological tools amplifies these gaps, supporting the finding's call for international expertise[26].

Furthermore, the Binance case in Nigeria demonstrates enforcement struggles, with regulators accusing the platform of facilitating terrorism financing through P2P trading but lacking the tools to trace transactions effectively[2]. This contrasts sharply with U.S. successes in 2020, where blockchain analytics disrupted terrorism financing campaigns[6], underscoring a

technological gap between Nigeria/Kenya and advanced jurisdictions. In Afghanistan, weak regulatory frameworks post-Taliban takeover enable cryptocurrency misuse[8], mirroring Kenya's regulatory infancy and Nigeria's enforcement challenges. The European Parliament report suggests that cryptocurrency's traceability offers potential while traditional systems dominate[10]. However, Nigeria and Kenya lack the forensic capacity to exploit this, as seen in AD Forensics' limited training efforts[5]. These cases align with a Scholar position, who notes varying global adoption levels and emphasizes that without international support, such as FATF standards or U.S.-style analytics, local frameworks remain ineffective against cross-border and pseudonymous threats[27,28],

The finding reveals that Nigeria and Kenya's CTF frameworks are ineffective against cryptocurrency's cross-border and pseudonymous nature due to Kenya's regulatory absence, Nigeria's enforcement shortcomings, and a shared lack of technological tools. The statistical evidence of transnational flows and pseudonymity aligns with thematic gaps in enforcement and technology, corroborated by global cases where advanced jurisdictions succeed with forensics unavailable locally, Nigeria's enforcement issues, driven by inconsistent policy application, allow P2P evasion despite a structured framework, while Kenya's regulatory vacuum enables exploitation through mobile money-crypto integrations (Respondent K)[14]. This supports a researcher, who argue that decentralization challenges oversight, yet contrasts with the European Parliament's view that traditional systems dominate, suggesting cryptocurrency's role is contextually heightened in under-regulated regions[25,10].

The technological deficit lacking blockchain analytics, as noted by Respondent J and Emmanuel and Michael, underpins the finding's call for international expertise, as exemplified by U.S. successes [22,6]. However, some Scholars posit that overregulation may

drive illicit activity underground, as Nigeria's P2P surge post-CBN bans shows [23]. International support via FATF alignment could address this, but Pavlidis a researcher warns of unintended consequences like reduced financial inclusion, particularly relevant in Kenya's mobile money context[26,29]. The global parallels amplify this, suggesting Nigeria and Kenya's challenges are part of a broader need for coordinated expertise and tools yet s Scholar questions the adaptability of current global standards to emerging technologies, urging further refinement[30,31].

This discussion confirms that existing CTF frameworks in Nigeria and Kenya are ineffective against cryptocurrency's cross-border and pseudonymous nature, driven by Kenya's regulatory void, Nigeria's enforcement failures, and insufficient technological tools. Global parallels highlight the efficacy of advanced forensics absent locally, necessitating enhanced international support and expertise through standards and training.

4.3.3 Transformation of Terrorism Financing Networks and Regional Security

The finding that cryptocurrency replaces cash-based systems with digital, anonymous networks in Nigeria and Kenya, boosting terrorist autonomy and global reach while straining regional security due to inadequate tracking capabilities and diffuse threat patterns, highlights a transformative shift in terrorism financing dynamics. This evolution enhances operational flexibility for terrorist groups, posing significant challenges to regional security frameworks.

The study confirms that cryptocurrency has shifted terrorism financing in Nigeria and Kenya from traditional cash-based systems to digital, anonymous networks. It fosters a transition to concealed, tech-enabled methods that enhance autonomy and complicate oversight. The data indicate widespread use of concealment strategies, reliance on exchanges, conversion of

digital assets into usable forms, and adoption of technological innovations by terrorist groups, reflecting a move away from physical cash flows. The limited emphasis on specific regional jurisdictions suggests a diffuse threat pattern, challenging targeted security responses[32]. This evidence supports the finding's assertion that cryptocurrency boosts terrorist autonomy and global reach, straining regional security due to the absence of advanced tracking tools to monitor these decentralized networks[33]. Replacing cash-based systems with digital methods marks a significant adaptation, undermining conventional counter-terrorism financing (CTF) strategies that rely on intercepting tangible transactions.

Study. The results provide a detailed perspective on this transformation, illustrating how cryptocurrency enhances autonomy and strains security in local contexts. In Nigeria, Respondent G explains that Boko Haram and ISWAP have shifted from cash couriers to digital transfers via P2P platforms, enabling independent funding and coordination with external groups (Respondent I). This autonomy reduces reliance on centralized funding, complicating network disruption. In Kenya, Respondent H notes Al-Shabaab's use of mobile money platforms like M-Pesa to convert cryptocurrency, evading banking scrutiny (Respondent F). At the same time, Respondent J highlights international donations via Bitcoin, expanding its global reach. These adaptations align with some Schoalrs position, who argue that cryptocurrency's anonymity facilitates illicit financial flows[34]. However, the diffuse threat patterns—lacking a strong regional focus—challenge localized security measures, Respondent K in Nigeria and Respondent L in Kenya emphasize inadequate tracking capabilities, with limited blockchain forensics leaving authorities unable to monitor these networks effectively[35]. This strains regional security, as autonomous cells operate across borders, amplifying threats in West and East Africa.

This shift and its security implications through global examples. In Nigeria, the EFCC documents Boko Haram's use of P2P traders to convert cryptocurrency into local currency, enhancing autonomy by bypassing AML/CFT regulations[11]. Similarly, the Taliban's Bitcoin adoption in Afghanistan post-2021 takeover sustains operations in a weak regulatory environment[17], mirroring Nigeria and Kenya's inadequate tracking capabilities. Globally, jihadist groups solicit cryptocurrencies for cross-border funding (Foundation for Defense of Democracies, cited in paralleling Kenya's Al-Shabaab donation networks[17]. Some Researchers work support this, noting cryptocurrency's role in funding international terrorism[33]. However, traditional systems may still play a significant role, a nuance contrasting with the evident shift in Nigeria and Kenya's contexts. The lack of advanced blockchain analytics in both countries, unlike more equipped jurisdictions, strains regional security as diffuse threats enabled by digital anonymity evade interception[2, 34]. These parallels highlight a global trend, amplifying the need for enhanced tracking capabilities.

The finding demonstrates that cryptocurrency replaces cash-based systems with digital, anonymous networks in Nigeria and Kenya, boosting terrorist autonomy and global reach while straining regional security. The statistical shift to concealed, tech-enabled methods aligns with thematic evidence of P2P and mobile money adaptations, corroborated by global cases where autonomy enhances operational resilience[14]. Nigeria's Boko Haram and Kenya's Al-Shabaab leverage these networks to operate independently, reducing vulnerability to centralized crackdowns (Respondent M), a trend supported by some works[32]. The diffuse threat patterns, lacking regional concentration, complicate security responses, as Respondents N and J noted, aligning with some work on cryptocurrency's global implications[34].

However, inadequate tracking capabilities lacking forensics as per Respondent K Some Scholars exacerbate this strain, contrasting with advanced jurisdictions[36]. However, some position suggest that regulatory efforts may lag behind technological adoption, a concern echoed in Nigeria's P2P reliance and Kenya's mobile money integration, posing a dilemma: inadequate tools fail to curb threats, yet regulatory gaps enable exploitation[37]. The global reach, evidenced by cross-border funding, supports the need for international coordination, yet some researchers highlight enforcement challenges in under-resourced settings, suggesting tailored solutions[38]. This complexity strains regional security, necessitating advanced tools and global cooperation, though the balance between digital and traditional threats remains a critical research gap. This discussion affirms that cryptocurrency replaces cash-based systems with digital, anonymous networks in Nigeria and Kenya, enhancing terrorist autonomy and global reach and straining regional security due to inadequate tracking and diffuse threats. Global parallels underscore the need for advanced forensics and coordination, yet the interplay with traditional systems suggests a multifaceted threat landscape.

4.3.4: Interconnections Between Local Markets, International Systems, and Terrorism Financing

The finding that local markets in Nigeria (P2P-driven) and Kenya (mobile money-linked) integrate with international financial systems amplifying terrorism financing through anonymity and weak oversight, necessitating global coordination to address cross-border flows, underscores a critical nexus between local financial ecosystems and global illicit networks. This integration heightens the risk of terrorism financing by leveraging cryptocurrency's features, posing significant challenges to national and regional security frameworks.

The study confirms that local cryptocurrency markets in Nigeria and Kenya connect with international financial systems, which means they amplify terrorism financing by facilitating cross-border flows and exploiting anonymity. The data indicate that cryptocurrency adoption influences traditional financial systems, introduces vulnerabilities to global security infrastructure, and supports cyber warfare and state-sponsored terrorism, reflecting its integration into broader illicit networks[39]. The pseudonymous nature of transactions impacts national security efforts, while the proliferation of cryptocurrencies affects economic sanctions and financial controls, highlighting weak oversight in local markets. This evidence supports the finding's assertion that P2P-driven markets in Nigeria and mobile money-linked systems in Kenya amplify terrorism financing through their global connectivity, requiring international coordination to address these anonymous, cross-border flows[40]. The lack of robust local regulatory mechanisms exacerbates this integration, enabling terrorists to exploit international systems beyond national jurisdictions.

A detailed view of how local markets integrate with international systems, amplifying terrorism financing risks. In Nigeria, Respondent A highlights that P2P platforms enable anonymity, linking local traders to international terrorist networks (Respondent C), such as those in the Sahel and Middle East (Respondent B), exploiting weak oversight due to inconsistent regulatory enforcement. In Kenya, Respondent F notes that mobile money systems like M-Pesa connect to global cryptocurrency markets, allowing Al-Shabaab to convert funds from international donors (Respondent I), leveraging the absence of formal regulations (Respondent G). These local-international linkages align with a Scholar, who argues that cryptocurrency's anonymity fuels terrorism financing across borders[41]. However, the specific mechanisms of P2P in Nigeria and mobile money in Kenya reflect distinct

adaptations to local infrastructures. Respondent C in Nigeria and Respondent J in Kenya emphasize the need for global coordination, as weak oversight and tracking limitations (e.g., lack of blockchain forensics) enable these cross-border flows[42]. This integration amplifies financing risks, necessitating international frameworks to address the transnational nature of these threats.

This integration and its implications through global parallels. In Nigeria, the Binance case illustrates how local P2P activities connect to international systems, with regulators struggling to oversee transactions linked to terrorism financing due to weak local controls[11]. In Afghanistan, Bitcoin adoption under Taliban control post-2021 exemplifies a similar vulnerability, integrating local markets into global illicit networks amid regulatory gaps[8], mirroring Nigeria and Kenya's oversight challenges. Globally, the use of cryptocurrencies for cross-border terrorism financing is evident, with groups exploiting anonymity in under-regulated jurisdictions like Pakistan[8]. Another position support this, linking terrorist attacks to cryptocurrency market dynamics and suggesting a broader pattern of integration that amplifies financing risks[43]. The lack of advanced tracking tools in Nigeria and Kenya, unlike more equipped contexts[13], underscores the need for global coordination, as local weak oversight enables seamless connections to international systems[43]. These cases highlight a global challenge, reinforcing the finding's call for coordinated action.

The finding demonstrates that local markets in Nigeria (P2P-driven) and Kenya (mobile money-linked) integrate with international financial systems, amplifying terrorism financing through anonymity and weak oversight. The statistical evidence of global vulnerabilities and cross-border flows aligns with thematic insights into P2P and mobile money linkages, corroborated by global cases where local weaknesses connect to international networks[10].

Nigeria's P2P markets and Kenya's mobile money systems exploit anonymity to facilitate funding from international sources (Respondents B and I), a trend supported by[39]. Weak oversight due to inconsistent enforcement in Nigeria and regulatory absence in Kenya exacerbates this, as Respondents G and C noted, aligning with some research on digital economy threats[42].

The need for global coordination is evident, as cross-border flows strain national capacities and lack forensics[41]. However, a study suggests that market reactions to terrorism may overestimate cryptocurrency's role, urging caution in resource allocation[44]. A Scholar advocates for international standards to curb anonymity, but while another warns that weak local enforcement, as in Nigeria and Kenya, undermines global efforts, suggesting a dual challenge: local capacity and global alignment[41,43]. This integration amplifies financing risks, requiring coordinated frameworks, though the balance between local adaptation and international oversight remains a critical tension for policy development.

This discussion confirms that local markets in Nigeria and Kenya integrate with international systems, amplifying terrorism financing through anonymity and weak oversight, necessitating global coordination to address cross-border flows. Global parallels highlight the urgency of enhanced oversight and tools, yet the interplay with local enforcement gaps suggests a complex challenge.

4.3.5: Policy Recommendations for Countering Cryptocurrency-Enabled Terrorism Financing

The finding that effective policies in Nigeria and Kenya require international regulatory alignment, advanced technical training, industry collaboration tailored to local systems (P2P

in Nigeria, mobile money in Kenya), and regional/global frameworks to counter cryptocurrency-enabled terrorism financing while balancing enforcement with rights highlights a multifaceted approach to addressing this evolving threat. This policy framework seeks to mitigate the vulnerabilities exposed by cryptocurrency's use in terrorism financing, balancing robust countermeasures with ethical considerations.

The finding underscores the need for comprehensive policy responses in Nigeria and Kenya, which means effective strategies must integrate international alignment, technical capacity, and collaborative efforts to counter cryptocurrency-enabled financing. The data indicate that security agencies actively monitor threats, perceive significant global security risks from cryptocurrency integration, and recognize the feasibility of mitigation strategies, suggesting a foundation for policy enhancement[44]. The potential for collaboration with the cryptocurrency industry further supports tailored approaches, while the impact of anonymity on national security efforts highlights the necessity of advanced tools and global frameworks. This evidence aligns with the finding's call for international regulatory alignment, technical training to address cross-border threats, industry collaboration to leverage local systems like P2P and mobile money, and balanced enforcement to protect rights[45]. The statistical insights emphasize a proactive yet adaptable policy stance, critical for tackling the diffuse and anonymous nature of cryptocurrency financing[46].

However, it further provides a detailed perspective on these policy needs, emphasizing tailored and globally coordinated solutions. In Nigeria, Respondent A advocates aligning local regulations with international standards like those of the Financial Action Task Force (FATF). At the same time, Respondent E stresses advanced training in blockchain analytics for law enforcement, Respondent B highlights industry collaboration with P2P-focused

cryptocurrency exchanges, tailoring policies to Nigeria's local system. Respondent F sees the regulatory landscape as an opportunity to integrate global best practices in Kenya. Respondent H proposes collaboration with mobile money platforms like M-Pesa to enhance oversight, Respondent C in Nigeria and Respondent J in Kenya emphasize regional bodies like the African Union (AU) or ECOWAS for coordinated frameworks, aligning with some thought, who advocate for international policy transformation to counter digital threats[47]. The balance with rights is implicit in calls for capacity building over punitive measures alone, supporting the finding's holistic approach to counter cryptocurrency financing effectively[48].

In Nigeria, the Binance case highlights the need for international regulatory alignment, with demands for user data reflecting cross-border coordination challenges[19]. However, Tigran Gambaryan's detention raises rights concerns, aligning with the finding's balance emphasis[2,48]. U.S. successes in disrupting financing campaigns via blockchain forensics[6] emplify advanced technical training's efficacy, a model for Nigeria and Kenya's needs. Globally, weak AML/CFT regimes in Afghanistan and Pakistan amplify cryptocurrency misuse, underscoring the necessity of regional/global frameworks, as seen in AD Forensics' training efforts[8,5]. Some Scholars advocate for public-private partnerships, supporting industry collaboration tailored to local P2P and mobile money systems[49]. These parallels highlight a global consensus on coordinated, tech-savvy policies balanced with rights considerations, reinforcing the finding's comprehensive strategy[50].

The finding illustrates that effective policies in Nigeria and Kenya require international regulatory alignment, advanced technical training, industry collaboration tailored to P2P and mobile money systems, and regional/global frameworks to counter cryptocurrency-enabled terrorism financing. The statistical evidence of monitoring and mitigation potential aligns

with thematic calls for training and collaboration (Respondents E and H), corroborated by global cases where technical and cooperative successes contrast with local gaps. Nigeria's P2P and Kenya's mobile money systems necessitate tailored industry partnerships, as supported by some scholar work while international alignment via FATF or AU frameworks addresses cross-border flows[50,47]. The balance with rights, evident in Gambaryan's case, resonates with some scholarly work who emphasize ethical enforcement[1,51].

However, some Scholars caution that overreliance on enforcement may neglect local economic contexts, risking exclusion, while another person highlights the need for legal safeguards in regulatory actions[49,48]. The global reach requires coordination, yet another Scholar notes that national security priorities may conflict with international efforts, suggesting a tension between local adaptation and global alignment[51]. Another Researcher proposes that industry collaboration as a bridge, but its feasibility in under-resourced settings like Kenya remains underexplored[46]. This complexity underscores the finding's call for a balanced, multi-pronged approach, necessitating further research into scalable training and rights-aligned frameworks.

This discussion affirms that effective policies in Nigeria and Kenya require international regulatory alignment, advanced technical training, tailored industry collaboration, and regional/global frameworks to counter cryptocurrency-enabled terrorism financing balanced with rights. Global parallels highlight the efficacy of such strategies, yet local and ethical challenges suggest a nuanced policy landscape.

Endnotes

1. T. Gambaryan. *Tweet on Regulatory Challenges and Binance Compliance Issues in Nigeria* [Tweet], X (formerly Twitter), 2024, Retrieved from https://x.com/TigranGambaryan/status/1890287335205384312?t=tpKO8ewb0p-seJjqHOBsLQ&s=19

2. A. Greenberg. *Tweet on Cryptocurrency and Global Regulatory Enforcement Trends* [Tweet], X (formerly Twitter), 2024, Retrieved from https://x.com/a_greenberg/status/1888930445766598971?t=ttoFa2zqe0gP4BRmhC4X4w&s=19

3. Wired. *The Untold Story of Crypto Crimefighters' Descent into Nigerian Prison,* 2024, Retrieved from https://www.wired.com/story/untold-story-crypto-crimefighters-descent-nigerian-prison-binance/

4. Chainalysis. *Cryptocurrency and Terrorism Financing Accuracy Check,* 2024, Retrieved from https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/

5. Crypto Times. *AD Forensics Trains Crypto Crime Fighters in Nigeria,* 2024, Retrieved from https://www.cryptotimes.io/2024/02/18/ad-forensics-trains-crypto-crime-fighters-in-nigeria/

6. U.S. Department of Justice. *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns,* Washington: U.S. Department of Justice, Office of Public Affairs, 2024, https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyberenabled-campaigns

7. T. Tarrant-Cornish. *Terrorist Dream Come True' ISIS Using Bitcoin to Fund Deadly Attacks and Buy Weapons,* Express, 2018, https://www.express.co.uk/finance/city/902517/ISIS-Bitcoin-terrorist-attackdeadly-weapons-funding-cryptocurrency-money-laundering

8. A. Cuthbertson & A. Sigalos. *Bitcoin Adoption in Afghanistan Spikes Amid Taliban Takeover,* 2021, https://www.independent.co.uk/life-style/gadgets-and-tech/bitcoin-afghanistancrypto-taliban-economy-b1907180.html

9. DL News. *Nigeria Probes Binance over Terror Funds and Money Laundering Allegations,* 2024, Retrieved from https://www.dlnews.com/articles/markets/nigeria-probes-binance-on-terror-funds-and-money-laundering/

10. T. Keatinge, D. Carisle, & F. Keen. *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses,* Brussels: European Parliament, Directorate General for International Policies. Policy Department for Citizens' Rights and Constitutional Affairs. Counter Terrorism, 2018.

11. Nairametrics. *Court Freezes N548.6 Million in Bybit and KuCoin Accounts over Naira Fluctuation Allegations,* 2024, Retrieved from https://nairametrics.com/2024/09/11/court-freezes-n548-6-million-belonging-to-bybit-kucoin-nigerian-crypto-users-over-naira-fluctuation-allegations/

12. Nairametrics. *Court Directs Binance to Release Data of Nigerian Users to EFCC over Alleged Terrorism Financing,* 2024, Retrieved from https://nairametrics.com/2024/03/18/court-directs-binance-to-release-data-of-nigerians-to-efcc-over-alleged-terrorism-financing/

13. New Lines Magazine. *The Rise and Fall of Cryptocurrency in Nigeria,* 2024, Retrieved from https://newlinesmag.com/reportage/the-rise-and-fall-of-cryptocurrency-in-nigeria/

14. Punch NG. *Why the US, Nigeria, and Others Are Cracking Down on Cryptocurrency "Kings",* 2024, Retrieved from https://punchng.com/why-us-nigeria-others-crack-down-on-crypto-currency-kings/?amp=#amp_tf=From%20%251%24s&aoh=17329557158439&referrer=https%3A%2F%2Fwww.google.com

15. Punch NG. *Terrorists Using Cryptocurrency Traders to Fund Insecurity in Nigeria—EFCC Report,* 2024, Retrieved from https://punchng.com/terrorists-using-cryptocurrency-traders-to-fund-insecurity-efcc/

16. Arise TV. *Police Interrogate CEO of Blord Group of Companies for Terrorism Funding and Cryptocurrency Fraud,* 2024, Retrieved from https://www.arise.tv/police-interrogate-ceo-blord-group-of-companies-for-terrorism-funding-cryptocurrency-fraud/

17. N. Popper. *Jihadists See a Funding Boon in Bitcoin,* The Wall Street Journal, 2018, https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin1519131601

18. The Africa Report. *Nigeria's Crypto Comeback: SEC Approves Local Exchanges Post-Binance Ban,* 2024, Retrieved from https://www.theafricareport.com/360383/nigerias-crypto-comeback-sec-approves-local-exchanges-post-binance-ban/

19. Premium Times Nigeria. *Nigerian Government Freezes $37M in Cryptocurrency Linked to Suspected Protest Organizers,* 2024, Retrieved from https://www.premiumtimesng.com/news/top-news/723986-exclusive-nigerian-govt-freezes-37m-worth-of-cryptocurrency-traced-to-suspected-protest-organisers.html

20. V. Dyntu & O. Dykyj. *Cryptocurrency as an Instrument of Terrorist Financing,* **Baltic Journal of Economic Studies,** 7(5), 2021, 67–72.

21. S. A. Warreth. *Comparing Far Right and Jihadi Use of Crowdfunding, Cryptocurrencies, and Blockchain Technology: Accessibility, Geography, Ideology,* 2020.

22. O. T. Emmanuel & A. A. Michael. *Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria,* **Journal of Auditing, Finance, and Forensic Accounting,** 8(2), 2020, 55–66.

23. Oladipupo, A.O and Amodu, A.A (2022). *Impact of Cryptocurrency Ban on the Development of cryptocurrency in Nigeria*, **Renaissance University Journal of Management and Social Science**,8(2)

24. A. Majumder, M. Routh, & D. Singha. *A Conceptual Study on the Emergence of Cryptocurrency Economy and its Nexus with Terrorism Financing,* In *The Impact of Global Terrorism on Economic and Political Development: Afro-Asian Perspectives* Emerald Publishing Limited, 2019, 125–138.

25. A. Ghosh, S., Gupta, A., Dua, N., & Kumar. *Security of Cryptocurrencies in Blockchain Technology: State-of-Art, Challenges and Future Prospects,* **Journal of Network and Computer Applications,** 163, 2020, 102635.

26. F. Costantino. *The FATF Recommendations and the Development of International Standards on Terrorist Financing,* In *Countering Terrorist and Criminal Financing* CRC Press, 2024, 31–42.

27. A. Eaddy. *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation), 2019.

28. M. Campbell-Verduyn & F. Giumelli. *Enrolling into Exclusion: African Blockchain and Decolonial Ambitions in an Evolving Finance/Security Infrastructure,* **Journal of Cultural Economy,** 15(4), 2022, 524–543.

29. O. Ariani & A. L. Ibrahim. *Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia,* **Jurnal Usm Law Review,** 7(1), 2023, 30–44.

30. G. Pavadilis. *The Dark Side of Anti-Money Laundering: Mitigating the Unintended Consequences of FATF Standards,* **Journal of Economic Criminology,** 2, 2023, 100040.

31. E. A. Akartuna, S. D. Johnson, & A. Thompton. *Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi Study,* **Technological Forecasting and Social Change,** 179, 2022, 121632.

32. S. D. Jayasekara. *How Effective are the Current Global Standards in Combating Money Laundering and Terrorist Financing?* **Journal of Money Laundering Control,** 24(2), 2021, 257–267.

33. H. M. C. Sebastião, P. J. O. R. D. Cunha, & P. M. C. Godinho. *Cryptocurrencies and Blockchain: Overview and Future Perspectives,* **International Journal of Economics and Business Research,** 21(3), 2021, 305–342.

34. A. Faturahman, V. Agarwal, & C. Lukita. *Blockchain Technology—the Use of Cryptocurrencies in Digital Revolution,* **IAIC Transactions on Sustainable Digital Innovation (ITSDI),** 3(1), 2021, 53–59.

35. J. M. Hashemi, Y. Nishikawa, & K. Dandapani. *Cryptocurrency, a Successful Application of Blockchain Technology,* **Managerial Finance,** 46(6), 2020, 715–733.

36. S. K. Fakunmoju, O. Banmore, A. Gbadamosi, & O. I. Okunbanjo. *Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance,* **Binus Business Review,** 13(1), 2022, 31–40.

37. A. T. Wardhana & B. W. Nugroho. *Abuse of Cryptocurrency to Funding International Terrorism Activities,* In *Proceedings Universitas Muhammadiyah Yogyakarta Undergraduate Conference,* 1(1), 2021, 353–362.

38. V. Ediagbonya & T. C. Tioluwani. *The Growth and Regulatory Challenges of Cryptocurrency Transactions in Nigeria,* In *the Complexities of Sustainability,* 2023, 267–297.

39. N. N. Reshetnikova, M. M. Magomedov, S. S. Zmiyak, A. V. Gagarinskii, & D. A. Buklanov. *Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security,* In *Current Problems and Ways of Industry Development: Equipment and Technologies,* Cham: Springer International Publishing, 2021, 355–363.

40. P. C. Patel & J. Richter. *The Relationship between Terrorist Attacks and Cryptocurrency Returns,* **Applied Economics,** 53(8), 2021, 940–961.

41. A. M. VÂRTEI. *Financing Terrorism: Economy's Dark Side,* In *Proceedings of the International Conference on Cybersecurity and Cybercrime-2023 Asociatia Romana pentru Asigurarea Securitatii Informatiei,* 2023, 216–223.

42. A. Andrianova. *Countering the Financing of Terrorism in the Conditions of Digital Economy,* In *Digital Transformation of the Economy: Challenges, Trends and New Opportunities,* Springer International Publishing, 2020, 20–31.

43. T. N. E. Al-Tawil. *Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches,* **Journal of Money Laundering Control,** 26(6), 2023, 1150–1164.

44. L. Almaqableh, K., Reddy, V., Pereira, V., Ramiah, D., Wallace, D., & J. F. Veron. *An Investigative Study of Links between Terrorist Attacks and Cryptocurrency Markets,* **Journal of Business Research,** 147, 2022, 177–188.

45. F. M. J. Teichmann & M. C. Falker. *Cryptocurrencies and Financial Crime: Solutions from Liechtenstein,* **Journal of Money Laundering Control,** 24(4), 2021, 775–788.

46. N. G. Packin & U. Volovelsky. *Digital Assets, Anti-Money Laundering and Counter Financing of Terrorism: An Analysis of Evolving Regulations and Enforcement in the Era of NFTs,* In *The Cambridge Handbook on Law and Policy for NFTs* (Nizan Geslevich Packin, ed.), Forthcoming, 2023.

47. S. M. S. Zaidi & Nirmal. *Emerging Realities in the International Political System: Transforming State's Foreign Policy,* **Herald of the Russian Academy of Sciences,** 2023, 1–14.

48. E. A. Valvi. *The Role of Legal Professionals in the European and International Legal and Regulatory Framework against Money Laundering,* **Journal of Money Laundering Control,** 26(7), 2023, 28–52.

49. O. J. Olujobi & E. T. Yebisi. *Combating the Crimes of Money Laundering and Terrorism Financing in Nigeria: A Legal Approach for Combating the Menace,* **Journal of Money Laundering Control,** 26(2), 2023, 268–289.

50. N. A. Al-Suwaidi & H. Nobanee. *Anti-Money Laundering and Anti-Terrorism Financing: A Survey of the Existing Literature and a Future Research Agenda,* **Journal of Money Laundering Control,** 24(2), 2021, 396–426.

51. S. Wagman. *Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing,* **Harv. Nat'l Sec. J.,** 14, 2022, 87.

Chapter Five

Conclusion

5.1 Summary of Findings

The findings from Objective 1 indicate that terrorist organisations in Nigeria and Kenya exploit cryptocurrency's anonymity and decentralised features to finance their activities, relying heavily on methods tailored to local contexts that challenge regulatory oversight.

Statistical Analysis reveals through Table 4.2 that terrorist groups in Nigeria (N = 67) and Kenya (N = 36) acquire cryptocurrency funds (Nigeria: 59.70%, $\bar{X}$ = 0.60; Kenya: 61.11%, $\bar{X}$ = 0.61), conceal transactions (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), use privacy-focused cryptocurrencies or mixing services (Nigeria: 55.22%, $\bar{X}$ = 0.55; Kenya: 55.56%, $\bar{X}$ = 0.56), and employ laundering tactics (Nigeria: 53.73%, $\bar{X}$ = 0.54; Kenya: 52.78%, $\bar{X}$ = 0.53), which means they prioritise anonymity-driven strategies over less-used options like DeFi platforms (Nigeria: 47.76%, $\bar{X}$ = 0.48; Kenya: 47.22%, $\bar{X}$ = 0.47).

Thematic Analysis highlights that in Nigeria, P2P trading and "smurfing" exploit weak KYC/AML enforcement, while in Kenya, terrorists integrate cryptocurrency with mobile money (e.g., M-Pesa) and use privacy coins like Monero, capitalising on regulatory gaps and decentralised systems.

Case Study Analysis shows global parallels, with groups like Al-Qaeda, Hamas, and ISIS using Bitcoin and privacy coins for donations and weapons, and Nigeria's Binance P2P case mirroring Taliban's Bitcoin use in Afghanistan, underscoring a consistent reliance on anonymity across contexts.

The findings from Objective 2 indicate that current counter-terrorism financing frameworks in Nigeria and Kenya are significantly undermined by cryptocurrency's cross-border reach and pseudonymity, exposing critical gaps in regulation and enforcement capabilities.

Statistical Analysis from Table 4.3 demonstrates that cryptocurrency facilitates cross-border transactions (Nigeria: 67.16%, $\bar{X}$ = 0.67; Kenya: 72.22%, $\bar{X}$ = 0.72), hinders tracking due to pseudonymity (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), and affects disruption via decentralised networks (Nigeria: 52.24%, $\bar{X}$ = 0.52; Kenya: 50.00%, $\bar{X}$ = 0.50), with over half noting its use for international terrorism (Nigeria: 55.22%, $\bar{X}$ = 0.55; Kenya: 55.56%, $\bar{X}$ =

0.56), which means existing systems struggle with global and anonymous financing challenges.

Thematic Analysis reveals that Nigeria's structured framework (EFCC, SEC) is weakened by poor P2P enforcement. At the same time, Kenya's lack of formal regulations and mobile money vulnerabilities leave transactions unmonitored, both hampered by limited blockchain forensics.

Case Study Analysis illustrates Nigeria's Binance investigation struggling with enforcement, contrasted by U.S. successes using blockchain analytics (e.g., 2020 disruptions), showing effectiveness depends on technical capacity and cooperation absent in both countries.

The findings from Objective 3 indicate that cryptocurrency adoption has transformed traditional terrorism financing in Nigeria and Kenya from cash-based to concealed, tech-enabled networks, enhancing operational secrecy and complicating regional security dynamics.

Statistical Analysis from Table 4.4 shows terrorists conceal transactions (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), use exchanges (Nigeria: 58.21%, $\bar{X}$ = 0.58; Kenya: 58.33%, $\bar{X}$ = 0.58), convert assets (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 55.56%, $\bar{X}$ = 0.56), and adopt tech innovations (Nigeria: 50.75%, $\bar{X}$ = 0.51; Kenya: 50.00%, $\bar{X}$ = 0.50), with less regional focus (Nigeria: 37.31%, $\bar{X}$ = 0.37; Kenya: 36.11%, $\bar{X}$ = 0.36), which means it shifts financing toward digital secrecy over traditional methods.

Thematic Analysis notes Nigeria's Boko Haram/ISWAP and Kenya's Al-Shabaab replacing cash with P2P and mobile money transfers, expanding autonomy and challenging law enforcement with decentralised funding.

Case Study Analysis highlights Boko Haram's P2P use and Taliban's Bitcoin adoption enhancing independence, with weak forensics in Nigeria/Kenya mirroring Afghanistan/Pakistan, amplifying regional security threats.

The findings from Objective 4 indicate that local cryptocurrency markets in Nigeria and Kenya interconnect with international financial systems, amplifying terrorism financing risks through anonymity and inadequate oversight, necessitating global coordination.

Statistical Analysis from Table 4.5 demonstrates that adoption impacts financial systems (Nigeria: 67.16%, $\bar{X} = 0.67$; Kenya: 72.22%, $\bar{X} = 0.72$), poses global vulnerabilities (Nigeria: 59.70%, $\bar{X} = 0.60$; Kenya: 61.11%, $\bar{X} = 0.61$), affects security via anonymity (Nigeria: 55.22%, $\bar{X} = 0.55$; Kenya: 55.56%, $\bar{X} = 0.56$), and supports cyber warfare (Nigeria: 52.24%, $\bar{X} = 0.52$; Kenya: 50.00%, $\bar{X} = 0.50$), which means local markets enable broader illicit networks.

Thematic Analysis shows Nigeria's P2P and mixers linking to Sahel/Middle East funding. Kenya's mobile money-crypto ties to Al-Shabaab's global donors, both driven by regulatory gaps fostering underground markets.

Case Study Analysis cites Nigeria's Binance case and Afghanistan's Bitcoin surge, illustrating local-global financial integration facilitating cross-border terrorism financing amid regulatory disparities.

The findings from Objective 5 indicate that context-specific policies in Nigeria and Kenya must bolster international cooperation and technical capacity to effectively counter cryptocurrency-enabled terrorism financing, addressing local and global challenges.

Statistical Analysis from Table 4.6 reveals that security agencies monitor threats (Nigeria: 74.63%, $\bar{X} = 0.75$; Kenya: 83.33%, $\bar{X} = 0.83$), global risks are significant (Nigeria: 71.64%, $\bar{X}$

= 0.72; Kenya: 77.78%, $\bar{X}$ = 0.78), mitigation is feasible (Nigeria: 62.69%, $\bar{X}$ = 0.63; Kenya: 66.67%, $\bar{X}$ = 0.67), and industry collaboration is supported (Nigeria: 56.72%, $\bar{X}$ = 0.57; Kenya: 61.11%, $\bar{X}$ = 0.61), which means robust monitoring and partnerships offer viable solutions.

Thematic Analysis recommends FATF alignment, blockchain forensics training, public-private partnerships (Nigeria: exchanges; Kenya: mobile money), and AU/ECOWAS coordination for regional strength.

Case Study Analysis points to U.S. forensics success and Nigeria's Binance efforts, suggesting harmonised AML/CFT rules, task forces, and community reporting balanced with rights as seen in Gambaryan's detention concerns.

5.2 Conclusion

The study demonstrated how cryptocurrency advanced terrorism funding practises through its redefinition of international connections and diplomatic operational challenges in Nigeria and Kenya. The Analysis of five main objectives revealed the conclusions and their corresponding implications, as follows.

This study has examined the sophisticated methods and strategies through which terrorist organisations in Nigeria and Kenya exploit cryptocurrency's anonymity and decentralisation to advance terrorism financing, revealing a critical dimension of local adaptation. The findings demonstrate that these groups leverage peer-to-peer trading in Nigeria and mobile money integrations in Kenya, tailoring their approaches to local financial ecosystems to obscure financial trails and evade detection. This strategic adaptability poses significant challenges for diplomatic efforts and regulatory authorities, strained by the absence of

advanced tracking tools and the inherent difficulties of monitoring decentralised networks. The evidence highlights a transformative shift in terrorism financing practices, amplifying operational flexibility and complicating interstate cooperation, with profound implications for regional security and global governance within an interconnected world.

This Analysis has revealed the ineffectiveness of existing counter-terrorism financing frameworks in Nigeria and Kenya in addressing cryptocurrency-enabled terrorism financing, underscoring a critical challenge within International Relations and Diplomatic Studies. The findings indicate that regulatory gaps undermine these frameworks, Nigeria's inconsistent enforcement, and Kenya's lack of formal regulations, coupled with a technological deficit that hampers the ability to counter cryptocurrency's cross-border and pseudonymous nature. This inefficacy strains diplomatic efforts to coordinate responses across national boundaries, exposing disparities in capacity and oversight that hinder multilateral security cooperation. The study illuminates the critical need for enhanced diplomatic alignment and technological capacity to safeguard regional and global stability against evolving financial threats in an interconnected international system.

This exploration has uncovered the transformative impact of cryptocurrency on terrorism financing networks in Nigeria and Kenya, shifting from cash-based systems to digital, anonymous structures, with significant implications for regional security within International Relations and Diplomatic Studies. The findings reveal that this transition enhances terrorist autonomy and global reach, straining regional security through diffuse threat patterns enabled by local adaptations such as peer-to-peer trading and mobile money integrations. The resultant complexity challenges diplomatic efforts to coordinate interstate responses, as the lack of advanced tracking capabilities exacerbates vulnerabilities across borders. This conclusion

underscores the profound diplomatic and security challenges posed by cryptocurrency's integration into terrorism financing, necessitating a deeper understanding of regional dynamics within the global security landscape.

This investigation has delineated the interconnections between local markets in Nigeria and Kenya and international financial systems, amplifying terrorism financing through cryptocurrency's anonymity and weak oversight, with critical implications for International Relations and Diplomatic Studies. The findings demonstrate that peer-to-peer-driven markets in Nigeria and mobile money-linked systems in Kenya integrate with global networks, heightening financing risks through cross-border flows that evade regulatory scrutiny. This integration poses significant diplomatic challenges, as disparities in oversight and capacity between advanced and under-resourced states complicate multilateral efforts to address these transnational threats. The study highlights the urgent need for diplomatic coordination to navigate the tensions between local adaptations and global governance, ensuring stability in an interconnected world.

This Analysis has illuminated the complex policy landscape required to counter cryptocurrency-enabled terrorism financing in Nigeria and Kenya, revealing a critical arena for International Relations and Diplomatic Studies. The findings underscore the need for a multifaceted approach to address the technological, regulatory, and diplomatic deficiencies that hinder effective responses to this evolving threat. The inefficacy of current frameworks, compounded by local adaptations such as peer-to-peer trading and mobile money integrations and the absence of advanced tools, challenge interstate cooperation and multilateral governance. This conclusion reaffirms the key role of diplomatic strategy in navigating the

relationship of technological innovation, security threats, and policy alignment, fostering a robust foundation for regional and global stability in an interconnected international system.

5.3 Recommendations

1. Establish a pioneering Diplomatic Cryptocurrency Intelligence Consortium, spearheaded by the African Union (AU), with Nigeria and Kenya as anchor states, to deploy state-of-the-art blockchain analytics for real-time monitoring of peer-to-peer trading platforms and mobile money integrations exploited by terrorist organisations. This consortium should integrate a dedicated diplomatic arm to facilitate multilateral intelligence sharing among ECOWAS, IGAD, and international partners such as the United Nations Office on Drugs and Crime (UNODC) and the Financial Action Task Force (FATF) while simultaneously launching a series of high-level diplomatic training academies to equip Nigerian and Kenyan diplomats and security officials with specialised knowledge of cryptocurrency's anonymity-driven strategies. This multifaceted approach will enhance interstate cooperation, address the operational flexibility of terrorist groups, and strengthen regional security diplomacy within an interconnected global framework.
2. Institute a transformative Regional Diplomatic Technology Alliance, convened under the auspices of ECOWAS and IGAD, to bridge the technological and regulatory deficits undermining counter-terrorism financing frameworks in Nigeria and Kenya. This alliance should orchestrate a comprehensive programme of blockchain forensic training for diplomats and law enforcement, procure cutting-edge analytical tools through strategic partnerships with advanced jurisdictions like the European Union and the United States, and negotiate a binding regional regulatory compact to harmonise anti-money laundering

and counter-terrorism financing measures. Leveraging diplomatic channels to secure international funding and technical expertise, this initiative will address Nigeria's enforcement inconsistencies and Kenya's regulatory void, fostering a robust multilateral framework to counter cryptocurrency's cross-border and pseudonymous threats.

3. Create an innovative Diplomatic Regional Security Observatory, anchored by the AU and supported by the United Nations, to monitor and mitigate the transformation of terrorism financing networks in Nigeria and Kenya to digital, anonymous platforms. This observatory should deploy advanced predictive analytics and real-time tracking technologies to identify diffuse threat patterns, establish a diplomatic early warning system to preempt security risks and convene annual regional summits to enhance interstate collaboration and intelligence sharing among ECOWAS, IGAD, and international partners. By addressing cryptocurrency's enhanced autonomy and global reach, this initiative will strengthen diplomatic coordination, fortify regional security, and navigate the complex dynamics of terrorism financing within a global security landscape.
4. Develop a groundbreaking Global-Local Diplomatic Convergence Framework, facilitated by the AU in collaboration with the FATF and significant international actors, to dismantle the interconnections between Nigeria's peer-to-peer-driven markets, Kenya's mobile money-linked systems, and global financial networks that amplify terrorism financing. This framework should establish a tripartite diplomatic task force involving Nigeria, Kenya, and advanced economies to monitor cross-border cryptocurrency flows, negotiate enforceable regulatory alignments with international standards, and foster public-private partnerships with local and international exchanges to enhance transparency and oversight. This initiative will strengthen multilateral diplomacy, mitigate transnational

financing risks, and ensure stability in an interconnected world by addressing disparities in capacity and weak regulatory structures.

5. Establish a visionary Diplomatic Policy Innovation Institute, jointly led by ECOWAS, IGAD, and G20 partners, to formulate and implement a forward-thinking policy architecture for Nigeria and Kenya to counter cryptocurrency-enabled terrorism financing. This institute should integrate advanced blockchain forensic research, develop context-specific regulatory frameworks tailored to local adaptations like peer-to-peer trading and mobile money integrations, and convene biannual diplomatic symposia to align national policies with international standards while ensuring rights-balanced enforcement strategies. This initiative will address technological, regulatory, and diplomatic deficiencies, leveraging interdisciplinary expertise and diplomatic collaboration, reinforcing multilateral governance and fostering a resilient foundation for regional and global security in an interconnected international system.

5.4 Contribution to Knowledge

This study enriches scholarly understanding across conceptual, theoretical, empirical, practical, and broader dimensions. It establishes its significance in addressing the intricate interplay of local adaptations, international interconnections, and diplomatic challenges in an interconnected globally.

For conceptual contribution, the study introduces a pioneering conceptual framework that reimagines cryptocurrency as a dynamic instrument of terrorism financing, intricately embedded within Nigeria and Kenya's socio-economic and political contexts. It advances a novel construct of "digital financial sovereignty," redefining financial anonymity in

International Relations to encapsulate how terrorist organisations exploit local adaptations such as peer-to-peer trading and mobile money integrations to navigate global financial networks. These dynamic approaches resulted in conceptual innovation extending traditional understandings of illicit finance, providing a sophisticated lens through which to scrutinise the nexus of local agency and international connectivity, thereby enriching the conceptual repertoire of international relations.

Theoretically, this study extends and integrates Social Network Theory (SNT) and Game Theory to illuminate the complex dynamics of cryptocurrency-enabled terrorism financing. Through SNT, it intricately maps the decentralised, anonymous networks forged by terrorist groups in Nigeria and Kenya, revealing how cryptocurrency fosters diffuse connections that challenge conventional hierarchical models of state control and interstate cooperation. This application underscores the emergent properties of these networks, enhanced autonomy and global reach, and their implications for diplomatic strategy. Concurrently, Game Theory models the strategic interactions between terrorist actors, state regulators, and international bodies as a more profound, non-zero-sum game with evolving payoff structures, offering a robust analytical framework for anticipating diplomatic outcomes. This dual-theoretical synthesis deepens the analytical toolkit of International Relations and positions the research at the forefront of security diplomacy scholarship.

Empirically, the study delivers a groundbreaking, context-specific analysis of cryptocurrency's role in terrorism financing, drawing on a dynamic array of statistical data, thematic insights from local stakeholders, and comparative case studies spanning Nigeria, Kenya, and international contexts such as Afghanistan and advanced jurisdictions. It provides original, rigorous evidence on the inefficacy of counter-terrorism financing frameworks, the

transformation of financing networks, and the interconnections between local markets and global systems, filling a critical empirical void in African security dynamics within International Relations. This multifaceted empirical contribution enhances the evidential foundation for diplomatic studies, offering nuanced insights that underscore the reputation of the research as meticulous and multifaceted.

Practically, the study advances a dynamic set of actionable insights for international implication and diplomatic practice, informing the formulation of policies, strategies, and interventions to counter cryptocurrency-enabled terrorism financing. It identifies the imperative for advanced technological tools, regulatory coherence, and interstate collaboration, meticulously tailored to local adaptations like peer-to-peer trading in Nigeria and mobile money integrations in Kenya. These findings equip diplomats, policymakers, and international organisations with a refined, multifaceted understanding of the diplomatic challenges posed by technological innovation, enabling more effective multilateral governance and security diplomacy. The emphasis on balancing enforcement with human rights considerations further reinforces the practical relevance of this work, affirming its dynamic impact on policy discourse in under-resourced contexts.

5.5 Suggestions for Further Studies

Based on the findings, the following are key implications, gaps, and directions for future research that emerge from this study:

1. **The Need for Advanced Blockchain Analytics in Regional Security Frameworks:** The study highlights the critical role of blockchain analytics in monitoring peer-to-peer trading

platforms and mobile money integrations exploited by terrorist organisations. Future research could focus on developing scalable tools and frameworks to enhance real-time monitoring capabilities within regional security alliances.

2. **Addressing Technological and Regulatory Deficits through Diplomatic Alliances:** A significant gap identified is the lack of harmonised regulatory standards and technological capacity across jurisdictions. Further investigation into the establishment of regional diplomatic technology alliances could provide insights into bridging these deficits and fostering multilateral cooperation.
3. **Predictive Modeling for Early Detection of Digital Threat Patterns:** Transforming terrorism financing networks into digital, anonymous platforms underscores the need for predictive analytics to identify emerging threats. Future studies could explore the development of advanced models to support early warning systems and strengthen interstate intelligence sharing.
4. **Understanding the Interconnections between Local Markets and Global Financial Networks:** The study reveals complex interconnections between local cryptocurrency adaptations in Nigeria and Kenya and global financial systems. Research could delve deeper into how these interconnections facilitate illicit finance and propose strategies to dismantle them while preserving legitimate economic activities.
5. **Designing Context-Specific Policy Architectures for Effective Governance:** Policy frameworks tailored to local contexts while aligning with international standards are urgently needed. Future work could examine the formulation of such architectures, balancing enforcement with human rights considerations and ensuring inclusivity in financial systems.

6. **Exploring the Concept of Digital Financial Sovereignty in Multilateral Governance:** The study introduces the novel Digital Financial Sovereignty. Further research could investigate its implications for state control, individual autonomy, and international relations, particularly in under-resourced contexts where technological innovation intersects security challenges.

Bibliography

Chapters in Books

Oladipupo, A. O. *The Role of Cryptocurrency in Geopolitical Conflicts: Cybersecurity Concerns in International Diplomacy*. *Book of Reading, Department of Politics and International Relations*, edited by Tunde Oseni, Akeem Amodu, and Olufemi Badru, Lead City University Press, 2024, 439–458.

Rawat, R., Mahor, V., Chirgaiya, A. S., & Rathore, A. S., *Applications of Social Network Analysis to Managing the Investigation of Suspicious Activities in Social Media Platforms,* In *Advances in Cybersecurity Management,* Springer International Publishing, 2021, 315–336.

Reshetnikova, N. N., Magomedov, M. M., Zmiyak, S. S., Gagarinskii, A. V., & Buklanov, D. A., *Directions of Digital Financial Technologies Development: Challenges and Threats to Global Financial Security,* In *Current Problems and Ways of Industry Development: Equipment and Technologies,* Cham: *Springer International Publishing,* 2021, 355–363.

Journals

Akartuna, E. A., Johnson, S. D., & Thompton, A., *Preventing the Money Laundering and Terrorist Financing Risks of Emerging Technologies: An International Policy Delphi Study,* **Technological Forecasting and Social Change,** 179, 2022, 121632.

Almaqableh, L., Reddy, K., Pereira, V., Ramiah, D., Wallace, D., & Veron, J. F., *An Investigative Study of Links between Terrorist Attacks and Cryptocurrency Markets,* **Journal of Business Research,** 147, 2022, 177–188.

Al-Suwaidi, N. A., & Nobanee, H., *Anti-Money Laundering and Anti-Corruption Financing: A Survey of the Existing Literature and a Future Research Agenda,* **Journal of Money Laundering Control,** 24(2), 2021, 396–426.

Al-Tawil, T. N. E., *Anti-Money Laundering Regulation of Cryptocurrency: UAE and Global Approaches,* **Journal of Money Laundering Control,** 26(6), 2023, 1150–1164.

Ariani, O., & Ibrahim, A. L., *Optimizing the Role of BNPT in Preventing Terrorism Financing Using Cryptocurrency in Indonesia,* **Jurnal Usm Law Review,** 7(1), 2023, 30–44.

Arifin, S. R. M. *Ethical Considerations in Qualitative Study.* **International Journal of Care Scholars,** 1(2), 2018, 30–33.

Balcaen, P., Bois, C. D., & Buts, C., *A Game-Theoretic Analysis of Hybrid Threats,* **Defence and Peace Economics,** 33(1), 2022, 26–41.

Bernanke, B. S., *The New Tools of Monetary Policy,* **American Economic Review,** 110(4), 2020, 943–983

Bright, D., Brewer, R., & Morselli, C., *Reprint of: Using Social Network Analysis to Study Crimes: Navigating the Challenges of Criminal Justice Records,* **Social Networks,** 69, 2022, 235–250.

Camacho, D., Panizo-Ledot, A., Bello-Orgaz, G., Gonzalez-Pardo, A., & Cambria, E., *The Four Dimensions of Social Network Analysis: An Overview of Research Methods, Applications, and Software Tools,* **Information Fusion,** 63, 2020, 88–120.

Campbell-Verduyn, M., & Giumelli, F., *Enrolling Into Exclusion: African Blockchain and Decolonial Ambitions in an Evolving Finance/Security Infrastructure,* **Journal of Cultural Economy,** 15(4), 2022, 524–543.

Dhali, M., Hassan, S., Mehar, S. M., Shahzad, K., & Zaman, F., *Cryptocurrency in the Darknet: Sustainability of the Current National Legislation,* **International Journal of Law and Management,** 65(3), 2023, 261–282.

Dyntu, V., & Dykyj, O. *Cryptocurrency as an Instrument of Terrorist Financing.* **Baltic Journal of Economic Studies,** 7(5), 2021, 67–72.

Emmanuel, O. T., & Michael, A. A., *Forensic Accounting: Breaking the Nexus between Financial Cybercrime and Terrorist Financing in Nigeria,* **Journal of Auditing, Finance, and Forensic Accounting,** 8(2), 2020, 55–66.

Fakunmoju, S. K., Banmore, O., Gbadamosi, A., & Okunbanjo, O. I., *Effect of Cryptocurrency Trading and Monetary Corrupt Practices on Nigerian Economic Performance,* **Binus Business Review,** 13(1), 2022, 31–40.

Zachariadis, M., Hileman, G., & Scott, S. V., *Governance and Control in Distributed Ledgers: Understanding the Challenges Facing Blockchain Technology in Financial Services,* **Information and Organization,** 29(2), 2019, 105–117.

Zaidi, S. M. S., *Emerging Realities in the International Political System: Transforming State's Foreign Policy,* **Herald of the Russian Academy of Sciences,** 2023, 1–14.

Ghosh, A., Gupta, S., Dua, A., & Kumar, N., *Security of Cryptocurrencies in Blockchain Technology: State-of-Art, Challenges and Future Prospects,* **Journal of Network and Computer Applications,** 163, 2020, 102635.

Gupta, S., Starr, M. K., Farahani, R. Z., & Ghodsi, M. M., *Prevention of Terrorism—An Assessment of Prior POM Work and Future Potentials,* **Production and Operations Management,** 29(7), 2020, 1789–181

Hashemi, J. M., Nishikawa, Y., & Dandapani, K., *Cryptocurrency, a Successful Application of Blockchain Technology,* **Managerial Finance,** 46(6), 2020, 715–733.

Hasibuan, H., Tijow, L., & Koos, S., *Terrorism Financing Countermeasures in an Evolving Ideological Dynamics of Global Counterterrorism,* **Lex Publica,** 10(1), 2023, 215–239.

Hayashi, P. G., Abib, G., & Hoppen, N. *Validity in Qualitative Research: A Processual Approach.* **The Qualitative Report,** 24(1), 2019, 98–112.

Ibrahim, S. A., *Decrypting the Risks of Cryptocurrency: Money Laundering, Terrorism Financing, and Proliferation Financing,* **Pakistan Horizon,** 74(1), 2021, 73–89.

Ibrahim, S. A., *Regulating Cryptocurrencies to Combat Terrorism-Financing and Money Laundering,* **Stratagem,** 2(1), 2019.

Irina, C., *Cryptocurrencies Legal Regulation,* **BRICS Law Journal,** 5(2), 2018, 128–153.

Jayasekara, S. D., *How Effective are the Current Global Standards in Combating Money Laundering and Terrorist Financing?* **Journal of Money Laundering Control,** 24(2), 2021, 257–267.

Mezmir, E. A. *Qualitative Data Analysis: An Overview of Data Reduction, Data Display, and Interpretation.* **Research on Humanities and Social Sciences,** 10(21), 2020, 15–27.

Morse, J. C., *Blacklists, Market Enforcement, and the Global Regime to Combat Terrorist Financing,* **International Organization,** 73(3), 2019, 511–545.

Moskowitz, T., *The Illicit Antiquities Trade as a Funding Source for Terrorism: Is Blockchain the Solution?* **Cardozo Arts & Ent. LJ,** 37, 2019, 193.

Nnam, M. U., Ajah, B. O., Arua, C. C., Okechukwu, G. P., & Okorie, C. O., *The War Must Be Sustained: An Integrated Theoretical Perspective of the Cyberspace-Boko Haram Terrorism Nexus in Nigeria,* **International Journal of Cyber Criminology,** 13(2), 2019.

Oladipupo, A.O and Amodu, A. A. *Impact of Cryptocurrency Ban on the Development of cryptocurrency in Nigeria,* **Renaissance University Journal of Management and Social Science**,8(2), 2022.

Oladipupo, A. O., Oyedokun, D. M., & Fasola, E. N. *Cryptocurrency Ban in Nigeria: Implications for Domestic and International Trade*. **International Journal of Research and Innovations in Social Sciences (IJRISS),** VII(1), 2023, 539–551

Oladipupo, A. O. & Amodu, A. A. *An Overview of Cryptocurrencies and the Nigeria Experience*. **Lead City Faculty of Social Science Journal,** 2023.

Olujobi, O. J., & Yebisi, E. T., *Combating the Crimes of Money Laundering and Terrorism Financing in Nigeria: A Legal Approach for Combating the Menace,* **Journal of Money Laundering Control,** 26(2), 2023, 268–289.

Pașca, V., & Orza, D. S., *Terrorism: Between the Need for Funding and Obtaining Funding Sources,* **Journal of Eastern European Criminal Law,** 1, 2019.

Patel, P. C., & Richter, J., *The Relationship between Terrorist Attacks and Cryptocurrency Returns,* **Applied Economics,** 53(8), 2021, 940–961.

Pavlidis, G., *The Dark Side of Anti-Money Laundering: Mitigating the Unintended Consequences of FATF Standards,* **Journal of Economic Criminology,** 2, 2023.

Popper, N. *Jihadists See a Funding Boon in Bitcoin.* **The Wall Street Journal,** 2018, Retrieved from https://www.wsj.com/articles/jihadists-see-a-funding-boon-in-bitcoin1519131601

Rawat, R., *Logical Concept Mappings and Social Media Analytics Relating to Cyber-Criminal Activities for Ontology Creation,* **International Journal of Information Technology,** 15(2), 2023, 893–903.

Rose, J., & Johnson, C. W. *Contextualizing Reliability and Validity in Qualitative Research: Toward More Rigorous and Trustworthy Qualitative Social Science in Leisure Research.* **Journal of Leisure Research,** 51(4), 2020, 432–451.

Sebastião, H. M. C., Cunha, P. J. O. R. D., & Godinho, P. M. C., *Cryptocurrencies and Blockchain: Overview and Future Perspectives,* **International Journal of Economics and Business Research,** 21(3), 2021, 305–342.

Shukhratovna, Y. S., To‘lqinovich, S. B., & Ibragimovna, B. L., *Monetary Policy of Uzbekistan and Its Improvement Ways in Implementing,* **The Journal of Contemporary Issues in Business and Government,** 27(1), 2021, 1551–1557.

Unal, S., & Altun, M., *The Role of Financial Intelligence in Combating the Financing of Terrorism,* **Journal of Money Laundering Control,** 24(3), 2021, 571–583.

Valvi, E. A., *The Role of Legal Professional in the European and International Legal and Regulatory Framework Against Money Laundering,* **Journal of Money Laundering Control,** 26(7), 2023, 28–52.

Wagman, S., *Cryptocurrencies and National Security: The Case of Money Laundering and Terrorism Financing,* **Harv. Nat'l Sec. J.,** 14, 2022, 87.

Wardhana, A. T., & Nugroho, B. W., *Abuse of Cryptocurrency to Funding International Terrorism Activities,* In *Proceedings* ***Universitas Muhammadiyah Yogyakarta Undergraduate Conference****,* 1(1), 2021, 353–362.

Weichbroth, P., Wereszko, K., Anacka, H., & Kowal, J., *Security of Cryptocurrencies: A View on the State-of-the-Art Research and Current Developments,* **Sensors,** 23(6), 2023, 3155.

Teichmann, F. M. J., & Falker, M. C., *Cryptocurrencies and Financial Crime: Solutions from Liechtenstein,* **Journal of Money Laundering Control,** 24(4), 2021, 775–788.

Fletcher, E., Larkin, C. J., & Corbet, S.,*Countering Money Laundering and Terrorist Financing: A Case of Cryptocurrency* **Research in International Business and Finance**, 2021,Vol.56

Magazine Articles

Chainalysis**.** *Cryptocurrency and Terrorism Financing Accuracy Check,* 2024, retrieved from https://www.chainalysis.com/blog/cryptocurrency-terrorism-financing-accuracy-check/

Constantinescu, M., *The Security Implications of Cryptocurrencies,* International Scientific Conference Strategies XXI, 2020, 179.

Newspaper

Premium Times Nigeria. *Nigerian Government Freezes $37M in Cryptocurrency Linked to Suspected Protest Organizers,* Premium Times Nigeria, 2024, Retrieved from https://www.premiumtimesng.com/news/top-news/723986-exclusive-nigerian-govt-freezes-37m-worth-of-cryptocurrency-traced-to-suspected-protest-organisers.html

Punch NG. *Terrorists Using Cryptocurrency Traders to Fund Insecurity in Nigeria—EFCC Report,* Punch NG., 2024, Retrieved from https://punchng.com/terrorists-using-cryptocurrency-traders-to-fund-insecurity-efcc/

Punch NG. *Why the US, Nigeria, and Others Are Cracking Down on Cryptocurrency "Kings",* Punch NG, 2024, Retrieved from https://punchng.com/why-us-nigeria-others-crack-down-on-crypto-currency-kings/?amp=#amp_tf=From%20%251%24s&aoh=17329557158439&referrer=https%3A%2F%2Fwww.google.com

Periodical Articles

T. Gambaryan. *Tweet on Regulatory Challenges and Binance Compliance Issues in Nigeria* [Tweet], X (formerly Twitter), 2024, Retrieved from https://x.com/TigranGambaryan/status/1890287335205384312?t=tpKO8ewb0p-seJjqHOBsLQ&s=19

A. Greenberg. *Tweet on Cryptocurrency and Global Regulatory Enforcement Trends* [Tweet], X (formerly Twitter), 2024, Retrieved from https://x.com/a_greenberg/status/1888930445766598971?t=ttoFa2zqe0gP4BRmhC4X4w&s=19

Counterterrorism, B. O., Country Reports on Terrorism. US Department of State, 2019.

Vârtei, A. M., *Financing Terrorism: Economy's Dark Side,* In *Proceedings of the International Conference on Cybersecurity and Cybercrime-2023* Asociatia Romana pentru Asigurarea Securitatii Informatiei, 2023, 216–223.

Schwarz, N., Chen, M. K., Poh, M. G., Jackson, K., Kao, M. F., Fernando, M., & Markevych, M., *Virtual Assets and Anti-Money Laundering and Combating the Financing of Terrorism (1): Some Legal and Practical Considerations,* International Monetary Fund, 2021.

Textbooks

Amini, M., Ouassini, A., & Ouassini, N., *Cyber Dimensions of Terrorism Funding,* In *Countering Terrorist and Criminal Financing,* CRC Press, 2023, 197–206.

Andrianova, A., *Countering the Financing of Terrorism in the Conditions of Digital Economy,* In *Digital Transformation of the Economy: Challenges, Trends and New Opportunities, Springer International Publishing,* 2020, 20–31.

Costantino, F., *The FATF Recommendations and the Development of International Standards on Terrorist Financing,* In *Countering Terrorist and Criminal Financing,* CRC Press, 2024, 31–42.

Crawford, T. H., *Actor-Network Theory,* In *Oxford Research Encyclopedia of Literature,* 2020.

Eisermann, D., *Cryptocurrencies as Threats to Public Security and Counter Terrorism: Risk Analysis and Regulatory Challenges,* Berlin Risk, 2020.

Keatinge, T., Carisle, D., & Keen, F. *Virtual Currencies and Terrorist Financing: Assessing the Risks and Evaluating Responses.* Brussels: European Parliament, Directorate General for International Policies. Policy Department for Citizens' Rights and Constitutional Affairs. Counter Terrorism**,** 2018.

Ma, W., *Terrorist Financing, War Crimes, and Crypto Geopolitics,* In *A Comprehensive Guide for Web3 Security: From Technology, Economic and Legal Aspects,* Springer International Publishing, 2023, 241–259.

Majumder, A., Routh, M., & Singha, D., *A Conceptual Study on the Emergence of Cryptocurrency Economy and its Nexus with Terrorism Financing, In* the *Impact of Global Terrorism on Economic and Political Development: Afro-Asian Perspectives,* Emerald Publishing Limited, 2019, 125–138.

Maschler, M., Zamir, S., & Solan, E., *Game Theory,* Cambridge University Press, 2020.

Packin, N. G., & Volovelsky, U., *Digital Assets, Anti-Money Laundering and Counter Financing of Terrorism: An Analysis of Evolving Regulations and Enforcement in*

the Era of NFTs, In The Cambridge Handbook on Law and Policy for NFTs (Nizan Geslevich Packin, ed.), Forthcoming, 2023.

Warreth, S. A., *Comparing Far Right and Jihadi Use of Crowdfunding, Cryptocurrencies, and Blockchain Technology: Accessibility, Geography, Ideology,* 2020.

Wilson, C., *International Institutions: An Underutilized Tool for Combating the Financing of Terrorism,* 2022.

Sandholm, W. H., *Evolutionary Game Theory,* In *Complex Social and Behavioral Systems: Game Theory and Agent-Based Model,* 2020.

Thesis

Ariwoola, A., *The State Adoption of Cryptocurrencies in Nigeria: The Place of Taxation as a Regulatory Instrument,* Available at SSRN 4532562, 2023.

Botha, R., *The Potential Anti-Money Laundering and Counter-Terrorism Financing Risks and Implications of Virtual Currencies on the Prevailing South African Regulatory and Supervisory Regime* (Master's thesis, University of Pretoria), 2019.

Carsello, A. L., *Combatting Crypto Crimes: An Examination of the Existing Regulations Surrounding Cryptocurrency* (Doctoral dissertation, Utica College), 2021

Dowling, B. *Provable security of internet protocols* (Doctoral dissertation, Queensland University of Technology). Queensland University of Technology ePrints, 2017.

Eaddy, A., *Innovation in Terrorist Financing: Interrogating Varying Levels of Cryptocurrency Adoption in al-Qaeda, Hezbollah, and the Islamic State* (Doctoral dissertation), 2019.

Ediagbonya, V., & Tioluwani, T. C., *The Growth and Regulatory Challenges of Cryptocurrency Transactions in Nigeria, In* t*he Complexities of Sustainability,* 2023, 267–297.

Haichao, W., *Exploring the Regulations of Cryptocurrencies in China, Global Regulations Based on Cryptocurrency Decentralization* (Doctoral dissertation, SIAM University), 2023.

Opebiyi, F. M., *Regulating User Interactions Within the Financial Technology Market: Cryptocurrencies in Nigeria* (Doctoral dissertation, University of Manchester), 2022.

Websites

Wired. *The Untold Story of Crypto Crimefighters' Descent into Nigerian Prison,* 2024, retrieved from https://www.wired.com/story/untold-story-crypto-crimefighters-descent-nigerian-prison-binance/

Arise TV**.** *Police Interrogate CEO of Blord Group of Companies for Terrorism Funding and Cryptocurrency Fraud,* 2024, retrieved from https://www.arise.tv/police-interrogate-ceo-blord-group-of-companies-for-terrorism-funding-cryptocurrency-fraud/

DL News**.** *Nigeria Probes Binance over Terror Funds and Money Laundering Allegations,* DL News, 2024, retrieved from https://www.dlnews.com/articles/markets/nigeria-probes-binance-on-terror-funds-and-money-laundering/

CBN, *Guidelines and Operations of Bank Accounts for Virtual Assets Service Providers (VASPs),* Retrieved from https://www.cbn.gov.ng/Out/2024/FPRD/GUIDELINES%20ON%20OPERATIONS%20OF%20BANK%20ACCOUNTS%20FOR%20VIRTUAL%20Asset%20Providers.pdf , 2023

Crypto Times. *AD Forensics Trains Crypto Crime Fighters in Nigeria,* Crypto Times, 2024, retrieved from https://www.cryptotimes.io/2024/02/18/ad-forensics-trains-crypto-crime-fighters-in-nigeria/

Cuthbertson, A., & Sigalos, A. *Bitcoin Adoption in Afghanistan Spikes Amid Taliban Takeover,* 2021, Retrieved from https://www.independent.co.uk/life-style/gadgets-and-tech/bitcoin-afghanistancrypto-taliban-economy-b1907180.html

Nairametrics**.** *Court Freezes N548.6 Million in Bybit and KuCoin Accounts over Naira Fluctuation Allegations,* Nairametrics, 2024, retrieved from https://nairametrics.com/2024/09/11/court-freezes-n548-6-million-belonging-to-bybit-kucoin-nigerian-crypto-users-over-naira-fluctuation-allegations/

New Lines Magazine**.** *The Rise and Fall of Cryptocurrency in Nigeria,* New Lines Magazine, 2024, retrieved from https://newlinesmag.com/reportage/the-rise-and-fall-of-cryptocurrency-in-nigeria/

The Africa Report**.** *Nigeria's Crypto Comeback: SEC Approves Local Exchanges Post-Binance Ban,* The Africa Report, 2024, retrieved from https://www.theafricareport.com/360383/nigerias-crypto-comeback-sec-approves-local-exchanges-post-binance-ban/

U.S Department of Justice. *Global Disruption of Three Terror Finance Cyber-Enabled Campaigns.* Washington: U.S. Department of Justice, Office of Public Affairs**,** 2024, Retrieved from https://www.justice.gov/opa/pr/global-disruption-three-terror-finance-cyberenabled-campaigns

Tarrant-Cornish, T. *'Terrorist Dream Come True': ISIS Using Bitcoin to Fund Deadly Attacks and Buy Weapons.* **Express,** 2018, Retrieved from

https://www.express.co.uk/finance/city/902517/ISIS-Bitcoin-terrorist-attackdeadly-weapons-funding-cryptocurrency-money-laundering

UN, *Advancing Rule of Law, Justice for All Through Technology Must Include Equal Internet Access, Human Rights Compliance, Sixth Committee Speakers Stress,* Retrieved from https://press.un.org/en/2023/gal3694.doc.htm , 2023.

Questionnaire

Demographic Data

1. Gender: ( ) Male ( ) Female ( ) Non-binary/Other
2. Age: ( ) Under 18 ( ) 18-24 ( ) 25-34 ( ) 35-44 ( ) 45-54 ( ) 55-64 ( ) 65 and over
3. Education Level: ( ) Primary ( ) Secondary ( ) Some College/Associate Degree ( ) Bachelor's Degree ( ) Master's Degree ( ) Doctoral Degree
4. Employment Status: ( ) Employed full-time ( ) Employed part-time ( ) Self-employed ( )
5. Ethnicity/Race: ( ) Yoruba ( ) Hausa/ Fulani ( ) Igbo
6. Marital Status: ( ) Single ( ) Married ( ) Divorced ( ) Widowed
7. Location: ( ) Urban ( ) Suburban ( ) Rural
8. Religion: ( ) Christianity ( ) Islam ( ) Other
9. Place of Work: _____ (Fill in)
10. Position: _____ (Fill in)

Section B

S/N	Items	Yes	No
A	**Identify the specific methods and strategies employed by terrorist organizations to utilize cryptocurrency for financing their activities.**		
1	Do terrorist organizations typically acquire cryptocurrency funds?		
2	Do terrorist groups convert cryptocurrency into usable assets or funds?		
3	Do terrorist organizations commonly use specific platforms or channels to transact with cryptocurrency?		
4	Do terrorist organizations conceal their cryptocurrency transactions to avoid detection?		
5	Do cryptocurrency exchanges play any role in facilitating terrorist financing?		
6	Do terrorist groups utilize privacy-focused cryptocurrencies or mixing services to obscure their financial activities?		
7	Are there specific regions or jurisdictions where terrorist organizations		

	are more active in utilizing cryptocurrency?		
8	Do terrorist organizations employ tactics to launder cryptocurrency funds?		
9	Do terrorist organizations exploit decentralized finance (DeFi) platforms for fundraising or money laundering?		
10	Have terrorist groups adopted technological innovations to enhance their use of cryptocurrency?		
B	**Evaluate the effectiveness of existing international regulatory frameworks and law enforcement efforts in countering cryptocurrency-based terrorism financing.**		
11	Do current regulatory frameworks address cryptocurrency-related terrorism financing?		
12	Do law enforcement agencies face challenges in investigating and prosecuting cryptocurrency-based terrorism financing?		
13	Are there international collaborations or information-sharing mechanisms in place to combat cryptocurrency-related terrorism financing?		
14	Do law enforcement agencies utilize tools or technologies to trace and track cryptocurrency transactions linked to terrorism financing?		
15	Do regulatory authorities monitor cryptocurrency exchanges and other platforms for compliance with anti-money laundering (AML) and counter-terrorism financing (CTF) regulations?		
16	Have there been notable successes in disrupting terrorist financing activities through cryptocurrency-related investigations?		
17	Do gaps exist in current regulatory frameworks or enforcement strategies regarding cryptocurrency-based terrorism financing?		
18	Do legal challenges, such as jurisdictional issues, impact the effectiveness of international efforts to counter cryptocurrency-related terrorism financing?		
19	What role do financial intelligence units (FIUs) play in detecting and preventing cryptocurrency-based terrorism financing?		
20	Are there lessons to be learned from successful cases of prosecuting cryptocurrency-related terrorism financing?		
C	**Analyze the impact of cryptocurrency on the dynamics of international terrorism, including its potential to facilitate cross-border activities and radicalization.**		

21	Has the adoption of cryptocurrency changed the funding sources and financial networks of terrorist organizations?		
22	Does cryptocurrency facilitate cross-border financial transactions for terrorist groups?		
23	Have terrorist organizations leveraged cryptocurrency for propaganda or recruitment purposes?		
24	Does cryptocurrency play a role in financing lone-wolf terrorist attacks or small-scale operations?		
25	Do extremist groups exploit social media and online platforms to solicit cryptocurrency donations?		
26	Do the pseudonymous nature of cryptocurrency transactions impact efforts to identify and track terrorist financing?		
27	Does the global nature of cryptocurrency exchanges impact counter-terrorism efforts?		
28	Have instances occurred where cryptocurrency has been used to fund international terrorist activities?		
29	Does the decentralized nature of cryptocurrency networks affect the ability to disrupt terrorist financing?		
30	Do terrorist organizations employ strategies to leverage cryptocurrency for ideological or operational goals?		
D	**Assess the Impact of Cryptocurrency Usage on the Global Security Landscape**		
31	Has the widespread adoption of cryptocurrency influenced traditional financial systems and security paradigms?		
32	Does the integration of cryptocurrency pose vulnerabilities to global security infrastructure?		
33	Do state actors navigate the security implications of cryptocurrency adoption?		
34	Does cryptocurrency play a role in cyber warfare and state-sponsored terrorism?		
35	Do security agencies monitor and respond to threats associated with cryptocurrency usage?		
36	Are there emerging security risks or threats unique to cryptocurrency ecosystems?		

37	Does the anonymity of cryptocurrency transactions impact national security efforts?		
38	Can strategies be implemented to mitigate the security risks posed by cryptocurrency usage?		
39	Does the proliferation of cryptocurrencies affect traditional methods of economic sanctions and financial controls?		
40	Are there opportunities for collaboration between the cryptocurrency industry and security stakeholders to enhance global security measures?		
E	**Develop comprehensive recommendations for policymakers and international organizations to strengthen global counter-terrorism efforts in the face of cryptocurrency challenges.**		
41	Can policymakers enhance regulatory frameworks to address cryptocurrency-related terrorism financing?		
42	Should international organizations implement measures to improve coordination and information-sharing regarding cryptocurrency threats?		
43	Can law enforcement agencies enhance their capabilities to investigate and disrupt cryptocurrency-based terrorism financing?		
44	Should technology companies play a role in combating cryptocurrency-enabled terrorism activities?		
45	Can public awareness and education campaigns mitigate the risks of cryptocurrency-enabled terrorism?		
46	Should standardized guidelines or protocols be established for cryptocurrency exchanges and platforms to combat terrorism financing?		
47	Can strategies be employed to enhance international cooperation in combating cryptocurrency-enabled terrorism?		
48	Can financial institutions strengthen their AML and CTF measures to detect and prevent cryptocurrency-related terrorism financing?		
49	Should specialized task forces or units be dedicated to addressing cryptocurrency-enabled terrorism within law enforcement agencies?		

Interview Questions

1. Identify the specific methods and strategies employed by terrorist organizations to utilize cryptocurrency for financing their activities:

a. **For Security Exchange Commission:** How do you monitor and detect suspicious cryptocurrency transactions potentially linked to terrorist organizations?

b. **For Financial Crime Commission:** What are the most common cryptocurrency-related tactics used by terrorist groups to finance their activities, and how do you combat them?

c. **For Security Advisers Officers:** Have you observed any trends or patterns in how terrorist organizations in our region utilize cryptocurrency for funding, and if so, how do you address them?

2. Evaluate the effectiveness of existing international regulatory frameworks and law enforcement efforts in countering cryptocurrency-based terrorism financing:

a. **For Security Exchange Commission:** Do you believe current international regulatory frameworks adequately address the challenges posed by cryptocurrency-based terrorism financing?

b. **For Economic and Financial Crime Commission:** How do you collaborate with international law enforcement agencies to combat cryptocurrency-based terrorism financing, and what improvements can be made?

c. **For National Security Advisers Office:** In your opinion, what are the key limitations or gaps in existing international efforts to counter cryptocurrency-based terrorism financing, and how can they be addressed?

3. Analyze the impact of cryptocurrency on the dynamics of international terrorism, including its potential to facilitate cross-border activities and radicalization:

a. **For Registered Crypto Trading Firms:** Have you noticed any instances where cryptocurrency transactions have been linked to cross-border terrorist financing, and how do you prevent such activities within your firm?

b. **For the Academia and experts in terrorist financing:** How does the adoption of cryptocurrency impact the radicalization process of individuals towards terrorism, and what preventative measures can be taken?

4. Assess the Impact of Cryptocurrency Usage on the Global Security Landscape:

a. **For Exchange Commission:** How does the integration of cryptocurrency affect traditional security measures, and what strategies are being considered to adapt to this evolving landscape?

b. **For Financial Crime Commission:** What are the key security risks posed by the widespread usage of cryptocurrency, and how do you prioritize addressing them?

c. **For National Security Advisers Office:** How does the proliferation of cryptocurrency impact our national security strategy, and what measures are in place to mitigate associated risks?

5. Develop comprehensive recommendations for policymakers and international organizations to strengthen global counter-terrorism efforts in the face of cryptocurrency challenges:

a. **For Registered Crypto Trading Firms:** How can cryptocurrency firms contribute to global counter-terrorism efforts, and what measures should be implemented internally?
b. **For Academia and experts in terrorist financing:** Based on your expertise, what strategies or initiatives should policymakers and international organizations prioritize to address the intersection of cryptocurrency and terrorism financing?

Bio-data

A. Personal Data

Full Name:	Abdul Malik Olalekan OLADIPUPO
Address:	No 191, Farinu Olore, Oroki, Oyo.
Email:	oladipupo.abdulmalik@lcu.edu.ng
Phone No:	08124996256
Date of birth:	20 June 1998
Place of Birth:	Oyo East, Oyo State
Nationality:	Nigerian
Marital Status:	Single
Next of Kin:	Mrs. Oladipupo Folake Misirat
	No 191, Farinu Olore, Oroki, Oyo

B. Educational Background

Educational Institutions Attended and Qualifications

- Ph.D. in International Politics and Diplomacy – Lead University, Ibadan (In View)
- M.Sc. In International Politics and Diplomacy 2022
- B.Sc. (Hons) International Relations – Lead University, Ibadan 2019

- S.S.C.E - Olivet Baptist High School, Oyo. 2015

C. Work Experience

- O.A.P on an online TV Station (OPATOLA TV)
- A Founding Member of Social Development and Accountability Project (SDAP)
- A Year I.T Experience in Osun State Governor Office. 2020
- A Columnist on Giant Blog. 2020
- A Columnist on Opera News. 2020
- A Columnist on 24/7 Blog. 2020
- Weekly Columnist on Spygist Blog 2022
- K.Y Pure Water Factory, Oroki, Oyo. 2014
- A Columnist on Marioreporta.com 2018
- Freelancer on Spygist Blog 2022
- Administrative Officer II, Lead City University, 2020-2023.
- Assistant Lecturer, Department of Politics and International Relations, Lead City University, 2023-date.

D. Membership of Academic and Professional Bodies

- Member, Nigeria United Model Union Society
- Member, New Horizon Certificate on Internet and Computer Core Certificate
- Member, New Horizon Certificate on Customer Relationship Management

- Associate Member IPD-CRM, Institute of Personality Development and Customer Relationship Management

E. Publications

Published Referred Conference Proceedings

- **Oladipupo, A.O and** Amodu, A.A**. (2023)** An Overview of Crypto currencies and the Nigeria experience. *Lead City Faculty of Social Science Annual Confrernce,* March 28, 2023.

- **Oladipupo, A.O (2024)** Blockchain Technology Experience and Public Administration in Nigeria, NPSA Southwest Conference, *Lead City University, Ibadan*, Oyo, March 26th-29th ,2024.

- **Oladipupo A. O (2024)**, Boko Haram Terrorism and the plight of the IDPs, Society for Peace and Studies Practice, University of Ibadan, Oyo State, *Nigeria Defense Academy(N.D.A.),* Kaduna, July 1-5,2025

- **Oladipupo A. O (2025),** Cryptocurrency, Governance and Gender Equality, 2nd Federal University of Wukari Faculty of Social Science Conference, Taraba State. May 4th –May 7th 2025.

- **Oladipupo A. O (2025),** Rethinking Sovereignty in the Age of Cryptocurrency: Post-Structuralist Intersection between Digital Currencies and State Power*, Multimedia University, Nairobi, Kenya.* June 25th -27th 2025.

- **Oladipupo A. O (2025) and** Amodu A.A **,** Comparative Analysis of Crytocurrency and Terrorism Financing in Nigeria and Kenya*,, Multimedia University, Nairobi, Kenya*. June 25th -27th 2025.

- **Oladipupo A. O (2025)** Cryttocureency aand Terroism Finaancing in Sub-Sharn Africa: A Compaarative Analyssis of Method and Strategies in Nigeria aand Kenya**,**Federa**l**

University of Technology Owerri (FUTO), Centre for Trans-Sahara Studies **,** 29th -31st October 2025.

Papers Accepted for Publications

- **Oladipupo, A.O and** Amodu, A.A (2**022).** Impact of Crypto currency Ban on the Development of crypto currency in Nigeria, *Renaissance University Journal of Management and Social Sciences,* 8(2)

- **Oladipupo A.O and** Oyedokun D.M **(2023).** Crypto currency Ban in Nigeria: implications for Domestic and International Trade, *International Journal of Research and innovation in Social Science (IJRISS),* 7(1)

- Martin, A.O, Oyedokun D.M **and Oladipupo A.O. (2023)** Sustainable Development and Governance for Sustainability in a Pluralistic and Interdependent World, *Abraka Humanities Review*, 12(1)

- **Oladipupo, A.O ,(2024)** The Role of Digital Leadership in the adoption and Implementation of Cryptocurrency, *Journal of Advanced research and Multidisciplinary Studies (JARMS),*4(4), 55-70.

- **Oladipupo, A.O (2024)** Cryptocurrency and Metaphysics: The Religion Perspectives, *African Journal of Culture, History, Religion and Tradition,* 7(3), 37-56.

- **Oladipupo, A.O, (2024)** Blockchain Technology Experience and Public Administration in Nigeria, *Africa Journal of Law, Political Research and Administration.* 7(3), 69-79.

- **Oladipupo, A.O, (2024),** Cryptocurrency, International Aid and Development: Opportunities and Challenges, African *Journal of Economics and Sustainable Development (AJESD),* 7(4), 268-278.

- **Oladipupo, A.O, (2024),** Addressing Gender Stereotyping in the Emergent World of Blockchain and *Cryptocurrency Administration, Journal of Advanced Research and Multidisciplinary Studies (JARMS),*4(4), 108-118

- **Oladipupo, A.O, (2024),** Crypto-enabled Espionage: A Growing threat to National Security,*African Journal of Social Sciences and Humanities Research (AJSSHR),* 7(4), 235-247

- **Oladipupo, A.O, (2024),** Cryptocurrency and Political Campaign Finance: Opportunities and Risks, *British Journal of Mass Communication and Media Research* (BJMCMR), 4(4) 1-12.

- **Oladipupo, A.O, (2024),** Reimaigining Political Reforms in the Lens of Technology: Unveiling the Democratizing Impact of Cryptocurrency, *African Journal of International Affairs and Development(AJIAD)* **-** In Press

- **Oladipupo A.O, &** Oladeji Taiwo Nurudeen (**2025)**, Crytocurrency and Global Finance: Intersections between International Security, Terrorist Financing and Financial Development, *Internatinal Journal of Cryptocurrency Research,* 5(10) 102-121.

- Oladeji Taiwo Nurudeen **& Oladipupo A.O (2025),** Terrorism Financing and Cryptocurrency: Implications for Financial Accountability, Security and Sustainable Economic Practices, *Internatinal Journal of Cryptocurrency Research* **- In Press**

- **Oladipupo, A.O, (2025),** Sanction Evasion 2.0**:** Unpacking the Role of Cryptocurrency in North Korea and Iran External Trade Relations, *Lead City Journal for Social Science (LCJSS),* Vol. 10(1) 14-25.

- **Oladipupo, A.O, (2025),** Deconstructing the Geopolitics of Cryptocurrency: Analyzing Bitcoin Impact on Economic Power Dynamics**,** *Kashere Journal for Politics and International Relations (KJPIR),* Federal University of Kashere, Gombe State**,** 3(3), 192-202.

- **Oladipupo, A.O, (2025),** Political Economy of Cryptocurrency Mining: China's Dominance Amd Implications for Global Governance, *BU-Journal of History amd International relations*, 7(1).11-23.

- **Oladipupo, A.O and** Amodu, A.A (2**025),** Comparative Analysis of Crytocurrency and Terrosim Financing in Nigeria and Kenya, *Police Academy International Journal of Economics and Management,* 12(1), 105-119.

- **Oladipupo, A.O,** Rethinking Sovereinty in the Age of Cryptocurrency: A Post Structuralist Intersection between Digital Currencies and State Power**,** *Nigeria Defence Academy Journal of Military Science and Interdisciplinary Studies,* 3(1*)* 26-37.

- **Oladipupo A. O (2025),** Terrorism Financing and Cryptocurrency: Nexus between Security, Development and Justice*, Educational Technology Quarterly*- In Press.

- **Oladipupo, A.O and** Amodu, A.A (2**025),** Cryptocurrency and Terroism in Africa: Lesson from Nigeria Regulatory Experience, *Nigeria Defence Academy Journal of Military Science and Interdisciplinary Studies*- In Press.

- **Oladipupo, A.O** and Obadimu Adekunle. M (2**025),** Crypto-Payment for Content and the Future of Broadcasting Monetization, *GVU Journal of Communication Studies*, 9(1), 211-223

- **Oladipupo, A.O,(2025),** Cryptocurrency , Terrorism Financing and the Dark web: An Exploratory study of Anonymous Transactions in Supporting Terrorist Activities, *ABUAD African Journal of Sustainable Development,*17(2)- **In Press**

- **Oladipupo, A.O,(2025),** The Darkweb of Cryptocurrency: Nexus between Digital Currencies, Cybercrime and Global Governance**,** *ABUAD Journal of Contemporary International Relations and Diplomacy***, 6 (2) ,24-39**

- **Oladipupo A.O (2025),** The Future of Cryptocurrency in International Relations: A Delphi Study of Expert Perceptions, Predictions, and Implications for Global Governance, *Routledege Open Research*- In Press.

Book Contribution

- **Oladipupo, A.O, (2025),** Cryptocurrency and Cross-Border Financial Crime: Strethening Global Regulatory Framework through International Cooperation and Information Sharing Networks, Book of Readings. In K.A Adeyemo,O. Campbell & O.Adepoju (Eds.),*A Book of Readings on Two Decades of Lead City University, Ibadan, Management and Social Science Perspectives to Contemporary Issues in Nigeria*, **Lead City University Press**, 203-215

- **Oladipupo, A.O, (2025)** The Role of Crypto currency in Geopolitical Conflicts: Cyber security Concerns in International Diplomacy. In T.Oseni A.Amodu & R. Badru (Eds.), *Politics and International Relations: A Book of Readings***, Lead City University Press,** 439-458

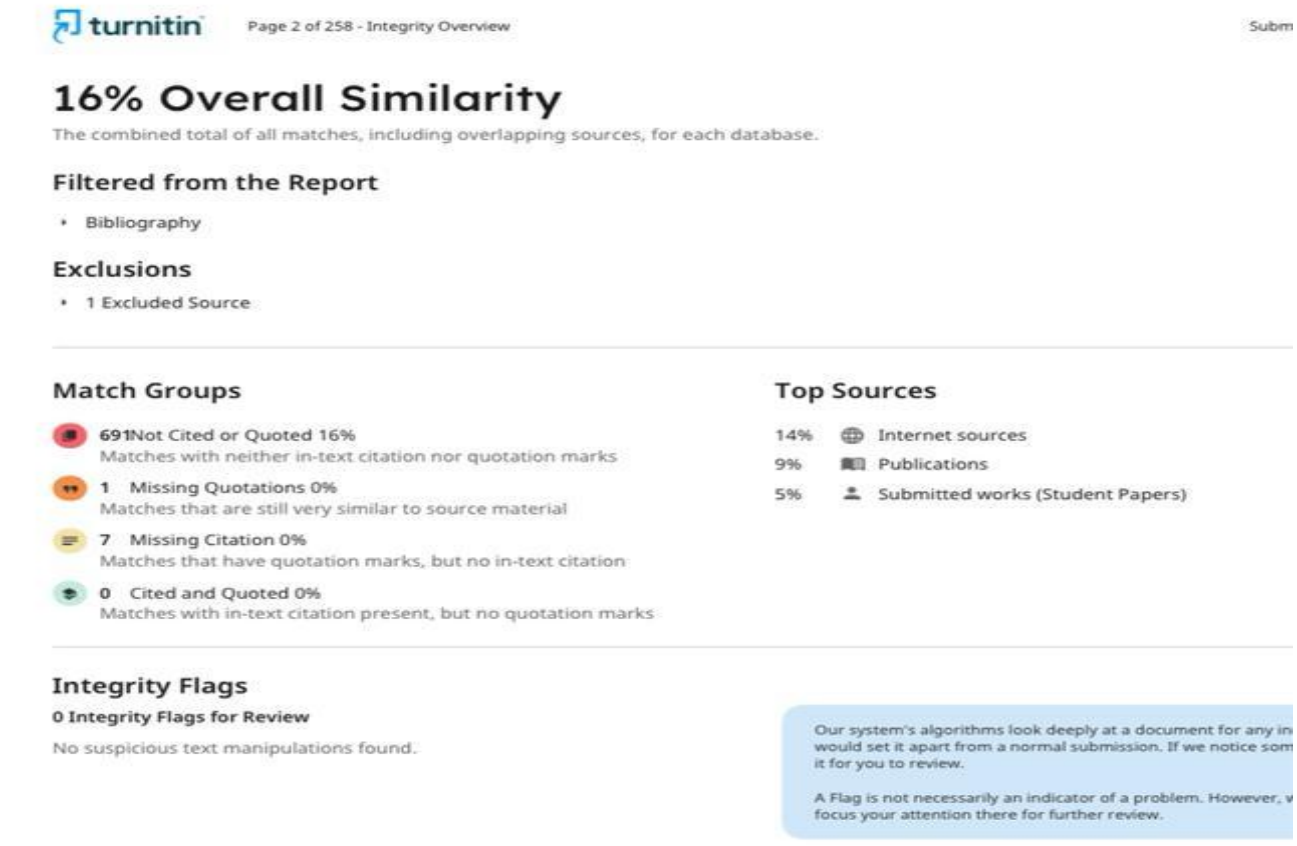
- **Oladipupo A.O, (2025),** Gender, Cryptocurrency and Gender Equality, In J.U Agbo, G.E Odok, S.A Aladejare, E.O Ameh, L.Aghwadu & N.C Joseph (Eds), *Institiutions, Governance and Social Change in Africa,* **Vast Publishers**, Ibadan. 352-360.

Signature **Data**

The University Compliance Certification

This is to certify that Abdulmalik Olalekan, OLADIPUPO with Matriculation No LCU/PG/002087 in the Politics and International Relations, Faculty of Management and Social Sciences, Lead City University, Ibadan carried out the thesis; Oyo State is in full compliance with the approved University Format and Style.

Signature **Date**



turnitin Page 2 of 258 - Integrity Overview Subm

16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Filtered from the Report

- Bibliography

Exclusions

- 1 Excluded Source

Match Groups

691 Not Cited or Quoted 16%
Matches with neither in-text citation nor quotation marks

1 Missing Quotations 0%
Matches that are still very similar to source material

7 Missing Citation 0%
Matches that have quotation marks, but no in-text citation

0 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

14% Internet sources
9% Publications
5% Submitted works (Student Papers)

Integrity Flags

0 Integrity Flags for Review

No suspicious text manipulations found.

Our system's algorithms look deeply at a document for any in
would set it apart from a normal submission. If we notice som
it for you to review.

A Flag is not necessarily an indicator of a problem. However, v
focus your attention there for further review.