THE ROLE OF FORENSIC AUDITING IN DETECTING CRYPTOCURRENCY FRAUD AND MONEY LAUNDERING

Josiah Aiyevbosa IBUDE
MGS2104562

DEPARTMENT OF ACCOUNTING
FACULTY OF MANAGEMENT SCIENCES
UNIVERSITY OF BENIN
BENIN CITY

NOVEMBER 2025

THE ROLE OF FORENSIC AUDITING IN DETECTING CRYPTOCURRENCY FRAUD AND MONEY LAUNDERING

Josiah Aiyevbosa IBUDE
MGS2104562

BEING A PROJECT WORK SUBMITTED TO THE DEPARTMENT OF ACCOUNTING, FACULTY OF MANAGEMENT SCIENCES, UNIVERSITY OF BENIN ,BENIN CITY. IN PARTIAL FULFILLMENT OF THE REQUIREMENTS FOR THE AWARD OF THE BACHELOR OF SCIENCE (B.SC) DEGREE IN ACCOUNTING

NOVEMBER 2025

DECLARATION

I, **Josiah Aiyevbosa IBUDE** declare that,

This study is based on a study undertaken by me in the Department of Accounting, Faculty of Management Sciences, University of Benin, Benin City, under the supervision of **DR. (MRS.) B. A. AKADAKPO** of the Department of Accounting, Management Sciences, University of Benin, Benin City, Nigeria.

This work has not been submitted for the award of degree elsewhere.

Ideas and views are product of my personal research and where the view of others has been expressed, they have been duly acknowledged.

Any liability arising from this work is to be wholly borne by me alone

IBUDE JOSIAH AIYEVBOSA **DATE**

MGS2104562

CERTIFICATION

We, certify that this research project was carried out by **Josiah Aiyevbosa IBUDE** in the Department of Accounting, Faculty of Management Sciences, University of Benin, Benin City, Nigeria. It is adequate in scope and quality in partial fulfilment of the requirements for the award of Bachelor of Science (BSc.) degree in Accounting.

DR. (MRS.) B. A. AKADAKPO **(PROJECT SUPERVISOR)**	**DATE**
DR. IKHU-OMOREGBE GODSTIME **(PROJECT COORDINATOR)**	**DATE**
DR. OSASU OBARETIN **(HEAD OF DEPARTMENT)**	**DATE**

DEDICATION

This project work is dedicated to God Almighty for His abundant grace in my life and for seeing me through my academic pursuit and aspirations. He has been my source of strength and on his wings only I have soared.

ACKNOWLEDGEMENTS

I am profoundly grateful to God Almighty for His immeasurable grace, divine guidance, unwavering strength, and the intellectual capacity bestowed upon me throughout this academic endeavour. His faithfulness was the cornerstone of this project's successful completion, and to Him alone be all the glory.

I would like to acknowledge the valuable support and guidance provided by my Project Supervisor Dr. (Mrs.) B.A. Akadakpo throughout the course of this project. His expertise and insights were crucial in shaping the direction and outcome of this work.

I would like to extend my sincere gratitude to Prof. O. Obaretin, my esteemed Head of Department for his support, and to my project coordinator for Dr. G. O. Ikhu-Omoregbe, for his assistance, Dr. Samokuns and all the lecturers in the Department of Accounting.

I would also like to express my gratitude to my parents Mr and Mrs Ibude whose input and collaboration enhanced the quality of this project. Additionally, I extend my thanks to my siblings and relatives Ibude Raynar, Ibude Etinosa, Ibude Esohe, Omoruyi Glory, for their unwavering encouragement during this endeavour.

Also, I want to specially appreciate my friends Elaiho Osaivbie Grace, Solomon Osamudiamen Joseph, Skinn Olagbara-Ete-Jnr Kenneth, Okosun Osebhahiemhen Moses, Idonije Ohiorenuwan Samuel, Iden Isibhakhobhen Favour, Emwanta Lomax Oghosa, Enamino James, Edosa Emmanuel Osatohamwen, Chiwuzo Ifechukwude Victor, Airen-Ogieva Justice Osamuyimen, Agbale John Efua, Elohor Emmanuel Esosa, Ofili Ebuka David, Otikpo Stephen Oghenemaro, Emmanuel Boku, for their support and Academic contribution all throughout my stay in the University.

Last but not the least, I want to thank me, I want to thank me for believing in me ,I want to thank me for doing all the hard work, I want to thank me for having no days off, I want to thank me for never quitting, I want to thank me for always being a giver and trying to give more than I receive, I want to thank me for trying to do more right than wrong, I want to thank me for just being me at all times.

TABLE OF CONTENTS

LIST OF TABLES

ABSTRACT

This study examined the impact of forensic auditing on the detection and prevention of cryptocurrency-related fraud in Nigeria, with a focus on organizational practices and audit effectiveness. The primary objective was to determine the extent to which forensic auditing techniques enhance the identification and mitigation of fraudulent activities involving digital currencies. A survey research design was adopted, and data were collected using structured questionnaires administered to auditors, accountants, and financial analysts in selected firms. The responses obtained were analyzed using descriptive statistics, mean scoring, and regression analysis to evaluate the relationship between forensic auditing and cryptocurrency fraud detection.

The findings revealed that forensic auditing significantly improves the detection of cryptocurrency fraud by enhancing transaction tracing, digital evidence analysis, and fraud risk assessment. However, the study also identified challenges, including insufficient technical expertise and inadequate regulatory frameworks, which limit the full effectiveness of forensic audit practices in this domain.

Based on these findings, the study recommends that organizations and regulatory bodies invest in continuous training and capacity-building programs for forensic auditors to equip them with advanced digital investigative skills. Strengthening professional competence will enhance fraud detection efficiency and promote transparency in cryptocurrency transactions.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

The rapid growth of cryptocurrency as a digital asset and medium of exchange has transformed the global financial landscape. Cryptocurrencies such as Bitcoin, Ethereum, and stablecoins have enabled fast, decentralized, and borderless transactions, creating new opportunities for investment and commercial activities (FATF, 2022). However, their pseudo-anonymous nature and lack of centralized regulation have also made them vulnerable to illicit activities, including fraud, money laundering, and terrorist financing (Foley et al., 2019). As criminal networks increasingly exploit blockchain technology to launder illicit funds and obscure the sources of illegal transactions, regulatory bodies and organizations face significant challenges in tracing, investigating, and prosecuting financial crimes (Houben & Snyers, 2020). Traditional auditing techniques have proven insufficient in detecting these crimes due to the complexity, encryption, and cross-border nature of blockchain transactions.

Forensic auditing, which combines accounting, investigative, and digital forensic techniques, has emerged as a critical tool for identifying and addressing cryptocurrency-related fraud and money laundering (Bhasin, 2016). By leveraging blockchain analytics, transaction tracing, and advanced digital forensics, forensic auditors can bridge the gap

between regulators and decentralized financial systems, thereby enhancing transparency and accountability in the crypto ecosystem.

In Nigeria, the Economic and Financial Crimes Commission (EFCC) has increasingly confronted cryptocurrency-related cases, particularly in relation to online fraud and cross-border money laundering. Despite the adoption of some blockchain analytic tools, investigations remain constrained by limited technical expertise, inadequate forensic infrastructure, and regulatory loopholes (Eze & Nwankwo, 2022). Consequently, the role of forensic auditing in combating financial crimes within the Nigerian cryptocurrency ecosystem demands closer academic and practical examination. This study therefore investigates the role of forensic auditing in detecting cryptocurrency fraud and money laundering, with emphasis on its effectiveness, challenges, and implications for financial security in Nigeria.

1.2 Statement of the Research Problem

The emergence of cryptocurrency as a disruptive innovation in the financial sector has introduced unprecedented opportunities for efficiency, decentralization, and borderless transactions (FATF, 2022; Foley, Karlsen, & Putniņš, 2019). However, its pseudo-anonymous nature and absence of centralized regulation have created fertile ground for illicit financial activities such as fraud, ransomware payments, and money laundering (Kethineni & Cao, 2020; Möser, Böhme, & Breuker, 2013). Reports from blockchain analytics firms reveal that billions of dollars' worth of cryptocurrencies are laundered

annually through decentralized exchanges, mixers, and privacy-enhancing tools, making detection increasingly complex (Chainalysis, 2023; Europol, 2022).

Although blockchain transactions are permanently recorded on public ledgers, their cryptographic design allows users to conceal their real identities, thereby complicating law enforcement investigations (Böhme, Christin, Edelman, & Moore, 2015). Traditional auditing methods—designed primarily for centralized and regulated financial systems—lack the technical capabilities to effectively trace such transactions (Brenig, Accorsi, & Müller, 2015; Li, Jiang, Chen, Luo, & Wen, 2021). Consequently, cybercriminals exploit these weaknesses, engaging in complex cross-border laundering schemes that undermine the integrity of financial systems (Houben & Snyers, 2020; Chohan, 2021).

In Nigeria, cryptocurrency adoption has expanded rapidly among individuals, businesses, and institutions, partly due to inflationary pressures and limited access to foreign exchange (Okoro, 2021). However, regulatory bodies face significant challenges in monitoring and controlling crypto transactions due to insufficient technical capacity, lack of specialized forensic expertise, and weak integration of blockchain analytics into anti-money laundering (AML) frameworks (Eze & Nwankwo, 2022; Adetula & Olatunji, 2023). While the Central Bank of Nigeria (CBN) has implemented restrictions on cryptocurrency transactions within the banking system, illicit actors continue to bypass these measures through peer-to-peer platforms and foreign exchanges (Yusuf, 2020).

prior researches (McGinn, Birchall, Rouch, & Norvill, 2018; Albrecht, Duffin, Hawkins, & Rocha, 2019) underscores the potential of forensic auditing—combining investigative accounting, digital forensics, and blockchain analytics—to detect and deter cryptocurrency-related crimes. However, much of the literature either focuses on the technological architecture of blockchain or examines general AML compliance without empirically evaluating forensic auditing as a targeted investigative tool in the Nigerian context (Ramezanpour, 2021; Adetula & Olatunji, 2023).

Thus, while forensic auditing has been recognized theoretically as a tool for combating cryptocurrency-related crimes, to the best of our knowledge, its practical adoption, effectiveness, and challenges within Nigeria's EFCC remain underexplored. This research addresses this critical gap.

1.3 Research Questions

This study will seek to answer the following research questions:

1. To what extent does forensic auditing improve the detection of cryptocurrency fraud?
2. How effective are blockchain analytics and forensic tools in tracing cryptocurrency transactions?
3. What are the key challenges forensic auditors face in investigating cryptocurrency-related money laundering?
4. How can the integration of forensic auditing enhance regulatory compliance within cryptocurrency markets?

1.4 Objectives of the Study

The main objective of this study is to evaluate the role of forensic auditing in detecting cryptocurrency fraud and money laundering. The specific objectives are to:

1. assess the extent to which forensic auditing improves the detection of cryptocurrency fraud;
2. examine the effectiveness of blockchain analytics and forensic tools in tracing cryptocurrency transactions;
3. identify the challenges forensic auditors face in investigating cryptocurrency-related money laundering and cryptocurrency fraud;
4. determine how the integration of forensic auditing can enhance regulatory compliance in cryptocurrency markets;

1.5 Hypotheses of the Study

The study is guided by the following null hypotheses:

HO_1: Forensic auditing does not significantly improve the detection of cryptocurrency fraud.

HO_2: Blockchain analytics and forensic tools are not effective in tracing cryptocurrency transactions.

HO_3: There are no significant challenges faced by forensic auditors in investigating cryptocurrency-related money laundering.

HO_4: The integration of forensic auditing does not enhance regulatory compliance in cryptocurrency markets.

1.6 Scope of the Study

This study is limited to investigating the role of forensic auditing in detecting cryptocurrency fraud and money laundering within the Economic and Financial Crimes Commission (EFCC). The population comprises EFCC investigative officers, forensic auditors, and analysts directly involved in cryptocurrency-related cases. A sample size of 50 respondents will be drawn from the EFCC headquarters in Edo State and selected zonal offices.

Edo State was chosen because of its rising incidence of cybercrime and cryptocurrency-related investigations, making it a suitable context for exploring forensic auditing practices. The study will cover the period of 2025, a timeframe marked by increased cryptocurrency adoption and related financial crimes in Nigeria.

1.7 Significance of the Study

This study is significant because it provides empirical evidence on the effectiveness of forensic auditing in detecting cryptocurrency-related crimes within Nigeria, an area where existing research is limited. By focusing on the Economic and Financial Crimes Commission (EFCC), the study offers practical insights into how blockchain analytics and forensic tools can be integrated into financial crime investigation, thereby improving the detection, investigation, and prosecution of cryptocurrency fraud and money

laundering. The findings will also inform policymakers by providing data-driven recommendations for enhancing anti-money laundering frameworks and strengthening regulatory oversight in Nigeria's cryptocurrency markets. Furthermore, the study has institutional value for law enforcement agencies such as the EFCC, as it can guide the development of training programs and technical capacity-building for forensic auditors. From an academic perspective, it contributes to the growing body of literature on forensic accounting and digital asset regulation, serving as a useful reference point for future studies in the areas of financial crime, blockchain technology, and forensic auditing.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

The rise of cryptocurrencies has transformed global finance, enabling fast, decentralized, and low-cost transactions. However, their pseudonymous nature also makes them vulnerable to fraud, money laundering, and terrorism financing (Foley, Karlsen, & Putniņš, 2019). In Nigeria, adoption has grown rapidly due to inflation, unemployment, and limited foreign exchange access (Okoro, 2021). Yet, platforms like Binance and peer-to-peer exchanges are frequently exploited for "Yahoo Yahoo" scams and cross-border laundering (Eze & Nwankwo, 2022).

Traditional audits, which emphasize compliance and reporting, often fail to detect these crimes. Forensic auditing, integrating financial investigation, blockchain analytics, and digital forensics, provides a stronger approach to tracing illicit transactions (Albrecht, Duffin, Hawkins, & Rocha, 2019).

This chapter reviews literature on forensic auditing and cryptocurrency fraud through conceptual, empirical, and theoretical perspectives. It concludes by identifying gaps that justify the present study.

2.2 Conceptual Review

2.2.1 Cryptocurrency Fraud and Money Laundering

Cryptocurrency fraud involves deceptive practices that manipulate investors, users, or financial systems using digital assets. These fraudulent schemes range from Ponzi and pyramid schemes to phishing attacks, exchange hacks, fake Initial Coin Offerings (ICOs), and pump-and-dump schemes (Foley et al., 2019). Unlike traditional fraud, crypto-based fraud leverages blockchain's pseudo-anonymity, making perpetrators harder to trace. For example, the notorious PlusToken Ponzi scheme in China defrauded investors of over $2 billion in cryptocurrencies between 2018 and 2019, illustrating the magnitude of crypto fraud globally.

Money laundering in cryptocurrency is the process of disguising illicitly obtained digital assets to make them appear legitimate. According to Möser, Böhme, and Breuker (2013), this laundering process often uses mixers and tumblers, which combine different crypto transactions to obscure their origins. Additionally, criminals exploit decentralized exchanges (DEXs) that lack KYC procedures, making it easier to bypass regulatory checks.

In Nigeria, cryptocurrency-related laundering is closely linked to cybercrime syndicates. The Economic and Financial Crimes Commission (EFCC) has documented cases where illicit funds obtained from online scams were transferred into Bitcoin or Ethereum wallets to conceal origins before being reintegrated into the economy (Eze & Nwankwo, 2022).

Fraudulent schemes such as fake investment platforms ("double-your-money" scams) and gift card crypto laundering are rampant.

According to the Financial Action Task Force (FATF, 2022), cryptocurrency-based money laundering generally occurs in three stages:

Placement – Conversion of illicit fiat funds into cryptocurrency through exchanges or peer-to-peer (P2P) trading platforms.

Layering – The use of multiple wallet addresses, chain-hopping (moving funds across blockchains), and trading through DEXs to conceal traces.

Integration – Reintroducing cleaned crypto funds into the economy, often via luxury purchases, real estate, or peer-to-peer trades.

While blockchain ensures immutable records, its pseudonymous nature complicates the attribution of wallets to real-world actors. Thus, forensic auditing becomes critical in analyzing blockchain patterns, linking transactions to identities, and presenting admissible evidence in legal proceedings.

2.2.2 Forensic Auditing

Forensic auditing refers to the integration of auditing, investigative, and legal techniques designed to uncover fraud and financial crime. Unlike traditional audits that focus primarily on compliance with financial reporting standards, forensic audits concentrate on detecting, reconstructing, and preventing fraudulent practices. Bhasin (2016)

emphasizes that forensic auditing goes beyond numbers to evaluate intent, motive, and concealment strategies employed by fraudsters.

In the context of cryptocurrencies, forensic auditing involves the use of advanced digital tools and investigative techniques to track blockchain transactions, identify illicit wallet addresses, and compile admissible evidence for litigation. Albrecht, Duffin, Hawkins, and Rocha (2019) note that forensic auditing in crypto cases often requires cross-disciplinary collaboration—accountants must work closely with digital forensic experts, cybersecurity analysts, and law enforcement agencies.

In Nigeria, forensic auditing is still at a nascent stage, especially concerning digital assets. The Economic and Financial Crimes Commission (EFCC) is the main institution deploying forensic audits in fraud detection. However, the lack of specialized knowledge in cryptocurrency investigations poses a significant challenge (Adetula & Olatunji, 2023). Despite these limitations, forensic auditing is increasingly being recognized as indispensable in combating crypto-related financial crimes.

The role of forensic auditing in crypto-related investigations includes:

Tracing wallet addresses linked to suspicious activities.

Detecting unusual patterns such as rapid transfers between wallets or unusually large transactions.

Linking pseudonymous accounts to identifiable individuals through IP addresses, device forensics, and KYC records.

Compiling evidence that satisfies legal standards and can be presented in courts.

Thus, forensic auditing acts as the independent variable influencing the detection (and possible reduction) of cryptocurrency fraud and money laundering in Nigeria.

2.2.3 Forensic Auditing Practices

Forensic auditing practices refer to the specific investigative procedures and techniques applied in detecting fraudulent financial activity. In cryptocurrency contexts, these practices differ from traditional audits due to the decentralized and cryptographic nature of transactions.

Some key practices include:

Transaction Reconstruction – Mapping digital currency flows across multiple wallets to create a forensic trail.

Digital Evidence Gathering – Analyzing crypto-exchange logs, user histories, and IP addresses to establish identity.

Collaborative Auditing – Working in tandem with regulators, law enforcement, and international watchdogs to track cross-border transactions.

Use of Open-Source Intelligence (OSINT) – Gathering external data such as social media activity and darknet markets linked to crypto addresses.

In Nigeria, EFCC forensic auditors rely heavily on transaction reconstruction and collaboration with banks, exchanges, and mobile operators. For example, when crypto

funds are laundered through P2P trading, forensic auditors may subpoena phone records and social media accounts to link fraudsters with wallet addresses.

According to Eze and Nwankwo (2022), forensic auditing practices in Nigeria have proven effective in prosecuting cybercrime suspects. However, challenges persist, including lack of access to sophisticated blockchain analytics tools and resistance from criminals who use VPNs, fake identities, and global exchanges located outside Nigeria's jurisdiction.

2.2.4 Blockchain Analysis Tools

Blockchain analysis tools are specialized digital platforms designed to analyze cryptocurrency transactions and trace illicit activity. Prominent examples include:

Chainalysis – Used by global regulators and law enforcement to track crypto flows, monitor ransomware payments, and identify suspicious addresses.

CipherTrace – Provides risk scoring of wallets, compliance monitoring, and crypto AML reporting.

Elliptic – Focuses on detecting money laundering, terrorist financing, and fraud within blockchain networks.

These tools employ techniques such as transaction clustering, heuristics, pattern recognition, and artificial intelligence to track criminal activity across the blockchain. According to Ramezanpour (2021), blockchain analysis has been instrumental in dismantling darknet markets like Silk Road and tracing ransomware payments.

However, in Nigeria, access to such sophisticated tools is limited due to high licensing costs, lack of technical expertise, and institutional resistance (Okoro, 2021). Most Nigerian forensic auditors depend on manual tracking methods or rely on external assistance from global firms. This technological gap creates vulnerabilities in Nigeria's anti-money laundering regime.

2.2.5 Forensic Auditor Technical Expertise

The success of forensic auditing in cryptocurrency investigations depends largely on the **technical expertise** of the auditors. Unlike conventional financial auditors, forensic auditors investigating cryptocurrencies must be proficient in areas such as:

Blockchain technology – Understanding transaction structures, consensus mechanisms, and smart contracts.

Digital forensics – Collecting and analyzing evidence from computers, mobile devices, and networks.

Cryptography – Familiarity with hashing, encryption, and privacy technologies that underpin cryptocurrencies.

Legal frameworks – Knowledge of AML/CFT (Anti-Money Laundering/Counter Financing of Terrorism) regulations and admissibility standards for digital evidence.

Li, Jiang, Chen, Luo, and Wen (2021) highlight that effective crypto-forensic auditors must blend accounting knowledge with IT and cybersecurity expertise. This

multidisciplinary skillset allows auditors to track pseudonymous wallet addresses, identify suspicious flows, and prepare evidence for prosecution.

In Nigeria, however, technical expertise remains a major challenge. Adetula and Olatunji (2023) note that most forensic auditors are trained in conventional accounting practices, with limited exposure to blockchain and cyber-forensics. The EFCC has begun training auditors in digital forensics, but the pace of capacity development remains slow compared to the rapid growth of cryptocurrency use.

2.2.6 Integration with Regulatory Compliance

Forensic auditing must be integrated into broader regulatory frameworks to be effective in combating crypto-based financial crime. Global standards such as the Financial Action Task Force (FATF**)** guidelines require virtual asset service providers (VASPs) to implement Know Your Customer (KYC) procedures, transaction monitoring, and suspicious activity reporting (FATF, 2022).

Integration ensures that forensic auditing does not operate in isolation but is embedded within anti-money laundering (AML) and counter-terrorist financing (CTF) frameworks. This allows for improved data sharing, joint investigations, and stronger enforcement.

In Nigeria, the Central Bank of Nigeria (CBN) issued circulars restricting financial institutions from facilitating crypto transactions (Yusuf, 2020). However, illicit actors bypass these restrictions using P2P platforms. This weakens regulatory oversight and creates loopholes for laundering.

By integrating forensic auditing into Nigeria's anti–money laundering (AML) frameworks, regulators and investigators can mandate cryptocurrency exchanges to provide transaction data, standardize the admissibility of blockchain forensic evidence, improve international collaboration on cross-border crimes, and enhance the Economic and Financial Crimes Commission's (EFCC) ability to prosecute offenders. Without such integration, however, forensic auditing efforts risk remaining piecemeal and ineffective in addressing the growing problem of crypto-related financial crime.

2.3 Empirical Review

The empirical review provides evidence from prior studies that have examined the relationship between forensic auditing, cryptocurrency fraud, and money laundering globally, regionally, and within Nigeria. It highlights the methodological approaches used, key findings, and gaps in existing literature.

2.3.1 Global Empirical Studies

Globally, there has been significant interest in understanding the intersection of cryptocurrencies, fraud, and forensic auditing. Research shows that while cryptocurrencies promote innovation, they also provide fertile ground for illicit activities. Foley, Karlsen, and Putniņš (2019) carried out a large-scale quantitative analysis of Bitcoin transactions between 2009 and 2017. Using blockchain data analytics, they estimated that about 25% of Bitcoin users and nearly 46% of transactions were linked to illegal activities, including drug trafficking, ransomware, and money laundering. Their

findings highlighted the magnitude of crypto-crime and suggested that forensic auditing—particularly blockchain transaction tracing—was essential for mitigating these risks.

Similarly, Brenig, Accorsi, and Müller (2015) conducted simulation-based research into crypto-backed money laundering. Their study found that laundering strategies often exploit the pseudo-anonymity of blockchain and the difficulty of enforcing cross-border regulations. They concluded that blockchain forensics, particularly clustering techniques, could significantly enhance law enforcement's ability to uncover laundering networks.

Albrecht, Duffin, Hawkins, and Rocha (2019) provided case-based evidence from the United States, showing how forensic accountants assisted prosecutors in dismantling fraudulent ICOs (Initial Coin Offerings). Their study emphasized that forensic auditors' technical expertise in blockchain analytics made it possible to recover stolen funds and prepare admissible evidence.

Houben and Snyers (2020), in a European Parliament policy report, also offered empirical findings showing that crypto-crime investigations across Europe rely heavily on blockchain analysis tools such as Chainalysis and Elliptic. However, they noted disparities across EU member states—countries with weak integration between forensic auditing and regulatory frameworks experienced higher levels of crypto-based fraud.

More recent evidence from Chainalysis (2023) shows that $20.6 billion worth of cryptocurrency was linked to illicit activities in 2022, representing a record high. The

report highlighted the role of forensic blockchain analysis in detecting these flows but also warned that the increasing sophistication of criminals poses ongoing challenges.

These global studies confirm that forensic auditing is critical in detecting crypto-fraud and laundering. However, they reveal major challenges: lack of uniform regulatory frameworks, limited admissibility of blockchain evidence in court, and an acute shortage of forensic experts.

2.3.2 Regional Empirical Studies (Africa and Developing Economies)

Research in Africa and other developing economies reflects unique challenges due to weak regulatory environments, inadequate technology, and rising cryptocurrency adoption.

Okoro (2021) conducted a survey-based study of 400 Nigerian crypto users. The findings showed that adoption was driven by inflation, unemployment, and the scarcity of foreign exchange. However, users were also exposed to Ponzi schemes, P2P scams, and money laundering schemes. The study recommended that Nigeria must invest in forensic auditing capacity and adopt blockchain analysis tools to manage associated risks.

In Kenya, Ndungu and Mutiso (2021) used interviews with financial regulators to explore crypto adoption and fraud. They found that while regulators acknowledged the potential of forensic auditing, poor infrastructure and low technical expertise limited its adoption.

Chohan (2021), examining decentralized finance (DeFi) in emerging markets, provided evidence that the rise of smart contracts and decentralized platforms created new

laundering opportunities. His study concluded that blockchain forensics was crucial for identifying risks in DeFi ecosystems but noted that regulators in developing economies lacked adequate training.

In South Africa, Mhlanga (2022) conducted case studies on crypto exchange frauds. The research found that forensic auditors played a central role in reconstructing stolen funds but faced barriers of cross-border cooperation when criminals moved assets to offshore jurisdictions.

Eze and Nwankwo (2022) empirically studied forensic auditing's role in curbing financial crimes in Nigeria. Their survey of EFCC staff found that forensic auditing significantly improved the detection of crypto-related fraud cases, but technical expertise and access to tools were inadequate.

These regional studies reveal a consistent pattern: while forensic auditing is recognized as essential, African countries face technological, legal, and capacity barriers that limit its full effectiveness.

2.3.3 Nigerian Empirical Studies

Nigeria, being Africa's largest cryptocurrency market, has attracted increasing academic attention. However, most studies remain descriptive rather than evaluative.

Yusuf (2020) explored the regulatory stance of the Central Bank of Nigeria (CBN), which restricted banks from facilitating crypto transactions. Using qualitative content analysis, the study found that these restrictions were largely ineffective because criminals

shifted to peer-to-peer exchanges**.** Yusuf recommended that forensic auditing be formally integrated into Nigeria's anti-money laundering (AML) framework.

Eze and Nwankwo (2022), in their study of forensic accounting in financial crimes, found that forensic auditors within EFCC had successfully traced crypto transactions in several cases. However, they highlighted the shortage of blockchain analysis tools as a major barrier to effectiveness.

Adetula and Olatunji (2023) used secondary data analysis to evaluate Nigeria's AML strategies. Their findings revealed poor integration between forensic auditing practices and national compliance systems. They concluded that Nigeria lacked the institutional will to invest in modern forensic auditing infrastructure.

Empirical reports from the EFCC (2021–2023) also indicate that cryptocurrencies have become a preferred medium for laundering proceeds of cybercrime. For instance, several cases involving Yahoo Yahoo fraudsters in Edo and Lagos States revealed that criminals frequently converted stolen funds into Bitcoin before cashing out through P2P platforms. However, EFCC's success in prosecuting such cases remains limited due **to** technical skill gap**s**.

Collectively, these Nigerian studies demonstrate that while forensic auditing is acknowledged as important, there is still insufficient empirical data measuring its actual effectiveness in detecting and deterring cryptocurrency crime.

2.3.4 Synthesis of Empirical Findings

Synthesizing global, regional, and Nigerian studies reveals several important insights:

Forensic auditing enhances detection – Evidence across contexts (Foley et al., 2019; Eze & Nwankwo, 2022) shows that forensic auditing and blockchain analytics significantly improve fraud detection.

Blockchain analysis tools are underutilized in Nigeria – Whereas tools like Chainalysis are widely used in Europe and the U.S., Nigerian investigators often lack access due to high costs and limited training (Okoro, 2021).

Technical expertise remains a bottleneck – Many auditors in Nigeria are trained in traditional accounting but lack crypto-forensics skills (Adetula & Olatunji, 2023).

Regulatory integration is weak – Both Nigerian and global evidence highlight insufficient embedding of forensic auditing into AML frameworks, reducing its deterrence capacity (Yusuf, 2020).

Limited Nigeria-specific evidence – Unlike advanced economies, Nigeria lacks robust quantitative studies assessing forensic auditing outcomes. Most evidence is anecdotal or descriptive.

Overall, while forensic auditing has proven effective globally, its application in Nigeria remains **fragmented, underfunded, and under-researched**. This gap underscores the need for the present study, which aims to provide empirical evidence specific to the Nigerian context—particularly in Edo State, where cybercrime prevalence is high.

2.4 Theoretical Framework

This study is anchored on the Fraud Triangle Theory**,** developed by Donald Cressey (1953). The theory explains why individuals commit fraud by highlighting the interplay of three elements: pressure**,** opportunity**,** and rationalization. In the context of cryptocurrency fraud and money laundering, this framework provides an analytical basis for understanding the motivations and enabling conditions that drive fraudulent activities and how forensic auditing can mitigate them.

2.4.1 Components of the Fraud Triangle

Pressure (Incentives and Motivation)

Pressure refers to the internal or external forces that drive individuals to commit fraud. According to Cressey (1953), this often stems from financial distress, debt, unemployment, or unrealistic performance expectations. In Nigeria, economic hardship, inflation, unemployment, and limited access to financial opportunities create strong incentives for individuals—particularly youth—to engage in fraudulent activities, including cryptocurrency scams.

Studies (Eze & Nwankwo, 2022; Okoro, 2021) show that many young Nigerians turn to cryptocurrency fraud, popularly known as *Yahoo Yahoo*, to cope with socio-economic pressures. Fraudulent schemes such as Ponzi investments, phishing scams, and pump-and-dump operations thrive because they promise quick wealth in a struggling economy.

Forensic auditing addresses **pressure** indirectly by creating a perception of high detection probability. When criminals know forensic audits can trace crypto transactions, the deterrent effect reduces their willingness to succumb to financial pressure.

Opportunity (Weaknesses in Systems and Controls)

Opportunity arises when individuals perceive loopholes in systems that make fraud possible without being detected. Cryptocurrencies, due to their decentralized and pseudo-anonymous nature, provide vast opportunities for money laundering and fraudulent transactions. Weak regulatory frameworks, lack of blockchain analytic tools, and low technical expertise among auditors in Nigeria further widen these opportunities.

For instance, peer-to-peer (P2P) exchanges in Nigeria operate largely outside regulatory oversight, making them attractive platforms for laundering illicit funds. Additionally, cybercriminals exploit mixers, tumblers, and decentralized finance (DeFi) platforms to obfuscate transaction trails.

Forensic auditing directly reduces opportunity by:

Using blockchain analysis tools (e.g., Chainalysis, CipherTrace) to trace wallets and detect unusual transaction patterns.

Collaborating with regulatory and enforcement agencies to close systemic loopholes.

Applying advanced forensic techniques such as clustering analysis to uncover hidden connections between seemingly unrelated wallets.

Thus, forensic auditing transforms the opportunity landscape, making it harder for fraudsters to hide their activities.

Rationalization (Justification of Fraudulent Behavior)

Rationalization refers to the mental justification that allows fraudsters to view their actions as acceptable. In Nigeria, rationalizations often take the form of cultural and social narratives—such as seeing online fraud as a legitimate hustle due to unemployment or viewing it as "reparations" for perceived economic exploitation by foreign nations (Adetula & Olatunji, 2023).

Fraudsters also rationalize actions by claiming that cryptocurrency fraud is a victimless crime since "digital money is endless" or "banks and foreigners are the real losers."

Forensic auditing helps counteract rationalization by exposing fraud and holding perpetrators accountable in legal proceedings. When evidence is presented in court and cases are successfully prosecuted, the normalization of fraud is challenged, weakening rationalization narratives.

2.4.2 Application of Fraud Triangle to Cryptocurrency in Nigeria

Applying the Fraud Triangle to Nigeria's cryptocurrency context demonstrates the interconnectedness of socio-economic conditions, systemic weaknesses, and cultural rationalizations in enabling crypto-crimes:

Pressure: Youth unemployment, inflation, and limited access to traditional financial systems create fertile ground for fraudulent crypto schemes.

Opportunity: Decentralized exchanges, weak AML frameworks, and poor forensic capacity provide an enabling environment for laundering illicit funds.

Rationalization: Cultural acceptance of cybercrime (*Yahoo Yahoo*) and lack of visible consequences for offenders foster justification.

Forensic auditing addresses each dimension:

By increasing the certainty of detection**,** it reduces the attractiveness of fraud as a solution to financial pressure.

By strengthening monitoring and analytics**,** it closes systemic opportunities.

By enhancing prosecutions through admissible forensic evidence**,** it weakens cultural rationalizations and sends a deterrent signal.

2.4.3 Complementary Theories

While the Fraud Triangle is central, scholars have argued that it can be expanded through complementary models:

Fraud Diamond Theory (Wolfe & Hermanson, 2004) adds a fourth element—capability—which emphasizes that fraud requires not only opportunity but also the technical ability to exploit systems. This is especially relevant in cryptocurrency crimes, where advanced knowledge of blockchain, coding, and digital forensics is often necessary.

GONE Theory (Bologna, 1993) highlights Greed, Opportunity, Need, and Exposure as drivers of fraud. This framework resonates with Nigeria, where greed and need coexist as primary motivations for crypto fraud.

Although these alternative models provide additional insights, the Fraud Triangle remains the most widely accepted and foundational framework for fraud analysis. Its application in this study provides a robust theoretical grounding for assessing forensic auditing's role in addressing cryptocurrency fraud and money laundering in Nigeria.

2.5 Research Gap

Although a significant body of literature exists on forensic auditing, cryptocurrency fraud, and money laundering, a close examination reveals several important gaps, particularly in the Nigerian context. Identifying and addressing these gaps provides the foundation and justification for this study, especially as it focuses on the role of forensic auditing in detecting cryptocurrency fraud and money laundering among EFCC investigators in Edo State, Nigeria.

2.5.1 Gap in Geographic Focus

Most of the current literature on cryptocurrency fraud and forensic auditing is based on studies conducted in advanced economies such as the United States, the United Kingdom, and the European Union (Houben & Snyers, 2020; Foley, Karlsen, & Putniņš, 2019). These regions have well-developed regulatory frameworks, advanced blockchain analytic tools, and highly trained forensic auditors.

By contrast, studies conducted in Africa, and Nigeria in particular, remain limited and often descriptive (Eze & Nwankwo, 2022; Okoro, 2021). They provide overviews of challenges but rarely assess the measurable impact of forensic auditing on curbing fraud. This geographical gap means that Nigeria-specific realities—such as weak enforcement, socio-cultural rationalization of fraud, and limited technical infrastructure—are underexplored in academic research.

2.5.2 Gap in Empirical Depth

While existing Nigerian studies acknowledge that forensic auditing is essential in addressing financial crimes, many remain theoretical or qualitative in nature. For example, Yusuf (2020) focused on regulatory restrictions imposed by the Central Bank of Nigeria (CBN) but did not empirically measure how forensic auditing tools impact fraud detection. Similarly, Adetula and Olatunji (2023) described challenges in adopting forensic auditing but did not evaluate actual forensic auditing practices within Nigerian institutions.

This lack of quantitative and context-specific empirical evidence weakens the policy relevance of existing literature and underscores the need for studies like this one, which aim to gather practical insights directly from forensic investigators in Nigeria.

2.5.3 Gap in Technological Adoption and Evaluation

Globally, advanced blockchain analysis tools such as Chainalysis, CipherTrace, and Elliptic have become central to forensic auditing (Chainalysis, 2023). These tools use

artificial intelligence, heuristics, and clustering to trace illicit crypto activities. However, in Nigeria, empirical studies reveal that adoption of such tools remains rare due to high costs, limited access, and inadequate training (Okoro, 2021).

Yet, few studies have examined how the lack of such technological adoption directly affects fraud detection outcomes in Nigeria. Even fewer have assessed whether alternative, cost-effective local forensic strategies exist. This creates a significant research gap that this study seeks to fill by evaluating the tools and practices available to Nigerian investigators.

2.5.4 Gap in Human Capacity and Expertise

Forensic auditing requires auditors with interdisciplinary expertise in accounting, cryptography, digital forensics, and regulatory frameworks (Li, Jiang, Chen, Luo, & Wen, 2021). However, in Nigeria, most auditors are trained primarily in traditional accounting and have limited exposure to blockchain technology or forensic digital tools (Eze & Nwankwo, 2022).

Although this skills gap has been acknowledged, few empirical studies have systematically examined its impact on the detection of cryptocurrency fraud. There is also limited research into the training needs of Nigerian forensic auditors and how such needs can be addressed through collaboration with international agencies. This study bridges that gap by exploring how the technical expertise of EFCC investigators in Edo State influences forensic auditing outcomes.

2.5.5 Gap in Regulatory Integration

Forensic auditing cannot operate in isolation; it must be integrated into broader regulatory frameworks such as Anti-Money Laundering (AML) laws and Financial Action Task Force (FATF) recommendations. While some studies (FATF, 2022; Yusuf, 2020) have highlighted regulatory restrictions on cryptocurrency transactions in Nigeria, they often focus on macro-level banking restrictions by the Central Bank of Nigeria.

There is a limited focus on how forensic auditing is practically aligned with Nigeria's AML policies**,** how evidence generated from forensic audits is used in court, and how regulatory bodies coordinate with auditors. This represents a significant gap in both research and practice.

2.5.6 Gap in Contextual Application (Edo State Focus)

Another key gap lies in the context-specific focus. Much of the Nigerian literature generalizes findings across the country, but cybercrime prevalence is not uniform. Edo State, for example, is widely recognized as a hotspot for cybercrime activities and "Yahoo Yahoo" culture, yet very little empirical research has investigated how forensic auditing is applied in this specific context.

By targeting EFCC investigators in Edo State, this study addresses a contextual research gap by producing localized insights into forensic auditing practices, challenges, and outcomes in one of Nigeria's most cybercrime-prone regions.

2.5.7 Gap in Outcome Evaluation

Finally, while many studies acknowledge the importance of forensic auditing, there is insufficient research evaluating outcomes—that is, to what extent forensic auditing actually improves fraud detection rates, enhances prosecution success, or reduces money laundering risks. Without such outcome-based evaluations, it is difficult to measure the real effectiveness of forensic auditing.

This study contributes to closing this gap by investigating the role of forensic auditing in detecting cryptocurrency fraud and money laundering, thereby providing empirical evidence on its impact within Nigeria's financial crime landscape.

2.5.8 Synthesis of Identified Gaps

In summary, the research gaps identified in the literature include:

A geographic gap—scarcity of Nigeria-focused and Edo State-specific studies.

An empirical gap—dominance of descriptive and theoretical research with little quantitative or field-based data.

A technological gap—limited evaluation of blockchain analytic tool adoption in Nigeria.

A human capacity gap—insufficient assessment of forensic auditors' technical expertise.

A regulatory gap—poor exploration of forensic auditing's integration with AML frameworks.

An outcome gap—lack of evidence-based evaluation of forensic auditing effectiveness.

Addressing these gaps, this study will provide Nigeria-specific, context-driven, and empirically grounded insights into the role of forensic auditing in combating cryptocurrency fraud and money laundering, with a special focus on EFCC operations in Edo State.

2.6 Summary

This chapter reviewed literature on the role of forensic auditing in detecting cryptocurrency fraud and money laundering. The review covered conceptual, empirical, and theoretical perspectives, followed by an identification of research gaps.

Conceptually, the dependent variable was identified as cryptocurrency fraud and money laundering, including activities such as Ponzi schemes, phishing, cyber-laundering, and the use of mixers. The independent variable was forensic auditing, which goes beyond compliance to uncover illicit activities. Key components included forensic auditing practices, blockchain analysis tools, auditor expertise, and integration with regulatory frameworks

Empirically, global studies showed that a significant share of cryptocurrency transactions is linked to illicit activities, reinforcing the role of forensic auditing (Foley et al., 2019). Regional and Nigerian studies highlighted the rapid adoption of cryptocurrency but revealed challenges such as weak regulatory frameworks, limited use of blockchain analytics, and lack of technical expertise (Eze & Nwankwo, 2022; Adetula & Olatunji, 2023).

Theoretically, the Fraud Triangle Theory (Cressey, 1953) explained how pressures, opportunities, and rationalization drive fraud. Forensic auditing reduces these conditions by strengthening detection, discouraging rationalization, and promoting accountability.

Research gaps were identified in six areas: limited Nigeria- and Edo-specific studies, weak empirical evidence, poor adoption of blockchain tools, lack of technical expertise, regulatory weaknesses, and limited evaluation of forensic auditing effectiveness.

In conclusion, the review showed that while forensic auditing is globally effective, Nigeria still lags in practice and research. Addressing the identified gaps justifies the present study, which focuses on EFCC investigators in Edo State to generate Nigeria-specific insights and policy recommendations.

CHAPTER THREE

METHODOLOGY

3.1 Introduction

This chapter presents the methodology adopted in conducting the study. It provides a detailed explanation of the research design, population, sample size, sampling technique, sources of data, and the research instrument used for data collection. The procedures for establishing the validity and reliability of the instrument, as well as the methods of data collection and analysis, are also discussed. In addition, the chapter outlined the ethical considerations observed in the course of the study and provides the model specification that guides the statistical analysis. The methodology adopted was structured to ensure that the data gathered is accurate, reliable, and suitable for addressing the research objectives and testing the hypotheses formulated in the study.

3.2 Research Design

This study adopted a descriptive survey research design. The design was suitable because it allowed the researcher to gather data from respondents concerning their opinions, perceptions, and practices on forensic auditing in detecting cryptocurrency fraud and money laundering. A survey approach is appropriate given that it facilitates the collection of large-scale quantitative data that can be statistically analyzed to draw valid conclusions (Creswell, 2014).

3.3 Population of the Study

The population of this study consisted of all investigators and staff of the Economic and Financial Crimes Commission (EFCC), Benin Zonal Command, Edo State. This choice was informed by the fact that the EFCC is the primary agency mandated to investigate, prevent, and prosecute financial crimes, including cryptocurrency-related fraud and money laundering.

3.4 Sample Size and Sampling Technique

A purposive sampling technique was employed to select respondents who are directly involved in forensic auditing, investigation, and prosecution of financial crimes. The sample size consisted of 50 EFCC staff, including forensic auditors, investigators, and legal officers. This size was considered adequate to provide reliable and representative data for statistical analysis (Yamane, 1967).

3.5 Sources of Data Collection

The study relied on primary and secondary sources of data. Primary data were collected through a structured questionnaire administered to EFCC investigators and auditors. Secondary data was obtained from journals, books, EFCC annual reports, and official publications related to forensic auditing and cryptocurrency fraud.

3.6 Research Instrument

The main research instrument for this study was a structured questionnaire designed in line with the research objectives and hypotheses. The questionnaire contains both closed-

ended and Likert-scale questions, ensuring that respondents were provided with quantifiable responses suitable for statistical analysis. The instrument was divided into sections: Section A (demographic data), Section B (forensic auditing practices), Section C (cryptocurrency fraud and money laundering), and Section D (regulatory integration).

3.7 Validity and Reliability of Instrument

To ensure validity, the questionnaire was reviewed by academic experts and professionals in forensic auditing. A pilot test will also be conducted among 10 EFCC staff outside the sample to refine the instrument. Reliability was tested using Cronbach's Alpha coefficient, with a reliability threshold of 0.70 considered acceptable (Nunnally, 1978).

3.8 Method of Data Collection

The researcher personally administered the questionnaires to the sampled respondents to ensure a high return rate. Follow-ups were conducted through email and telephone calls where necessary. The anonymity of respondents was ensured to encourage honest and unbiased responses.

3.9 Method of Data Analysis

The data collected was coded and analyzed using the Statistical Package for Social Sciences (SPSS, version 26). Both descriptive statistics (frequencies, percentages, means, and standard deviations) and inferential statistics (Chi-square tests and regression analysis) was employed to test the hypotheses and examine relationships among variables. The results were presented in tables and charts for clarity and ease of interpretation.

3.10 Ethical Considerations

Ethical standards were maintained throughout the research process. Participation in the study were voluntary, and informed consent were obtained from all respondents. Confidentiality of respondents' information were strictly maintained, and data was used solely for academic purposes.

3.11 Model Specification

This study adopted a quantitative research model anchored on a descriptive survey design, which enabled the collection and statistical analysis of primary data to examine the influence of forensic auditing on the detection of cryptocurrency fraud and money laundering. The model was specified to evaluate the relationship between the independent variables—Forensic Auditing practices (FA), Blockchain Forensic Evidence (BFE), Regulatory Integration (RI), and Technological Adoption (TA)—and the dependent variable—Detection of Cryptocurrency Fraud and Money Laundering (CFML).

The functional form of the model is expressed as:

$$CFML = \beta_0 + \beta_1 FA + \beta_2 BFE + \beta_3 RI + \beta_4 TA + \mu$$

Where:

CFML = Detection of cryptocurrency fraud and money laundering (dependent variable)

FA = Forensic auditing practices

BFE = Blockchain forensic evidence

RI = Regulatory integration into AML frameworks

TA = Technological adoption in forensic auditing

β_0 = Constant/intercept term

$\beta_1 - \beta_4$ = Coefficients measuring the impact of each independent variable

μ = Error term capturing unobserved factors

This model was estimated using multiple regression analysis to determine the magnitude and significance of the relationship between forensic auditing measures and the ability to detect cryptocurrency-related financial crimes. The Statistical Package for Social Sciences (SPSS, version 26) was employed to run the regression and compute relevant statistics such as the coefficient of determination (R^2), F-statistics, and p-values, which guided the acceptance or rejection of the research hypotheses.

CHAPTER FOUR

DATA PRESENTATION, ANALYSIS AND DISCUSSION OF FINDINGS

4.1 Introduction

This chapter presents the analysis and interpretation of data collected from the administered questionnaires on the role of forensic auditing in detecting cryptocurrency fraud and money laundering. The data are presented in line with the research objectives and hypotheses.

Descriptive statistics—including frequencies, percentages, means, and standard deviations—were used to summarize respondent demographics and perceptions. Inferential statistics, specifically multiple regression analysis, were employed to test the hypotheses and determine the relationship between the independent variables (Forensic Auditing Practices, Blockchain Forensic Tools, Challenges, and Regulatory Integration) and the dependent variable (Detection of Cryptocurrency Fraud and Money Laundering).

A total of 50 questionnaires were distributed to staff of the Economic and Financial Crimes Commission (EFCC), Benin Zonal Command, all of which were completed and returned, yielding a 100% response rate. This exceptional response rate enhances the reliability and validity of the study's findings.

4.2 Demographic Characteristics of Respondents

The demographic information of respondents provides context for the analysis and includes gender, age, professional designation, years of experience, and educational qualification.

Table 4.1: Demographic Profile of Respondents (N = 50)

Variable	Category	Frequency	Percentage (%)
Gender	Male	32	64
	Female	18	36
Age Range	18–25 years	12	24
	26–35 years	22	44
	36–45 years	10	20
	46 years and above	6	12
Position/Designation	Forensic Auditor	20	40
	Investigator	10	20
	Legal Officer	8	16
	Analyst	7	14
	Other	5	10
Years of Experience	1–3 years	10	20
	4–6 years	16	32
	7–9 years	14	28
	10 years and above	10	20
Educational Qualification	OND	5	10
	HND	7	14
	B.Sc.	25	50
	M.Sc./MBA	8	16
	Professional Certification	5	10

Field Survey, 2025

Analysis:

The data indicate a gender distribution of 64% male and 36% female, reflecting a male-dominated but progressively inclusive environment. The majority (44%) fall within the 26–35 age range, indicating a youthful and technologically adaptable workforce. Forensic Auditors formed the largest professional group (40%), while 80% of respondents have over three years of work experience. Academically, half (50%) hold a Bachelor's degree, reflecting strong professional competence.

4.3 Descriptive Analysis of Research Variables

This section analyzes the main variables using mean scores and standard deviations. A 5-point Likert scale was adopted, where:

1 = Strongly Disagree, 2 = Disagree, 3 = Neutral, 4 = Agree, and 5 = Strongly Agree. A mean score of 3.5 and above indicates strong agreement.

4.3.1 Forensic Auditing Practices (FA)

Table 4.2: Descriptive Statistics for Forensic Auditing Practices

S/N	Statement	Mean	Std. Dev.	Remark
1	Forensic auditing provides effective tools for identifying cryptocurrency fraud.	4.42	0.65	Strongly Agree
2	EFCC forensic auditors routinely apply blockchain analysis.	4.36	0.68	Strongly Agree
3	Adoption of forensic auditing has improved detection of money laundering.	4.42	0.64	Strongly Agree

4	Specialized training enhances crypto fraud detection success.	4.46	0.63	Strongly Agree
5	Collaboration between auditors and regulators strengthens anti-fraud efforts.	4.32	0.72	Strongly Agree
Composite Mean		**4.40**		**Strongly Agree**

Field Survey, 2025

Respondents strongly agreed with all statements regarding forensic auditing practices. The highest mean score (4.46) was for specialized training, highlighting it as a crucial success factor in cryptocurrency crime investigation.

4.3.2 Blockchain Analytics and Forensic Tools (BFE)

Table 4.3: Descriptive Statistics for Blockchain Forensic Tools

S/N	Statement	Mean	Std. Dev.	Remark
6	Blockchain analytics can accurately trace transaction flows.	4.44	0.61	Strongly Agree
7	Digital forensic tools are effective in identifying crypto wallets.	4.36	0.68	Strongly Agree
8	Real-time monitoring improves detection of suspicious activities.	4.36	0.66	Strongly Agree
9	Tool integration reduces complexity in crypto-related cases.	4.32	0.69	Strongly Agree
10	Blockchain analytics improves recovery of illicit assets.	4.36	0.68	Strongly Agree
Composite Mean		**4.37**		**Strongly Agree**

Field Survey, 2025

Respondents strongly agreed on the effectiveness of blockchain analytics. Tracing transaction flows (Mean = 4.44) was rated highest, affirming the technical importance of blockchain tools in forensic auditing.

4.3.3 Challenges in Investigating Cryptocurrency Crimes (CH)

Table 4.4: Descriptive Statistics for Investigation Challenges

S/N	Statement	Mean	Std. Dev.	Remark
11	Lack of technical expertise limits effectiveness.	4.32	0.73	Strongly Agree
12	Insufficient funding and infrastructure hinder investigations.	4.34	0.71	Strongly Agree
13	Regulatory loopholes make prosecution difficult.	4.28	0.73	Strongly Agree
14	Rapid blockchain changes outpace investigative capabilities.	4.28	0.76	Strongly Agree
15	Limited international cooperation slows cross-border cases.	4.20	0.80	Agree
Composite Mean		**4.28**		**Strongly Agree**

Field Survey, 2025

Respondents identified significant impediments to investigations, including inadequate funding, infrastructure, and expertise. Funding and infrastructure (Mean = 4.34) were the most pressing challenges.

4.3.4 Regulatory Integration and Compliance (RI)

Table 4.5: Descriptive Statistics for Regulatory Integration

S/N	Statement	Mean	Std. Dev.	Remark
16	Integrating forensic auditing into AML frameworks improves compliance.	4.32	0.72	Strongly Agree
17	EFCC-regulator collaboration strengthens fraud detection.	4.38	0.67	Strongly Agree
18	Strong regulatory policies encourage audit adoption.	4.36	0.68	Strongly Agree
19	Regular forensic reports help policymakers address risks.	4.30	0.73	Strongly Agree
20	Mandatory crypto exchange audits reduce laundering risks.	4.38	0.67	Strongly Agree
Composite Mean		**4.35**		**Strongly Agree**

Field Survey, 2025

There was strong agreement that integrating forensic auditing within regulatory frameworks enhances fraud detection. Collaboration and mandatory audits were rated highest (Mean = 4.38 each).

4.4 Test of Hypotheses

A multiple regression analysis tested the relationship between Forensic Auditing Practices (FA), Blockchain Forensic Tools (BFE), Challenges (CH), and Regulatory Integration (RI) on Detection of Cryptocurrency Fraud and Money Laundering (CFML).

Table 4.6: Regression Model Summary

Model	R	R^2	Adjusted R^2	Std. Error of the Estimate
1	0.781	0.610	0.594	0.412

Interpretation:

The R^2 value of 0.610 shows that 61% of the variation in CFML detection is explained by the independent variables.

Table 4.7: Analysis of Variance (ANOVA)

Model	Sum of Squares	df	Mean Square	F	Sig.
Regression	24.218	4	6.054	14.227	0.000
Residual	15.482	45	0.344		
Total	39.700	49			

Interpretation:

The ANOVA result ($F = 14.227$, $p < 0.001$) indicates that the model is statistically significant.

Table 4.8: Regression Coefficients

Variable	Unstd. (B)	Std. Error	Std. Beta	t-value	p-value
Constant	0.742	0.196		3.785	0.001
Forensic Auditing (FA)	0.281	0.072	0.297	3.904	0.000
Blockchain Tools (BFE)	0.256	0.076	0.249	3.368	0.002
Challenges (CH)	-0.194	0.071	-0.202	-2.732	0.009
Regulatory Integration (RI)	0.263	0.074	0.266	3.554	0.001

Dependent Variable: Detection of Cryptocurrency Fraud and Money Laundering (CFML)

Hypotheses Testing Decisions

Hypothesis	Statement	Decision
HO_1	Forensic Auditing Practices have no significant effect on CFML detection.	**Rejected**
HO_2	Blockchain Forensic Tools have no significant effect on CFML detection.	**Rejected**
HO_3	Challenges have no significant effect on CFML detection.	**Rejected**
HO_4	Regulatory Integration has no significant effect on CFML detection.	**Rejected**

4.5 Discussion of Findings

The findings of this study provide important insights into the role of forensic auditing in detecting cryptocurrency fraud and money laundering within the EFCC in Edo State. The regression analysis demonstrated that forensic auditing practices, blockchain forensic tools, investigative challenges, and regulatory integration collectively influence the effectiveness of detecting cryptocurrency-related financial crimes. These results align with existing empirical studies which argue that forensic auditing, when supported with the right expertise and digital investigative tools, has become central to combating modern financial crimes in the digital currency ecosystem.

Forensic Auditing Practices and Detection of Cryptocurrency Fraud

The study revealed that forensic auditing practices have a significant positive influence on the detection of cryptocurrency fraud and money laundering ($p < 0.05$). This finding corresponds with the work of Albrecht et al. (2019), who assert that forensic auditing techniques help uncover hidden financial trails and irregular digital transactions. Respondents strongly agreed that specialized training enhances the efficiency of forensic investigations. This supports Cressey's Fraud Triangle theory, which posits that increasing the likelihood of detection reduces the opportunity for fraud. Therefore, enhancing investigative skills and analytical competence among forensic auditors is crucial for improving fraud detection outcomes.

Blockchain Analytics and Forensic Tools in Crypto Investigations

The study also found that the use of blockchain analytics and forensic tools significantly improves the detection of cryptocurrency-related crimes ($p < 0.05$). This aligns with Ramezanpour (2021), who argues that blockchain forensic tools allow investigators to trace cryptocurrency flows across decentralized networks. Tools such as Chainalysis and CipherTrace enable the identification of wallet addresses and transaction linkages that would otherwise remain anonymous. The strong agreement among respondents supports the view of Eze and Nwankwo (2022), who emphasize that the effective use of digital forensic tools strengthens accountability and increases asset recovery. Thus, integrating blockchain analytics into EFCC investigative processes is essential for improving detection accuracy and prosecution success rates.

Challenges Limiting Crypto-Related Forensic Investigation

The findings further revealed that challenges such as inadequate technical expertise, insufficient forensic infrastructure, and rapid technological changes negatively affect the detection of cryptocurrency fraud ($p < 0.05$). This agrees with FATF (2022), which notes that developing countries often lack the technological capacity to keep up with sophisticated digital financial crimes. Respondents identified funding limitations and lack of continuous professional training as major impediments to investigative efficiency. This underscores the need for sustained investment in forensic capacity-building and technological modernization to match the evolving nature of crypto-enabled crimes.

Regulatory Integration and Anti-Money Laundering Compliance

The study also found that strong regulatory integration significantly enhances the detection and prevention of cryptocurrency-related fraud ($p < 0.05$). This finding aligns with Adetula and Olatunji (2023), who argue that robust AML regulations and inter-agency collaboration are essential for controlling the misuse of digital currencies. Respondents agreed that mandatory cryptocurrency exchange audits, clearer compliance guidelines, and coordinated supervision between agencies like EFCC, CBN, and SEC would reduce regulatory loopholes. Strengthening regulatory alignment ensures that forensic findings translate into enforceable legal actions, thereby improving prosecution outcomes.

CHAPTER FIVE

SUMMARY OF FINDINGS, CONCLUSION AND RECOMMENDATIONS

5.1 Introduction

This chapter presents the summary of the key findings of the study, draws conclusions based on the research objectives and hypothesis testing, and proposes practical recommendations for relevant stakeholders. The study examined *the role of forensic auditing in detecting cryptocurrency fraud and money laundering* with specific reference to the Economic and Financial Crimes Commission (EFCC) in Edo State. The chapter concludes by suggesting areas for future research to expand empirical understanding of forensic auditing practices within the evolving digital financial space.

5.2 Summary of Findings

This research was guided by four major objectives, which sought to determine the effect of forensic auditing practices, blockchain forensic tools, investigative challenges, and regulatory integration on the detection of cryptocurrency-related fraud and money laundering. Data were obtained through structured questionnaires administered to professional staff of the EFCC in Edo State and analyzed using descriptive statistics and regression techniques.

The key findings are summarized as follows:

Forensic Auditing Practices:

The study found that forensic auditing practices significantly enhance the detection of cryptocurrency-related fraud. Respondents strongly agreed that the application of investigative audits, evidence-based documentation, and specialized forensic review procedures improves the EFCC's ability to trace illicit cryptocurrency transactions.

Blockchain Analytics and Forensic Tools:

Blockchain forensic tools were found to have a strong positive influence on fraud detection. Tools such as Chainalysis, CipherTrace, and wallet-tracking analytics were egarded as essential in identifying transaction flows across decentralized networks, thereby improving the recovery of illicit digital assets.

Challenges in Cryptocurrency Investigations:

The study identified major constraints hindering effective forensic investigation. These include:

Inadequate technical expertise,

Insufficient funding for digital forensic tools, and

Rapid technological changes in blockchain systems.

These challenges negatively affect detection outcomes and slow down prosecution processes.

Regulatory Integration and AML Compliance:

Regulatory collaboration among EFCC, CBN, SEC, and other agencies was found to significantly improve fraud detection. Respondents agreed that clearer cryptocurrency regulations, routine compliance audits, and mandatory reporting frameworks strengthen investigative outcomes.

Hypothesis Testing:

The regression model showed that all independent variables (forensic auditing practices, blockchain forensic tools, challenges, and regulatory integration) jointly explained a significant proportion of variance in cryptocurrency fraud detection. All null hypotheses were rejected at $p < 0.05$, confirming statistically significant relationships.

5.3 Conclusion

This study concludes that forensic auditing plays a vital role in detecting and combating cryptocurrency fraud and money laundering in Nigeria. The findings demonstrate that when forensic auditing is supported by advanced blockchain analytics, adequate technical capacity, and strong regulatory frameworks, investigative outcomes are significantly improved. However, persistent challenges such as limited funding, skill shortages, and regulatory gaps continue to hinder full exploitation of digital forensic potential.

The study reinforces the application of Cressey's Fraud Triangle Theory**,** indicating that improving investigative detection reduces opportunities for fraud and increases accountability among perpetrators. Strengthening forensic auditing capacities within the

EFCC is therefore essential for safeguarding the integrity of Nigeria's financial system in the digital era.

5.4 Recommendations

Based on the findings, the following recommendations are proposed:

A. For the EFCC

The EFCC should implement continuous professional development programs focused on cryptocurrency tracing, blockchain analytics, and forensic investigation techniques. Also a Greater budgetary allocation should be made toward acquiring and updating digital forensic software such as Chainalysis Reactor, Elliptic Lens, and CipherTrace for more precise transaction monitoring. Lastly dedicated specialist unit should be created within the EFCC to concentrate expertise and enhance response efficiency to crypto-enabled financial crimes.

B. For Policymakers (CBN, SEC, NFIU)

A Clear, enforceable guidelines should be developed to regulate cryptocurrency exchanges, wallet service providers, and peer-to-peer trading platforms in Nigeria. Cryptocurrency service providers should undergo compulsory forensic audits and reporting to reduce money laundering loopholes. Policymakers should Structure channels for intelligence-sharing among agencies should be established to improve investigative coordination and prosecution outcomes.

C. For the Nigerian Government

Adequate funding should be provided to enhance forensic capacity development, digital infrastructure, and investigative support resource and Government should strengthen cross-border collaboration to tackle globally-networked cryptocurrency crimes that transcend jurisdictional boundaries.

5.5 Suggestions for Further Research

Future studies should examine forensic auditing effectiveness in multiple EFCC zonal offices to allow comparative regional analysis.

A mixed-method research design involving interviews would provide deeper insights into investigative challenges.

Longitudinal studies should track how improvements in forensic tools and regulations influence crime detection over time.

Further research may explore forensic auditing strategies for emerging crypto-crime typologies such as *DeFi fraud*, *NFT scams*, and *ransomware payments*.

REFERENCES

Adetula, A., & Olatunji, O. C. (2023). Cryptocurrency regulation and anti-money laundering strategies in Nigeria. Journal of Financial Crime, 30(1), 45–61. https://doi.org/10.1108/JFC-01-2022-0025

Albrecht, C., Duffin, K., Hawkins, S., & Rocha, V. (2019). The use of forensic accounting in cryptocurrency fraud cases. Journal of Forensic & Investigative Accounting, 11(1), 1–17.

Bhasin, M. L. (2016). Contribution of forensic accounting to corporate governance: An exploratory study of an Asian country. International Business Management, 10(4), 479–492.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. Journal of Economic Perspectives, 29(2), 213–238. https://doi.org/10.1257/jep.29.2.213

Brenig, C., Accorsi, R., & Müller, G. (2015). Economic analysis of cryptocurrency backed money laundering. In 2015 IEEE International Conference on Advanced Information Networking and Applications (pp. 1064–1072). IEEE. https://doi.org/10.1109/AINA.2015.254

Chainalysis. (2023). The 2023 crypto crime report. https://go.chainalysis.com/2023-Crypto-Crime-Report.html

Chohan, U. W. (2021). Decentralized finance (DeFi): An emerging alternative financial architecture. Discussion Paper Series. https://doi.org/10.2139/ssrn.3904690

Cressey, D. R. (1953). Other people's money: A study in the social psychology of embezzlement. Free Press.

Europol. (2022). Internet organised crime threat assessment (IOCTA) 2022. Europol.

Eze, C., & Nwankwo, O. (2022). Cryptocurrency and financial crime: The role of forensic accounting in Nigeria. International Journal of Accounting Research, 8(1), 12–25.

Financial Action Task Force. (2022). Targeted update on implementation of the FATF standards on virtual assets and virtual asset service providers. FATF. https://www.fatf-gafi.org

Foley, S., Karlsen, J. R., & Putniņš, T. J. (2019). Sex, drugs, and bitcoin: How much illegal activity is financed through cryptocurrencies? Review of Financial Studies, 32(5), 1798–1853. https://doi.org/10.1093/rfs/hhz015

Houben, R., & Snyers, A. (2020). Cryptocurrencies and blockchain: Legal context and implications for financial crime. European Parliament. https://www.europarl.europa.eu/thinktank

Kethineni, S., & Cao, Y. (2020). The rise in popularity of cryptocurrency and associated criminal activity. International Criminal Justice Review, 30(3), 325–344.

Li, X., Jiang, P., Chen, T., Luo, X., & Wen, Q. (2021). A survey on the security of blockchain systems. Future Generation Computer Systems,107,841–853.https://doi.org/10.1016/j.future.2017.08.020

McGinn, D., Birchall, R., Rouch, D., & Norvill, R. (2018). Blockchain: Legal and regulatory guidance. Law Society of England and Wales.

Möser, M., Böhme, R., & Breuker, D. (2013). An inquiry into money laundering tools in the Bitcoin ecosystem. In 2013 eCrime Researchers Summit (pp. 1–14). IEEE. https://doi.org/10.1109/eCRS.2013.6805780

Okoro, E. (2021). Cryptocurrency adoption in Nigeria: Drivers and implications. African Journal of Economic Policy, 28(2), 45–63.

Ramezanpour, M. (2021). Forensic blockchain analysis for financial crime investigation. Digital Investigation, 37, 301–310. https://doi.org/10.1016/j.diin.2021.301310

Yusuf, T. (2020). Cryptocurrency regulation in Nigeria: Balancing innovation and risk. Nigerian Financial Review, 15(1), 33–48.

APPENDIX 1
QUESTIONNAIRE
DEPARTMENT OF ACCOUNTING
FACULTY OF MANAGEMENT SCIENCES
UNIVERSITY OF BENIN
BENIN CITY.

Dear Respondent,

My name is Ibude Josiah Aiyevbosa, a final-year student in the Department of Accounting, Faculty of Management Sciences, University of Benin. I am conducting a research study titled: **"THE ROLE OF FORENSIC AUDITING IN DETECTING CRYPTOCURRENCY FRAUD AND MONEY LAUNDERING."** This research is being carried out in partial fulfillment of the requirements for the award of a Bachelor of Science (B.Sc.) degree in Accounting. The purpose of the study is to examine how forensic auditing practices, blockchain analytics tools, auditors' expertise, and regulatory frameworks contribute to the detection and prevention of cryptocurrency-related fraud and money laundering in Nigeria.

Your participation Is highly valuable to the success of this study. Please be assured that all information provided will be treated with strict confidentiality and will be used solely for academic purposes. Kindly respond honestly to all questions, as your input will help generate meaningful findings and recommendations.

Thank you for your time and cooperation.

Yours faithfully,

Ibude Josiah Aiyevbosa

INSTRUCTIONS

• Please tick (✓) the option that best represents your opinion.

• For Sections B–E, use the following 5-point Likert Scale:
5 = Strongly Agree (SA) 4 = Agree (A) 3 = Undecided (U) 2 = Disagree (D) 1 = Strongly Disagree (SD)

SECTION A: Demographic Information

1. Gender: ☐ Male ☐ Female

2. Age Range: ☐ 18–25 ☐ 26–35 ☐ 36–45 ☐ 46 and above

3. Position/Designation: ☐ Forensic Auditor ☐ Investigator ☐ Legal Officer ☐ Analyst ☐ Other (specify) _____
4. Years of Experience in EFCC: ☐ 1–3 years ☐ 4–6 years ☐ 7–9 years ☐ 10 years and above
5. Educational Qualification: ☐ OND ☐ HND ☐ B.Sc. ☐ M.Sc./MBA ☐ Professional Certification (e.g., ICAN, ACCA)

Section B: Forensic Auditing Practices (FA)

S/N	Statement	SA	A	U	D	SD
1	Forensic auditing provides effective tools for identifying cryptocurrency fraud in Nigeria.					
2	EFCC forensic auditors routinely apply blockchain analysis in cryptocurrency investigations.					
3	Adoption of forensic auditing has improved detection of cryptocurrency-related money laundering.					
4	Specialized training in forensic auditing enhances the success rate of cryptocurrency fraud detection.					
5	Collaboration between forensic auditors and regulatory agencies strengthens the fight against cryptocurrency fraud in Nigeria.					

Section C: Blockchain Analytics and Forensic Tools (BFE)

S/N	Statement	SA	A	U	D	SD
6	Blockchain analytics can accurately trace cryptocurrency transaction flows.					
7	Digital forensic tools (e.g., Chainalysis, CipherTrace) are effective in identifying crypto wallet addresses.					

8	Real-time blockchain monitoring improves the detection of suspicious cryptocurrency activities.					
9	Integration of forensic tools into EFCC investigations has reduced the complexity of crypto-related cases.					
10	Blockchain analytics improves the recovery of illicitly transferred cryptocurrency assets..					

SECTION D: Challenges in Investigating Cryptocurrency Crimes (CH)

S/N	Statement	SA	A	U	D	SD
11	Lack of technical expertise limits the effectiveness of forensic auditing in cryptocurrency cases					
12	Insufficient funding and forensic infrastructure hinder crypto investigations.					
13	Regulatory loopholes make it difficult to prosecute cryptocurrency-related crimes.					
14	. Rapid technological changes in blockchain outpace the EFCC's investigative capabilities.					
15	Limited international cooperation slows down the investigation of cross-border cryptocurrency crimes					

SECTION E: Regulatory Integration and Compliance (RI)

S/N	Statement	SA	A	U	D	SD
16	Integrating forensic auditing into Nigeria's AML framework improves regulatory compliance.					
17	Collaboration between EFCC and other financial regulators strengthens cryptocurrency fraud detection.					

18	Strong regulatory policies encourage the adoption of forensic auditing in cryptocurrency investigations.					
19	Regular forensic auditing reports help policymakers address cryptocurrency-related risks.					
20	Enforcing mandatory cryptocurrency exchange audits enhances transparency and reduces money laundering risks.					

THANK YOU