# A STUDY ON THE ROLE OF TRANSACTION MONITORING IN THE DETECTION AND PREVENTION OF CRYPTOCURRENCY FRAUD AND MONEY LAUNDERING: IMPLICATIONS FOR FRAUD MONITORING PROFESSIONALS

by

George Antoine Helou, BSc. (Econ), MSc., MBA

DISSERTATION

Presented to the Swiss School of Business and Management Geneva

In Partial Fulfilment

Of the Requirements

For the Degree

DOCTOR OF BUSINESS ADMINISTRATION

SWISS SCHOOL OF BUSINESS AND MANAGEMENT GENEVA

April, 2024

A STUDY ON THE ROLE OF TRANSACTION MONITORING IN THE DETECTION AND PREVENTION OF CRYPTOCURRENCY FRAUD AND MONEY LAUNDERING: IMPLICATIONS FOR FRAUD MONITORING PROFESSIONALS

by

George Antoine Helou

Supervised by

Prof. Dr. Dragan Peraković, Ph.D.

APPROVED BY

Dissertation chair

RECEIVED/APPROVED BY:

Admissions Director

## Dedication

This work is dedicated to my lord and saviour Jesus of Nazareth.

**Acknowledgement**

I would like to express my sincere appreciation to my thesis supervisor Prof. Dr. Dragan Peraković, for his expert guidance throughout the research process. My thanks also go to the research participants who were extremely helpful to me during the data collection phase.

# ABSTRACT

## A STUDY ON THE ROLE OF TRANSACTION MONITORING IN THE DETECTION AND PREVENTION OF CRYPTOCURRENCY FRAUD AND MONEY LAUNDERING: IMPLICATIONS FOR FRAUD MONITORING PROFESSIONALS

George Antoine Helou

2024

Dissertation Chair: Dr. Iva Buljubašić, Ph.D.

Co-Chair: Dr. Ljiljana Kukec, Ph.D.

Given the anonymity and unregulated nature of financial transactions, money laundering and cryptocurrency fraud are a growing problem in the financial industry. Numerous studies have acknowledged this fact and advocated a complex socio-technical approach to improve the understanding of cryptocurrency-related crimes and risk assessment. However, the proliferation of cryptocurrencies has made it more difficult to combat these crimes. As most virtual currencies and other digital assets offer pseudo anonymity and operate in a decentralised manner, the effectiveness of tools and techniques to detect and prevent money laundering and cryptocurrency fraud has also been questioned. Therefore, this study assesses the effectiveness of rule-based and behaviour-based transaction monitoring tools, emphasises the importance of cooperation between financial institutions and regulators, highlights the fundamental differences between traditional and modern fraud detection tools, and offers recommendations for fraud monitoring professionals. The study uses a mixed methods approach, collecting qualitative data from eleven secondary sources and quantitative data through questionnaires distributed to twelve participants. The results of the study

show that while rule-based monitoring is essential for national regulators, over-reliance on this method leads to low fraud detection and high false positive rates. On the other hand, behaviour-based monitoring techniques were more effective and improved detection rates due to their low false positive rate. The study found that cooperation and collaboration between crypto developers, financial institutions and regulators is crucial to foster innovation and ensure the safety of investors and other stakeholders. In addition, the study found that traditional tools to prevent money laundering and fraud related to cryptocurrencies are insufficient, whereas modern tools such as graph methodology are effective in detecting criminal patterns and fraudulent transactions. It has therefore been suggested that the banking and financial sector adopt a multi-layered approach to transaction monitoring that includes a combination of traditional and modern tools, as well as rule-based and behaviour-based monitoring methods.

**Keywords:** Cryptocurrency, Money Laundering, Fraud, Transaction Monitoring, Fraud Monitoring Professional

TABLE OF CONENTS

LIST OF TABLES AND FIURES ..... ix

CHAPTER I: INTRODUCTION ..... 1

1.1 Introduction ..... 1
1.2 Overview of Cryptocurrency and Money Laundering ..... 1
1.3 Importance of Transaction Monitoring in Detecting and Preventing Cryptocurrency Fraud and Money Laundering ..... 3
1.4 Statement of the Research Problem ..... 3
1.5 Research Questions ..... 4
1.6 Hypothesis Formulation ..... 5
1.7 Significance of the Research ..... 5
1.8 Research Objectives and Contributions ..... 6
1.9 Significance of the Research Objectives ..... 6
1.10 Structure of the Dissertation ..... 7

CHAPTER II: LITERATURE REVIEW ..... 8

2.1 Introduction ..... 8
2.2 Theoretical Framework ..... 11
2.3 Transaction Monitoring ..... 11
2.4 The Current State of Transaction Monitoring In the Traditional Banking and Financial Sector ..... 13
2.5 The Effectiveness of Transaction Monitoring In Detecting and Preventing Cryptocurrency Fraud and Money Laundering ..... 15
2.6 Ethical Considerations for Detecting and Preventing Cryptocurrency Fraud and Money Laundering ..... 20
2.7 Recommendations for Increasing the Effectiveness of Detecting and Preventing Money Laundering and Cryptocurrency Fraud ..... 23
2.8 Literature Gap ..... 25
2.9 Summary of the Literature Review ..... 26

CHAPTER III: RESEARCH METHODOLOGY ..... 28

3.1 Overview of the Research Problem ..... 28
3.2 Research Method ..... 28
3.3 Research Design ..... 29
3.4 Research Philosophy ..... 29
3.5 Justification of Research Design and Research Method ..... 30
3.6 Research Design Limitations ..... 32
3.7 Data Collection ..... 33
3.8 Data Analysis ..... 35
3.9 Ethical Considerations ..... 37
3.10 Chapter Summary ..... 37

CHAPTER IV: RESULTS AND FINDINGS ..... 39

4.1 Introduction ..... 39
4.2 Presentation and Analysis of the Collected Primary Data ..... 39
4.3 Presentation and Analysis of Collected Secondary Data ..... 55
4.4 Summary of Results and Findings ..... 62

CHAPTER V: DISCUSSION OF RESEARCH QUESTIONS ..... 64

5.1 Discussion of Research Question One ..... 64
5.2 Discussion of Research Question Two ..... 66
5.3 Discussion of Research Question Three ..... 69

CHAPTER VI: CONCLUSION AND RECOMMENDATIONS ..... 72

6.1 Summary of Main Results and Findings ..... 72
6.2 Implications for Practitioners ..... 73
6.3 Recommendations for Banking and Financial Institutions ..... 74
6.4 Recommendations for Future Research ..... 76
6.5 Limitations of the Study ..... 77
6.6 Conclusion ..... 78

REFERENCES ..... 79

APPENDICES ..... 89

APPENDIX A: QUESTIONNAIRE ..... 89

APPENDIX B: CONSENT FORM ..... 94

APPENDIX C: PARTICIPANT'S DETAILS ..... 95

APPENDIX D: INPUT DATA ..... 97

LIST OF TABLES AND FIGURES

Figure 1: Estimated cost of cybercrime worldwide (in trillion US Dollars)……. 2

Table 1: Inclusion/Exclusion Table ..... 35
Table 2: Gender ..... 40
Table 3: Age Statistics ..... 41
Table 4: Age ..... 41
Table 5: Education Level ..... 42
Table 6: Paired Samples Statistics ..... 43
Table 7: Paired Samples Correlations ..... 44
Table 8: Paired Samples Effect Sizes ..... 45
Table 9: Variables Entered/Removed ..... 47
Table 10: Model Summary ..... 48
Table 11: ANOVA ..... 49
Table 12: Coefficients ..... 50
Table 13: Paired Samples Statistics ..... 51
Table 14: Paired Samples Correlations ..... 52
Table 15: Paired Samples Test ..... 53
Table 16: Paired Samples Effect Sizes ..... 54
Table 17: Sources and Coded Themes ..... 55

# LIST OF ABBREVIATIONS

P2P – Peer-to-Peer

DeFi – Decentralised Finance

AML – Anti-Money Laundering

GBAD – Graph-Based Anomaly Detection

VPN – Virtual Private Network

RBA – Risk-Based Analysis

FATF – Financial Action Task Force

AML/CFT – Anti-Money Laundering and Counter-Terrorist Financing

FCA – Financial Conduct Authority

FIUs – Financial Intelligence Units

SC – Supply Chains

LOF – Local Outlier Score

ML – Machine Learning

AIDS – Artificial Intelligence and Data Science

AI – Artificial Intelligence

ACM – Association for Computing Machinery

# CHAPTER I: INTRODUCTION

## 1.1 Introduction

With the increasing use of cryptocurrencies, national and international regulators are becoming more concerned. According to Lin et al. (2022), blockchain is an open and distributed ledger technology that operates in a peer-to-peer (P2P) network using a consensus-based methodology. Furthermore, most blockchain frameworks are open, decentralised, anonymous and autonomous. Soana (2021) referred to blockchain tools as state-of-the-art money laundering tools. Furthermore, Kuperberg, Kemper and Durak (2019) found that regulations for non-fungible tokens (NFTs) and decentralised finance (DeFi) have not been adequately implemented. Money laundering and criminal activities are exacerbated by the lack of clear regulations for NFT and DeFi protocols. In this context, there is a need to evaluate transaction monitoring systems to combat the increase in illicit money laundering.

## 1.2 Overview of Cryptocurrency and Money Laundering

In 2009, a new class of digital currencies known as cryptocurrencies emerged. Oana Florea and Nitu (2020) and Spohn (2018) highlighted Bitcoin as the first cryptocurrency created by Satoshi Nakamoto. According to the findings, Bitcoin and other cryptocurrencies have undergone a significant transformation over the past decade. By creating a currency that is not backed by permits, laws or secret transfers, this transformation has made a significant contribution to the traditional financial sector. Dziura, Jaki and Rojek (2020) extend the findings of Oana Florea and Nitu (2020) and Spohn (2018) by noting that criminals have been quick to recognise and acknowledge the unique features of cryptocurrencies that allow them to evade law enforcement. Users of cryptocurrencies adopt pseudonyms; consequently, transactions take place without

intermediaries and can cross international borders. Also according to Wegberg, Oerlemans and Van Deventer (2018), Bitcoin facilitates digital financial crime. Cybercriminals are primarily motivated by anonymity, ease of use and freedom from laws and borders. Figure 1 shows projections from Statista's Cybersecurity Outlook (Fleck, 2022). The global cost of cybercrime is projected to increase from $8.44 trillion in 2022 to $23.84 trillion in 2027 (Fleck, 2022). According to Pagano and Sedunov (2018), Bitcoin is becoming an increasingly valuable asset for criminal organisations. For example, cybercriminals demand that ransomware victims convert their funds from fiat currency to Bitcoin and send them to a specific Bitcoin address. Bitcoin is used to trade large quantities of illegal goods such as weapons and drugs on the black market. In this context, the findings suggest that the rise and acceptance of cryptocurrencies has contributed significantly to the increase in cybercrime.

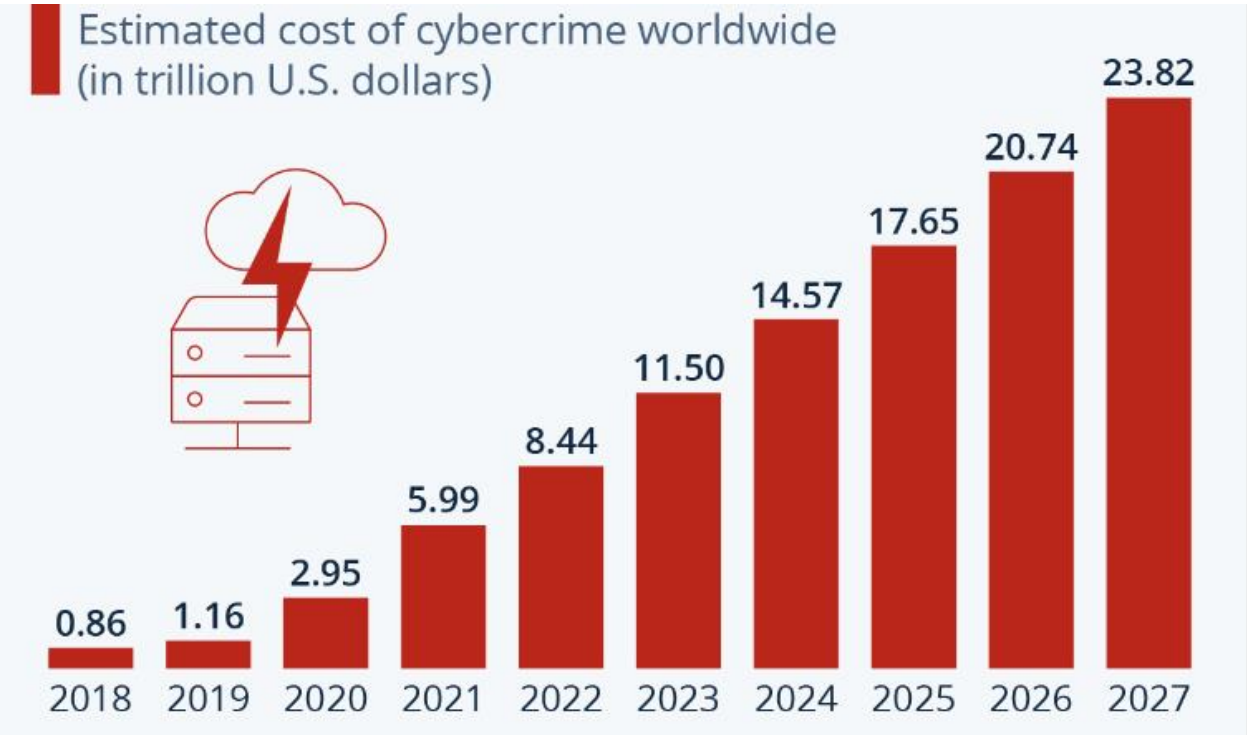


**Figure 1:** Estimated cost of cybercrime worldwide (in trillion US Dollars) (Source: Fleck, 2022)

### 1.3 Importance of Transaction Monitoring in Detecting and Preventing Cryptocurrency Fraud and Money Laundering

Commercial banks and other traditional financial institutions implement anti-money laundering (AML) frameworks to prevent money laundering by identifying the associated risks, transactions and money launderers. First, Han et al. (2020) suggest that financial institutions conduct their business in a way that can withstand scrutiny by third parties, such as shareholders, regulators, customers and governments. Turki et al. (2020), for example, extend the findings of Han et al. (2020) by suggesting that more emphasis should be placed on the integration of government information sources and less on gaps in data collection due to manual processes. In addition, transaction monitoring enhances analytical and technologically advanced procedures for verifying transactions in the financial sector. Ilijevski, Ilik and Babanoski (2023), like Turki et al. (2020), note that in 2021 the European Commission presented a comprehensive package of legislative proposals to strengthen anti-money laundering and anti-terrorism rules in the financial sector. The legislative package aimed to enhance programmes to detect suspicious activities and transactions in order to close the gaps in cyberspace that cybercriminals exploit for money laundering and terrorist financing. These legislative proposals establish a coherent financial framework to improve compliance with financial rules on combating terrorism and money laundering for certain economic operators, in particular individuals conducting cross-border transactions.

### 1.4 Statement of the Research Problem

Due to the lack of regulation and the anonymity of cryptocurrencies, money laundering and cryptocurrency fraud pose a significant problem for the financial industry. Desmond, Lacey

and Salmon (2019) and Avhustova (2018) consider the cryptocurrency process to be a sophisticated socio-technical system. Desmond, Lacey and Salmon (2019) observed a lack of literature examining money laundering and cybercrime within cryptocurrencies using a complex sociotechnical framework approach to evaluate how regulators, criminals and law enforcement understand processes and assess risks within cryptocurrency frameworks. The results suggest that adopting this methodology to evaluate cryptocurrency and cybercrime research would likely improve criminal risk assessments and understanding of risk management processes. According to Vassallo, Vella and Ellul (2021), the recent emergence of numerous cryptocurrencies has further complicated the fight against crime. Cryptocurrencies do not require a central authority and offer pseudo-anonymity to their users. Therefore, criminals can pose as legitimate customers. Nevertheless, monitoring transactions is an important method and tool for detecting and preventing cryptocurrency fraud and money laundering. For this reason, it is important to examine the role of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering, and to highlight the implications for fraud monitoring professionals.

### 1.5 Research Questions

1. How effective are rule-based transaction monitoring and behaviour-based transaction monitoring in detecting and preventing cryptocurrency fraud?
2. How does cooperation between regulators and financial institutions affect the effectiveness of transaction monitoring?
3. How do modern technological fraud detection tools differ from traditional fraud detection tools?

## 1.6 Hypothesis Formulation

**$H_1$:** Common rule-based and behaviour-based transaction monitoring frameworks detect and prevent cryptocurrency fraud.

**$H_0$:** Common rule-based and behaviour-based transaction monitoring frameworks are not able to effectively detect and prevent cryptocurrency fraud.

**$H_2$:** The performance of transaction monitoring practices is improved when regulators and financial institutions work together.

**$H_0$:** The performance of transaction monitoring practices is not improved when regulators and financial institutions work together.

**$H_3$:** Modern transaction monitoring tools are superior to traditional tools and methods.

**$H_0$:** Traditional transaction monitoring tools are superior to modern alternatives.

## 1.7 Significance of the Research

This study is of practical value as it provides insights and recommendations for those involved in the prevention of financial crime related to cryptocurrencies. It is the responsibility of financial institutions such as banks and cryptocurrency exchanges to implement effective transaction monitoring systems to prevent financial crime. This study will provide recommendations for banking and financial institutions to improve their fraud prevention strategies with regards to cryptocurrency transaction monitoring. This study will also explore the legal framework for cryptocurrency transaction monitoring to help formulate financial crime prevention policies and guidelines. This research will also contribute to the development of theoretical models and frameworks for understanding the role of transaction monitoring in detecting and preventing financial crime in the cryptocurrency space.

## 1.8 Research Objectives and Contributions

This study aims to investigate the effectiveness of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering, and to provide recommendations for fraud monitoring professionals to improve their fraud detection capabilities.

Other objectives include:

1. Assess the techniques and tools commonly used to monitor transactions in the financial sector.
2. Assess the impact of cooperation and communication on the efficiency of regulators and financial institutions.
3. Provide recommendations for efficient transaction monitoring systems to detect and prevent cryptocurrency fraud and money laundering.
4. Provide implications for fraud monitoring professionals.

## 1.9 Significance of the Research Objectives

Examining commonly used transaction monitoring tools and techniques is critical to identifying the best areas and practices for improving the detection of fraudulent behaviour and thus developing more effective transaction monitoring systems that lead to more secure financial transactions. In order to develop more effective approaches and strategies to prevent money laundering and other cybercrimes, it is essential to assess how financial institutions and regulators are adapting to new transaction monitoring practices. It is important to assess the role of communication and cooperation in improving the efficiency of regulatory and financial institutions, as financial fraud is usually cross-border and requires cooperation between regulators.

On the other hand, it is important to recommend efficient transaction monitoring frameworks to develop more effective ones. This can enable financial systems to improve regulations to prevent financial crime and thus protect the integrity of financial systems. Finally, fraud monitoring professionals can be equipped with the necessary fraud detection capabilities to lead the appropriate decision-making processes to improve fraud monitoring systems.

### 1.10 Structure of the Dissertation

The dissertation is divided into six chapters. The first chapter discusses the context and importance of transaction monitoring for the detection and prevention of cryptocurrency fraud and money laundering. The second chapter reviews the literature and the literature gap that needs to be assessed. The third chapter describes the research methodology, which includes the research method, design and philosophy. In addition, this chapter justifies the chosen methodological research process. Chapter four presents the qualitative and quantitative findings of the study. In chapter five, the results and broader literature are evaluated. Chapter six presents the conclusions of the study, including recommendations and implications for fraud monitoring professionals.

# CHAPTER II: LITERATURE REVIEW

## 2.1 Introduction

### 2.1.1 General topic and its significance

This study examines the role of transaction monitoring in the detection and prevention of cryptocurrency fraud and money laundering. The transaction monitoring study can help financial industry professionals understand the importance of these systems and their role in regulatory compliance and financial crime prevention. It can also help professionals understand the different techniques and technologies used in transaction monitoring and how they can implement and maintain these systems in their organisations. Identifying common frauds affecting financial institutions such as cryptocurrency exchanges or banks can help prevent the spread of fraud and money laundering. Secondly, the types of fraud that lead to the greatest financial losses were identified. This enabled the identification of future research directions with significant practical implications for market participants. These include the need to develop and implement modern computer applications that enable the detection of a wider range of emerging abuses.

### 2.1.2 Prevailing trends and perspectives

Current trends suggest that cryptocurrencies are vulnerable to financial fraud and money laundering despite their limited global development. Similarly, Kutera (2022) and Pourhabibi et al. (2020) found that most traditional financial systems lack research and development on security issues related to cryptocurrency fraud. Based on Kutera's (2022) and Pourhabibi et al.'s (2020) assessment of the analogy between the traditional financial system and cryptocurrency fraud, Wan, Xiao and Zhang's (2022) observation is that a lot of attention is paid to illegal cryptocurrency transactions, especially phishing scams that result in significant losses to individuals. Pourhabibi

et al. (2020) proposed a graph-based anomaly detection (GBAD) strategy that primarily focuses on the interdependencies between different object data targets in the context of machine learning and data mining techniques. Financial institutions have increasingly adopted this strategy to assess network connectivity and relationship patterns that reveal unusual patterns.

The findings suggest that the rapid growth of cryptocurrencies has led to a significant increase in illicit activity. Despite the existence of advanced technological measures, there is a lack of technological advances in terms of effective transaction monitoring. Existing techniques, such as GBAD, have proven useful in assessing fraudulent activity throughout the network system. As technology advances, despite promising fraud detection techniques, new technologies are being introduced to facilitate financial fraud, such as virtual private networks (VPNs). Hu and Xu (2021) and Katterbauer, Syed and Cleenewerck (2022) are pessimistic that technological advances will contribute to an increase in financial fraud. Katterbauer, Syed and Cleenewerck (2022) examined VPNs, while Hu and Xu (2021) studied smart contracts. From a broader perspective, Hu and Xu (2021) assess the increased crime rates on Ethereum as a result of the popularity of smart contracts, such as the Parity Wallet Hack in 2017 and the DAO attack in 2016, which resulted in a loss of around US$400 million in revenue. More recently, the financial security of Ethereum smart contracts has led to less damaging but more covert financial scams, such as honeypots and Ponzi schemes masquerading as certified smart contracts. Katterbauer, Syed and Cleenewerck (2022) come to a similar conclusion in a similar line of research: The use of VPN can facilitate criminal activity. The technological advances in cryptocurrencies thus have both positive and negative consequences.

### 2.1.3 Scope of the literature review

The purpose of this literature review is to assess the role of transaction monitoring in the detection and prevention of cryptocurrency fraud and money laundering by comparing and contrasting the findings of the relevant literature. The purpose of the literature review is also to identify key areas of agreement and disagreement in cryptocurrency fraud research. The purpose of this literature review is to identify recurring themes and theories that are central to the transaction monitoring debate and to the evaluation of cryptocurrency fraud. Consequently, the purpose of this literature review is to identify a research gap that highlights areas in need of further investigation.

### 2.1.4 Overview of the structure of the literature review

The study identifies the following primary research areas. First, the primary theoretical framework guiding the literature review is presented. The concept of transaction monitoring is then critically assessed. Second, the current state of transaction monitoring is assessed through a critical analysis of the traditional financial sector. Furthermore, this literature review assesses the effectiveness of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering. In this context, the ethical implications of transaction monitoring systems and frameworks for cryptocurrencies were examined. To achieve its objectives, the study proposes strategies and techniques to improve money laundering and cryptocurrency fraud detection systems. Gaps in the literature were identified in the conclusion of the literature review section.

## 2.2 Theoretical Framework

Risk-based analysis (RBA) has been used to assess the role of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering. While Vovk et al. (2020) and Savona and Riccardi (2019) demonstrated the importance of RBA as an effective technique recommended by the FATF, Sinha (2019) argued that RBA cannot fully compensate for the limitations of the rule-based approach. In particular, Vovk et al. (2020) noted that the RBA evaluates primary financial monitoring entities based on their ability to identify, assess and understand risks and take effective action to mitigate them. Similarly, Savona and Riccardi (2019) noted that FATF Recommendation 1 calls for anti-money laundering (AML) measures that are proportional to fraud risk; low fraud risks requiring fewer AML measures than high money laundering risks. Sinha (2019) examines the RBA at two levels, in contrast to the findings of Vovk et al. (2020): He assesses the definition and application of risk in light of recent legislative changes and highlights the contradiction between the view of the legal basis of the RBA and the Financial Conduct Authority's (FCA) plans for its implementation. In this respect, the RBA has not fully compensated for the limitations of the rule-based approach. However, it has created a culture of "ticking off" among financial institutions, as evidenced by the increased FCA sanctions. As a result, while the RBA is an important part of the financial system, it does not have the necessary features to fully compensate for the limitations of the rule-based approach.

## 2.3 Transaction Monitoring

To ensure data security within blockchain technology, financial systems monitor blockchain transactions. Amudha (2021) observed efficient transaction monitoring in Blockchain transactions, while Jin et al. (2022) detected fraud in smart contracts using Blockchain technology.

For example, Amudha (2021) proposed to retrieve user data through transaction monitoring for time and ID-based processing. As such, fraud monitoring professionals request customer data and the server retrieves it by matching it with the blockchain. RBA incorporates cryptographic techniques to protect blockchain transactions from malicious blockchain users. Jin et al. (2022) disagree with Amudha's (2021) concept of effective transaction monitoring systems, arguing that smart contracts facilitate fraudulent schemes and that Ethereum is beneficial to fraudsters. Most transaction monitoring systems have two major limitations: limited technological methods for timely early warnings and the inability to integrate data from multiple sources, resulting in an inefficient and outdated transaction monitoring system. Similar to Jin et al.'s (2022) perspective on limited transaction monitoring systems, Murko and Vrhovec (2019) suggest that fraud wallet services resemble online wallets and increase the anonymity of transactions, facilitating the skimming of certain cryptocurrency transfers. Therefore, by providing user data information, the blockchain-based transaction monitoring system can effectively detect and prevent fraudulent transactions. However, fraudulent cryptocurrency wallets and smart contracts continue to hinder the detection of cryptocurrency fraud and money laundering.

In this regard, the RBA framework makes the transaction monitoring process more flexible. Similarly, Ansari (2018), Chao et al. (2019) and Oztas et al. (2022) have considered the flexibility of the RBA framework when assessing the risk characteristics of cryptocurrency users. According to Ansari (2018), it is first necessary to assess the risk of the customer, classify the customer as low-risk or high-risk, and then decide whether to execute the requested financial transaction. According to Oztas et al. (2022), AML aims to reduce instances of money laundering through the implementation and enforcement of laws, regulations and techniques. The FATF also aims to detect

and prevent fraudulent activities. The FATF's RBA framework allows financial institutions to focus primarily on due diligence and transaction monitoring. Moreover, the classification algorithms of Chao et al. (2019) are component systems for transaction monitoring that assess abnormal behaviour. The algorithm classifies the dataset by evaluating class labels with a surveillance classification technique that effectively improves transaction monitoring systems. The RBA therefore enables FATF and AML regulations to improve transaction monitoring.

## 2.4 The Current State of Transaction Monitoring In the Traditional Banking and Financial Sector

Collaborative model. Coordination and communication between users, often facilitated by technology, is outlined in the collaborative model. Accordingly, Hasham, Joshi, and Mikkelsen (2019) and Katterbauer, Syed, and Cleenewerck (2022) found that financial institutions such as cryptocurrency exchanges and banks strive to provide sophisticated services and products by effectively coordinating their financial activities. In general, the coordination strategy yields greater returns than the traditional supply chain. First, Hasham, Joshi and Mikkelsen (2019) argue that the collaborative model maintains the status quo, where cybersecurity, fraud and financial crime each maintain independent responsibilities, roles and reporting. Each area establishes its own paradigm, collaborates and coordinates risk taxonomy and analytics for transaction breaches, fraud and surveillance. According to Katterbauer, Syed and Cleenewerck (2022), the collaborative model requires the autonomy of the cybersecurity, fraud and financial crime departments and their respective tasks and roles. Each department uses its own framework, risk taxonomy, analytics and data to monitor transactions, fraudulent activity and other vulnerabilities. A disadvantage of this

strategy is that it limits exposure to financial crime risks and can lead to gaps in coverage and overlap of groups. Integration is also somewhat limited.

Moreover, the collaborative model uses RBA to integrate and modify heuristic transaction monitoring arrangements within traditional financial institutions. Ansari (2018) and Um and Kim (2019) investigated the process of embedding and adapting RBA for effective fraud detection and prevention in traditional financial institutions. Ansari (2018) found that RBA promotes the embedding of knowledge based on monitoring and adjusting perceived differences for knowledge based on the differences of others. Um and Kim (2019) concluded that RBA promotes a resource-based perspective that maintains competitive advantage and sustainability by leveraging external resources. RBA requires an all-encompassing systemic framework that governs AML to support comprehensive decision-making processes. Furthermore, the incorporation of idiosyncratic resources from external entities results in valuable and exclusive services in transaction monitoring systems, enhancing the security of traditional financial institutions.

By integrating electronic networks, robust business models and cyberspace, traditional financial institutions are evaluating their corporate communication and collaboration with their customers, stakeholders and investors. Lakshmi et al. (2020), Hasham, Joshi and Mikkelsen (2019) and Li et al. (2020) have observed the benefits of transparency in cyberspace. For example, Lakshmi et al. (2020) suggested that the intranet continuously manages critical information and enables an immediate flow of internal information and a data flow of external financial payments, which is consistent with the reliability and effectiveness of an organisation's operations. Furthermore, Hasham, Joshi and Mikkelsen (2019) note that while financial regulators are aware

of the concept, it does not provide banks and other financial institutions with sufficient transparency to fully assess the risk of financial crime. Moreover, the collaborative model often leads to gaps in coverage or overlaps between categories, and it ignores the scalability benefits of broader functional integration. Because the strategy relies on smaller, autonomous units, banks are less able to recruit top talent. Li et al. (2020) note that many organisations are deploying collaborative intrusion detection networks (CIDNs) to protect their resources and improve detection performance. However, these detection techniques and systems are often vulnerable to insider attacks, which requires the implementation of appropriate security protocols.

### 2.5 The Effectiveness of Transaction Monitoring In Detecting and Preventing Cryptocurrency Fraud and Money Laundering

Partially integrated model for fraud monitoring, financial crime and cybersecurity. Using a partially integrated model and a unified model, the effectiveness of cryptocurrency transaction monitoring was evaluated. First, Hasham, Joshi, and Mikkelsen (2019) and Katterbauer, Syed, and Cleenewerck (2022) discovered that monitoring is implemented as a secondary layer of security in accordance with a predetermined set of regulations. According to Hasham, Joshi and Mikkelsen (2019), in the partially integrated model, each entity maintains its independence but operates within a unified structure and taxonomy and adheres to commonly agreed rules and obligations. As a result, a unified framework for prevention (customer authentication) is established, risk identification and assessment processes (especially taxonomies) are standardised, and identical interdiction techniques are used.

In this context, many financial institutions are evaluating a model that primarily integrates fraud, financial crime and cyber security as a secondary line of defence. Benefits include centralised risk identification and monitoring, as well as a reduced likelihood of security breaches and duplication of effort. The technology is compatible with the current organisational structure and does not interfere with business operations. As long as independent reporting is maintained, there is no improvement in transparency. Moreover, as operational departments remain smaller, there are no scalability benefits and the model is less attractive to top staff. Katterbauer, Syed and Cleenewerck (2022) agree with Hasham, Joshi and Mikkelsen (2019) that departments can retain autonomy while adhering to a single standard and taxonomy. Some established standards and regulations are followed. Therefore, a single framework for prevention, risk assessment and risk evaluation procedures is needed. Cociug and Andrtsceac (2020) argue that the current organisational framework does not increase transparency despite the uniformity of risk identification and monitoring. Moreover, there are few economies of scale, which complicates operational system units. Moreover, a new strategy extends the scope of the RBA to cross-border risks. Cociug and Andrtsceac (2020) and Hasham, Joshi and Mikkelsen (2019) note that the EU anti-money laundering and counter-terrorist financing (AML/CFT) framework has introduced uniform guidelines on the direct powers and disclosure obligations of relevant financial actors, as well as a robust structure for EU financial intelligence units (FIUs) to assess fraudulent activities and cooperate with each other.

Financial institutions can promote the adoption of a collaborative model that enhances cybersecurity by adopting a model that is partially inclusive. First, Rejeb et al. (2021) claim that blockchain technologies have the potential to improve collaboration between transaction parties in

modern supply chains by accelerating information-sharing mechanisms, improving decision-making and incentive models, and facilitating communication between SC partners. Ali (2020) refutes Rejeb et al.'s (2021) claim that blockchain technology improves incentive and decision-making models by highlighting the shortcomings of Monero. Ali (2020) explains that Monero differs from other digital currencies in that it hides transaction values with ring signatures, increasing the level of privacy associated with these transactions. Monero aims to randomly shuffle the public keys of its users so that no one can identify a specific user. In addition, the Monero blockchain contains a unique algorithm that generates a wallet address that can only be accessed by the payee. Even with state-of-the-art monitoring technologies such as CipherTrace and Chainalysis, monitoring transactions via blockchain analytics is extremely difficult. Cybercriminals prefer Monero over other cryptocurrencies because it reduces the risk of law enforcement surveillance associated with most cryptocurrencies. Despite the attractive incentives offered by cryptocurrencies, they remain vulnerable to cybercrime due to inadequate law enforcement surveillance.

Prior to mutual evaluation within a country, differences in compliance are primarily due to differences in the level of preparedness for legal and regulatory requirements. Murrar (2021) noted that the UK has fully implemented the FATF guidelines, while Bahrain and Russia have only partially implemented them. Accordingly, Stojanovi et al. (2021) and Oztas et al. (2022) found that most financial institutions use rule-based solutions for transaction monitoring, where experts set the rules. It is estimated that over 95% of reported transactions are false positives, which is costly and time-consuming for financial institutions. According to Oztas et al. (2022), the local outlier factor (LOF) was originally developed for relatively high-dimensional datasets. A local outlier

score (LOF) is calculated to measure the local irregularity of an element observation (rather than globally for the whole dataset). The procedure is local in the sense that the LOF score of each object considers only a specific locality. Despite the limitations of the partially integrated model, the concepts developed, including LOF, improve the assessment of irregularities in illicit financial activities and processes.

Unified model for fraud monitoring, financial crime and cybersecurity. The comprehensive unified model integrates financial crime, cybersecurity and fraud monitoring activities into a single framework with common risk management systems and assets, according to Hasham, Joshi and Mikkelsen (2019) and Katterbauer, Syed and Cleenewerck (2022). Hasham, Joshi and Mikkelsen (2019) highlight the model's unified customer perspective and distributed analytics. Risk convergence improves enterprise-wide threat visibility by highlighting key underlying risks. In addition to achieving economies of scale for key components, the unified model improves the bank's ability to attract and retain the most talented people. A weakness of the paradigm is the extensive organisational changes that make bank operations seem foreign to bank regulators. Financial risks remain different despite organisational changes and risk convergence. Similarly, Katterbauer, Syed and Cleenewerck (2022) concluded that the unified model leads to the management of common assets and systems through which all organisational risks are managed. Furthermore, it enables a single view of clients and the sharing of analytics as well as improved enterprise-wide threat visibility and risk identification. Common techniques for identifying hacking assets use machine learning (ML) algorithms such as SVM and K-Means, as well as topic modelling, deep learning and keyword search, according to Ebrahimi et al. (2022). In contrast to the positive assessment of transaction monitoring under a unified model by Katterbauer, Syed and

Cleenewerck (2022), Cheau et al. (2020) found that relatively few companies insure against the risk of data degradation or privacy compromise, as well as the risk of volatility of cryptocurrencies. A financial market can be manipulated through the fraudulent dissemination of information packages, coordinated participation in quotations and the falsification of indicators.

General Adversarial Networks. General Adversarial Networks improve cryptocurrency unit classification and fraud detection in transaction monitoring systems. Zola (2022) and Cao (2020) present transaction monitoring systems enhanced by General Adversarial Networks. For example, Zola (2022) stated that transaction monitoring models and personnel can use R-Hybrid and SM-Hybrid to improve entity categorisation accuracy, especially for GCNs. Models evaluated on datasets pre-processed with SM-Hybrid showed the highest classification efficiency of the two techniques, suggesting that new synthetic behaviours facilitate the learning process of ML techniques. Cao (2020) found that artificial intelligence and data science (AIDS) techniques such as probabilistic modelling, risk analysis, clustering, sequential modelling, behavioural modelling, event analysis, semi-supervised learning, classification, reinforcement learning and deep neural models are able to manage the financial risks associated with financial services, systems, instruments, markets and participants in terms of specific and general business tasks, objectives and problems. R-Hybrid, SM-Hybrid and AIDS techniques improve the effectiveness of cryptocurrency fraud detection and prevention by identifying malware that would otherwise affect accounts, resulting in unusual activity and suspicious transactions. Despite the effectiveness of the collaborative, partially integrated and unified models in detecting financial fraud and money laundering, gaps caused by human resources and disruptive technologies still need to be addressed.

## 2.6 Ethical Considerations for Detecting and Preventing Cryptocurrency Fraud and Money Laundering

Emerging ethical issues are already impacting the work of computer scientists who use machine learning to solve problems, forcing them to make difficult decisions. The implementation of ML algorithms has repeatedly emphasised the need to take ethical considerations into account. Therefore, Dierksmeier and Seele (2019) and Engin et al. (2020) argue that personal and social factors need to be considered when implementing technological innovations in transaction monitoring. Personal factors include data ownership and control, and accessibility to digital services. Ethical considerations from a social perspective focus on information symmetry and data access rights, including data manipulation. In this context, Dierksmeier and Seele (2019) note that blockchain proponents emphasise the potential for more transparent supply chains. Some blockchain operators, such as VeChain, IBM and Circular, combine supply chain management with blockchain's smart contract capabilities. Supply chain components are interconnected and equipped with radio frequency identification chips or other tracking devices that can be accessed remotely. Müller (2021), citing Dierksmeier and Lake (2019), concludes that companies advocate the use of AI because they need to adapt to a dynamic environment characterised by innovation, development and automation. To be successful, businesses need to become more adaptable, use technology effectively and innovate continuously. Continuous adaptation enables companies to act in a more socially responsible manner by helping to detect and even prevent fraudulent activities both within the company and with third parties. In this regard, ethical risk assessment effectively prepares companies for future regulations and innovations. Dierksmeier and Seele (2019) and Müller (2019) identify democratic and ethical considerations as well as technological innovation. Democratic and ethical considerations include the following: economic considerations (including

income distribution and business practices such as taxation of technological services), customer rights (including transparency and privacy, manipulated consumer behaviour and automated recommendations), regulatory issues related to accountability and legitimacy of algorithmic solutions in public decision-making, cognitive changes such as technological singularity, and social considerations. It is therefore essential to consider social and personal perspectives when analysing publicly disclosed transactions.

However, the ethical significance of transaction monitoring in detecting fraud goes beyond the social and economic consequences of its application in the real world. The emphasis on ethics in transaction monitoring necessitates the development of new methods for ethical impact. Ali (2020) and Braaten and Vaughn (2019) emphasise points of exchange, including financial intermediaries. Professional and ethical considerations need to be developed for the management team. Next, Braaten and Vaughn (2019) introduced the convenience theory, which states that white-collar criminals have the opportunity to engage in illicit financial activities because of their professional role and social status. Business professionals such as accountants and lawyers, as well as corporate executives such as managing directors, board members, chief financial officers and chief executive officers, abuse their positions to commit white-collar crimes for personal or corporate gain. Similar to Braaten and Vaughn (2019), Ali (2020) noted that exchange points are critical in determining whether corporate officials launder money, whether criminals launder money, or whether criminals use cryptocurrencies to commit fraud. Therefore, anti-money laundering laws and regulations must also apply to exchange points. These regulations include establishing a local presence to facilitate the exchange of cryptocurrencies and providing a platform for ethical institutions. These regulations are intended to help customers and law

enforcement agencies identify legitimate cryptocurrency transfers. Ultimately, customers will be able to recognise legitimate crypto assets.

The ethical aspects of the regulations for cryptocurrency transactions and financial institutions also need to be considered. Legal and ethical considerations focus on the legal implications of smart contracts, virtual assets, technological advances and personal data. In addition, Saltz et al. (2019) and Gerlick and Liozu (2020) explore the ethical considerations required for the successful adoption of disruptive algorithmic models in transaction monitoring. While Gerlick and Liozu (2020) focus on the training, testing and validation of ethical practices, Saltz et al. (2019) explore the potential drawbacks of adopting ethical practices in training. Gerlick and Liozu (2020) note that ethical control mechanisms are still evolving, with a focus on structured identification of critical risks, enterprise-level management and implementation of independent protocols within critical infrastructures. In this way, financial institutions can integrate controls to reduce the predictive power of algorithmic models while increasing transparency to enhance customer trust. Following Gerlick and Liozu's (2020) thinking on ethical adoption practices, Saltz et al. (2019) suggest that the traditional paradigm for integrating ethical considerations requires the use of a code of ethics, such as the Association for Computing Machinery (ACM) Code of Conduct and Ethics. The Code of Conduct was revised in 2018 as disruptive technological innovations have been recognised and the extent to which technological innovations are integrated into the social fabric and people's daily lives has changed significantly. However, the recently enacted ethical frameworks and codes are not sufficient to address the ethics of machine learning in transaction monitoring. Therefore, computer science professionals facing the challenges of transaction monitoring need to incorporate a broader range of ethical considerations.

## 2.7 Recommendations for Increasing the Effectiveness of Detecting and Preventing Money Laundering and Cryptocurrency Fraud

### 2.7.1 Existing challenges

Current recommendations to increase the efficiency of transaction monitoring focus on AI-based disruptive technologies and effective training techniques to improve the skills of banking and financial firms' employees. First, Stojanovi et al. (2021) and Vitvitskiy et al. (2021) note that the technical aspect of transaction monitoring is a major problem. For example, Vitvitskiy et al. (2021) point out that the negligence of banking and financial firms in conducting key verifications leads to a loss of customer credibility, inadequate regulatory frameworks that criminals exploit to commit cryptocurrency fraud, and corruption that leads to inadequate identification of cryptocurrency users when conducting online transactions, resulting in an increase in money laundering. Stojanovi et al (2021) noted that the lack of real-time processing in current transaction monitoring technologies renders fraud detection systems ineffective. In general, fraud detection methods based on manual transmissions are relatively ineffective. Detecting common fraud patterns requires significant time and resources, making fraud detection challenging. Abdallah (2022) agrees with Stojanovi et al. (2021) that the profiles of fraudulent and typical behaviours are usually dynamic. Existing data and knowledge about cryptocurrency fraud is usually unreliable and biased. Furthermore, suspicious cryptocurrency transactions are not reported immediately. Therefore, illegal cryptocurrency activities are only detected when a customer makes a report. As such, proposed solutions for existing transaction monitoring systems should focus on improving technological models and effective staff training.

### 2.7.2 Solving existing difficulties

Deep learning, outlier detection and artificial intelligence methods are proposed as solutions to current transaction monitoring problems. The efficiency of automated fraud detection depends on a sampling strategy that uses anomaly detection and variable selection techniques. Vassallo et al. (2021) and Bynagari and Ahmed (2021) propose the use of eXtreme Gradient Boosting (XGBoost), which evaluates evolving data streams subject to concept drift, along with generalised stacking that updates the underlying ensemble. While Vassallo et al. (2021) investigated the potential integration of decision tree-based generative gradient algorithms in line with effective hyperparameter data sampling and optimisation techniques, Bynagari and Ahmed (2021) evaluated the transformation of an evolving technology to adapt to growing datasets by integrating stacking that enables general fraud prediction. Consequently, the application of artificial intelligence (AI) techniques solves transaction monitoring problems. The use of AI-based predictive analytics paradigms that evolve in response to new user analytics and data points will strengthen established decision support paradigms.

The second recommendation relates to improving the skills and motivation of banking and financial firms' employees. While Nyrerod, Andreadakis and Spagnolo (2022) conclude that effective reward programmes improve transaction monitoring, Vitvitskiy et al. (2021) argue that the transaction monitoring framework requires improved training techniques. Nyrerod, Andreadakis and Spagnolo (2022) note that effective reward programmes are lenient for money laundering and witness protection, but not for offenders who have previously committed financial fraud. Moreover, reward programmes must be proportionate to the amount of work required to detect crimes. Therefore, the ceiling for money programmes should be higher than the provisions

set in the Kleptocracy Reward Programme. In contrast, Vitvitskiy et al. (2021) focused on permanent training programmes for financial audit specialists as well as fraud monitoring professionals and the development of investigative teams to investigate cryptocurrency fraud based on technological advances. In addition, financial experts and law enforcement officials need to be considered. Citing Nyrerod, Andreadakis and Spagnolo (2022) and Vitvitskiy et al. (2021), who focus on improving the level of competence and motivation of staff, Hairudin et al. (2020) emphasised the need for a regulatory body to amend and enact legal and moral standards and improve the establishment of necessary rules and regulations. A trade-off needs to be made between the level of international/national regulation and the level of independence within transaction monitoring networks to increase the overall security and scale of monitoring platforms.

### 2.8 Literature Gap

To broaden the scope of cryptocurrency fraud and AML research, illicit financial transactions such as terrorist financing, drug trafficking, bribery, corruption, identity theft, fraud and money laundering need to be investigated. In addition, the extent to which cryptocurrencies are monitored and regulated in each country where they are introduced needs to be researched. Since the concept of cryptocurrencies is frowned upon in most financial circles, it is even more important to determine what is ethical, illegal and immoral. To achieve a nuanced and fair ethical positioning of cryptocurrencies, it is necessary to evaluate ethical theories to include evidence of moral ambiguity.

## 2.9 Summary of the Literature Review

The purpose of this study is to evaluate the effectiveness of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering. By conducting a literature review, the research used RBA to evaluate, identify and understand the steps of transaction monitoring. In addition, transaction monitoring was assessed to determine the ability of the ID-based processing system to detect fraud and money laundering. As the study only examines cryptocurrency-based transactions, further research is required. In this regard, the study assessed the current state of transaction monitoring in traditional banking and financial institutions as well as cryptocurrency exchanges and the effectiveness of transaction monitoring in detecting cryptocurrency fraud. First, the study used a collaborative model in which traditional banking and financial institutions as well as cryptocurrency exchanges maintained the status quo in each area, including fraud, financial crime and cybersecurity. Second, the study included a partially integrated model for fraud, financial crime and cybersecurity, as well as a unified model to assess the effectiveness of transaction monitoring in detecting cryptocurrency fraud and money laundering. In addition, the study included ethical considerations for fraud and money laundering detection. The ethical considerations focus on the social and personal perspective based on respect for transparency and privacy of citizens. The conclusion of the study assesses the effectiveness of the recommendations to improve transaction monitoring systems. Traditional banking and financial institutions as well as cryptocurrency exchanges need to prioritise the integration of advanced systems such as XGBoost, which focus on data flow, staff motivation and training.

The review of the relevant literature confirms that the scope of ethical considerations is not sufficient to ensure financial security in economic transactions. It therefore calls for national and

international organisations to adopt additional regulations. It is crucial to find an acceptable and transparent method of monitoring, recording and regulating cryptocurrencies to reduce uncertainty between users and holders of accounting information; this will, in turn, reduce accounting risks. In the absence of cryptocurrency regulations, cryptocurrency-based transactions are vulnerable to fraud and money laundering. Given the importance of ethics in the adoption of new technologies, ML professionals facilitating the adoption of ML algorithms need to consider the implications of their work. If these issues are not addressed, the improper use of ML can damage a company's reputation and financial health.

# CHAPTER III: RESEARCH METHODOLOGY

## 3.1 Overview of the Research Problem

This study aims to assess the effectiveness of transaction monitoring in detecting and preventing cybercrime related to cryptocurrencies.

## 3.2 Research Method

Using a mixed research methodology, the sequential exploratory research will assess the role of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering. Onghena, Maes and Heyvaert (2018) defined mixed research methodology as a study that combines experimental and qualitative techniques and methods to answer the specific research questions of the study. In particular, Timans, Wouters and Heilbron (2019) reported that researchers integrate qualitative research methods in mixed research studies to conduct rigorous and in-depth empirical investigations of a particular phenomenon by assessing specific cases in the context of the research study. Goodwin and William (2020) characterised the quantitative research method in mixed research studies as an experimental method that aims to assess the causal relationship between the independent variable and the outcome when the independent variable is manipulated and the outcome variable is repeatedly assessed under specific levels of the independent variable. Wester and McKibben (2019) integrate and extend the findings of Timans, Wouters and Heilbron (2019) and Goodwin and William (2020), noting that the mixed methods research approach explores the complex experiences and content of individuals in counselling, thereby enhancing understanding of evidence-based treatments. In this regard, the exploratory research study aims to assess the effectiveness of communication and cooperation processes between financial regulators and financial institutions. Defining a theoretical framework, selecting specific methods and

establishing integrated procedures for sampling, data analysis and interpretation of results are essential steps in conducting a mixed-methods study.

### 3.3 Research Design

The present research study will have an exploratory research design. According to Kişi (2022) and De Langhe and Schliesser (2017), an exploratory research design is often used when the research objective is new or when data and knowledge about the phenomenon under study are limited. The role of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering is a relatively new phenomenon that requires exploratory research. Exploratory research, according to De Langhe and Schliesser (2017), develops an initial understanding of the phenomenon under study, formulates a hypothesis and generates research questions that serve to identify further research gaps. In a mixed-methods research study, Asenahabi (2019) noted that the sequential exploratory research design begins with the analysis of qualitative research data and then explores participants' perceptions. The data is then analysed and the findings are fed into a second phase of quantitative research. The research findings suggest that the qualitative research phase is used to develop an instrument that best fits the sample being studied in order to identify the most appropriate instruments for the subsequent quantitative research phase.

### 3.4 Research Philosophy

The sequential exploratory study will follow a pragmatic research philosophy. Kelly and Cordeiro (2020) and Timans, Wouters and Heilbron (2019) claim that the pragmatic research philosophy incorporates beliefs and actions into the decision-making process. In pragmatic philosophy, evaluation or enquiry contributes significantly to conscious human action in response

to specific obstacles or problems. Evaluation or enquiry is followed by specific adaptation and changed behaviour in response to a particular problem. Similarly, pragmatism does not distinguish between enquiry and everyday life. Pragmatism is relevant to both practitioners and theorists because it incorporates enquiry into everyday cases. Timans, Wouters and Heilbron (2019) extend the findings of Kelly and Cordeiro (2020) by suggesting that pragmatism provides an action-oriented and experiential framework in which the practices and purposes of enquiry are seen as significant for solving problems related to how people experience and understand the activities of the world in a pragmatic sense. This includes a working knowledge of conceptual relations that enables the researcher to engage with the real world in a more comprehensive way. In the context of pragmatism, therefore, all epistemological and ontological questions are closely related to experience.

## 3.5 Justification of Research Design and Research Method

### 3.5.1 Justification for research method

Mixed methods research allows the researcher to combine qualitative and quantitative approaches to fully understand the research problem. In the case of cryptocurrencies, for example, both qualitative data from secondary sources and quantitative data from participants contribute to a full understanding of the research questions and hypotheses. In this context, Nguyen, Tran and Nguyen (2021) suggested that integrating qualitative and quantitative research data allows researchers to develop insightful patterns that validate the qualitative data through rigorous analysis. The combination of qualitative and quantitative research methods leads to information-rich data and data-driven outcomes for discovering practical business and organisational solutions. According to Onghena, Maes and Heyvaert (2018), the mixed research method provides answers

that are specific to the research questions and hypotheses under investigation. For example, the mixed research method has been used to assess the effectiveness and feasibility of AML programmes in traditional banking and financial institutions as well as cryptocurrency exchanges. According to Mondal and Mondal (2018), the mixed research method encourages the development of new theoretical frameworks. Theoretical sampling, the integration of multiple data collection methods, the use of different data analysis techniques and the application of replicated logic that extends or develops a new theory are key features of mixed research studies that aim to develop new theories. As such, the present exploratory study analysed data using quantitative and qualitative research methods, thematic analysis and regression analysis, leading to important conclusions and recommendations for fraud monitoring professionals.

### 3.5.2 Justification for research design

The justification for an exploratory research design lies in its ability to answer unanswered research questions and test hypotheses. Casula, Rangarajan and Shields (2020) claim that an exploratory research design evaluates theory using deductive reasoning, moving from a broad to a narrow perspective. Furthermore, the hypotheses of the study provide a framework for exploratory research that links the research objectives to other stages of the research process, including data selection, variable creation and statistical testing. According to Shim (2016), an exploratory research design is used in preliminary research to assess unidentified research problems when the researcher has limited or no knowledge. It is also characterised by its adaptability and perspective. Therefore, an exploratory research design is chosen when the research question is vague or general. Exploratory research studies provide valuable results that offer new insights and thus provide answers to research questions to evaluate phenomena in a different light. Lastly, an exploratory

research design enables more precise formulation of research problems in the field of transaction monitoring, cryptocurrency, fraud, money laundering, collection of explanations, generation of insights, elimination of impractical concepts and formulation of hypotheses.

### 3.5.3 Justification for research philosophy

In terms of epistemology, pragmatic research philosophy is justified by the concept of avoiding metaphysical debates about the role of transaction monitoring by valuing truth rather than merely providing a practical understanding of concrete questions. While pragmatic research philosophy focuses on an interpretivist understanding of a socially constructed reality, Kelly and Cordeiro (2020) propose to question the meaning and value of research data by assessing its practical implications. Maarouf (2019) extended Kelly and Cordeiro's (2020) findings by noting that pragmatism is particularly relevant in organisational contexts that integrate knowledge creation practices and processes, which has led some classical pragmatists to prioritise learning and understanding. Consequently, the application of pragmatism in organisational contexts can facilitate the exploration and understanding of the relationships between action and knowledge in that context.

## 3.6 Research Design Limitations

The exploratory research design is based on a small sample size, as it is only possible to recruit a few participants for the study due to banking secrecy. In this respect, the results of the study cannot be generalised globally. According to Malmivaara (2019), a small sample size limits generalisability. Both Mundra and Rajapakse (2016) and McKim (2017) noted that exploratory research designs carry a high risk of biased sample selection, which affects the validity of the study

findings due to their lack of representativeness. As a result, the representativeness of the research findings is limited. Nevertheless, the problem of small sample size was solved by evaluating participants from different banking and financial institutions that have implemented cryptocurrency-based transaction monitoring systems.

## 3.7 Data Collection

### 3.7.1 Primary data collection

The study will use a questionnaire to collect data. The researcher will distribute the questionnaires to professionals employed by banking and financial institutions that have adopted cryptocurrencies, including Standard Chartered, Fidelity, Goldman Sachs, Citadel Securities and Citi Group. Through LinkedIn, the researcher will disseminate the consent forms (see Appendix B). In particular, this research focuses on employees of banks and financial institutions that have adopted cryptocurrency-based transaction monitoring systems. After obtaining informed consent from the participants, the researcher will distribute the questionnaires through email or social media platforms. Arora (2017) recommended questionnaires because of their standardisation process. Since all participants are asked the same questions in the same way, questionnaires provide a standardised method of data collection, which increases the reliability of the study.

### 3.7.2 Secondary data collection

The study includes studies from databases such as ScienceDirect, Academic Search Premier Project MUSE, JSTOR and ProQuest. Charoenthammachoke et al. (2020) found that the ScienceDirect and ProQuest databases provide access to a wide range of scholarly materials, including journal articles. Such articles would be useful in assessing the role of transaction

monitoring in detecting and preventing cryptocurrency fraud and money laundering. Charoenthammachoke et al. (2020) note that ProQuest's extensive filters and options facilitate the evaluation of relevant journals and articles in the field of cryptocurrency. According to Trimble (2018), JSTOR is a large digital library that provides access to scholarly articles and journals. It contains a variety of scholarly articles on technology, such as historical perspectives, theoretical analyses and case studies. It offers tools such as citation tracking that can be used to evaluate the results of technology research. "Transaction monitoring", "cryptocurrency", "finance", "financial institutions", "blockchain", "bitcoin", "cybercrime", "cyberspace", "crime", "money laundering", "anti-money laundering" and "banks" are some of the most commonly used search terms. After identifying the most important search terms, the exploratory study uses Boolean operators such as "AND" and "OR". Examples include "cybercrime OR money laundering" and "transaction monitoring AND anti-money laundering". According to Hyvernat (2014), Boolean operators integrate complex search queries that can be used to find more relevant data by refining the search results. The use of relevant databases, search terms and Boolean operators leads to more accurate search results and the identification of relevant research articles and journals.

### 3.7.3 Inclusion/exclusion criteria

Inclusion criteria include articles that discuss the role of transaction monitoring in cybercrime and therefore provide reliable and useful data for the main objective of the research. Excluded are reviews and case studies that examine cryptocurrencies in a way that has nothing to do with cybercrime and transaction monitoring. In addition, articles published between 2018 and 2023 will be included in the research. The research study will only consider articles written in English and will exclude translations. Finally, only studies with clearly defined research questions

and methods will be included in the study, while those with unclear research questions and inadequate research methods will be excluded. Table 1 lists the inclusion and exclusion criteria.

**Table 1: Inclusion/Exclusion Table**

| Inclusion | Exclusion |
|---|---|
| Published articles on transaction monitoring and anti-money laundering. | News blogs, case studies and unpublished articles. |
| Qualitative and quantitative studies. | Studies without defined research methodologies. |
| Studies published between 2018 and 2023. | Studies published before 2018. |
| Studies with clear research questions and methodology. | Studies without clear research questions or methodology. |

### 3.8 Data Analysis

#### 3.8.1 Primary method data analysis

Using SPSS software, the exploratory research will include regression, paired t-tests and descriptive analyses. The study will identify significant values and p-values of the regression model using ANOVA and correlation coefficient tests. The regression analysis will also assess the correlations between transaction monitoring and AML success rate in detecting or preventing cryptocurrency cybercrime. The quantitative data variable will assume a reference category when conducting a regression analysis. The regression coefficients will be interpreted to explain the relationship between transaction monitoring and a decrease in cybercrime when cryptocurrencies are integrated into traditional banking and financial systems as well as cryptocurrency exchanges.

The paired t-test is included in the analysis to determine whether there are statistically significant differences in the mean of the effectiveness of rule-based transaction monitoring systems and behaviour-based transaction monitoring systems, and in the effectiveness of modern technological fraud detection tools and traditional fraud detection tools. Finally, the descriptive statistics from the analysis are used to describe the characteristics and provide an overview of the participants in terms of their gender, education level and age. The measures of central tendency from the descriptive data help to describe the variability, distribution and characteristics of the data.

### 3.8.2 Secondary method data analysis

In the qualitative research method, thematic analysis is used to examine secondary data and answer the relevant research questions. After the initial phase of code generation, the focus of analysis shifts to categorising specific codes into initial themes. Campbell et al. (2021) note that for each of the themes identified, the researcher needs to produce a thorough analysis that goes beyond a mere description or paraphrase of the data identified. This includes identifying the narrative of each theme and situating the theme and narrative within the larger context of the data set in accordance with the research objectives. Thematic analysis, according to Javadi and Zarea (2016), goes beyond explicit phrases or words and focuses on identifying and describing both explicit and implicit concepts. Codes developed for themes or concepts are linked to the raw data or used as summary markers for analysis, which may involve comparing the relative frequency of themes or topics within a given dataset, assessing the co-occurrence of codes, or graphing the relationship between codes. In this respect, thematic analysis allows the researcher to pinpoint relationships between different concepts and compare them to similar data. Using a combination

of thematic analysis and exploratory research, this study will establish links between different concepts related to transaction monitoring and provide implications for fraud monitoring professionals.

### 3.9 Ethical Considerations

The researcher will distribute consent forms (see Appendix B) that allow participants to be fully informed about the nature and aims of the study. Wheeler (2017) emphasised that the consent form is a crucial ethical factor that enables researchers to obtain informed consent from research participants. Furthermore, Vilhuber (2018) emphasised the confidentiality of participants. In this regard, the researcher will take the necessary measures to ensure the confidentiality of the participants, especially due to banking secrecy laws. Then, the researcher will interview the participants and explain to them the main purpose of the study. Glattke (2017) emphasised the importance of describing the nature of the study and giving participants the opportunity to evaluate informed consent.

### 3.10 Chapter Summary

This chapter describes the methodology of the research study. The study was designed as a mixed-methods study, as it uses both qualitative and quantitative research methods and therefore addresses a broader range of research questions. Furthermore, the study is exploratory in nature and follows a pragmatic research philosophy. The primary method of data collection will involve employees of banking and financial institutions that have adopted cryptocurrencies, while secondary data sources will include studies focusing on cryptocurrencies and transaction

monitoring tools and techniques. Primary data will be analysed using regression analysis and descriptive statistics, while secondary data will be subject to thematic analysis.

# CHAPTER IV: RESULTS AND FINDINGS

## 4.1 Introduction

Emerging and revolutionary cryptocurrencies offer unprecedented accessibility, anonymity and decentralisation. This newfound freedom has brought a dark side to the cryptocurrency market, characterised by money laundering schemes and a proliferation of cryptocurrency fraud. With numerous actors, institutions, stakeholders and organisations adopting cryptocurrencies, it is crucial to develop effective mechanisms to protect them from illegal activities in the digital world of cryptocurrencies. In this regard, the purpose of this research was to examine the effectiveness of transaction monitoring as a notable strategy to detect and prevent cryptocurrency fraud and money laundering. The study also sought to assess the current state of transaction monitoring techniques and tools within the traditional banking and financial institutions as well as cryptocurrency exchanges, identify their strengths and limitations, and provide actionable recommendations for fraud monitoring professionals to effectively detect and prevent illicit activities related to cryptocurrency transactions. This chapter presents the qualitative and quantitative findings derived from the study's primary and secondary data. It reveals vulnerabilities, anomalies and patterns that can be used to improve security measures by shedding light on the intricate web of cryptocurrency transactions.

## 4.2 Presentation and Analysis of the Collected Primary Data

Twelve respondents provided primary data that was analysed using SPSS software. This section includes descriptive statistics to summarise the model and the data set, and inferential statistics to compare and generalise the results from the larger population of the study.

### 4.2.1 Descriptive Statistics

The gender distribution among the twelve participants in this study is summarised in Table 2. The frequency column in Table 2 indicates the frequency with which each gender category occurs in the data set. Eight participants identified as male, three participants identified as female and one participant identified as non-binary. This means that 66.7% of the study participants were male, 25% female and 8.3% non-binary.

**Table 2: Gender**

Gender

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | Male | 8 | 66.7 | 66.7 | 66.7 |
| | Female | 3 | 25.0 | 25.0 | 91.7 |
| | Non-binary | 1 | 8.3 | 8.3 | 100.0 |
| | Total | 12 | 100.0 | 100.0 | |

(Source: SPSS)

Tables 3 and 4 below show the age distribution of the twelve participants in the study. In Table 4, frequency column, one respondent is in the age group "18-24", five respondents are in the age group "25-34", two respondents are in the age group "35-44", two respondents are in the age group "45-54" and two respondents are in the age group "55-64". From this frequency distribution, 41.7% of the respondents are in the age group "25-34", 16.7% each are in the age groups "35-44", "45-54" and "55-64" and 8.3% are in the age group "18-24". The statistics presented in Table 3 show that the mean and median ages are between 35 and 44 years as indicated by the mean and

median ages of 3.92 and 3.50 respectively. Furthermore, the standard deviation of the model of 1.311 shows that there is some variability within the data set.

**Table 3: Age Statistics**

Statistics

Age

| | | |
|---|---|---|
| N | Valid | 12 |
| | Missing | 0 |
| Mean | | 3.92 |
| Median | | 3.50 |
| Std. Deviation | | 1.311 |
| Variance | | 1.720 |

(Source: SPSS)

**Table 4: Age**

Age

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | 18-24 | 1 | 8.3 | 8.3 | 8.3 |
| | 25-34 | 5 | 41.7 | 41.7 | 50.0 |
| | 35-44 | 2 | 16.7 | 16.7 | 66.7 |
| | 45-54 | 2 | 16.7 | 16.7 | 83.3 |
| | 55-64 | 2 | 16.7 | 16.7 | 100.0 |
| | Total | 12 | 100.0 | 100.0 | |

(Source: SPSS)

Table 5 gives an overview of the distribution of education levels among the twelve study participants. Table 5 shows that one respondent has a "high school degree or below", five have a "bachelor's degree", four have a "master's degree" and two have a "doctorate or professional degree". In terms of percentages, 41.7% of respondents have a bachelor's degree, 33.3% have a master's degree, 16.7% have a doctorate or professional degree and 8.3% have a high school degree or below.

**Table 5: Education Level**

Education

| | | Frequency | Percent | Valid Percent | Cumulative Percent |
|---|---|---|---|---|---|
| Valid | High School or below | 1 | 8.3 | 8.3 | 8.3 |
| | Bachelor's Degree | 5 | 41.7 | 41.7 | 50.0 |
| | Master's Degree | 4 | 33.3 | 33.3 | 83.3 |
| | Doctorate or Professional Degree | 2 | 16.7 | 16.7 | 100.0 |
| | Total | 12 | 100.0 | 100.0 | |

(Source: SPSS)

### 4.2.2 Research hypothesis one

The first alternative hypothesis tested in this study is whether common rule-based and behaviour-based transaction monitoring frameworks effectively detect and prevent cryptocurrency fraud. In contrast, the null hypothesis tested below states that common rule-based and behaviour-based transaction monitoring frameworks are not able to effectively detect and prevent

cryptocurrency fraud. To test these hypotheses, a paired t-test was conducted to determine whether there was a significant difference between the effectiveness scores of rule-based and behaviour-based transaction monitoring.

The paired samples statistics from the paired t-test of rule-based and behaviour-based transaction monitoring frameworks are shown in Table 6. The mean score for the effectiveness of the rule-based framework is 3.17, while the mean score for the effectiveness of the behaviour-based framework is 3.58. This shows that respondents rate the effectiveness of behaviour-based transaction monitoring slightly higher (mean 3.58) than that of rule-based monitoring (3.17). The standard deviation for both frameworks is 0.937 for the rule-based framework and 0.996 for the behaviour-based framework. With such a comparable standard deviation, it can be assumed that the overall variability of the model is similar.

**Table 6: Paired Samples Statistics**

Paired Samples Statistics

| | | Mean | N | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Pair 1 | Rule-based framework Effectiveness | 3.17 | 12 | .937 | .271 |
| | Behaviour-based framework Effectiveness | 3.58 | 12 | .996 | .288 |

(Source: SPSS)

The correlation between the two variables "rule-based framework effectiveness" and "behaviour-based framework effectiveness" is shown in Table 7. This correlation assesses the degree of correlation between the effectiveness ratings of these two types of transaction monitoring systems. Table 7 shows that the correlation coefficient is 0.568, indicating a moderately positive correlation between the effectiveness ratings of the rule-based and behaviour-based transaction monitoring systems. This result indicates that as the effectiveness rating of one type of framework increases, the rating of the other type of framework tends to increase and vice versa. Since the correlation is less than 1, it is not perfect. Furthermore, the p-value of the model is 0.054, slightly above the significance threshold of 0.05. At the 0.05 level, the correlation is therefore not statistically significant.

**Table 7: Paired Samples Correlations**

Paired Samples Correlations

| | | N | Correlation | Sig. |
|---|---|---|---|---|
| Pair 1 | Rule-based framework Effectiveness & Behaviour-based framework Effectiveness | 12 | .568 | .054 |

(Source: SPSS)

The "paired samples effect sizes" in Table 8 provide information on the effect sizes for the paired sample t-test comparing the effectiveness ratings of "rule-based framework effectiveness" and "behaviour-based framework effectiveness". The effect size of the model, as measured by

Cohen's d, is 0.900, while the Hedges' correction accounting for small sample sizes is 0.933, as shown in Table 8. Consequently, both Cohen's d and the Hedges' correction indicate a positive effect size, suggesting that the "behaviour-based framework" is on average rated as more effective than the "rule-based framework".

**Table 8: Paired Samples Effect Sizes**

Paired Samples Effect Sizes

| | | | | | 95% Confidence Interval | |
|---|---|---|---|---|---|---|
| | | | Standardiser a | Point Estimate | Lower | Upper |
| Pair 1 | Rule-based framework Effectiveness - Behaviour-based framework Effectiveness | Cohen's d | .900 | -.463 | -1.051 | .144 |
| | | Hedges' correction | .933 | -.447 | -1.014 | .139 |

a. The denominator used in estimating the effect sizes.

Cohen's d uses the sample standard deviation of the mean difference.

Hedges' correction uses the sample standard deviation of the mean difference plus a correction factor.

(Source: SPSS)

Therefore, from the above paired t-tests, it can be concluded that a behaviour-based transaction monitoring framework is significantly more effective than a rule-based framework.

Thus, the first alternative hypothesis is accepted and the first null hypothesis is rejected, as both approaches detect and prevent cryptocurrency fraud, albeit with different effectiveness levels.

### 4.2.3 Research hypothesis two

The second alternative hypothesis of this study examines whether cooperation between regulators and financial institutions improves the performance of transaction monitoring practices. The corresponding null hypothesis states that cooperation between regulators and financial institutions does not improve transaction monitoring performance. To determine whether there is a significant relationship between the independent variable (cooperation between regulators and financial institutions) and the dependent variable (performance effectiveness), a regression analysis was conducted to test this hypothesis.

The variables that were included in or removed from the regression model are summarised in Table 9. As all the variables indicated were included in the analysis, the regression analysis clearly shows the underlying relationship between cooperation and performance.

**Table 9: Variables Entered/Removed**

Variables Entered/Removed

| Model | Variables Entered | Variables Removed | Method |
|---|---|---|---|
| 1 | Cooperation Effectiveness | . | Enter |

a. Dependent Variable: Performance Effectiveness

b. All requested variables entered.

(Source: SPSS)

The model summary for the regression analysis is provided in Table 10 below. It contains important statistics that can be used to determine whether the regression model is of high quality and appropriate for the analysis at hand. The R-squared value of 0.619 indicates that “cooperation effectiveness” explains about 61.9% of the variation in “performance effectiveness”. This indicates that there is a strong correlation between these variables. The adjusted R-squared value of 0.581 is slightly lower than the R-squared value, suggesting that the current model could be improved by adding additional adjustments or variables. Furthermore, the standard error of the estimate (0.583) provides an estimate of the typical error in predicting “performance effectiveness” based on “cooperation effectiveness”. In general, smaller values of the standard error within the model indicate a better fit between the model and the data.

**Table 10: Model Summary**

Model Summary

| Model | R | R Square | Adjusted R Square | Std. Error of the Estimate |
|---|---|---|---|---|
| 1 | .787a | .619 | .581 | .583 |

a. Predictors: (Constant), Cooperation Effectiveness

(Source: SPSS)

ANOVA is useful to determine the statistical significance of the regression model. According to Table 11, the regression model explains a sum of squares of 5.523, with 1 degree of freedom (df). This result indicates that the model adequately explains a substantial part of the variability of the dependent variable. In contrast, the sum of squares of the residuals at 10 degrees of freedom (df) is 3.394, which represents the variation in the dependent variable that cannot be explained to a greater extent. By dividing the sum of the squares by their degrees of freedom, the mean regression square (5.523) and the mean residual square (0.339) can be calculated. The mean regression square of the model is relatively large, indicating that it explains a substantial part of the variation. As shown in Table 11, the p-value associated with the F-ratio is 0.002 (or 0.2%). This low p-value, which is below the significance threshold of 0.05, indicates substantial evidence against the null hypothesis. It indicates that “cooperation effectiveness” significantly influences “performance effectiveness”.

**Table 11: ANOVA**

ANOVAa

| Model | | Sum of Squares | df | Mean Square | F | Sig. |
|---|---|---|---|---|---|---|
| 1 | Regression | 5.523 | 1 | 5.523 | 16.272 | .002b |
| | Residual | 3.394 | 10 | .339 | | |
| | Total | 8.917 | 11 | | | |

a. Dependent Variable: Performance Effectiveness

b. Predictors: (Constant), Cooperation Effectiveness

(Source: SPSS)

The coefficients of the regression model are shown in Table 12 below. “Cooperation effectiveness” has an unstandardised coefficient of 0.818, which means that a one unit increase in “cooperation effectiveness” increases “performance effectiveness” by 0.818 units. The standardisation coefficient (beta) for “cooperation effectiveness” is 0.787%. This means that a one standard deviation increase in “cooperation effectiveness” is associated with a 0.787% increase in “performance effectiveness”. Furthermore, the model's t-value of 4.034 and p-value of less than 0.05 show that “cooperation effectiveness” is a statistically significant predictor of “performance effectiveness”.

**Table 12: Coefficients**

Coefficients

| Model | | Unstandardised Coefficients | | Standardised Coefficients | | | 95.0% Confidence Interval for B | | Correlations | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | | B | Std. Error | Beta | t | Sig. | Lower Bound | Upper Bound | Zero-order | Partial | Part |
| 1 | (Constant) | .515 | .779 | | .661 | .523 | -1.221 | 2.251 | | | |
| | Cooperation Effectiveness | .818 | .203 | .787 | 4.034 | .002 | .366 | 1.270 | .787 | .787 | .787 |

a. Dependent Variable: Performance Effectiveness

(Source: SPSS)

Therefore, according to the regression model above, cooperation between regulators and financial institutions seems to improve transaction monitoring practices. As such, the second alternative hypothesis is accepted, while the second null hypothesis is rejected.

### 4.2.4 Research hypothesis three

The third and final alternative hypothesis examined whether modern transaction monitoring tools are more effective than traditional tools and methods. The corresponding null hypothesis states that traditional transaction monitoring tools are more effective than their modern counterparts. To test this hypothesis, a paired t-test was conducted comparing the effectiveness ratings of modern and traditional transaction monitoring tools.

The table below summarises the key characteristics of the effectiveness ratings given by the twelve study participants for traditional and modern tools. The mean rating for "modern tools effectiveness" is 3.75, while the mean rating for "traditional tool effectiveness" is 2.33, as shown in Table 13. The standard deviation in the table below measures the spread or variability of the ratings within each group; thus, a larger standard deviation means greater variability of ratings within the group and vice versa. The standard deviation for "modern tools effectiveness" is 0.866, and the standard deviation for "traditional tool effectiveness" is 0.888. Since the standard deviation for both sets of tools is relatively similar, this suggests similar levels of variability in the ratings.

**Table 13: Paired Samples Statistics**

Paired Samples Statistics

| | | Mean | N | Std. Deviation | Std. Error Mean |
|---|---|---|---|---|---|
| Pair 1 | Traditional Tool Effectiveness | 2.33 | 12 | .888 | .256 |
| | Modern Tools Effectiveness | 3.75 | 12 | .866 | .250 |

(Source: SPSS)

The correlation between the effectiveness of traditional and modern tools is analysed in Table 14 to determine the degree of relationship or association between the two sets of tools. Table 14 shows that the correlation coefficient of the model is 0.118, indicating a very weak positive correlation between the ratings of "traditional tool effectiveness" and "modern tools effectiveness". This statistic indicates that as the effectiveness rating of one set of tools tends to increase, so does the

rating of the other set, but the correlation is very weak and tends towards zero. Furthermore, the significance level (p-value) of the correlation is 0.714. The p-value (0.714) is significantly larger than the standard significance level (0.05). This indicates that the correlation is not statistically significant at the 0.05 level, so that on the basis of this sample it cannot be concluded with a high degree of certainty that there is a significant correlation between the two variables.

**Table 14: Paired Samples Correlations**

Paired Samples Correlations

| | | N | Correlation | Sig. |
|---|---|---|---|---|
| Pair 1 | Traditional Tool Effectiveness & Modern Tools Effectiveness | 12 | .118 | .714 |

(Source: SPSS)

The results of a paired samples t-test to determine whether there is a statistically significant difference between the two related sets of observations are shown in Table 15. The mean difference is -1.417, as shown in Table 15. The negative mean difference means that on average, “traditional tool effectiveness” received lower ratings than “modern tools effectiveness”. This indicates that respondents consider modern tools to be more effective than traditional tools. The t-value of the model of -4.214 indicates a significant difference between traditional and modern tools. The p-value of 0.001 is also low, indicating that the underlying differences between modern and traditional tools are statistically significant at a 95% confidence interval.

**Table 15: Paired Samples Test**

Paired Samples Test

| | | Paired Differences | | | | | t | df | Sig. (2-tailed) |
|---|---|---|---|---|---|---|---|---|---|
| | | Mean | Std. Deviation | Std. Error Mean | 95% Confidence Interval of the Difference Lower | Upper | | | |
| Pair 1 | Traditional Tool Effectiveness - Modern Tools Effectiveness | -1.417 | 1.165 | .336 | -2.157 | -.677 | -4.214 | 11 | .001 |

(Source: SPSS)

The “Paired Samples Effect Sizes’ in Table 16 provide information on the effect sizes for the paired samples t-test comparing “traditional tool effectiveness” and “modern tools effectiveness”. These effect sizes help to understand the practical relevance of the observed differences between these two sets of ratings. The effect size measured with Cohen's d is 1.165, while the Hedges’ correction factor is 1.206. Cohen's d and the Hedges’ correction indicate a large effect size, meaning a substantial and practically significant difference between "traditional tool effectiveness" and "modern tools effectiveness". The 95% confidence intervals for Cohen's d and the Hedges’ correction are given to illustrate the plausible range of effect sizes. In both cases, the confidence intervals do not contain the value zero, indicating the presence of a statistically significant and practically meaningful effect.

**Table 16: Paired Samples Effect Sizes**

Paired Samples Effect Sizes

| | | | | | 95% Confidence Interval | |
|---|---|---|---|---|---|---|
| | | | Standardised | Point Estimate | Lower | Upper |
| Pair 1 | Traditional Tool Effectiveness - Modern Tools Effectiveness | Cohen's d | 1.165 | -1.217 | -1.958 | -.445 |
| | | Hedges' correction | 1.206 | -1.175 | -1.890 | -.430 |

a. The denominator used in estimating the effect sizes.

Cohen's d uses the sample standard deviation of the mean difference.

Hedges' correction uses the sample standard deviation of the mean difference plus a correction factor.

(Source: SPSS)

Therefore, from the above paired t-tests, the effectiveness of modern transaction monitoring tools is significantly greater than that of the traditional tools. As such, the third alternative hypothesis that modern transaction monitoring tools are more effective than traditional tools and methods is accepted, while the corresponding null hypothesis is rejected.

### 4.3 Presentation and Analysis of Collected Secondary Data

The secondary studies included provided qualitative data, excerpts of which were coded and analysed thematically. After analysis, three major themes were identified in the extracts, as shown in Table 2 below.

**Table 17: Sources and Coded Themes**

| Source | Theme 1: Technology and Tools for Transaction Monitoring | Theme 2: Institutional and Regulatory Collaboration in Cryptocurrency Security | Theme 3: Evolution of Fraud Detection Tools |
|---|---|---|---|
| Aljihani et al. (2021) | ✓ | | |
| Karthikeyan et al. (2021) | ✓ | | |
| Campbell-Verduyn (2018) | ✓ | | |
| Pettersson Ruiz and Angelis (2022) | ✓ | | |
| Cummings, Johan, and Pant (2019) | | ✓ | |
| Limba, Stankevičius, and Andrulevičius (2019) | | ✓ | |

| | | | |
|---|---|---|---|
| Nabilou (2019) | | ✓ | |
| Kurshan, Shen, and Yu (2020) | | | ✓ |
| Lokanan (2023) | | | ✓ |
| Vosyliūtė and Maknickienė (2022) | | | ✓ |
| Egbiri and Azinge (2018) | | | ✓ |

### 4.3.1 Theme 1: Technology and Tools for Transaction Monitoring

As shown in Table 17, this theme was coded in four studies. Two of the studies coded for this topic focused on behaviour-based transaction monitoring technology and tools, while the other two focused on rule-based transaction monitoring technologies and tools for cryptocurrencies. Aljihani et al. (2021) published the first article on behaviour-based transaction monitoring technologies and tools, which aimed to develop and improve attack detection techniques for distributed software systems using blockchain technology. The rapid increase in the number and speed of cyber-attacks on distributed software systems prompted this study. According to Aljihani et al. (2021), a promising method for detecting transaction problems and attacks is the behaviour-based attack detection method, which considers the reliability and immutability of detection systems. According to the study, the integration of blockchain technology improves the immutability of data and makes the detection system more reliable. The article also highlights the underlying benefits of using specification-based recognition methods. Aljihani et al. (2021) conclude that using specification-based detection methods in conjunction with behaviour-based transaction monitoring technology and tools significantly reduces false positives by detecting both

trusted and infrequent or unusual behaviour in the system. Although the study points out that it is relatively difficult to extract all trusted behaviours using the technology and method, the researchers claim that the integration of blockchain technology can provide huge benefits, such as improving the overall reliability, accuracy and robustness of stored data, transactions or characteristics. Despite this finding, the article by Aljihani et al. (2021) does not identify the fundamental trade-off between immutability and performance in blockchain adoption. This hinders the widespread adoption of the recommendation by fraud monitoring professionals. The second article that highlights the issue in relation to behaviour-based transaction monitoring technologies and tools is a study by Karthikeyan et al. (2021), which explores the use of behavioural analysis to assess fraudulent activity. In contrast to Aljihani et al. (2021), the study by Karthikeyan et al. (2021) details the approaches, models and different types of behavioural analysis used in transaction monitoring. For example, the researchers identified behaviour pattern mining as an important technique for examining user activity by extracting meaningful data from existing behaviour logs. Karthikeyan et al. (2021) also identified system behavioural analysis, which refers to all incoming and outgoing system activities of the hardware or software, and user behaviour analysis, which considers web browsing behaviour, keystroke behaviour, and network transaction behaviour to denote users' regular activities, such as their regular buying sites, search items, purchase websites, and transactions. In this study, researchers Karthikeyan et al. (2021) identified a number of problems related to behavioural analysis and classification, but did not provide explanations or recommendations for overcoming these obstacles.

Two other articles on the same topic examined rule-based transaction monitoring tools and technologies. The first article is by Campbell-Verduyn (2018) and aims to assess the effectiveness

of the global anti-money laundering regime in light of the challenges posed by new types of 'altcoins'. Campbell-Verduyn (2018) provides two main arguments in support of rule-based transaction monitoring tools and technologies. The first argument is that current cryptocurrency transactions reinforce the need for global anti-money laundering efforts, as current threats are less related to the use of digital currencies and more to the capabilities of blockchain technologies. The second argument relates to the Financial Action Task Force's risk-based approach, where the existing opportunities and threats of cryptocurrencies are effectively balanced by rules and regulations. In contrast to the above arguments, Campbell-Verduyn (2018) argues that a more uniform risk- and rule-based approach should be implemented because it gives national regulators the discretion to implement measures to achieve the common goal of reducing money laundering. In today's global governance, a rule-based approach is more flexible and decentralised, the study noted. The other study on rule-based transaction monitoring technologies and tools is an article by Pettersson Ruiz and Angelis (2022), which examines the use of machine learning to de-anonymise money launderers in cryptocurrencies. According to the researchers, current fraud and money laundering prevention practices, including the rule-based approach, are ineffective in detecting illicit currency movements. The qualitative findings from the study's interviews also support the notion that current methods require task optimisation because they are inefficient. In contrast to Campbell-Verduyn (2018), who acknowledges the importance of a rule-based approach, Pettersson Ruiz and Angelis (2022) argue that the use of a rule-based approach is not justified in itself because it is too simplistic to capture the complexity of digital currencies and money laundering as the number of cryptocurrency transactions increases. The premise is that rule-based approaches to transaction monitoring are characterised by high rates of false positives and low detection rates, and are therefore overly susceptible to bias.

### 4.3.2 Theme 2: Institutional and Regulatory Collaboration in Cryptocurrency Security

As shown in Table 17, the topic was coded using three studies, including an article by Cummings, Johan and Pant (2019) that examines the Securities and Exchange Commission's pronouncements and initial statements on the fundamental issues in applying older legal frameworks to an ever-changing ecosystem. Current international regulatory trends highlighted in the study include the Canadian regime used by companies selling goods and services online that accept digital currencies, even though digital currencies are not legal tender. The Reserve Bank of India does not recognise virtual currencies as legal tender in India because they do not have physical properties. China has suppressed the cryptocurrency industry by refusing to recognise virtual currencies and Initial Coin Offerings. Cummings, Johan and Pant (2019) point out the shortcomings of the existing regulatory framework and emphasise the importance of internal collaboration between developers and government agencies, particularly in regulating crypto-assets and fostering an ecosystem based on outcomes that benefit all stakeholders. Although this study highlights the importance of considering new financial techniques, it does not answer the question of what constitutes effective regulation that promotes innovation. The topic was also coded in the study by Limba, Stankevičius, and Andrulevičius (2019), who offer a national security perspective of the risk mitigations needed to promote sustainable cryptocurrency. This study starts from the premise that cryptocurrencies, blockchain and virtual currencies are becoming a national security concern as they are fast becoming the main vehicle for illicit commodity transactions and a significant tool for money laundering. Four respondents to the study confirmed the need for regulation of cryptocurrencies in four broad areas: the potential transfer of accounts to third parties, the inability to stop cryptocurrency transactions, the fragmented regulation of the product given its enormous reach and impact, and the unclear regulatory authorities for virtual currencies and

similar financial instruments. Consequently, Limba, Stankevičius, and Andrulevičius (2019) assert that creating risk mitigation for the cryptocurrency market is necessary and that advancing the regulatory framework for the banking sector should be a top priority. According to the study, such advances will play an important role in preventing money laundering as international instruments will make it more difficult. Nabilou (2019), which examines how Bitcoins can be regulated under decentralised arrangements, is another study that highlights the issue of regulatory and institutional cooperation. Unlike Cummings, Johan and Pant (2019) Limba, Stankevičius, and Andrulevičius (2019), this study recognises from the outset that Bitcoin is a decentralised system with regulatory and legal implications. Therefore, the study suggests shifting the policy debate from whether cryptocurrencies should be regulated to how they should be regulated. According to Nabilou (2019), a viable approach that effectively targets the use cases and applications of cryptocurrencies is a decentralised regulatory architecture that engages existing and emerging industry players, as well as the existing regulatory infrastructure. Other notable regulatory recommendations from the study include regulating the virtual currency market through the banking system to enhance investor and customer protection and address financial integrity concerns and risks, and regulating cryptocurrencies through payment institutions to address systemic, legal, operational, liquidity and credit risks. However, despite the recommendations for effective and efficient decentralised regulatory strategies, the study did not shed light on the levels or layers of decentralisation required to achieve the indirect regulatory approach recommended by the researchers.

### 4.3.3 Theme 3: Evolution of Fraud Detection Tools

As shown in Table 17, this concept has been codified in four studies. Two of these studies highlighted traditional fraud and money laundering detection tools and recommended the inclusion

of more modern techniques that can adapt to the ever-changing technological and digital financial landscape. One of these studies is Kurshan, Shen and Yu's (2020) research on recent trends in financial crime and the difficulties in implementing the graphical solution. According to the researchers, traditional fraud detection tools and techniques, including the rule-based approach, are outdated and ineffective in preventing digital fraud and money laundering with virtual currencies. In general, traditional fraud detection tools fail to address the changing nature of financial crime, as criminals adapt and develop increasingly sophisticated techniques to commit fraud or money laundering. These tools are also synonymous with false positives, which are costly and waste investigative time, leading to inefficiency and compliance fatigue. Against this backdrop, Kurshan, Shen and Yu (2020) advocate the application of graph computing principles that integrate machine learning and artificial intelligence solutions for the detection of fraud and other financial crimes. Similarly, Egbiri and Azinge (2018) in their article highlighted the traditional money laundering process in the context of existing traditional fraud detection techniques, including the rule-based approach. The researchers agreed with Kurshan, Shen and Yu (2020) that rule-based approaches are largely inadequate in light of the increasing use of Bitcoin, which brings new regulatory challenges. According to Egbiri and Azinge (2018), the current rules and regulatory framework cannot prevent money laundering or protect consumers. According to the researchers, a new regulatory framework is needed so that all bitcoin and cryptocurrency operators are subject to a standardised system.

Two of the remaining articles on the "Evolution of fraud detection tools" dealt with the use, application and integration of modern technological fraud detection tools and techniques. The studies by Lokanan (2023) shed light on the use of visualisation techniques in detecting financial

fraud such as money laundering and cryptocurrency fraud. For this purpose, the researcher analysed the available literature on fraud detection and divided the results into two categories. The first section addressed the current application of visualisation techniques, while the second section discussed the different visual analysis methods and the challenges associated with each technique. Lokanan (2023) stated that unsupervised clustering analysis and graph methodology are indispensable visual analysis techniques for detecting money laundering transactions and their criminal relationships. In addition to the visualisation approaches presented by Lokanan (2023), Vosyliūtė and Maknickienė (2022) also emphasise the importance of integrating computational intelligence in the detection of fraud and money laundering offences. This recommendation is based on the fact that technological advances have made the detection of digital financial fraud more complex and difficult. Therefore, the researchers believe that modern problems require modern technical solutions, such as the use of computational intelligence-based techniques to detect additional patterns and develop new parameters to ensure efficient and accurate detection of digital financial fraud. However, this study provides only a limited overview of what computational intelligence is and its overall suitability for digital financial fraud detection. Furthermore, given the plethora of available computational tools, the researchers have not identified or differentiated the individual tools according to their application.

### 4.4 Summary of Results and Findings

The results of the qualitative data from the selected studies and the quantitative data from the questionnaire were presented in Chapter 4. The first alternative hypothesis that joint behaviour-based transaction monitoring and rule-based transaction monitoring detect and prevent cryptocurrency fraud is supported by the quantitative results, while the corresponding null

hypothesis is rejected. The second alternative hypothesis that cooperation between regulators and financial institutions improves transaction monitoring practices is also accepted, while the null hypothesis is rejected. In addition, the third alternative hypothesis that modern transaction monitoring tools are more effective than traditional tools and methods is accepted, while the corresponding null hypothesis is rejected. The qualitative findings revealed three main themes. The first theme was "Technology and tools for transaction monitoring", where both rule-based and behaviour-based transaction monitoring technologies and tools were discussed in terms of their advantages and disadvantages. The second theme was "Institutional and Regulatory Collaboration in Cryptocurrency Security", where collaboration was seen as essential to improving the monitoring of fraud and money laundering outcomes. The final topic was "The Evolution of Fraud Detection Tools", where traditional and modern techniques were evaluated and their effectiveness highlighted.

# CHAPTER V: DISCUSSION OF RESEARCH QUESTIONS

## 5.1 Discussion of Research Question One

The first research question examined the effectiveness of behaviour-based and rule-based transaction monitoring in detecting and preventing cryptocurrency fraud. The qualitative findings related to the topic of "Technology and Tools for Transaction Monitoring" helped answer this question. Campbell-Verduyn (2018) and another study by Pettersson Ruiz and Angelis (2022) claim that rule-based transaction monitoring provides a more structured method for monitoring cryptocurrency transactions. It offers national regulators a flexible approach to combating fraud and money laundering, which can be of particular importance. In the wake of complex cryptocurrencies, Petterson Ruiz and Angelis (2022) noted that over-reliance on rule-based approaches leads to oversimplification, which in turn results in low detection rates, increased bias and a high number of false positives. In contrast, Karthikeyan et al. (2021) and Aljihani et al. (2021) claim that behaviour-based transaction monitoring tools improve attack detection techniques, especially for distributed software systems. According to the results of the two studies, behaviour-based transaction monitoring uses the immutability of blockchain technology to improve the detection of fraudulent behaviour. Unlike the rule-based method, this approach reduces the rate of false positives despite the inherent trade-off of adopting blockchain technology. In addition to the qualitative results, the quantitative results from testing the first hypothesis also contributed to answering the first research question. The paired t-test revealed a moderate positive correlation between the ratings of the effectiveness of rule-based and behaviour-based transaction monitoring systems. In addition, Cohen's d and the Hedges' correction indicated a positive effect size, suggesting that the behaviour-based framework is rated more effective on average than the rule-based framework, confirming the first alternative hypothesis.

The above study results are consistent with other research findings. For example, Petterson Ruiz and Angelis' (2022) conclusion that rule-based transaction monitoring is characterised by low detection rates, increased bias and false positives is consistent with the findings of Stojanovi et al. (2021) and Oztas et al. (2022). According to Stojanovi et al. (2021) and Oztas et al. (2022), although most financial institutions have adopted rule-based approaches to monitor their transactions, 95% of reported transactions are false positives, which is time-consuming and costly for financial institutions. Comparing risk-based and rule-based approaches, Sinha (2019) found that the rule-based approach has significant limitations, including the lack of sufficient functionality to fully monitor transactions. The qualitative and quantitative findings related to behaviour-based transaction monitoring tools and techniques are consistent with those in the academic literature. For example, Chao et al. (2019) found that behaviour-based transaction monitoring methods enable financial institutions to focus on transaction monitoring and due diligence to detect fraud and money laundering. Behaviour-based monitoring, according to the researchers, improves the surveillance system and transaction monitoring by assessing abnormal behaviour using surveillance classification techniques. The findings regarding the effectiveness of behaviour-based transaction monitoring tools and techniques are also consistent with the findings of Zola (2022) and Cao (2020) in the literature. According to the two studies, synthetic behaviour facilitates the learning process of ML techniques, resulting in SM-hybrid and R-hybrid monitoring techniques with high classification effectiveness. In addition, the researchers found that data science and artificial intelligence, including behavioural modelling, improve the efficiency of transaction monitoring by identifying unusual activity, malware and suspicious transactions.

In preventing and detecting cryptocurrency fraud and money laundering, both rule-based transaction monitoring techniques and behaviour-based transaction monitoring approaches have their strengths and weaknesses, according to current research and literature. Despite the fact that rule-based transaction monitoring provides a structured approach to national regulations, it remains too simplistic and is therefore associated with low detection rates, increased bias and a high rate of false positives. This is not the case with behaviour-based transaction monitoring tools and techniques that use the immutability of blockchain technology to detect fraudulent behaviour. Unlike rule-based transaction monitoring, behaviour-based approaches have a low false positive rate and are relatively effective in detecting fraud and money laundering in distributed software systems. Although the effectiveness of behaviour-based monitoring methods should not be underestimated, the combination of both methods can greatly facilitate the detection and prevention of fraud and money laundering.

### 5.2 Discussion of Research Question Two

The second research question was how cooperation between regulators and financial institutions influences the effectiveness of transaction monitoring practices. Under the second theme, “Institutional and Regulatory Collaboration on Cryptocurrency Security”, the qualitative findings confirmed the importance of transaction monitoring collaboration in preventing cryptocurrency fraud and money laundering. According to Cummings, Johan and Pant (2019), collaboration between crypto developers and government agencies should be encouraged as it promotes innovation and ensures the safety of investors and other stakeholders. These findings also apply to Limba, Stankevičius, and Andrulevičius (2019), whose study highlights the importance of regulatory measures to promote the sustainable use of cryptocurrencies.

Cooperation between regulators and financial institutions would help address issues related to the transfer of accounts to third parties and the need for a unified regulatory framework, it is argued. Nabilou's (2019) study also highlighted the limitations of a decentralised approach to cryptocurrencies and advocated for a centralised regulatory framework that engages industry participants and builds on existing regulatory infrastructure. According to the researcher, this is how payment institutions and banking systems can effectively address the systemic risks posed by virtual currencies and cryptocurrencies. The quantitative results, especially the results of the test of the second research hypothesis, also contribute to answering the second research question. The regression analysis revealed a strong correlation between the variables of cooperation effectiveness and performance effectiveness. The low p-value and high t-value of the model indicate that the variable of cooperation effectiveness significantly influences the variable of performance effectiveness. Therefore, cooperation between regulators and financial institutions improves the performance of transaction monitoring practices, confirming the second alternative hypothesis.

The results of this study suggest that cooperation between regulators and financial institutions is warranted as it helps to improve transaction monitoring practices. The qualitative and quantitative data results mentioned above are consistent with several findings in the literature. For example, the findings are consistent with those of Cociug and Andrtsceac (2020) and Hasham, Joshi and Mikkelsen (2019), who recommend in their study that the scope of the RBA be expanded to include cross-border risks. An example of this is the EU Anti-Money Laundering and Countering the Financing of Terrorism (AML/CFT) framework, which, according to Cociug and Andrtsceac (2020) and Hasham, Joshi and Mikkelsen (2019), has promoted uniform guidance on disclosure obligations and direct powers for different financial actors and, most importantly, has

provided a robust framework for EU Financial Intelligence Units (FIUs) to cooperate in assessing risks. For example, Hasham, Joshi and Mikkelsen (2019) and Katterbauer, Syed and Cleenewerck (2022) have found that effective coordination between financial institutions and stakeholders yields greater returns than promoting the traditional model. Furthermore, Hasham, Joshi and Mikkelsen (2019) argue that collaborative models within traditional banking and financial institutions as well as cryptocurrency exchanges maintain the status quo, with each area, be it fraud, financial crime or cybersecurity, retaining its independent reporting, roles and responsibilities, and developing its own paradigm and risk taxonomy. Although Katterbauer, Syed and Cleenewerck (2022) recognise the importance of the collaborative model, they believe, as noted in this study, that collaboration can unfortunately reduce financial crime risks and limit integration. Ansari (2018) and Um and Kim (2019) are two other academic studies that agree with the current findings on collaboration. According to these two studies, a universal system framework for AML is needed to enable an all-inclusive decision-making process. This universal system framework is the result of collaboration and, if properly implemented, increases the security of traditional banking and financial institutions as well as cryptocurrency exchanges. However, a number of studies refute the benefits of the collaborative model in transaction monitoring as outlined in this research. For example, the study by Hasham, Joshi and Mikkelsen (2019) not only highlights the existing model of collaboration within traditional banking and financial institutions, but also concludes that collaboration means little transparency in effectively managing financial crime risks. Li et al. (2020) argue in another study that collaborative models overlook the scalability benefits of broader functional integration. Such collaborative models are vulnerable to insider attacks and require the implementation of appropriate security protocols.

Therefore, cooperation and collaboration between regulators and financial institutions, as well as collaboration within traditional banking and financial institutions, are essential for promoting effective transaction monitoring practices against cryptocurrency fraud and money laundering, as both the results of the current study and the literature show. Cooperation can lead to better coordination between financial actors, a robust framework for fraud monitoring professionals and uniform guidelines. Nevertheless, collaborative models can limit transparency, ignore the scalability of broader functional integration and be vulnerable to insider attacks that require security protocols.

### 5.3 Discussion of Research Question Three

The third research question was how modern technological fraud detection tools differ from traditional fraud detection tools. Studies by Kurshan, Shen and Yu (2020) found that traditional fraud detection tools, such as the rule-based approach, are ineffective in preventing digital fraud and money laundering related to cryptocurrencies. This limitation was also noted by Egbiri and Azinge (2018), whose research confirmed that traditional rule-based fraud and money laundering detection tools are inadequate. According to these researchers, a new legal framework is needed to standardise cryptocurrency operators and Bitcoin operations. Lokanan (2023) reiterated in his studies the comparative advantage of using visualisation techniques to prevent money laundering and detect cryptocurrency fraud. According to the researcher, sophisticated technological fraud detection tools such as unsupervised clustering analysis and graph methodology are critical in identifying criminal relationships and fraudulent transactions and addressing the challenges posed by evolving financial fraud. In the same context, Vosyliūtė and Maknickienė (2022) agreed that modern problems require modern solutions. They suggested the incorporation of artificial

intelligence-based techniques to improve fraud detection results and to identify the intricate web of digital financial fraud and money laundering. In addition to the qualitative results presented earlier, the quantitative results, particularly the testing of the third hypothesis, shed light on the comparative effectiveness of modern technological and traditional fraud detection tools. The quantitative results show that the effectiveness of modern tools received a significantly higher mean score than that of traditional tools, indicating that the vast majority of respondents rated modern tools and techniques as highly effective in preventing fraud and money laundering. Furthermore, the negative mean difference of the paired t-tests' t-value indicates that the majority of respondents considered modern tools to be more effective than traditional tools and methods; therefore, the third alternative hypothesis was accepted and the corresponding null hypothesis rejected.

The above qualitative and quantitative findings regarding the effectiveness of modern and traditional fraud detection tools are consistent with the findings in the literature. The study by Jin et al. (2022), which focuses on traditional fraud detection tools, acknowledges that traditional fraud monitoring systems are not as effective and suffer from two major limitations. According to the study, the first limitation of traditional fraud detection tools is that they are unable to integrate data from multiple sources, making them an outdated and inadequate system. The second limitation is that traditional fraud detection tools have limited technological methods for timely early warning. Another study that sheds light on the effectiveness of traditional fraud detection tools is that of Oztas et al. (2022), which finds not only that most financial institutions use rule-based solutions, but also that this approach has a false positive rate of over 95%, making it more costly for companies. In addition, the literature discusses the effectiveness of modern fraud detection tools,

with Pourhabibi et al. (2020) and Lokanan (2023) recommending graph-based anomaly detection that integrates data mining and machine learning techniques for fraud detection. According to Pourhabibi et al. (2020), graph-based anomaly detection helps in describing the relationship patterns and connectivity of a network to detect unusual transaction trends. According to Amudha (2021), advanced fraud detection tools such as cryptography techniques protect blockchain transactions from malicious blockchain users. This finding is in line with current evidence on the effectiveness of modern fraud detection tools. The research conducted by Rajeb et al. (2021) is also consistent with recent findings on the effectiveness of modern fraud detection tools. According to this study, the implementation of blockchain technology in this context improves collaboration between transaction parties and, more importantly, speeds up information sharing mechanisms, improves communication between parties and facilitates better decision-making by fraud monitoring professionals.

Therefore, to prevent money laundering and other forms of digital fraud, modern technological fraud detection tools offer more advantages than traditional fraud detection tools. Traditional fraud detection tools are unsuitable for digital and virtual currencies due to their high false positive rate, which is expensive and time-consuming. Traditional fraud detection tools have limited technological methods to ensure timely early warning and do not integrate data from multiple sources, making them outdated and insufficient. However, modern fraud detection tools are more effective as they have a low false positive rate. Due to the complexity of digital fraud and money laundering, these tools are indispensable to detect criminal relationships and identify fraudulent transactions. They also facilitate the exchange of information and improve cooperation between the actors and parties involved in the transactions.

# CHAPTER VI: CONCLUSION AND RECOMMENDATIONS

## 6.1 Summary of Main Results and Findings

The anonymity, accessibility and decentralised nature of cryptocurrencies have given rise to the dark side of the cryptocurrency market, which includes fraud and money laundering. As financial institutions increasingly use digital and virtual currencies, it is essential to develop robust strategies that effectively protect users and stakeholders from illicit activities in the digital world. Against this backdrop, the current study emphasises the importance of monitoring cryptocurrency transactions to detect and prevent fraud and money laundering. The study assessed the current state of transaction monitoring tools and techniques and highlighted their effectiveness, strengths and weaknesses.

With regard to transaction monitoring techniques, this study found that rule-based transaction monitoring is an essential structured approach for national regulators to combat fraud and money laundering. However, relying too much on rule-based transaction monitoring makes the approach too simplistic, resulting in a high rate of false positives and a low fraud detection rate. The situation is different with behaviour-based transaction monitoring tools and techniques, which use the immutability of the blockchain to reduce false alarms and detect fraud.

This study also assessed the effectiveness of cooperation between regulators and financial institutions. The results showed that cooperation between crypto developers, financial institutions and regulators is essential for promoting effective transaction monitoring practices. Such cooperation is essential for fostering innovation in digital and virtual currencies and protecting market participants and investors. Moreover, it was noted that a centralised approach to

cryptocurrencies is essential to address issues related to account transfers and to promote consistency in regulatory measures and frameworks.

Furthermore, the study compared the effectiveness of traditional fraud detection tools with that of modern technological fraud detection tools. According to the study, traditional fraud detection tools which use a rule-based approach, are not sufficient to prevent digital fraud and money laundering related to cryptocurrencies. The use of modern tools and techniques, such as graph methodology, visualisation techniques and unsupervised clustering analysis, improves the detection of fraudulent transactions and criminal patterns. Therefore, traditional methods are less effective than modern tools and techniques in detecting and preventing cryptocurrency fraud and money laundering.

### 6.2 Implications for Practitioners

As the cryptocurrency market continues to evolve, practitioners are encouraged to be proactive and vigilant when developing strategies to protect stakeholders and ensure market security. This study highlights the need for a balanced transaction monitoring strategy. For example, practitioners need to recognise the need for both rule-based monitoring approaches to promote structure and compliance, and behaviour-based monitoring approaches to detect fraudulent activity and effectively reduce false positive rates. Combining these two strategies increases the likelihood of establishing a robust and comprehensive fraud detection system.

Furthermore, the study found that modern technological tools and techniques are more effective than their traditional counterparts. Given the shortcomings of traditional fraud detection

tools identified in the study, practitioners need to be open to incorporating modern technological tools such as graph methodology and unsupervised cluster analysis to improve their fraud detection capabilities. The growing scale of digital currencies requires innovative approaches to combat sophisticated fraud and money laundering schemes. Practitioners' ability to detect fraudulent transactions and fraudulent criminal patterns and relationships in cryptocurrency transactions can be enhanced through innovation.

Facilitating cooperation and collaboration in identifying and preventing cryptocurrency fraud and money laundering is another implication for practitioners. The study recognises the importance of collaboration between cryptocurrency developers, financial institutions and regulators, as well as within traditional banking and financial institutions using a unified collaborative model. Therefore, practitioners need to proactively engage all stakeholders and partners in the cryptocurrency market to foster innovation and ensure investor and stakeholder safety and regulatory compliance. Hence, practitioners can directly contribute to fostering a trustworthy and secure cryptocurrency ecosystem by promoting collaboration and dialogue.

### 6.3 Recommendations for Banking and Financial Institutions

The following recommendations should be considered by banking and financial institutions, as well as cryptocurrency exchanges to improve transaction monitoring and prevent fraud and money laundering in cryptocurrencies:

1. Introduce a layered approach to transaction monitoring: The present study has shown the effectiveness of rule-based and behaviour-based transaction monitoring techniques. Adopting a

layered approach to transaction monitoring that incorporates both rule-based and behaviour-based techniques will improve fraud detection, reduce false positives and identify suspicious activity and other critical threats. This will allow banking and financial institutions to capture a broader range of fraudulent behaviour and reduce the risk of missing critical threats.

2. Strengthening compliance and cooperation: Proactive cooperation with relevant regulators would help banking and financial institutions develop a consistent and comprehensive regulatory framework for cryptocurrencies. Such cooperation will create a secure environment for crypto innovation and ensure the protection of all parties involved in the transactions. Financial institutions can clarify the expectations of users of virtual and digital currencies by engaging in dialogue with regulators, complying with existing regulations and advocating for new regulations that meet the evolving challenges of cryptocurrencies.

3. Invest in advanced security education and training: Banking and financial institutions must prioritise education and training programmes that provide their employees with security skills and knowledge about cryptocurrencies. This recommendation is based on the dynamic nature of the cryptocurrency industry, which requires that employees are equipped with the most up-to-date skills to detect, prevent and respond to cryptocurrency-related fraud and money laundering. It should be noted that a well-trained workforce is an essential first line of defence in detecting and preventing fraud and money laundering.

4. Incorporate advanced data analytics and machine learning into the monitoring of financial transactions: This recommendation stems from the fact that the complexity and sheer volume of

data associated with detecting money laundering and cryptocurrency fraud is one of the biggest obstacles. Banking and financial institutions can effectively improve their transaction monitoring capabilities by investing in machine learning and data analytics. They will also be able to analyse large volumes of transaction data in real time to detect anomalies and fraudulent or suspicious patterns. In addition, machine learning algorithms will ensure the effectiveness of transaction monitoring by being able to learn and adapt from previous data. Based on machine learning algorithms, it is also possible to develop predictive models to proactively detect and combat potential cases of money laundering or fraud.

5. Regular compliance audits and updates: It is important to recognise that cryptocurrency regulations are constantly changing in most jurisdictions. To stay compliant with the latest regulatory framework, banking and financial institutions need to keep up with all changes related to cryptocurrency activities and conduct regular compliance audits. Financial institutions benefit from having a dedicated department or team responsible for monitoring and implementing regulatory changes. Such a team helps banking and financial institutions keep up with evolving regulations and the need to adapt procedures and processes to maintain a solid compliance and security reputation and avoid fines and other related legal issues.

### 6.4 Recommendations for Future Research

Future research should address the various facets of monitoring virtual currency transactions, cryptocurrency fraud and money laundering to fill the existing knowledge gap. Future research should first conduct a thorough analysis of cryptocurrency mixing services and explain their role in facilitating fraud and money laundering. This study should incorporate real-world

examples, examine new mixing techniques and evaluate the effectiveness of anti-money laundering measures for virtual currencies. Second, future research should highlight the vulnerabilities of cryptocurrency wallets and provide an understanding of the user behaviour that fraudsters often target. By describing the different methods cybercriminals use to compromise cryptocurrency wallets, the fraud can be better understood and appropriate preventive measures or solutions can be prescribed. Future research should also examine the impact of regulatory differences on cryptocurrency fraud and money laundering. As mentioned earlier, different countries and regions have different regulatory requirements for cryptocurrency fraud and money laundering. Therefore, future research should investigate how different approaches affect the behaviour of money launderers and fraudsters. This study should identify the patterns and trends that are important for evidence-based regulatory cooperation frameworks in the fight against cryptocurrency crime.

### 6.5 Limitations of the Study

Twelve participants and eleven secondary sources were used to collect quantitative and qualitative data respectively. However, according to Kang (2021), the use of a small sample, such as the one used in the study, may limit the generalisability of the results as the sample may not accurately represent the total population. According to Kang (2021), the limited data from such a sample may make it difficult for researchers to draw meaningful conclusions about the entire population. In addition, the small sample size may have reduced the statistical power of the results, as the sensitivity for detecting significant differences and associations is low despite the possibility that they exist. This suggests that the current study may be prone to sampling error, leading to

unreliable or inaccurate estimates, especially in statistical analyses. Therefore, future studies should consider a larger sample to validate the results.

## 6.6 Conclusion

In conclusion, this study has shed light on the dynamic and complex areas of cryptocurrency fraud and money laundering, including the multiple challenges that characterise the landscape of evolving virtual and digital currencies. Following a comprehensive analysis of transaction monitoring strategies, technological advances and regulatory cooperation, the study has identified key lessons for improving transaction monitoring practices and preventing fraud and money laundering. The study highlighted the importance of adopting a multi-layered approach that includes both rule-based and behaviour-based transaction monitoring practices. Collaboration and cooperation were also crucial for financial institutions, cryptocurrency developers and regulators, as they fostered innovation and ensured the overall security of the cryptocurrency ecosystem.

# REFERENCES


Abdallah, A.H., 2022. Challenges of applying Ethiopian VAT on electronic commerce transaction. Amsterdam LF, 14, p. 1.

Ali, N., 2022. Crimes related to cryptocurrency and regulations to combat crypto crimes. Journal of Policy Research, 8(3), pp. 289-302.

Aljihani, H., Eassa, F., Almarhabi, K., Algarni, A. and Attaallah, A., 2021. Standalone behaviour-based attack detection techniques for distributed software systems via Blockchain. Applied Sciences, 11(12), p.5685.

Amudha, G., 2021. Dilated transaction access and retrieval: Improving the information retrieval of blockchain-assimilated Internet of Things transactions. Wireless Personal Communications, pp. 1-21.

Arora, R., 2017. Questionnaire designing: Some useful tips. International Journal of Contemporary Research and Review.

Asenahabi, B.M., 2019. Basics of research design: A guide to selecting an appropriate research design. International Journal of Contemporary Applied Researches, 6(5), pp. 1–14.

Avhustova, O.O., 2018. The economic content of cryptocurrency and accounting of cryptocurrency in Ukraine. Economy and Society, 18.

Braaten, C. and Vaughn, M.S., 2021. Convenience theory of cryptocurrency crime: A content analysis of US federal court decisions. Deviant Behaviour, 42(8), pp. 958-978.

Bynagari, N.B. and Ahmed, A.A.A., 2021. Anti-money laundering recognition through the gradient boosting classifier. Academy of Accounting and Financial Studies Journal, 25(5), pp. 1-11.

Campbell, K., Orr, E., Durepos, P., Nguyen, L., Li, L., Whitmore, C., Gehrke, P., Graham, L. and Jack, S., 2021. Reflexive thematic analysis for applied qualitative health research. The Qualitative Report, 26(6), pp. 1–18.

Campbell-Verduyn, M., 2018. Bitcoin, crypto-coins, and global anti-money laundering governance. Crime, Law and Social Change, 69, pp.283-305.

Cao, L., 2020. AI in Finance: A review. SSRN Electronic Journal, pp. 1-36.

Casula, M., Rangarajan, N. and Shields, P., 2020. The potential of working hypotheses for deductive exploratory research. Quality & Quantity, 55(1), pp. 1703–1725.

Chao, X., Kou, G., Peng, Y. and Alsaadi, F.E., 2019. Behaviour monitoring methods for trade-based money laundering integrating macro and micro prudential regulation: A case from China. Technological and Economic Development of Economy, 25(6), pp. 1081-1096.

Charoenthammachoke, K., Leelawat, N., Tang, J. and Kodaka, A., 2020. Business continuity management: A preliminary systematic literature review based on the Science Direct database. Journal of Disaster Research, 15(5), pp. 546–555.

Cociug, V. and Andrtsceac, T., 2020. Risk-based approach in the European Union legislation to prevent money laundering and financing of terrorism. Economy and Sociology, 1(1), pp. 43-52.

Cumming, D.J., Johan, S. and Pant, A., 2019. Regulation of the crypto-economy: Managing risks, challenges, and regulatory uncertainty. Journal of Risk and Financial Management, 12(3), p.126.

De Langhe, R. and Schliesser, E., 2017. Evaluating philosophy as exploratory research. Metaphilosophy, 48(3), pp. 227–244.

Desmond, D.B., Lacey, D. and Salmon, P., 2019. Evaluating cryptocurrency laundering as a complex socio-technical system: A systematic literature review. Journal of Money Laundering Control, 22(3), pp. 6-70.

Dierksmeier, C. and Seele, P., 2020. Blockchain and business ethics. Business Ethics: A European Review, 29(2), pp. 348-359.

Dziura, M., Jaki, A. and Rojek, T., 2020. Restructuring Management models – Changes – Development. Poland: TNOiK Dom Organizatora.

Ebrahimi, M., Chai, Y., Samtani, S. and Chen, H., 2022. Cross-lingual cybersecurity analytics in the international dark web with adversarial deep representation learning. MIS Quarterly, 46(2), pp. 1209-1226.

Egbiri, E.I. and Azinge, N.V., 2018. Bitcoin Regulation: Imperfect Knowledge of Identities and the Money Laundering Risk: A West African Perspective. JACL, 2, p.163.

Engin, Z., Van Dijk, J., Lan, T., Longley, P.A., Treleaven, P., Batty, M. and Penn, A., 2020. Data-driven urban management: Mapping the landscape. Journal of Urban Management, **9**(2), pp. 140-150.

Fleck, A., 2022. Infographic: Cybercrime expected to skyrocket in coming years. Statista.

Florea, I.O. and Nitu, M., 2020. Money laundering through cryptocurrencies. The Romanian Economic Journal, pp. 1–6.

Gerlick, J.A. and Liozu, S.M., 2020. Ethical and legal considerations of artificial intelligence and algorithmic decision-making in personalised pricing. Journal of Revenue and Pricing Management, 19(2), pp. 85-98.

Glattke, T.J., 2017. International research collaborations: Ethical and regulatory considerations. The ASHA Leader, 12(17), pp. 19–21.

Goodwin, L.D. and William, G., 2020. Qualitative vs. quantitative research or qualitative and quantitative research? Nursing Research, 33(6), pp. 378–384.

Hairudin, A., Sifat, I.M., Mohamad, A. and Yusof, Y., 2022. Cryptocurrencies: A survey on acceptance, governance and market dynamics. International Journal of Finance & Economics, 27(4), pp. 4633-4659.

Han, J., Huang, Y., Liu, S. and Towey, K., 2020. Artificial intelligence for anti-money laundering: A review and extension. Digital Finance, 2(3-4), pp. 211–239.

Hasham, S., Joshi, S. and Mikkelsen, D., 2019. Financial crime and fraud in the age of cybersecurity. McKinsey & Company, pp. 1-11.

Hothersall, S.J., 2018. Epistemology and social work: Enhancing the integration of theory, practice and research through philosophical pragmatism. European Journal of Social Work, 22(5), pp. 1–11.

Hu, H. and Xu, Y., 2021. SCSGuard: Deep scam detection for Ethereum smart contracts. Cryptography and Security, pp. 1-8.

Hyvernat, P., 2014. Some properties of inclusions of multisets and contractive Boolean operators. Discrete Mathematics, 329, pp. 69–76.

Ilijevski, I., Ilik, G. and Babanoski, K., 2023. Cryptocurrency abuse for the purposes of money laundering and terrorism financing: Policies and practical aspects in the European Union and North Macedonia. ESI Preprints, 15, pp. 23–43.

Javadi, M. and Zarea, K., 2016. Understanding thematic analysis and its pitfall. Journal of Client Care, 1(1), pp. 34–40.

Jin, J., Zhou, J., Jin, C., Yu, S., Zheng, Z. and Xuan, Q., 2022. Dual-channel early warning framework for Ethereum Ponzi schemes. Big Data and Social Computing, pp. 260-274.

Kang, H., 2021. Sample size determination and power analysis using the G* Power software. Journal of educational evaluation for health professions, 18.

Karthikeyan, T., Govindarajan, M. and Vijayakumar, V., State of Art of Various Analysis and Fraudulent Activity Prediction Techniques Based on Behaviour Analysis.

Katterbauer, K., Syed, H. and Cleenewerck, L., 2022. Financial cybercrime in the Islamic Finance Metaverse. Journal of Metaverse, 2(2), pp. 56-61.

Kelly, L.M. and Cordeiro, M., 2020. Three principles of pragmatism for research on organisational processes. Methodological Innovations, 13(2), pp. 1–10.

Kişi, N., 2022. Exploratory research on the use of blockchain technology in recruitment. Sustainability, 14(16), p. 10098.

Kuperberg, M., Kemper, S. and Durak, C., 2019. Blockchain usage for government-issued electronic IDs: A survey. Lecture Notes in Business Information Processing, pp. 155–167.

Kurshan, E., Shen, H. and Yu, H., 2020, September. Financial crime & Fraud detection using graph computing: Application considerations & Outlook. In 2020 Second International Conference on Transdisciplinary AI (TransAI) (pp. 125-130). IEEE.

Kutera, M., 2022. Cryptocurrencies as a subject of financial fraud. Journal of Entrepreneurship, Management and Innovation, 18(4), pp. 45-77.

Lakshmi, P., Stalin David, D., Kalaria, I., Jayadatta, S., Sharma, A. and Saravanan, D., 2021. Research on collaborative innovation of e-commerce business model for commercial transactions. Turkish Journal of Physiotherapy and Rehabilitation, 32(3), pp. 787-794.

Li, W., Wang, Y., Li, J. and Au, M.H., 2021. Toward a blockchain-based framework for challenge-based collaborative intrusion detection. International Journal of Information Security, 20(2), pp. 127-139.

Limba, T., Stankevičius, A. and Andrulevičius, A., 2019. Towards sustainable cryptocurrency: Risk mitigations from a perspective of national security. Journal of security and sustainability issues, 9, pp.375-389.

Lin, D., Wu, J., Xuan, Q. and Tse, C.K., 2022. Ethereum transaction tracking: Inferring evolution of transaction networks via link prediction. Physica A: Statistical Mechanics and its Applications, 600, p. 127504.

Lokanan, M.E., 2023. Financial fraud detection: The use of visualisation techniques in credit card fraud and money laundering domains. Journal of Money Laundering Control, 26(3), pp.436-444.

Maarouf, H., 2019. Pragmatism as a supportive paradigm for the mixed research approach: Conceptualising the ontological, epistemological, and axiological stances of pragmatism. International Business Research, 12(9), pp. 1–12.

Malmivaara, A., 2019. Generalisability of findings from randomised controlled trials is limited in the leading general medical journals. Journal of Clinical Epidemiology, 107, pp. 36–41.

McKim, C.A., 2017. The value of mixed methods research. Journal of Mixed Methods Research, 11(2), pp. 202–222.

Mondal, P. and Mondal, S., 2018. Quantitative and qualitative research: A mixed method approach in educational science. International Journal of Technical Research & Science, 3(7).

Müller, S., 2021. The new ecosystem of the digital age: Impact of blockchain technology on the accounting environment and financial statement fraud detection. Lisboa: ISCTE Business School.

Mundra, P.A. and Rajapakse, J.C., 2016. Gene and sample selection using T-score with sample selection. Journal of Biomedical Informatics, 59, pp. 31–41.

Murko, A. and Vrhovec, S.L., 2019. Bitcoin adoption: Scams and anonymity may not matter but trust into Bitcoin security does. Proceedings of the Third Central European Cybersecurity Conference, pp.1-6.

Nabilou, H., 2019. How to regulate bitcoin? Decentralised regulation for a decentralised cryptocurrency. International Journal of Law and Information Technology, 27(3), pp.266-291.

Nguyen, N.X., Tran, K. and Nguyen, T.A., 2021. Impact of service quality on in-patients' satisfaction, perceived value, and customer loyalty: A mixed-methods study from a developing country. Patient Preference and Adherence, 15, pp. 2523–2538.

Oana Florea, I. and Nitu, M., 2020. Money laundering through cryptocurrencies. The Romanian Economic Journal, pp. 1–6.

Onghena, P., Maes, B. and Heyvaert, M., 2018. Mixed methods single case research: State of the art and future directions. Journal of Mixed Methods Research, pp. 1–20.

Oztas, B., Cetinkaya, D., Adedoyin, F. and Budka, M., 2022. Enhancing transaction monitoring controls to detect money laundering using machine learning. ICEBE, pp. 1-3.

Pagano, M.S. and Sedunov, J., 2018. Bitcoin and the demand for money: Is Bitcoin more than just a speculative asset? SSRN Electronic Journal, pp. 1–96.

Pettersson Ruiz, E. and Angelis, J., 2022. Combating money laundering with machine learning–applicability of supervised-learning algorithms at cryptocurrency exchanges. Journal of Money Laundering Control, 25(4), pp.766-778.

Pourhabibi, T., Ong, K.-L., Kam, B.H. and Boo, Y.L., 2020. Fraud detection: A systematic literature review of graph-based anomaly detection approaches. Decision Support Systems, 133, pp. 11-33.

Rejeb, A., Keogh, J.G., Simske, S.J., Stafford, T. and Treiblmaier, H., 2021. Potentials of blockchain technologies for supply chain collaboration: A conceptual framework. The International Journal of Logistics Management, 32(3), pp. 973-994.

Saltz, J., Skirpan, M., Fiesler, C., Gorelick, M., Yeh, T., Heckman, R., Dewar, N. and Beard, N., 2019. Integrating ethics within machine learning courses. ACM Transactions on Computing Education, 19(4), pp. 1-26.

Savona, E.U. and Riccardi, M., 2019. Assessing the risk of money laundering: Research challenges and implications for practitioners. European Journal on Criminal Policy and Research, 25(1), pp. 1-4.

Shim, H.-S., 2016. An exploratory study on the analysing introduction purpose of corporate real estate property management. SH Urban Research & Insight, 6(1), pp. 103–116.

Sinha, G., 2019. Is it the answer to effective anti-money laundering compliance? In: Benson, K., King, C. and Walker, C. (Eds.). Assets, crimes and the state. London: Routledge, pp.1-14.

Soana, G., 2021. Regulating cryptocurrencies checkpoints: Fighting a trench war with cavalry? Economic Notes, 51(1).

Spohn, D., 2018. Bitcoin Poison? Anecdotal evidence from Bitcoin miners' revenue. Applied Economics and Finance, 5(4), pp. 15–30.

Timans, R., Wouters, P. and Heilbron, J., 2019. Mixed methods research: What it is and what it could be. Theory and Society, 48(2), pp. 193–216.

Trimble, L., 2018. Accessibility at JSTOR: From box-checking to a more inclusive and sustainable future. Learned Publishing, 31(1), pp. 21–24.

Turki, M., Hamdan, A., Cummings, R.T., Sarea, A., Karolak, M. and Anasweh, M., 2020. The regulatory technology “RegTech” and money laundering prevention in Islamic and conventional banking industry. Heliyon, 6(10), pp. 40–69.

Um, K.H. and Kim, S.M., 2019. The effects of supply chain collaboration on performance and transaction cost advantage: The moderation and nonlinear effects of governance mechanisms. International Journal of Production Economics, 217, pp. 97-111.

Vassallo, D., Vella, V. and Ellul, J., 2021. Application of gradient boosting algorithms for anti-money laundering in cryptocurrencies. SN Computer Science, 2(3), p. 143.

Vilhuber, L., 2018. Relaunching the journal of privacy and confidentiality. Journal of Privacy and Confidentiality, 8(1).

Vitvitskiy, S.S., Kurakin, O.N., Pokataev, P.S., Skriabin, O.M. and Sanakoiev, D.B., 2021. Formation of a new paradigm of anti-money laundering: The experience of Ukraine. Problems and Perspectives in Management, 19(1), pp. 354-363.

Vosyliūtė, I. and Maknickienė, N., 2022. Investigation of financial fraud detection by using computational intelligence.

Vovk, V., Zhezherun, Y., Bilovodska, O., Babenko, V. and Biriukova, A., 2020. Financial monitoring in the bank as a market instrument in the conditions of innovative development and digitalisation of economy: Management and legal aspects of the risk-based approach. International Journal of Industrial Engineering & Production Research, 31(4), pp. 559-570.

Wan, Y., Xiao, F. and Zhang, D., 2022. Early-stage phishing detection on the Ethereum transaction network. Soft Computing, pp. 1-13.

Wegberg, R. van, Oerlemans, J.-J. and Van Deventer, O., 2018. Bitcoin money laundering: Mixed results? An explorative study on money laundering of cybercrime proceeds using Bitcoin. Journal of Financial Crime, 25(2), pp. 419–435.

Wester, K. and McKibben, B., 2019. Integrating mixed methods approaches in counselling outcome research. Counselling Outcome Research and Evaluation, 10(1), pp. 1–11.

Wheeler, R., 2017. The evolution of informed consent. British Journal of Surgery, 104(9), pp. 1119–1120.

Zola, F., 2022. Behavioural analysis in cybersecurity using machine learning. A study based on graph representation, class imbalance and temporal dissection. Spain: UPNA.

APPENDICES

## APPENDIX A: QUESTIONNAIRE

### Part 1: Demographic Data

1. What is your gender?

   1 - Male

   2 - Female

   3 - Non-binary

   4 - I prefer not to say

2. What is your age?

   1 - Under 18

   2 - 18-24

   3 - 25-34

   4 - 35-44

   5 - 45-54

   6 - 55-64

   7 - 65 or older

3. What is your current education level?

   1 - High School or below

   2 - Bachelor's Degree

   3 - Master's Degree

   4 - Doctorate or Professional Degree

**Part 2: Research Questions**

1. To what extent do you believe that behaviour-based transaction monitoring effectively detects and prevents cryptocurrency fraud?

   1 - Strongly Disagree

   2 - Disagree

   3 - Neutral

   4 - Agree

   5 - Strongly Agree

2. To what extent do you believe that rule-based transaction monitoring effectively detects and prevents cryptocurrency fraud?

   1 - Strongly Disagree

   2 - Disagree

   3 - Neutral

   4 - Agree

   5 - Strongly Agree

3. Is cooperation between regulators and financial institutions important for improving transaction monitoring practices?

   1 - Strongly Disagree

   2 - Disagree

   3 - Neutral

   4 - Agree

   5 - Strongly Agree

4. Are modern technological fraud detection tools effective compared to traditional cryptocurrency fraud detection tools?

   1 - Strongly Disagree

   2 - Disagree

   3 - Neutral

   4 - Agree

   5 - Strongly Agree

5. Are traditional fraud detection tools effective compared to modern technological fraud detection tools in the cryptocurrency space?

   1 - Strongly Disagree

   2 - Disagree

   3 - Neutral

   4 - Agree

   5 - Strongly Agree

6. How satisfied are you with the current state of cooperation and communication between regulators and financial institutions in your region regarding transaction monitoring?

   1 - Very Dissatisfied

   2 - Dissatisfied

   3 - Neutral

   4 - Satisfied

   5 - Very Satisfied

7. How concerned are you about the potential risks of cryptocurrency fraud and money laundering?

   1 - Not Concerned at All

   2 - Slightly Concerned

   3 - Moderately Concerned

   4 - Very Concerned

   5 - Extremely Concerned

8. How likely are you to recommend the introduction of efficient transaction monitoring systems to prevent cryptocurrency fraud and money laundering?

   1 - Very Unlikely

   2 - Unlikely

   3 - Neutral

   4 - Likely

   5 - Very Likely

9. In your opinion, how well do the techniques and tools currently used in the financial sector for transaction monitoring meet the requirements for preventing cryptocurrency fraud and money laundering?

   1 - Not Well at All

   2 - Not Well

   3 - Neutral

   4 - Well

   5 - Very Well

10. To what extent can improving transaction monitoring practices and cooperation significantly reduce cryptocurrency fraud and money laundering?

    1 - Not at All

    2 - Slightly

    3 - Moderately

    4 - Significantly

    5 - Completely

**APPENDIX B: CONSENT FORM**

Dear Research Participant,

A study on the role of transaction monitoring in the detection and prevention of cryptocurrency fraud and money laundering: Implications for fraud monitoring professionals invites you to participate as a study participant. This study aims to investigate the effectiveness of transaction monitoring in detecting and preventing cryptocurrency fraud and money laundering and to provide recommendations for fraud monitoring professionals to improve their fraud detection capabilities. The study includes a questionnaire with multiple response options for each question. It takes approximately 20 minutes to complete the questionnaire. Participation in this study involves minimal risk but brings tremendous benefits, including improving approaches and strategies used by fraud monitoring professionals to detect and prevent money laundering and fraudulent activity. Your responses to the questionnaire, including demographic information such as your name and other personal identifiers, will be kept confidential. The information is stored securely and is inaccessible to unauthorised persons. Participation in this study is completely voluntary. You are therefore free to withdraw or refuse to participate in the study at any time.

I have read and understood the above information and agree to participate voluntarily in this study.

Name of participant: _____

Signature of participant: _____ Date: _____

## APPENDIX C: PARTICIPANT'S DETAILS

| User ID | Age | Gender<br>(M = Male)<br>(F = Female)<br>(NB = Non-Binary) | Position | Education | Organisation |
|---|---|---|---|---|---|
| | 28 | M | Credit Fraud Analyst | Bachelor's Degree | Standard Chartered |
| | 35 | F | Data Analyst | Master's Degree | Fidelity |
| | 42 | M | Security Operations Analyst | Doctorate or Professional Degree | Citadel Securities |
| | 55 | F | Cybersecurity Analyst | Master's Degree | Goldman Sachs |
| | 21 | NB | Compliance Officer | High School or Below | Fidelity |
| | 45 | M | Forensic Accountant | Bachelor's Degree | Citadel Securities |
| | 31 | F | Risk Management Analyst | Master's Degree | Goldman Sachs |
| | 62 | M | Cybersecurity Analyst | Doctorate or Professional Degree | Standard Chartered |

| | | | | | |
|---|---|---|---|---|---|
| | 48 | M | Credit Fraud Analyst | Master's Degree | Citi Group |
| . | 28 | F | Compliance Officer | Bachelor's Degree | Fidelity |
| . | 33 | M | Fraud Prevention Specialist | Bachelor's Degree | Fidelity |
| . | 27 | F | Risk Management Analyst | Bachelor's Degree | Standard Chartered |

APPENDIX D: INPUT DATA

| ID | Gender | Age | Education | Behaviour-based framework Effectiveness | Rules-based framework Effectiveness | Cooperation Effectiveness | Modern Tools Effectiveness | Traditional Tool Effectiveness | Satisfaction | Concern Recommendation | Reduction Effectiveness |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 1 | Male | 28 | Bachelor's Degree | 4 | 3 | 4 | 5 | 2 | 4 | 5 | 4 |
| 2 | Female | 35 | Master's Degree | 5 | 4 | 5 | 4 | 3 | 3 | 4 | 5 |
| 3 | Male | 42 | Doctorate or Professional Degree | 3 | 2 | 3 | 3 | 2 | 2 | 3 | 3 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | Female | 55 | Master's Degree | 4 | 4 | 4 | 4 | 4 | 4 | 5 | 4 |
| 5 | Non-binary | 21 | High School or below | 2 | 2 | 3 | 2 | 2 | 3 | 2 | 2 |
| 6 | Male | 45 | Bachelor's Degree | 4 | 3 | 4 | 4 | 3 | 3 | 5 | 4 |
| 7 | Female | 31 | Master's Degree | 3 | 4 | 3 | 5 | 1 | 4 | 4 | 4 |
| 8 | Male | 62 | Doctorate or Professional Degree | 2 | 2 | 2 | 3 | 2 | 2 | 3 | 2 |

| | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| 9 | Male | 48 | Master's Degree | 4 | 5 | 5 | 4 | 2 | 4 | 4 | 4 |
| 10 | Female | 28 | Bachelor's Degree | 5 | 3 | 4 | 4 | 3 | 3 | 4 | 4 |
| 11 | Male | 33 | Bachelor's Degree | 3 | 3 | 4 | 4 | 3 | 3 | 4 | 4 |
| 12 | Female | 27 | Bachelor's Degree | 4 | 3 | 4 | 3 | 1 | 3 | 4 | 3 |